



**ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΛΕΥΚΩΣΙΑΣ**

Κοινό Πρόγραμμα Μεταπτυχιακών Σπουδών
«Δίκαιο της Οικονομίας και των Επιχειρήσεων»

Ακαδημαϊκό έτος 2025-2026

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του Θωμά Γόγαλη, Α.Μ.: U164N0801

**Η αλληλεπίδραση Smart Contracts και AI Agents στο πλαίσιο της
NIS2:**

**Προς ένα νέο νομικό καθεστώς για την αυτονομία των ψηφιακών
οντοτήτων**

Επιβλέπων:
Απόστολος Μάνθος

Άρτα, Ιούλιος 2026

Περιεχόμενα

Πίνακας Συντομογραφιών	5
1. Περίληψη.....	6
Abstract	6
2. Εισαγωγή και ερευνητικό πλαίσιο	8
2.1. Οριοθέτηση του προβλήματος: η σύγκλιση blockchain και τεχνητής νοημοσύνης ως ρυθμιστική πρόκληση	8
2.2. Ερευνητικά ερωτήματα.....	11
2.3. Μεθοδολογία	12
2.4. Δομή της εργασίας.....	13
3. Θεωρητικό και τεχνολογικό υπόβαθρο.....	15
3.1. Η τεχνολογία blockchain: εννοιολογική χαρτογράφηση υπό νομική οπτική	15
3.2. Οι έξυπνες συμβάσεις	16
3.2.1. Λειτουργία και χαρακτηριστικά	16
3.2.2. Η νομική φύση: σύμβαση ή μέσο εκτέλεσης;.....	16
3.3. Οι αυτόνομοι πράκτορες τεχνητής νοημοσύνης.....	18
3.3.1. Έννοια και ορισμοί	18
3.3.2. Από τον αυτοματισμό στην αυτονομία.....	18
3.4. Μορφές αλληλεπίδρασης έξυπνων συμβάσεων και αυτόνομων πρακτόρων	19
3.5. Τυπολογία βαθμίδων αυτονομίας των ψηφιακών οντοτήτων	20
4. Το ρυθμιστικό πλαίσιο της NIS2 και η κυβερνοασφάλεια	23
4.1. Από τη NIS στη NIS2: σκοπός, καινοτομίες και ελληνική ενσωμάτωση	23
4.2. Το πεδίο εφαρμογής: τομείς, κανόνες μεγέθους και κατηγορίες οντοτήτων	24
4.3. Το ζήτημα της υπαγωγής: πού εντάσσονται τα οικοσυστήματα smart contracts και AI agents	24
4.3.1. Πάροχοι υποδομών και υπηρεσιών blockchain	24
4.3.2. Πάροχοι υπηρεσιών τεχνητής νοημοσύνης.....	26
4.4. Οι ουσιαστικές υποχρεώσεις υπό το πρίσμα της αυτονομίας.....	26
4.5. Τα όρια της NIS2 απέναντι στα αποκεντρωμένα συστήματα.....	28
4.6. Η σχέση με τα παράλληλα ευρωπαϊκά καθεστώτα	29
5. Νομική ευθύνη και λογοδοσία των αυτόνομων ψηφιακών οντοτήτων	31
5.1. Το πρόβλημα του καταλογισμού	31
5.2. Η συμβατική διάσταση	32
5.2.1. Κατάρτιση της σύμβασης και δήλωση βούλησης	32
5.2.2. Αντιπροσώπευση και συγγενή εργαλεία	33
5.2.3. Ελαττώματα βούλησης, ερμηνεία και εκπλήρωση.....	34
5.3. Η εξωσυμβατική διάσταση	35

5.3.1. Η αδικοπρακτική ευθύνη και τα όριά της.....	35
5.3.2. Η νέα Οδηγία για την ευθύνη λόγω ελαττωματικών προϊόντων.....	35
5.4. Η συζήτηση για την «ηλεκτρονική προσωπικότητα»	36
5.5. Λογοδοσία στα αποκεντρωμένα σχήματα: το παράδειγμα των DAOs	37
5.6. Ενδιάμεσο συμπέρασμα: η ευθύνη υπό το πρίσμα των βαθμίδων αυτονομίας. 38	
6. Προς ένα μοντέλο νομικής και ρυθμιστικής συμμόρφωσης.....	40
6.1. Οι αρχές του μοντέλου.....	40
6.2. Συμμόρφωση εκ σχεδιασμού στον κύκλο ζωής του συστήματος.....	41
6.3. Το κλιμακωτό μοντέλο ανά βαθμίδα αυτονομίας	41
6.4. Διακυβέρνηση, ταυτότητα και γνωστοποίηση των πρακτόρων.....	42
6.5. Προτάσεις de lege ferenda	43
6.6. Σύνοψη του μοντέλου	44
7. Συμπεράσματα και προτάσεις για μελλοντική έρευνα	46
8. Βιβλιογραφία	48
Ελληνόγλωσση	48
Ξενόγλωσση	48
Νομολογία	50
Νομοθεσία	50
Ιστοσελίδες	51

Πίνακας Συντομογραφιών

AK	Αστικός Κώδικας
βλ.	βλέπε
EE	Ευρωπαϊκή Ένωση
EE L	Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, σειρά L
επ.	επόμενα
KYA	Κοινή Υπουργική Απόφαση
N.	Νόμος
ό.π.	όπως παραπάνω
παρ.	παράγραφος
π.χ.	παραδείγματος χάριν
σελ.	σελίδα
σημ.	σημείο
σσ.	σελίδες
TN	Τεχνητή Νοημοσύνη
TΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών
ΦΕΚ	Φύλλο Εφημερίδας της Κυβερνήσεως
AI	Artificial Intelligence (Τεχνητή Νοημοσύνη)
AI Act	Κανονισμός (ΕΕ) 2024/1689 για την τεχνητή νοημοσύνη
CFTC	Commodity Futures Trading Commission (ΗΠΑ)
CRA	Cyber Resilience Act, Κανονισμός (ΕΕ) 2024/2847
DAO	Decentralized Autonomous Organization (αποκεντρωμένος αυτόνομος οργανισμός)
DeFi	Decentralized Finance (αποκεντρωμένη χρηματοοικονομική)
DLT	Distributed Ledger Technology (τεχνολογία καταμεμημένου καθολικού)
DNS	Domain Name System
DORA	Digital Operational Resilience Act, Κανονισμός (ΕΕ) 2022/2554
ELI	European Law Institute
ENISA	Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια
LLM	Large Language Model (μεγάλο γλωσσικό μοντέλο)
MiCA	Markets in Crypto Assets, Κανονισμός (ΕΕ) 2023/1114
NIS2	Οδηγία (ΕΕ) 2022/2555 για την ασφάλεια δικτύων και πληροφοριακών συστημάτων
PLD	Product Liability Directive, Οδηγία (ΕΕ) 2024/2853

1. Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει τη νομική και ρυθμιστική διάσταση της αλληλεπίδρασης μεταξύ των έξυπνων συμβάσεων (smart contracts) και των αυτόνομων πρακτόρων τεχνητής νοημοσύνης (AI agents), υπό το πρίσμα της Οδηγίας (ΕΕ) 2022/2555 (NIS2) και του Ν. 5160/2024, με τον οποίο η Οδηγία ενσωματώθηκε στην ελληνική έννομη τάξη. Η ενσωμάτωση συστημάτων τεχνητής νοημοσύνης σε περιβάλλοντα blockchain δημιουργεί νέες μορφές αυτονομίας στη λήψη αποφάσεων και στην εκτέλεση συμβατικών υποχρεώσεων χωρίς ανθρώπινη παρέμβαση. Το φαινόμενο αυτό θέτει σε δοκιμασία βασικές έννοιες του δικαίου των δικαιωμάτων και του δικαίου της κυβερνοασφάλειας. Η εργασία εισάγει μια τυπολογία πέντε βαθμίδων αυτονομίας των ψηφιακών οντοτήτων και την αξιοποιεί ως αναλυτικό εργαλείο σε τρία επίπεδα. Στο ρυθμιστικό επίπεδο διαπιστώνεται ότι η NIS2 και τα παράλληλα ευρωπαϊκά νομοθετήματα, όπως ο AI Act, ο DORA, ο Cyber Resilience Act και ο Data Act, καλύπτουν τους κεντρικοποιημένους κρίκους του οικοσυστήματος, αφήνουν όμως ακάλυπτο τον αποκεντρωμένο πυρήνα του. Στο επίπεδο της ευθύνης διαπιστώνεται ότι τα εργαλεία του ιδιωτικού δικαίου επαρκούν στις χαμηλές βαθμίδες αυτονομίας και αστοχούν στις υψηλές, με χαρακτηριστικότερο παράδειγμα τους αποκεντρωμένους αυτόνομους οργανισμούς, ενώ η νέα Οδηγία (ΕΕ) 2024/2853 για την ευθύνη λόγω ελαττωματικών προϊόντων καλύπτει σημαντικό μέρος του κενού από την πλευρά του παραγωγού. Με την εργασία προτείνεται ένα κλιμακωτό μοντέλο συμμόρφωσης, το οποίο συνδέει την ένταση των υποχρεώσεων με τη βαθμίδα αυτονομίας, καθώς και συγκεκριμένες προτάσεις de lege ferenda, όπως η γενίκευση της υποχρέωσης μηχανισμού διακοπής, η γνωστοποίηση της ιδιότητας του πράκτορα, η αντικειμενική ευθύνη του φορέα εκμετάλλευσης με υποχρεωτική ασφάλιση και η δημιουργία νομικής μορφής για τους αποκεντρωμένους οργανισμούς.

Λέξεις κλειδιά: έξυπνες συμβάσεις, αυτόνομοι πράκτορες τεχνητής νοημοσύνης, NIS2, κυβερνοασφάλεια, νομική ευθύνη

Abstract

This master's thesis examines the legal and regulatory dimension of the interaction between smart contracts and autonomous artificial intelligence agents (AI agents) in light of Directive (EU) 2022/2555 (NIS2) and Greek Law 5160/2024, which transposed the Directive into the Greek legal order. The integration of artificial intelligence systems into blockchain environments creates new forms of autonomy in decision-making and in the

performance of contractual obligations without human intervention, testing fundamental concepts of the law of juridical acts and of cybersecurity law. The thesis introduces a typology of five levels of autonomy of digital entities and employs it as an analytical tool on three levels. At the regulatory level, it is found that NIS2 and the parallel European instruments, such as the AI Act, DORA, the Cyber Resilience Act and the Data Act, cover the centralised links of the ecosystem but leave its decentralised core uncovered. At the level of liability, it is found that the tools of private law suffice at the lower levels of autonomy but fail at the higher ones, with decentralised autonomous organisations (DAOs) as the most characteristic example, while the new Directive (EU) 2024/2853 on liability for defective products covers a significant part of the gap on the producer's side. The thesis proposes a tiered compliance model, which links the intensity of obligations to the level of autonomy, as well as specific *de lege ferenda* proposals, such as the generalisation of the obligation to provide a termination mechanism, the disclosure of an agent's status, strict liability of the operator coupled with compulsory insurance, and the creation of a legal form for decentralised organisations.

Keywords: smart contracts, autonomous AI agents, NIS2, cybersecurity, legal liability

2. Εισαγωγή και ερευνητικό πλαίσιο

2.1. Οριοθέτηση του προβλήματος: η σύγκλιση blockchain και τεχνητής νοημοσύνης ως ρυθμιστική πρόκληση

Δύο από τις σημαντικότερες τεχνολογίες των τελευταίων ετών, η τεχνολογία blockchain και η τεχνητή νοημοσύνη, αναπτύχθηκαν για μεγάλο χρονικό διάστημα σε παράλληλες πορείες, με διαφορετικά πεδία εφαρμογής και διαφορετικές ρυθμιστικές αφετηρίες. Η πρώτη υποσχέθηκε συναλλαγές χωρίς μεσάζοντες, μέσω της αποκεντρωμένης και αμετάβλητης καταγραφής τους. Η δεύτερη υποσχέθηκε την αυτοματοποίηση της κρίσης και της λήψης αποφάσεων. Το σημείο συνάντησής τους βρίσκεται στις έξυπνες συμβάσεις (smart contracts). Πρόκειται για προγράμματα υπολογιστή που εκτελούνται αυτόματα πάνω στην αλυσίδα (on-chain), όταν πληρωθούν οι προϋποθέσεις, που έχουν προκαθοριστεί, χωρίς τη διαμεσολάβηση τρίτου προσώπου¹. Από τη θεωρητική σύλληψη του Szabo έως την πρακτική υλοποίηση στην πλατφόρμα Ethereum², η έξυπνη σύμβαση εξελίχθηκε από τεχνολογικό πείραμα σε βασική υποδομή της αποκεντρωμένης οικονομίας, ενώ πλέον διαθέτει και ρητό νομοθετικό ορισμό στο ενωσιακό δίκαιο³. Αντίστοιχο ορισμό έχει θεσπίσει και ο Έλληνας νομοθέτης με τον Ν. 4961/2022 στο άρθρο 31 παρ. 9 όπου αναφέρεται ότι ««Έξυπνο συμβόλαιο (smart contract)»: σύνολο κωδικοποιημένων λειτουργιών υπολογιστή, το οποίο οριστικοποιείται και εκτελείται μέσω τεχνολογίας κατανεμημένου καθολικού σε αυτοματοποιημένη ηλεκτρονική μορφή μέσω οδηγιών για την εκτέλεση ενεργειών, παραλείψεων ή ανοχών, οι οποίες βασίζονται στην ύπαρξη ή μη συγκεκριμένων προϋποθέσεων, σύμφωνα με όρους που καταγράφονται απευθείας σε ηλεκτρονικό κώδικα, προγραμματισμένες εντολές ή προγραμματισμένη γλώσσα»⁴.

Για πολλά χρόνια η «αυτονομία» των έξυπνων συμβάσεων παρέμενε αυστηρά ντετερμινιστική. Ο κώδικας εκτελούσε ακριβώς ό,τι είχε προδιαγραφεί, χωρίς περιθώριο απόκλισης ή προσαρμογής. Η εικόνα αυτή αλλάζει ριζικά με την εμφάνιση των αυτόνομων

¹Szabo, N. (1997), 'Formalizing and Securing Relationships on Public Networks', First Monday, 2(9). Ο όρος «έξυπνη σύμβαση» (smart contract) αποδίδεται στον Nick Szabo, ο οποίος τον χρησιμοποίησε ήδη από τη δεκαετία του 1990 για να περιγράψει πρωτόκολλα συναλλαγών που εκτελούν αυτόματα τους όρους μιας σύμβασης.

²Buterin, V. (2014), Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform.

³Βλ. τον νομοθετικό ορισμό της «έξυπνης σύμβασης» στο άρθρο 2 του Κανονισμού (ΕΕ) 2023/2854 (Data Act), ως προγράμματος υπολογιστή που χρησιμοποιείται για την αυτοματοποιημένη εκτέλεση συμφωνίας ή μέρους αυτής, καθώς και τις ουσιώδεις απαιτήσεις του άρθρου 36 του ίδιου Κανονισμού για τις έξυπνες συμβάσεις σε συμφωνίες κοινοχρησίας δεδομένων.

⁴ Ν. 4961/2022 «Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις» (ΦΕΚ Α' 146/27.07.2022), ο οποίος περιλαμβάνει ρυθμίσεις για τις τεχνολογίες κατανεμημένου καθολικού και τις έξυπνες συμβάσεις.

πρακτόρων τεχνητής νοημοσύνης (AI agents), ιδίως εκείνων που βασίζονται στα μεγάλα γλωσσικά μοντέλα (large language models). Αυτή είναι και η ουσιαστική αλλαγή που επέφερε η τεχνητή νοημοσύνη με την εισαγωγή των πρακτόρων (agents). Πρόκειται για συστήματα λογισμικού, που μπορούν να θέτουν και να επιδιώκουν στόχους, να σχεδιάζουν αλληλουχίες ενεργειών και να αλληλεπιδρούν με εξωτερικά εργαλεία. Το σημαντικότερο για την παρούσα εργασία είναι ότι μπορούν να κατέχουν κρυπτογραφικά πορτοφόλια, να συναλλάσσονται σε blockchain και να συνάπτουν, να τροποποιούν και να εκτελούν έξυπνες συμβάσεις χωρίς συνεχή ανθρώπινη εποπτεία⁵. Με αυτόν τον τρόπο τα blockchain περιβάλλοντα μετατρέπονται σε οικοσυστήματα όπου «ψηφιακές οντότητες» με μη προβλέψιμη συμπεριφορά αναλαμβάνουν λειτουργίες, που το δίκαιο παραδοσιακά επιφυλάσσει στα πρόσωπα, όπως τη διαπραγμάτευση, τη δήλωση βούλησης και την εκπλήρωση της παροχής. Παραδοσιακές έννοιες, λοιπόν, του Αστικού Κώδικα, όπως για παράδειγμα η ερμηνεία των συμβάσεων κατά το άρθρο 200, όπου απαιτείται να γίνεται σύμφωνα με την καλή πίστη και αφού ληφθούν υπόψιν τα συναλλακτικά ήθη μετατρέπονται σε αναχρονιστικά εργαλεία αφού είναι αδύνατον να εφαρμοστούν σε περιπτώσεις όπου η εκτέλεση μια σύμβασης ελέγχεται από πράκτορες τεχνητής νοημοσύνης που λειτουργούν αυτόνομα. Η έννοια της δήλωσης βούλησης σε αυτά τα αυτόνομα περιβάλλοντα πρέπει να αναζητηθεί ενδεχομένως βαθιά στον πυρήνα της κάθε εφαρμογής, αναγόμενη στα παραγωγικά αίτια, που οδήγησαν αυτή στην λήψη της εκάστοτε συγκεκριμένης (αυτοματοποιημένης) απόφασης.

Η εξέλιξη αυτή δεν είναι απλώς μια τεχνολογική καινοτομία. Αποτελεί μια ρυθμιστική πρόκληση. Στο επίπεδο της κυβερνοασφάλειας, η διασύνδεση των αυτόνομων πρακτόρων με τις έξυπνες συμβάσεις πολλαπλασιάζει τα σημεία επίθεσης. Στις γνωστές ευπάθειες του κώδικα των έξυπνων συμβάσεων προστίθενται πλέον οι ευπάθειες των ίδιων των μοντέλων τεχνητής νοημοσύνης, όπως οι επιθέσεις έγχυσης εντολών (prompt injection), η δηλητηρίαση των δεδομένων εκπαίδευσης και η χειραγωγή των πηγών πληροφόρησης (oracles). Χαρακτηριστική είναι η υπόθεση της πλατφόρμας Mango Markets (2022), όπου η χειραγωγή της τιμής αναφοράς οδήγησε σε αφαίρεση κρυπτοστοιχείων αξίας άνω των εκατό εκατομμυρίων δολαρίων και σε ποινική δίωξη στις Ηνωμένες Πολιτείες⁶, αν και τελικώς το δικαστήριο της Νέας Υόρκης οδηγήθηκε σε αθωωτική απόφαση λόγω τοπικής

⁵Marino, B., Juels, A. (2025), ‘Giving AI Agents Access to Cryptocurrency and Smart Contracts Creates New Vectors of AI Harm’, arXiv preprint arXiv:2507.08249.

⁶ Βλ. την υπόθεση United States v. Eisenberg (S.D.N.Y.), σχετικά με τη χειραγωγή των τιμών αναφοράς στην πλατφόρμα Mango Markets. Βλ. και Marino, B., Juels, A. (2025), ό.π.

αναρμοδιότητας, αφού τα αδικήματα φέρονται να διαπράχθησαν στο Πουέρτο Ρίκο⁷. Οι συνέπειες μπορεί να είναι μη αναστρέψιμες, δεδομένου ότι οι συναλλαγές σε blockchain δεν ανακαλούνται. «Η τεχνολογία του Blockchain επιτρέπει στον χρήστη να καταγράφει το ιστορικό σε οτιδήποτε αποδίδει αυτός αξία, χωρίς να υπάρχει κίνδυνος να παραποιηθούν ούτε καν από τον ίδιο τα εν λόγω δεδομένα»⁸. Παράλληλα έχουν εκφραστεί ανησυχίες σχετικά με «προβλήματα ιδιωτικότητας», την πρόσκρουση σε «πολλές αρχές του GDPR» αλλά και την απαίτηση «υψηλής υπολογιστικής ισχύος» και «τεράστιας ενεργειακής κατανάλωσης»⁹. Στο επίπεδο του ιδιωτικού δικαίου, η αυτόνομη δράση του πράκτορα κλονίζει τις κλασικές προϋποθέσεις του καταλογισμού. Ποιος «δηλώνει βούληση» όταν το μοντέλο επιλέγει το ίδιο τον αντισυμβαλλόμενο και τους όρους της συναλλαγής; Στο επίπεδο, τέλος, του ρυθμιστικού δικαίου, τίθεται το ερώτημα εάν και πώς τα υφιστάμενα κανονιστικά εργαλεία, που σχεδιάστηκαν για οργανωμένες «οντότητες» με νομική προσωπικότητα, έδρα και διοίκηση, μπορούν να συλλάβουν αποκεντρωμένα συστήματα, τα οποία ενδέχεται να μην ελέγχονται από κανέναν.

Κεντρικό σημείο αναφοράς της παρούσας εργασίας αποτελεί η Οδηγία (ΕΕ) 2022/2555 (NIS2)¹⁰, η οποία διαμορφώνει το ευρωπαϊκό πλαίσιο για την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας. Σε σχέση με την προκάτοχό της, την Οδηγία (ΕΕ) 2016/1148, η NIS2 διευρύνει σημαντικά το πεδίο των υπόχρεων τομέων και οντοτήτων, τις υποχρεώσεις διαχείρισης κινδύνων και αναφοράς περιστατικών, καθώς και τις εποπτικές και κυρωτικές εξουσίες, στις οποίες περιλαμβάνεται και η προσωπική ευθύνη των διοικήσεων. Στην ελληνική έννομη τάξη η Οδηγία ενσωματώθηκε με τον Ν. 5160/2024¹¹, ενώ οι απαιτήσεις ασφάλειας εξειδικεύθηκαν με το Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων¹². Το πλαίσιο μάλιστα συνεχίζει

⁷ Για την έκβαση της υπόθεσης βλ. Thomson Reuters, Practical Law, US v. Eisenberg, διαθέσιμο σε: [https://uk.practicallaw.thomsonreuters.com/w-047-2998?transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/w-047-2998?transitionType=Default&contextData=(sc.Default)&firstPage=true) (τελευταία πρόσβαση: Αύγουστος 2026).

⁸ Καλογεράκης, Γ., Θεοδωράκης, Ν. (2019), «Blockchain: εφαρμογές, προοπτικές και προκλήσεις για το ελληνικό νομικό σύστημα», Δίκαιο Μέσων Ενημέρωσης & Επικοινωνίας (ΔiMEE) 1/2019, σσ. 5-22.

⁹ Κανέλλος, Λ. (2020), The GDPR Handbook. Για DPOs, Επιχειρήσεις & Οργανισμούς, Αθήνα: Νομική Βιβλιοθήκη, σελ. 363.

¹⁰ Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972 και την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2), ΕΕ L 333 της 27.12.2022, σ. 80.

¹¹ Ν. 5160/2024 «Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 [...] (Οδηγία NIS 2) και άλλες διατάξεις» (ΦΕΚ Α' 195/27.11.2024).

¹² ΚΥΑ 1689/2025 «Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων» (ΦΕΚ Β' 2186/06.05.2025).

να εξελίσσεται, καθώς έχουν ήδη προταθεί στοχευμένες τροποποιήσεις της Οδηγίας σε ευρωπαϊκό επίπεδο¹³. Παράλληλα, η NIS2 δεν λειτουργεί απομονωμένη. Συνδέεται και σε ορισμένα σημεία επικαλύπτεται με τον Κανονισμό για την Τεχνητή Νοημοσύνη¹⁴, με τα ειδικότερα νομοθετήματα για την κυβερνοανθεκτικότητα¹⁵ και με το νέο καθεστώς ευθύνης λόγω ελαττωματικών προϊόντων¹⁶. Για το λόγο αυτό, η χαρτογράφηση αυτού του κανονιστικού πλέγματος, στον βαθμό, που αφορά τα αυτόνομα οικοσυστήματα των smart contracts και των AI agents, είναι αναγκαία προϋπόθεση για κάθε προσπάθεια συστηματικής ερμηνείας.

Η πρωτοτυπία αλλά και η δυσκολία του φαινομένου βρίσκεται στο ότι κανένα από τα παραπάνω νομοθετήματα δεν σχεδιάστηκε με ρητή αναφορά στη σύγκλιση των δύο τεχνολογιών. Και αυτό ίσως αποτελεί μια παραδοχή αλλά και έναν περιορισμό της παρούσας εργασίας. Η NIS2 προϋποθέτει «οντότητες», που μπορούν να φέρουν υποχρεώσεις. Ο AI Act ρυθμίζει τα «συστήματα ΤΝ» μέσω των παρόχων και των φορέων εφαρμογής τους. Το δίκαιο για τον καταλογισμό της αστικής ευθύνης αναζητά πρόσωπο στο οποίο θα καταλογιστεί η ζημία. Όταν όμως ένας αυτόνομος πράκτορας, εγκατεστημένος σε αποκεντρωμένη υποδομή, εκτελεί έξυπνες συμβάσεις, που ο ίδιος «αποφάσισε» να συνάψει, οι κατηγορίες αυτές δοκιμάζονται στα όριά τους. Η παρούσα εργασία φιλοδοξεί να συμβάλει στη συζήτηση αυτή. Δεν επιδιώκει να δώσει οριστικές απαντήσεις, κάτι που άλλωστε δεν θα ήταν εφικτό, αλλά να επιχειρήσει να αναλύσει συστηματικά το ισχύον πλαίσιο και να διατυπώσει ένα λειτουργικό μοντέλο συμμόρφωσης, το οποίο θα στηρίζεται σε μια τυπολογία βαθμίδων αυτονομίας των ψηφιακών οντοτήτων, αναγνωρίζοντας παράλληλα τους περιορισμούς που υπάρχουν από το ισχύον νομικό πλαίσιο τόσο σε εθνικό όσο και ευρωπαϊκό επίπεδο.

2.2. Ερευνητικά ερωτήματα

¹³Βλ. την πρόταση της Ευρωπαϊκής Επιτροπής της 20ής Ιανουαρίου 2026 για στοχευμένες τροποποιήσεις της Οδηγίας NIS2, στο πλαίσιο της δέσμης μέτρων για την ψηφιακή απλούστευση (digital omnibus), με στόχο την ενίσχυση της ασφάλειας δικαίου και την απλοποίηση της συμμόρφωσης.

¹⁴Κανονισμός (ΕΕ) 2024/1689 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουνίου 2024, για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Κανονισμός για την Τεχνητή Νοημοσύνη, AI Act).

¹⁵Κανονισμός (ΕΕ) 2022/2554 για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα (DORA) και Κανονισμός (ΕΕ) 2024/2847 σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία (Cyber Resilience Act).

¹⁶Οδηγία (ΕΕ) 2024/2853 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2024, για την ευθύνη λόγω ελαττωματικών προϊόντων, η οποία επεκτείνει ρητά την έννοια του «προϊόντος» στο λογισμικό.

Με βάση τα παραπάνω, η εργασία διαρθρώνεται γύρω από τρία ερευνητικά ερωτήματα.

Το πρώτο ερώτημα αφορά το πεδίο εφαρμογής. Σε ποιο βαθμό και υπό ποιες προϋποθέσεις τα οικοσυστήματα αλληλεπίδρασης smart contracts και AI agents, καθώς και οι φορείς, που τα αναπτύσσουν, τα λειτουργούν ή παρέχουν υπηρεσίες μέσω αυτών, εμπίπτουν στο πεδίο εφαρμογής της NIS2 και του Ν. 5160/2024; Και ποιες ουσιαστικές υποχρεώσεις, όπως η διαχείριση κινδύνου, η ασφάλεια της εφοδιαστικής αλυσίδας και η αναφορά περιστατικών, απορρέουν από την υπαγωγή αυτή;

Το δεύτερο ερώτημα αφορά την ευθύνη. Πώς κατανέμεται η νομική ευθύνη και η λογοδοσία για τις πράξεις και τις παραλείψεις των αυτόνομων ψηφιακών οντοτήτων, τόσο στο πεδίο του δικαίου των δικαιοπραξιών (κατάρτιση, ερμηνεία και εκτέλεση των συμβάσεων) όσο και στο πεδίο της εξωσυμβατικής ευθύνης; Και ποια είναι τα όρια των υφιστάμενων δογματικών εργαλείων, όπως η αντιπροσώπευση, ο βοηθός εκπλήρωσης και η ευθύνη του παραγωγού;

Το τρίτο ερώτημα αφορά τη συμμόρφωση. Είναι δυνατή και σκόπιμη η διαμόρφωση ενός συνεκτικού μοντέλου νομικής και ρυθμιστικής συμμόρφωσης για τα αυτόνομα αυτά οικοσυστήματα; Και ποια χαρακτηριστικά θα έπρεπε να έχει το μοντέλο αυτό, ώστε να συμφιλιώνει την τεχνολογική καινοτομία με τις απαιτήσεις της κυβερνοασφάλειας και της προστασίας των συναλλασσομένων;

2.3. Μεθοδολογία

Η εργασία εκπονείται υπό νομική οπτική. Ως κύρια μέθοδος ακολουθείται η νομική ανάλυση του ισχύοντος ευρωπαϊκού και εθνικού δικαίου, με αξιοποίηση της γραμματικής, της συστηματικής και της τελεολογικής ερμηνείας των κρίσιμων διατάξεων, ιδίως της Οδηγίας NIS2 και του Ν. 5160/2024. Η ανάλυση αυτή συνδυάζεται με συγκριτική μελέτη διεθνών και κυρίως ευρωπαϊκών πρακτικών. Εξετάζονται οι ρυθμιστικές επιλογές που έχουν διαμορφωθεί σε επίπεδο Ευρωπαϊκής Ένωσης και κρατών μελών, καθώς και οι θέσεις των ευρωπαϊκών θεσμικών φορέων και οργανισμών, ώστε να αναδειχθούν τα σημεία σύγκλισης, οι αποκλίσεις και οι βέλτιστες πρακτικές.

Επειδή το αντικείμενο βρίσκεται στην τομή του δικαίου και της τεχνολογίας, η νομική ανάλυση υποστηρίζεται από εννοιολογική χαρτογράφηση των τεχνολογικών λειτουργιών. Οι κρίσιμοι τεχνικοί μηχανισμοί, δηλαδή το κατανεμημένο καθολικό, οι έξυπνες συμβάσεις, οι αυτόνομοι πράκτορες και οι μηχανισμοί διασύνδεσής τους,

παρουσιάζονται όχι ως αυτοσκοπός, αλλά στον βαθμό, που απαιτείται για την ορθή νομική τους αξιολόγηση. Με αυτόν τον τρόπο τα τεχνολογικά χαρακτηριστικά «μεταφράζονται» σε νομικά κρίσιμα κριτήρια, όπως η αυτονομία, η προβλεψιμότητα, η δυνατότητα ανθρώπινης παρέμβασης και η δυνατότητα προσδιορισμού του υπεύθυνου προσώπου. Η εργασία, λοιπόν, μοιραία, λόγω της θεματολογίας της αναφέρεται σε ζητήματα τεχνικής φύσεως αξιοποιώντας τους αναγκαίους τεχνικούς όρους, χωρίς όμως να εισχωρεί σε βάθος σε αυτούς, αφού εκπονείται από νομική σκοπιά.

Σε επίπεδο πηγών, η εργασία στηρίζεται σε βιβλιογραφική έρευνα που περιλαμβάνει βιβλία, επιστημονικά άρθρα, μελέτες, καθώς και δημοσιεύσεις και εκθέσεις ευρωπαϊκών οργανισμών και θεσμικών φορέων, όπως ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), η Ευρωπαϊκή Επιτροπή και οι ομάδες εμπειρογνομόνων της, το Ευρωπαϊκό Κοινοβούλιο και το European Law Institute (ELI). Παράλληλα αξιοποιούνται τα ίδια τα νομοθετικά κείμενα και οι προπαρασκευαστικές τους εργασίες. Τέλος, στα Κεφάλαια 6 και 7, όπου επιχειρείται να προταθεί ένα μοντέλο διαβαθμισμένου ελέγχου, η εργασία κινείται σε επίπεδο *de lege ferenda* και διατυπώνει αιτιολογημένες προτάσεις για τη βελτίωση του ρυθμιστικού πλαισίου.

Κατά την εκπόνηση της εργασίας χρησιμοποιήθηκαν επίσης εργαλεία παραγωγικής τεχνητής νοημοσύνης ως ερευνητικό και υποστηρικτικό βοήθημα, σύμφωνα με την Πολιτική για τη Χρήση Εργαλείων Τεχνητής Νοημοσύνης του Πανεπιστημίου Λευκωσίας (Policy for the Use of AI Tools at the University of Nicosia) και ιδίως με τις αρχές της διαφάνειας, της λογοδοσίας και της ακαδημαϊκής ακεραιότητας, που καθιερώνονται σε αυτήν. Η χρήση τους αφορούσε την αναζήτηση και την οργάνωση βιβλιογραφίας και νομοθετικών πηγών, τη διαμόρφωση της δομής των κεφαλαίων, την προετοιμασία αρχικών σχεδίων κειμένου και τη γλωσσική επιμέλεια. Σύμφωνα με την απαίτηση κριτικής αξιολόγησης του περιεχομένου, που παράγεται από τέτοια εργαλεία, το σύνολο του κειμένου ελέγχθηκε και αναθεωρήθηκε από τον συγγραφέα, ο οποίος επαλήθευσε την ακρίβεια των πληροφοριών και των παραπομπών στις πρωτογενείς πηγές, δηλαδή στα νομοθετικά κείμενα, στη νομολογία και στη βιβλιογραφία, που παρατίθενται. Ο συγγραφέας φέρει την αποκλειστική και πλήρη ευθύνη για το περιεχόμενο, τις κρίσεις, τα συμπεράσματα και τις προτάσεις της εργασίας. Η χρήση των εργαλείων αυτών γνωστοποιήθηκε στον επιβλέποντα καθηγητή.

2.4. Δομή της εργασίας

Η εργασία διαρθρώνεται σε επτά κεφάλαια, πέραν της παρούσας εισαγωγής. Το Κεφάλαιο 3 παρέχει το αναγκαίο θεωρητικό και τεχνολογικό υπόβαθρο. Παρουσιάζει τη λειτουργία της τεχνολογίας blockchain και των έξυπνων συμβάσεων, τη νομική φύση των τελευταίων, την εξέλιξη των αυτόνομων πρακτόρων τεχνητής νοημοσύνης και τις μορφές αλληλεπίδρασής τους, και εισάγει την τυπολογία βαθμίδων αυτονομίας, που διατρέχει το σύνολο της εργασίας. Το Κεφάλαιο 4 αναλύει το ρυθμιστικό πλαίσιο της NIS2 και της ελληνικής ενσωμάτωσής της, με έμφαση στο ζήτημα της υπαγωγής των υπό εξέταση οικοσυστημάτων στο πεδίο εφαρμογής της και στη σχέση της με τα παράλληλα ευρωπαϊκά νομοθετήματα. Το Κεφάλαιο 5 εξετάζει το πρόβλημα της νομικής ευθύνης και της λογοδοσίας των αυτόνομων ψηφιακών οντοτήτων. Το Κεφάλαιο 6 συνθέτει τα πορίσματα των προηγούμενων κεφαλαίων σε ένα προτεινόμενο μοντέλο νομικής και ρυθμιστικής συμμόρφωσης, ενώ το Κεφάλαιο 7 συνοψίζει τα συμπεράσματα και διατυπώνει προτάσεις για μελλοντική έρευνα. Στο τέλος παρατίθεται η ενδεικτική βιβλιογραφία.

3. Θεωρητικό και τεχνολογικό υπόβαθρο

Η νομική αξιολόγηση της αλληλεπίδρασης των έξυπνων συμβάσεων με τους αυτόνομους πράκτορες προϋποθέτει την εννοιολογική χαρτογράφηση των τεχνολογικών λειτουργιών, που βρίσκονται πίσω από αυτά. Το παρόν κεφάλαιο δεν επιδιώκει να παράσχει τεχνική ανάλυση. Αποσκοπεί στην ανάδειξη εκείνων των χαρακτηριστικών της τεχνολογίας, που έχουν κανονιστική σημασία, δηλαδή εκείνων που καθορίζουν την υπαγωγή στα σχετικά ρυθμιστικά καθεστώτα και τη λειτουργία των κανόνων για την ευθύνη. Το κεφάλαιο ολοκληρώνεται με τη διατύπωση μιας τυπολογίας βαθμίδων αυτονομίας των ψηφιακών οντοτήτων, η οποία θα αποτελέσει το αναλυτικό εργαλείο των επόμενων κεφαλαίων.

3.1. Η τεχνολογία blockchain: εννοιολογική χαρτογράφηση υπό νομική οπτική

Η αλυσίδα συστοιχίων (blockchain) αποτελεί ειδικότερη μορφή της τεχνολογίας κατανεμημένου καθολικού (distributed ledger technology, DLT). Πρόκειται για ένα ψηφιακό αρχείο καταγραφής συναλλαγών, το οποίο δεν τηρείται από κάποιον κεντρικό φορέα, αλλά αναπαράγεται και επικαιροποιείται ταυτόχρονα σε πλήθος κόμβων ενός δικτύου, βάσει ενός μηχανισμού συναίνεσης¹⁷. Από νομική σκοπιά, τρία είναι τα κρίσιμα λειτουργικά χαρακτηριστικά. Το πρώτο είναι η αποκέντρωση. Η απουσία κεντρικού διαχειριστή σημαίνει, στην ακραία εκδοχή της, ότι δεν υπάρχει προφανές υπόχρεο πρόσωπο, δηλαδή δεν υπάρχει εκείνος ο οποίος θα είναι ο αποδέκτης των έννομων συνεπειών¹⁸. Το δεύτερο είναι η πρακτική αμεταβλητότητα των εγγραφών. Ό,τι καταχωρίζεται στην αλυσίδα δεν αναιρείται. Αυτό έχει ως συνέπεια οι έννομες συνέπειες της ακύρωσης, της υπαναχώρησης και της εκατέρωθεν επιστροφής των παροχών, να μην μπορούν να εκτελεστούν πάνω στην αλυσίδα παρά μόνο μέσω νέων, αντίστροφων συναλλαγών. Το τρίτο χαρακτηριστικό είναι η διαφάνεια σε συνδυασμό με την ψευδωνυμία. Οι συναλλαγές είναι δημόσια ορατές, συνδέονται όμως με κρυπτογραφικές διευθύνσεις και όχι απαραίτητα με ταυτοποιημένα πρόσωπα. Σημαντική είναι, τέλος, η διάκριση μεταξύ ανοικτών (permissionless – πχ Bitcoin, Ethereum κλπ) και αδειοδοτημένων (permissioned - πχ Hyperledger Fabric, R3 Corda, JPMorgan Quorum) αλυσίδων¹⁹, καθώς η ύπαρξη ή μη

¹⁷Nakamoto, S. (2008), Bitcoin: A Peer-to-Peer Electronic Cash System.

¹⁸De Filippi, P., Wright, A. (2018), Blockchain and the Law: The Rule of Code, Cambridge, MA: Harvard University Press, σελ. 33 επ.

¹⁹Η διάκριση μεταξύ ανοικτών (permissionless) και αδειοδοτημένων (permissioned) αλυσίδων έχει σημαντικές κανονιστικές συνέπειες. Στις δεύτερες υπάρχει φορέας διαχείρισης με εξουσία ελέγχου της πρόσβασης και έτσι ο εντοπισμός υπόχρεου προσώπου είναι ευχερέστερος, ενώ στις πρώτες ο εντοπισμός αυτός είναι ιδιαίτερα δυσχερής.

φορέα, που ελέγχει την πρόσβαση καθορίζει σε μεγάλο βαθμό τη δυνατότητα αποτελεσματικής εποπτείας.

3.2. Οι έξυπνες συμβάσεις

3.2.1. Λειτουργία και χαρακτηριστικά

Η έξυπνη σύμβαση είναι, στην τεχνική της διάσταση, ένα πρόγραμμα υπολογιστή αποθηκευμένο πάνω στην αλυσίδα, το οποίο εκτελείται αυτόματα όταν πληρωθούν οι προϋποθέσεις, που έχουν προγραμματιστεί (if this then that²⁰). Η λογική της είναι απλή: εάν συμβεί το γεγονός X, τότε εκτελείται η ενέργεια Ψ. Η εκτέλεσή της είναι ντετερμινιστική και αυτοδύναμη. Δεν απαιτεί, αλλά ούτε και ανέχεται, μεταγενέστερη ανθρώπινη παρέμβαση, ενώ η μη εκπλήρωση με την τεχνική έννοια καθίσταται αδύνατη, στο μέτρο που η «παροχή» συνίσταται σε μια μεταβολή πάνω στην αλυσίδα, όπως η μεταβίβαση κρυπτοστοιχείων²¹. Τα χαρακτηριστικά αυτά εξηγούν τα πλεονεκτήματα, που αποδίδονται στον θεσμό, δηλαδή τη μείωση του κόστους των συναλλαγών, την εξάλειψη του κινδύνου του αντισυμβαλλομένου και την κατάργηση των μεσαζόντων. Εξηγούν όμως και τις εγγενείς αδυναμίες του. Ο κώδικας δεν μπορεί να αποτυπώσει αόριστες νομικές έννοιες, όπως η καλή πίστη ή ο εύλογος χρόνος, παραμένει άκαμπτος απέναντι σε απρόβλεπτες περιστάσεις, ενώ η ορθή εκτέλεση εξαρτάται από την ποιότητα του κώδικα και των εξωτερικών δεδομένων που τον τροφοδοτούν²².

3.2.2. Η νομική φύση: σύμβαση ή μέσο εκτέλεσης;

Το ερώτημα της νομικής φύσης των έξυπνων συμβάσεων έχει απασχολήσει εκτενώς τη θεωρία. Η ονομασία τους είναι, κατά κοινή ομολογία, παραπλανητική. Η έξυπνη σύμβαση δεν είναι απαραίτητα «σύμβαση» με τη νομική έννοια, ούτε είναι «έξυπνη» με την έννοια της κρίσης ή της προσαρμοστικότητας²³. Στην ελληνική θεωρία, ο Ιγγλεζάκης θεωρεί ότι η έξυπνη σύμβαση είναι έγκυρη αφού «οι δηλώσεις βούλησης αποδίδονται στα πρόσωπα που αποδέχονται τους όρους της σύμβασης» αφού «οι συναλλασσόμενοι επιλέγουν ελεύθερα αν της σύμβασης που είναι προδιατυπωμένοι, ενώ η εξωτερική της δήλωσης βούλησης

²⁰ Saeidi, M., Calvert, M., Au, A. W., Sarma, A., & Bobba, R. B. (2022). If this context then that concern: Exploring users' concerns with IFTTT applets. *Proceedings on Privacy Enhancing Technologies*, 2022(1), 166–186. <https://arxiv.org/pdf/2012.12518>

²¹ EU Blockchain Observatory and Forum (2019), Legal and Regulatory Framework of Blockchains and Smart Contracts, Thematic Report.

²² Werbach, K., Cornell, N. (2017), 'Contracts Ex Machina', *Duke Law Journal*, 67(2), σελ. 313 επ.

²³ Mik, E. (2017), 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity', *Law, Innovation and Technology*, 9(2), σελ. 269 επ.

με ηλεκτρονικά μέσα είναι έγκυρη»²⁴. Ορθότερη εμφανίζεται η λειτουργική διάκριση τριών περιπτώσεων. Στην πρώτη περίπτωση, η έξυπνη σύμβαση αποτελεί απλό μέσο αυτοματοποιημένης εκτέλεσης μιας συμβατικής σχέσης, που έχει καταρτιστεί με παραδοσιακό τρόπο, λειτουργεί δηλαδή σαν ένας μηχανισμός πληρωμής. Στη δεύτερη περίπτωση, η έξυπνη σύμβαση αποτυπώνει η ίδια τους συμβατικούς όρους, εν όλω ή εν μέρει, σε κώδικα (code as contract). Στην τρίτη περίπτωση, η έξυπνη σύμβαση λειτουργεί ως αυτοτελές τεχνικό εργαλείο χωρίς υποκείμενη συμβατική σχέση. Υπό το ελληνικό δίκαιο, όπου ισχύει πλέον και ο ειδικός Ν. 4961/2022 για τις αναδυόμενες τεχνολογίες²⁵, η κατάρτιση σύμβασης μέσω έξυπνης σύμβασης δεν προσκρούει καταρχήν σε εμπόδιο, αφού σύμφωνα με το άρθρο 49 παρ. 1 ορίζεται ότι το έξυπνο συμβόλαιο δεσμεύει τα μέρη από την ολοκλήρωση της προσχώρησής τους σε αυτό, ενώ για την κατάρτισή του εφαρμόζονται τα άρθρα 185 έως 196 του Αστικού Κώδικα, με εξαίρεση το άρθρο 194, ενώ σύμφωνα με το άρθρο 49 παρ. 5^α οι όροι μια έξυπνης σύμβασης δύνανται να ενσωματώνονται ακόμη σε κώδικα προγράμματος ηλεκτρονικού υπολογιστή.

Η δήλωση βούλησης μπορεί να εξωτερικευθεί και μέσω προγραμματισμένου κώδικα, εφόσον η ενεργοποίησή του ανάγεται σε ανθρώπινη απόφαση²⁶. Τα δύσκολα ζητήματα ανακύπτουν αλλού. Η ερμηνεία, λοιπόν, του κώδικα ως δήλωσης, στη μεταχείριση του σφάλματος και της πλάνης και στη δυνατότητα άσκησης διαπλαστικών δικαιωμάτων πάνω σε μια αμετάβλητη υποδομή. Στην ευρωπαϊκή συζήτηση, το European Law Institute έχει διατυπώσει αρχές, που επιχειρούν να γεφυρώσουν την τεχνολογική πραγματικότητα με το κεκτημένο της προστασίας του καταναλωτή²⁷. Παράλληλα, ο ευρωπαίος νομοθέτης εισήγαγε για πρώτη φορά, με το άρθρο 36 του Data Act, δεσμευτικές ουσιώδεις απαιτήσεις για τις έξυπνες συμβάσεις. Ανάμεσα σε αυτές ξεχωρίζει η υποχρέωση πρόβλεψης μηχανισμών ασφαλούς τερματισμού και διακοπής, δηλαδή ενός «διακόπτη» που επιβάλλεται από τον νόμο²⁸. Η νομοθετική αυτή επιλογή έχει ιδιαίτερη σημασία για την παρούσα εργασία, καθώς δείχνει ότι ο ευρωπαίος νομοθέτης αντιμετωπίζει την πλήρη και

²⁴ Ιγγλεζάκης, Ι. (2022), Το δίκαιο της ψηφιακής οικονομίας, Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκουλα, σελ. 240.

²⁵ Ν. 4961/2022, ό.π.

²⁶ Βλ. άρθρα 185-192 ΑΚ για τον μηχανισμό κατάρτισης της σύμβασης με πρόταση και αποδοχή. Η δήλωση βούλησης μπορεί κατά την κρατούσα άποψη να εξωτερικευθεί με οποιονδήποτε πρόσφορο τρόπο, συνεπώς και μέσω προγραμματισμένου κώδικα, εφόσον αυτός ανάγεται σε απόφαση προσώπου.

²⁷ European Law Institute (2022), ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection, Report of the European Law Institute.

²⁸ Άρθρο 36 του Κανονισμού (ΕΕ) 2023/2854 (Data Act), το οποίο θεσπίζει ουσιώδεις απαιτήσεις για τις έξυπνες συμβάσεις που χρησιμοποιούνται στην εκτέλεση συμφωνιών κοινοχρησίας δεδομένων, μεταξύ των οποίων μηχανισμούς ασφαλούς τερματισμού και διακοπής (termination and interruption).

μη αναστρέψιμη αυτονομία του κώδικα όχι ως δεδομένο, αλλά ως κίνδυνο που πρέπει να περιοριστεί.

3.3. Οι αυτόνομοι πράκτορες τεχνητής νοημοσύνης

3.3.1. Έννοια και ορισμοί

Στην επιστήμη της τεχνητής νοημοσύνης, ως πράκτορας (agent) νοείται κάθε οντότητα, που αντιλαμβάνεται το περιβάλλον της και δρα πάνω σε αυτό για να πετύχει κάποιους στόχους²⁹. Ο ορισμός αυτός, αν και ευρύς, αναδεικνύει τα δύο στοιχεία που ενδιαφέρουν τον νομικό. Το πρώτο είναι η αντίληψη, δηλαδή η λήψη και η επεξεργασία της πληροφορίας. Το δεύτερο είναι η δράση, δηλαδή η παραγωγή αποτελεσμάτων στον εξωτερικό κόσμο. Ο ευρωπαίος νομοθέτης υιοθέτησε, με το άρθρο 3 σημ. 1 του AI Act, έναν λειτουργικό ορισμό του «συστήματος ΤΝ», με κεντρικά στοιχεία τη λειτουργία με διαφορετικά επίπεδα αυτονομίας και την ικανότητα συναγωγής (inference) του τρόπου παραγωγής των εκροών από τις εισροές³⁰. Η ρητή νομοθετική αναγνώριση ότι η αυτονομία είναι μέγεθος δεκτικό διαβαθμίσεων, ότι δηλαδή υπάρχουν «επίπεδα» αυτονομίας, παρέχει το κανονιστικό έρεισμα και την βάση για την τυπολογία, που προτείνει η παρούσα εργασία. Στη νομική θεωρία, εξάλλου, έχει επισημανθεί από παλαιότερα ότι οι τεχνητοί πράκτορες θέτουν ζητήματα, που ξεπερνούν την παραδοσιακή διχοτομία μεταξύ προσώπου και πράγματος, καθώς συνδυάζουν την εργαλειακή φύση με μια λειτουργική «διακριτική ευχέρεια»³¹.

3.3.2. Από τον αυτοματισμό στην αυτονομία

Η κρίσιμη εννοιολογική τομή, την οποία η νομική ανάλυση οφείλει να αποτυπώσει με ακρίβεια, είναι εκείνη μεταξύ του αυτοματισμού και της αυτονομίας. Το αυτοματοποιημένο σύστημα εκτελεί προδιαγεγραμμένες εντολές. Η συμπεριφορά του είναι πλήρως προβλέψιμη από τον προγραμματιστή του και κάθε εκροή του ανάγεται, έστω και έμμεσα, σε ανθρώπινη επιλογή. Το αυτόνομο σύστημα, αντίθετα, επιλέγει το ίδιο τη

²⁹Russell, S., Norvig, P. (2021), Artificial Intelligence: A Modern Approach, 4th ed., Hoboken: Pearson, όπου ο πράκτορας ορίζεται ως οντότητα, που αντιλαμβάνεται το περιβάλλον της μέσω αισθητήρων και δρα πάνω σε αυτό μέσω ενεργοποιητών.

³⁰Άρθρο 3 σημ. 1 του Κανονισμού (ΕΕ) 2024/1689 (AI Act), κατά το οποίο ως «σύστημα ΤΝ» νοείται μηχανικό σύστημα σχεδιασμένο να λειτουργεί με διαφορετικά επίπεδα αυτονομίας, το οποίο συνάγει από τις εισροές που λαμβάνει πώς να παράγει στοχευμένες εκροές, όπως προβλέψεις, περιεχόμενο, συστάσεις ή αποφάσεις. Βλ. και αιτιολογική σκέψη 12 του ίδιου Κανονισμού για τα εννοιολογικά στοιχεία της αυτονομίας και της συναγωγικής ικανότητας.

³¹Chopra, S., White, L.F. (2011), A Legal Theory for Autonomous Artificial Agents, Ann Arbor: University of Michigan Press, σελ. 5 επ.

συμπεριφορά του για να πετύχει έναν στόχο, με βάση μοντέλα, που έχουν προκύψει από εκπαίδευση σε δεδομένα. Η συμπεριφορά του είναι πιθανολογική και όχι ντετερμινιστική. Αυτό σημαίνει ότι ούτε ο κατασκευαστής ούτε ο χρήστης μπορούν να προβλέψουν πλήρως τις ενέργειές του σε κάθε συγκεκριμένη περίπτωση. Η νεότερη γενιά πρακτόρων που βασίζονται στα μεγάλα γλωσσικά μοντέλα κάνει τη διάκριση αυτή ακόμη πιο έντονη. Πρόκειται για συστήματα που μπορούν να αναλύουν έναν γενικό στόχο σε επιμέρους ενέργειες, να χρησιμοποιούν εξωτερικά εργαλεία, στα οποία περιλαμβάνονται κρυπτογραφικά πορτοφόλια και διεπαφές με blockchain, να προσαρμόζουν τη στρατηγική τους με βάση τα αποτελέσματα και να λειτουργούν για μεγάλα χρονικά διαστήματα χωρίς ανθρώπινη έγκριση κάθε επιμέρους πράξης³². Παράλληλα, η ίδια η τεχνητή νοημοσύνη έχει αναδειχθεί σε κεντρικό στοιχείο του ευρωπαϊκού τοπίου απειλών κυβερνοασφάλειας, τόσο ως εργαλείο επιθέσεων όσο και ως στόχος τους³³. Η διαπίστωση αυτή έχει προφανή σημασία για την ένταξη του φαινομένου στο πεδίο της NIS2.

3.4. Μορφές αλληλεπίδρασης έξυπνων συμβάσεων και αυτόνομων πρακτόρων

Η σύγκλιση των δύο τεχνολογιών εκδηλώνεται σε κλιμακούμενες μορφές. Στην ηπιότερη εκδοχή, το σύστημα τεχνητής νοημοσύνης λειτουργεί περιφερειακά προς την έξυπνη σύμβαση, ως πηγή δεδομένων ή κρίσης. Τροφοδοτεί την αλυσίδα, μέσω των μηχανισμών που ονομάζονται oracles³⁴, με εξωτερικές πληροφορίες ή αξιολογήσεις, από τις οποίες εξαρτάται η ενεργοποίηση της σύμβασης, όπως συνέβαινε για παράδειγμα στα παραμετρικά ασφαλιστήρια πτήσεων, όπου η αποζημίωση για την καθυστέρηση καταβαλλόταν αυτόματα μόλις η πηγή δεδομένων επιβεβαίωνε το γεγονός³⁵. Ήδη στη μορφή αυτή, η αξιοπιστία της εκτέλεσης μετατοπίζεται από τον κώδικα της σύμβασης στην ποιότητα και την ακεραιότητα του μοντέλου, που παράγει την πληροφορία. Στην εντονότερη εκδοχή, ο πράκτορας γίνεται ο ίδιος συναλλασσόμενος. Κατέχει ή ελέγχει κρυπτογραφικό πορτοφόλι, επιλέγει αντισυμβαλλομένους και όρους, και συνάπτει ή εκτελεί έξυπνες

³²Marino, B., Juels, A. (2025), ό.π.

³³ENISA (2025), ENISA Threat Landscape 2025, όπου η τεχνητή νοημοσύνη αναδεικνύεται σε καθοριστικό στοιχείο του τοπίου απειλών, τόσο ως εργαλείο των επιτιθέμενων όσο και ως στόχος επιθέσεων, για παράδειγμα μέσω δηλητηρίασης μοντέλων και επιθέσεων στην εφοδιαστική αλυσίδα λογισμικού τεχνητής νοημοσύνης.

³⁴Ως oracles νοούνται οι μηχανισμοί, που τροφοδοτούν την αλυσίδα με εξωτερικά δεδομένα, δηλαδή δεδομένα εκτός αλυσίδας (off-chain), όπως τιμές ή γεγονότα. Από την ακεραιότητα των δεδομένων αυτών εξαρτάται σε μεγάλο βαθμό η ορθή εκτέλεση της έξυπνης σύμβασης.

³⁵ Χαρακτηριστικό παράδειγμα από τη συναλλακτική πρακτική αποτέλεσε η εφαρμογή παραμετρικής ασφάλισης καθυστερήσεων πτήσεων fuzzy της AXA (2017-2019), η οποία λειτουργούσε με έξυπνες συμβάσεις στην αλυσίδα Ethereum.

συμβάσεις για λογαριασμό του εντολέα του, ενίοτε και χωρίς συγκεκριμένη εντολή. Αυτό συμβαίνει ήδη σε εφαρμογές αποκεντρωμένης χρηματοοικονομικής (DeFi), σε συστήματα αυτοματοποιημένης διαχείρισης χαρτοφυλακίων και σε αγορές μεταξύ μηχανών (machine-to-machine commerce)³⁶. Στην οριακή, τέλος, εκδοχή, ο πράκτορας εντάσσεται σε αποκεντρωμένους αυτόνομους οργανισμούς (DAOs) ή λειτουργεί ο ίδιος πάνω σε αποκεντρωμένη υποδομή, χωρίς να υπάρχει πρόσωπο με πραγματική εξουσία ελέγχου ή διακοπής της λειτουργίας του. Η εμπειρία έχει ήδη δείξει ότι στα σχήματα αυτά η αστοχία του κώδικα ή η χειραγώγηση των εισροών μπορεί να πάρει συστημικές διαστάσεις. Χαρακτηριστική παραμένει η περίπτωση του The DAO (2016), όπου η εκμετάλλευση ευπάθειας του κώδικα οδήγησε σε αφαίρεση κρυπτοστοιχείων μεγάλης αξίας και τελικά στη διχοτόμηση (hard fork) της αλυσίδας Ethereum. Το γεγονός αυτό ανέδειξε τόσο τα όρια του δόγματος code is law όσο και το κενό λογοδοσίας στα αποκεντρωμένα σχήματα³⁷. Η Ομάδα Εμπειρογνομόνων της Ευρωπαϊκής Επιτροπής για την ευθύνη και τις νέες τεχνολογίες είχε άλλωστε επισημάνει εγκαίρως ότι ο συνδυασμός της αυτονομίας, της πολυπλοκότητας και της πολλαπλότητας των εμπλεκόμενων μερών δημιουργεί τα λεγόμενα «κενά ευθύνης» (liability gaps)³⁸.

3.5. Τυπολογία βαθμίδων αυτονομίας των ψηφιακών οντοτήτων

Από την παραπάνω χαρτογράφηση προκύπτει ότι η «αυτονομία των ψηφιακών οντοτήτων» δεν είναι ενιαίο μέγεθος, αλλά ένα φάσμα. Η παρούσα εργασία προτείνει, ως αναλυτικό εργαλείο, μια τυπολογία πέντε βαθμίδων. Τα κριτήρια της κατάταξης είναι νομικά κρίσιμα. Το πρώτο είναι η ένταση της ανθρώπινης εμπλοκής στη λήψη της κάθε επιμέρους απόφασης. Το δεύτερο είναι η προβλεψιμότητα της συμπεριφοράς του συστήματος. Το τρίτο είναι η ύπαρξη και η αποτελεσματικότητα μηχανισμών παρέμβασης και διακοπής (kill switch). Το τέταρτο είναι η δυνατότητα προσδιορισμού ενός προσώπου με πραγματική εξουσία ελέγχου³⁹.

³⁶ Marino, B., Juels, A. (2025), ό.π.

³⁷ DuPont, Q. (2018), 'Experiments in Algorithmic Governance: A History and Ethnography of The DAO, a Failed Decentralized Autonomous Organization', σε Campbell-Verduyn, M. (επιμ.), Bitcoin and Beyond, London: Routledge. Βλ. και De Filippi, P., Wright, A. (2018), ό.π.

³⁸ Expert Group on Liability and New Technologies (New Technologies Formation) (2019), Liability for Artificial Intelligence and Other Emerging Digital Technologies, Ευρωπαϊκή Επιτροπή, σελ. 32 επ.

³⁹ Η δομή της τυπολογίας εμπνέεται μεθοδολογικά από κλιμακωτά συστήματα ταξινόμησης του αυτοματισμού που έχουν καθιερωθεί σε άλλα πεδία, όπως τα επίπεδα αυτοματισμού οδήγησης του προτύπου SAE J3016. Δεν ταυτίζεται ωστόσο με αυτά, καθώς τα κρίσιμα εδώ κριτήρια είναι νομικά και όχι αμιγώς τεχνικά (<https://www.sae.org/standards/j3016-taxonomy-definitions-terms-related-driving-automation-systems-road-motor-vehicles>)

Βαθμίδα 0, ντετερμινιστική εκτέλεση: πρόκειται για την κλασική έξυπνη σύμβαση χωρίς στοιχείο τεχνητής νοημοσύνης. Ο κώδικας εκτελεί προδιαγεγραμμένες εντολές και κάθε εκροή ανάγεται σε ανθρώπινη επιλογή κατά τον σχεδιασμό (by design). Η συμπεριφορά είναι πλήρως προβλέψιμη, με την επιφύλαξη των σφαλμάτων του κώδικα, και ο καταλογισμός δεν παρουσιάζει ιδιαίτερες δογματικές δυσκολίες.

Βαθμίδα 1, υποβοηθούμενη απόφαση: το σύστημα τεχνητής νοημοσύνης λειτουργεί συμβουλευτικά, για παράδειγμα προτείνει μια συναλλαγή ή αξιολογεί έναν κίνδυνο, αλλά κάθε δεσμευτική ενέργεια προϋποθέτει ρητή ανθρώπινη έγκριση (human-in-the-loop). Η δήλωση βούλησης ανάγεται εύκολα στο φυσικό ή νομικό πρόσωπο.

Βαθμίδα 2, εποπτευόμενη αυτονομία: ο πράκτορας εκτελεί συναλλαγές χωρίς προηγούμενη έγκριση κάθε επιμέρους πράξης, αλλά μέσα σε όρια, που έχουν καθοριστεί ρητά εκ των προτέρων, όπως συγκεκριμένες εντολές, ποσοτικά όρια και κατάλογος επιτρεπόμενων αντισυμβαλλομένων. Η λειτουργία του τελεί υπό διαρκή ανθρώπινη εποπτεία, με δυνατότητα άμεσης παρέμβασης (human-on-the-loop).

Βαθμίδα 3, οριοθετημένη πλήρης αυτονομία: ο πράκτορας θέτει ο ίδιος ενδιάμεσους στόχους και επιλέγει τα μέσα για την επίτευξη ενός γενικού σκοπού, συναλλασσόμενος χωρίς προηγούμενη έγκριση. Η ανθρώπινη εμπλοκή περιορίζεται στον καθορισμό του σκοπού και στον εκ των υστέρων έλεγχο. Διατηρείται πάντως λειτουργικός μηχανισμός διακοπής και υπάρχει υπεύθυνο πρόσωπο, που αναπτύσσει ή λειτουργεί το σύστημα.

Βαθμίδα 4, μη εποπτευόμενη ή αποκεντρωμένη αυτονομία: ο πράκτορας λειτουργεί πάνω σε αποκεντρωμένη υποδομή, χωρίς πρόσωπο με πραγματική εξουσία ελέγχου ή διακοπής και χωρίς αποτελεσματικό μηχανισμό παρέμβασης (human-out-of-the-loop). Πρόκειται για την οριακή περίπτωση, στην οποία εντοπίζονται τα σοβαρότερα κενά ευθύνης και εποπτείας.

Η αξία της τυπολογίας είναι διπλή. Από τη μία πλευρά, επιτρέπει τη διαφοροποιημένη νομική αξιολόγηση. Όπως θα αναλυθεί στο Κεφάλαιο 5, τα παραδοσιακά δογματικά εργαλεία, δηλαδή η αντιπροσώπευση, ο βοηθός εκπλήρωσης και η ευθύνη του παραγωγού, λειτουργούν ικανοποιητικά στις χαμηλές βαθμίδες, ενώ δοκιμάζονται ή αστοχούν στις υψηλές. Από την άλλη πλευρά, παρέχει τη βάση για ένα κλιμακωτό μοντέλο ρυθμιστικής συμμόρφωσης, το οποίο θα αναπτυχθεί στο Κεφάλαιο 6. Σύμφωνα με το μοντέλο αυτό, η ένταση των υποχρεώσεων κυβερνοασφάλειας και εποπτείας θα πρέπει να βρίσκεται σε αναλογία με τη βαθμίδα αυτονομίας. Η προσέγγιση αυτή είναι συμβατή τόσο

με τη λογική της βασισμένης στον κίνδυνο ρύθμισης του AI Act όσο και με τη διαχείριση κινδύνου κατά το άρθρο 21 της NIS2.

4. Το ρυθμιστικό πλαίσιο της NIS2 και η κυβερνοασφάλεια

Το παρόν κεφάλαιο εξετάζει το ρυθμιστικό πλαίσιο της Οδηγίας NIS2 και της ελληνικής της ενσωμάτωσης. Η ανάλυση ξεκινά από τον σκοπό και τις βασικές καινοτομίες της Οδηγίας και προχωρά στο πεδίο εφαρμογής της. Στη συνέχεια εξετάζεται το κρίσιμο για την παρούσα εργασία ερώτημα, δηλαδή αν και πώς τα οικοσυστήματα αλληλεπίδρασης έξυπνων συμβάσεων και αυτόνομων πρακτόρων υπάγονται στις υποχρεώσεις της. Το κεφάλαιο ολοκληρώνεται με την ανάδειξη των ορίων της Οδηγίας απέναντι στα αποκεντρωμένα συστήματα και με τη χαρτογράφηση της σχέσης της με τα παράλληλα ευρωπαϊκά νομοθετήματα.

4.1. Από τη NIS στη NIS2: σκοπός, καινοτομίες και ελληνική ενσωμάτωση

Η Οδηγία (ΕΕ) 2016/1148, γνωστή ως Οδηγία NIS, υπήρξε το πρώτο οριζόντιο νομοθέτημα της Ένωσης για την κυβερνοασφάλεια. Η εφαρμογή της ανέδειξε ωστόσο σημαντικές αδυναμίες. Το πεδίο εφαρμογής της ήταν στενό, τα κράτη μέλη προσδιόριζαν τα ίδια τους υπόχρεους φορείς με αποκλίνοντα κριτήρια και οι απαιτήσεις ασφάλειας και αναφοράς διέφεραν ουσιωδώς από χώρα σε χώρα⁴⁰. Η Οδηγία NIS2 ήρθε να θεραπεύσει τις αδυναμίες αυτές. Οι βασικές της καινοτομίες μπορούν να συνοψιστούν σε τέσσερα σημεία. Πρώτον, το πεδίο εφαρμογής διευρύνεται σημαντικά και καλύπτει πλέον δεκαοκτώ τομείς υψηλής κρισιμότητας ή άλλης κρισιμότητας. Δεύτερον, η υπαγωγή γίνεται κατά κανόνα αυτόματα, με βάση τον συνδυασμό του τομέα δραστηριότητας και του μεγέθους της επιχείρησης, χωρίς να απαιτείται πράξη ορισμού από το κράτος μέλος. Τρίτον, οι υποχρεώσεις διαχείρισης κινδύνων και αναφοράς περιστατικών εναρμονίζονται και εξειδικεύονται. Τέταρτον, ενισχύεται ουσιαστικά το εποπτικό και κυρωτικό οπλοστάσιο, με πρόστιμα που φθάνουν τα 10.000.000 ευρώ ή το 2% του παγκόσμιου κύκλου εργασιών για τις βασικές οντότητες, καθώς και με πρόβλεψη προσωπικής ευθύνης των μελών των διοικητικών οργάνων.

Στην ελληνική έννομη τάξη η Οδηγία ενσωματώθηκε με τον Ν. 5160/2024. Ο νόμος ορίζει την Εθνική Αρχή Κυβερνοασφάλειας ως αρμόδια αρχή και ενιαίο σημείο επαφής, προβλέπει την κατάρτιση καταλόγου βασικών και σημαντικών οντοτήτων και οργανώνει το σύστημα εποπτείας και κυρώσεων. Η εφαρμογή του εξειδικεύεται με σειρά κανονιστικών πράξεων. Με την ΚΥΑ 1689/2025 θεσπίστηκε το Εθνικό Πλαίσιο Απαιτήσεων

⁴⁰Βλ. αιτιολογικές σκέψεις 1 έως 5 της Οδηγίας (ΕΕ) 2022/2555, όπου καταγράφονται οι αποκλίσεις στην εφαρμογή της Οδηγίας (ΕΕ) 2016/1148 μεταξύ των κρατών μελών και η ανάγκη ενός πιο εναρμονισμένου πλαισίου.

Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων, το οποίο καθορίζει τα συγκεκριμένα μέτρα, που οφείλουν να εφαρμόζουν οι υπόχρεοι φορείς, ενώ με προγενέστερη κοινή υπουργική απόφαση τέθηκε σε λειτουργία η Ψηφιακή Πλατφόρμα Εγγραφής Οντοτήτων, με προθεσμία εγγραφής, που έληξε στις 30 Σεπτεμβρίου 2025⁴¹. Το ρυθμιστικό οικοδόμημα, τέλος, παραμένει δυναμικό και σε ευρωπαϊκό επίπεδο, καθώς η Επιτροπή πρότεινε τον Ιανουάριο του 2026 στοχευμένες τροποποιήσεις της Οδηγίας για την απλούστευση της συμμόρφωσης⁴².

4.2. Το πεδίο εφαρμογής: τομείς, κανόνας μεγέθους και κατηγορίες οντοτήτων

Η υπαγωγή στη NIS2 στηρίζεται σε δύο σωρευτικά κριτήρια. Το πρώτο είναι τομεακό. Η οντότητα πρέπει να δραστηριοποιείται σε έναν από τους τομείς του Παραρτήματος Ι (τομείς υψηλής κρισιμότητας, όπως η ενέργεια, οι μεταφορές, η υγεία, οι ψηφιακές υποδομές και η διαχείριση υπηρεσιών ΤΠΕ) ή του Παραρτήματος ΙΙ (άλλοι κρίσιμοι τομείς, όπως τα τρόφιμα, τα χημικά και οι πάροχοι ψηφιακών υπηρεσιών). Το δεύτερο κριτήριο είναι ο κανόνας του μεγέθους. Κατά κανόνα υπάγονται οι οντότητες που φθάνουν ή υπερβαίνουν τα όρια των μεσαίων επιχειρήσεων, δηλαδή απασχολούν τουλάχιστον 50 εργαζομένους ή έχουν ετήσιο κύκλο εργασιών και ισολογισμό άνω των 10.000.000 ευρώ⁴³. Ο κανόνας αυτός έχει σημαντικές εξαιρέσεις. Ορισμένες κατηγορίες, όπως οι πάροχοι υπηρεσιών εμπιστοσύνης, τα μητρώα ονομάτων τομέα ανωτάτου επιπέδου και οι πάροχοι υπηρεσιών DNS, υπάγονται ανεξαρτήτως μεγέθους, όπως και οντότητες που είναι κρίσιμες για τη διατήρηση βασικών κοινωνικών ή οικονομικών δραστηριοτήτων. Οι υπόχρεες οντότητες κατατάσσονται περαιτέρω σε βασικές και σημαντικές, με διαφοροποιημένο καθεστώς εποπτείας. Οι βασικές υπόκεινται σε προληπτική και κατασταλτική εποπτεία, ενώ οι σημαντικές μόνο σε κατασταλτική⁴⁴.

4.3. Το ζήτημα της υπαγωγής: πού εντάσσονται τα οικοσυστήματα smart contracts και AI agents

4.3.1. Πάροχοι υποδομών και υπηρεσιών blockchain

⁴¹ΚΥΑ 1689/2025, ό.π. Βλ. επίσης την ΚΥΑ 1381/2025 (ΦΕΚ Β' 463/10.02.2025) για την Ψηφιακή Πλατφόρμα Εγγραφής Οντοτήτων της Εθνικής Αρχής Κυβερνοασφάλειας, όπως τροποποιήθηκε, με προθεσμία εγγραφής των υπόχρεων οντοτήτων έως τις 30 Σεπτεμβρίου 2025.

⁴² Πρόταση της Ευρωπαϊκής Επιτροπής της 20ής Ιανουαρίου 2026 για στοχευμένες τροποποιήσεις της Οδηγίας NIS2, ό.π.

⁴³Άρθρο 2 παρ. 1 της Οδηγίας (ΕΕ) 2022/2555, με παραπομπή στο άρθρο 2 του παραρτήματος της σύστασης 2003/361/ΕΚ για τον ορισμό των μεσαίων επιχειρήσεων. Οι εξαιρέσεις από τον κανόνα του μεγέθους προβλέπονται στις παρ. 2 έως 4 του ίδιου άρθρου.

⁴⁴Άρθρο 3 της Οδηγίας (ΕΕ) 2022/2555 για τη διάκριση μεταξύ βασικών και σημαντικών οντοτήτων.

Η Οδηγία δεν αναφέρει πουθενά τις λέξεις blockchain, smart contract ή τεχνητή νοημοσύνη στους καταλόγους των υπόχρεων οντοτήτων. Η υπαγωγή πρέπει επομένως να αναζητηθεί ερμηνευτικά, μέσα από τις υφιστάμενες κατηγορίες. Το πρώτο και ασφαλέστερο κανάλι υπαγωγής είναι οι υποκείμενες υποδομές. Οι κόμβοι των blockchain δικτύων και οι εφαρμογές, που εκτελούν έξυπνες συμβάσεις φιλοξενούνται κατά κανόνα σε υπηρεσίες υπολογιστικού νέφους και σε κέντρα δεδομένων. Οι πάροχοι των υπηρεσιών αυτών εντάσσονται ρητά στον τομέα των ψηφιακών υποδομών του Παραρτήματος I⁴⁵ και μάλιστα οι υποχρεώσεις τους έχουν ήδη εξειδικευθεί με τον Εκτελεστικό Κανονισμό (ΕΕ) 2024/2690⁴⁶. Το δεύτερο κανάλι είναι οι υπηρεσίες, που παρέχονται πάνω από την υποδομή. Οι εταιρείες, που διαχειρίζονται κόμβους για λογαριασμό τρίτων, προσφέρουν πρόσβαση σε blockchain μέσω διεπαφών ή αναλαμβάνουν τη λειτουργία και την ασφάλεια συστημάτων πελατών, μπορούν, κατά περίπτωση, να χαρακτηριστούν πάροχοι διαχειριζόμενων υπηρεσιών ή διαχειριζόμενων υπηρεσιών ασφάλειας, κατηγορίες που επίσης ανήκουν στο Παράρτημα I. Το τρίτο κανάλι αφορά τις πλατφόρμες συναλλαγών. Οι κεντροποιημένες πλατφόρμες, που φέρνουν σε επαφή αγοραστές και πωλητές κρυπτοστοιχείων ή ψηφιακών αγαθών ενδέχεται να εμπίπτουν στην έννοια της επιγραμμικής αγοράς του Παραρτήματος II⁴⁷. Τέλος, για τους παρόχους υπηρεσιών κρυπτοστοιχείων, που αδειοδοτούνται κατά τον Κανονισμό MiCA ισχύει μια σημαντική ιδιαιτερότητα. Ως χρηματοοικονομικές οντότητες υπάγονται στον Κανονισμό DORA, ο οποίος λειτουργεί ως *lex specialis* απέναντι στη NIS2 και εκτοπίζει τις αντίστοιχες υποχρεώσεις της⁴⁸.

Η εικόνα αυτή δείχνει ότι το ευρωπαϊκό δίκαιο συλλαμβάνει ικανοποιητικά τους κεντροποιημένους κρίκους της αλυσίδας αξίας. Αφήνει όμως ακάλυπτο τον σκληρό πυρήνα του φαινομένου. Το ίδιο το αποκεντρωμένο δίκτυο, δηλαδή το σύνολο των

⁴⁵Παράρτημα I της Οδηγίας (ΕΕ) 2022/2555, τομείς «Ψηφιακές υποδομές» και «Διαχείριση υπηρεσιών ΤΠΕ (μεταξύ επιχειρήσεων)».

⁴⁶Εκτελεστικός Κανονισμός (ΕΕ) 2024/2690 της Επιτροπής, της 17ης Οκτωβρίου 2024, για τον καθορισμό των τεχνικών και μεθοδολογικών απαιτήσεων των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας και για τον περαιτέρω προσδιορισμό των περιπτώσεων στις οποίες ένα περιστατικό θεωρείται σημαντικό, όσον αφορά μεταξύ άλλων τους παρόχους υπηρεσιών υπολογιστικού νέφους, υπηρεσιών κέντρων δεδομένων, διαχειριζόμενων υπηρεσιών και διαχειριζόμενων υπηρεσιών ασφάλειας, καθώς και τους παρόχους ψηφιακών υπηρεσιών.

⁴⁷Παράρτημα II της Οδηγίας (ΕΕ) 2022/2555, τομέας «Πάροχοι ψηφιακών υπηρεσιών», ο οποίος περιλαμβάνει τους παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης.

⁴⁸Άρθρο 4 της Οδηγίας (ΕΕ) 2022/2555 για τη σχέση με τομεακές νομικές πράξεις της Ένωσης. Για τις χρηματοοικονομικές οντότητες, στις οποίες περιλαμβάνονται και οι πάροχοι υπηρεσιών κρυπτοστοιχείων κατά τον Κανονισμό (ΕΕ) 2023/1114 (MiCA), ο Κανονισμός (ΕΕ) 2022/2554 (DORA) λειτουργεί ως *lex specialis*.

ανεξάρτητων κόμβων, που συντηρούν ένα ανοικτό blockchain, δεν αποτελεί «οντότητα» με την έννοια της Οδηγίας, αφού δεν υπάρχει πρόσωπο, που να παρέχει την υπηρεσία. Το ίδιο ισχύει και για τα πρωτόκολλα που λειτουργούν πλήρως αποκεντρωμένα. Είναι χαρακτηριστικό ότι ακόμη και ο Κανονισμός MiCA δηλώνει ρητά ότι δεν καταλαμβάνει τις υπηρεσίες κρυπτοστοιχείων, που παρέχονται με πλήρως αποκεντρωμένο τρόπο⁴⁹. Δημιουργείται έτσι ένα κανονιστικό παράδοξο. Όσο πιο αποκεντρωμένο είναι ένα σύστημα, δηλαδή όσο μεγαλύτερος είναι ο συστημικός κίνδυνος από την απουσία ελέγχου, τόσο πιθανότερο είναι να διαφεύγει από το πεδίο εφαρμογής των κανόνων κυβερνοασφάλειας.

4.3.2. Πάροχοι υπηρεσιών τεχνητής νοημοσύνης

Ανάλογη είναι η εικόνα και για την πλευρά της τεχνητής νοημοσύνης. Οι πάροχοι, που διαθέτουν αυτόνομους πράκτορες, ως υπηρεσία, μέσω υπολογιστικού νέφους θα υπαχθούν συνήθως στη NIS2 υπό την ιδιότητα του παρόχου υπηρεσιών υπολογιστικού νέφους ή του παρόχου διαχειριζόμενων υπηρεσιών, εφόσον πληρούν και τον κανόνα του μεγέθους. Η ανάπτυξη και η διάθεση του λογισμικού του πράκτορα, αυτή καθαυτή, δεν αποτελεί ωστόσο ρυθμιζόμενη δραστηριότητα κατά τη NIS2. Ο κατασκευαστής ενός μοντέλου ή ενός πράκτορα, που απλώς πωλεί ή παραχωρεί το προϊόν του δεν είναι υπόχρεη οντότητα. Η έλλειψη αυτή μετριάζεται με δύο τρόπους. Ο πρώτος είναι έμμεσος και περνά μέσα από την εφοδιαστική αλυσίδα. Η υπόχρεη οντότητα, που ενσωματώνει έναν πράκτορα στη λειτουργία της οφείλει, στο πλαίσιο της ασφάλειας της εφοδιαστικής αλυσίδας του άρθρου 21, να αξιολογεί την ασφάλεια των προμηθευτών της και να απαιτεί συμβατικές εγγυήσεις. Ο δεύτερος τρόπος είναι τα παράλληλα καθεστώτα, δηλαδή ο AI Act για τα συστήματα υψηλού κινδύνου και ο Cyber Resilience Act για τα προϊόντα με ψηφιακά στοιχεία, τα οποία θα εξεταστούν στην ενότητα 4.6.

4.4. Οι ουσιαστικές υποχρεώσεις υπό το πρίσμα της αυτονομίας

Για τις οντότητες που υπάγονται στη NIS2, οι ουσιαστικές υποχρεώσεις οργανώνονται σε τρεις πυλώνες. Ο πρώτος πυλώνας είναι η διακυβέρνηση. Τα διοικητικά όργανα εγκρίνουν τα μέτρα διαχείρισης κινδύνων, επιβλέπουν την εφαρμογή τους και μπορούν να θεωρηθούν υπεύθυνα για τις παραβάσεις, ενώ υποχρεούνται και σε τακτική κατάρτιση⁵⁰. Ο δεύτερος πυλώνας είναι τα μέτρα διαχείρισης κινδύνων του άρθρου 21. Ο

⁴⁹Βλ. αιτιολογική σκέψη 22 του Κανονισμού (ΕΕ) 2023/1114 (MiCA), κατά την οποία οι υπηρεσίες κρυπτοστοιχείων, που παρέχονται με πλήρως αποκεντρωμένο τρόπο, χωρίς κανέναν ενδιάμεσο, δεν εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού.

⁵⁰ Άρθρο 20 της Οδηγίας (ΕΕ) 2022/2555.

κατάλογος των ελάχιστων μέτρων περιλαμβάνει, μεταξύ άλλων, τις πολιτικές ανάλυσης κινδύνων, τη διαχείριση περιστατικών, την επιχειρησιακή συνέχεια, την ασφάλεια της εφοδιαστικής αλυσίδας, την ασφάλεια στην απόκτηση, την ανάπτυξη και τη συντήρηση των συστημάτων, την κρυπτογραφία και τον έλεγχο πρόσβασης⁵¹. Ο τρίτος πυλώνας είναι η αναφορά περιστατικών. Το άρθρο 23 καθιερώνει ένα κλιμακωτό σύστημα με έγκαιρη προειδοποίηση εντός 24 ωρών, κοινοποίηση εντός 72 ωρών και τελική έκθεση εντός ενός μηνός⁵². Στην Ελλάδα οι υποχρεώσεις αυτές εξειδικεύονται με το Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας. Στην πράξη τα μέτρα αυτά μεταφράζονται σε συγκεκριμένες τεχνικές και οργανωτικές επιλογές. Μια οντότητα που λειτουργεί υπηρεσίες συνδεδεμένες με έξυπνες συμβάσεις οφείλει, για παράδειγμα, να εφαρμόζει πολυπαραγοντική επαλήθευση ταυτότητας στα κρίσιμα συστήματά της, να φυλάσσει τα κρυπτογραφικά κλειδιά σε ασφαλές υλικό, να αξιολογεί τους προμηθευτές λογισμικού της στο πλαίσιο της ασφάλειας της εφοδιαστικής αλυσίδας και να διαθέτει δοκιμασμένο σχέδιο επιχειρησιακής συνέχειας για την περίπτωση παραβίασης.

Το ενδιαφέρον ερώτημα για την παρούσα εργασία είναι πώς οι γενικές αυτές υποχρεώσεις μεταφράζονται σε ένα περιβάλλον αυτόνομων ψηφιακών οντοτήτων. Η τυπολογία των βαθμίδων αυτονομίας του Κεφαλαίου 3 προσφέρει εδώ ένα χρήσιμο κλειδί ανάγνωσης. Στις χαμηλές βαθμίδες, η διαχείριση κινδύνου επικεντρώνεται στην ποιότητα του κώδικα. Κρίσιμα μέτρα είναι ο έλεγχος του κώδικα των έξυπνων συμβάσεων (audit), η τυπική επαλήθευση και η ασφαλής ανάπτυξη κατά το άρθρο 21. Στις μεσαίες βαθμίδες, όπου ο πράκτορας συναλλάσσεται μέσα σε προκαθορισμένα όρια, το κέντρο βάρους μετατοπίζεται στην αρχιτεκτονική της εποπτείας. Η οντότητα οφείλει να αποδεικνύει ότι τα όρια είναι τεχνικά δεσμευτικά, ότι η ανθρώπινη παρέμβαση είναι πραγματικά εφικτή και ότι κάθε ενέργεια του πράκτορα καταγράφεται με τρόπο, που επιτρέπει τον εκ των υστέρων έλεγχο. Στις υψηλές βαθμίδες, τα ζητήματα γίνονται οξύτερα. Η υποχρέωση αναφοράς εντός 24 ωρών προϋποθέτει ότι η οντότητα αντιλαμβάνεται εγκαίρως το περιστατικό, κάτι καθόλου αυτονόητο, όταν ο πράκτορας λειτουργεί συνεχώς και τροποποιεί ο ίδιος τη στρατηγική του. Αντίστοιχα, η αποτελεσματική διαχείριση περιστατικών προϋποθέτει μηχανισμό άμεσης διακοπής, δηλαδή τον «διακόπτη» που συναντήσαμε ήδη στο άρθρο 36 του Data Act. Την ανάγκη αυτής της προσαρμογής επιβεβαιώνει και ο ENISA, καθώς υποστηρίζει ότι «τα υπάρχοντα τεχνικά και οργανωτικά πρότυπα γενικής χρήσης (όπως τα

⁵¹ Άρθρο 21 παρ. 1 και 2 της Οδηγίας (ΕΕ) 2022/2555.

⁵² Άρθρο 23 της Οδηγίας (ΕΕ) 2022/2555.

ISO-IEC 27001 και ISO-IEC 9001) μπορούν να συμβάλουν στον μετριασμό ορισμένων από τους κινδύνους που αντιμετωπίζει η Τεχνητή Νοημοσύνη με τη βοήθεια συγκεκριμένων οδηγιών σχετικά με τον τρόπο εφαρμογής τους σε ένα πλαίσιο Τεχνητής Νοημοσύνης. Αυτή η σκέψη πηγάζει από το γεγονός ότι, ουσιαστικά, η Τεχνητή Νοημοσύνη είναι λογισμικό και επομένως τα μέτρα ασφαλείας λογισμικού μπορούν να μεταφερθούν στον τομέα της Τεχνητής Νοημοσύνης»⁵³. Με αυτόν τον τρόπο, η λογική της NIS2 συγκλίνει με τη λογική του κλιμακωτού μοντέλου, που θα προταθεί στο Κεφάλαιο 6, ⁵⁴ αφού «η κακόβουλη χρήση της Τεχνητής Νοημοσύνης θα μπορούσε να απειλήσει τη φυσική ασφάλεια (π.χ., μη κρατικοί φορείς που μετατρέπουν τα καταναλωτικά drones σε όπλα), την ψηφιακή ασφάλεια (π.χ., μέσω εγκληματιών που εκπαιδεύουν μηχανήματα για να κάνουν hacking) και την πολιτική ασφάλεια (π.χ., μέσω επιτήρησης, δημιουργίας προφίλ και καταστολής που καταργούν την ιδιωτικότητα ή μέσω αυτοματοποιημένων και στοχευμένων καμπανιών παραπληροφόρησης)»⁵⁵.

4.5. Τα όρια της NIS2 απέναντι στα αποκεντρωμένα συστήματα

Η ανάλυση που προηγήθηκε αναδεικνύει τρία δομικά όρια της Οδηγίας απέναντι στα πλήρως αποκεντρωμένα οικοσυστήματα, όπως το πρωτόκολλο Bitcoin ή τα αποκεντρωμένα πρωτόκολλα ανταλλαγής κρυπτοστοιχείων, δηλαδή απέναντι στη Βαθμίδα 4 της τυπολογίας. Το πρώτο όριο είναι υποκειμενικό. Η Οδηγία απευθύνεται σε «οντότητες», δηλαδή σε νομικά ή φυσικά πρόσωπα, που παρέχουν υπηρεσίες. Σε ένα ανοικτό δίκτυο χωρίς διαχειριστή δεν υπάρχει τέτοιο πρόσωπο. Οι προγραμματιστές, που έγραψαν τον κώδικα, ενδέχεται να έχουν αποσυρθεί, οι κόμβοι είναι διάσπαρτοι σε όλο τον κόσμο και κανείς δεν παρέχει την υπηρεσία με την έννοια, που προϋποθέτει ο νομοθέτης. Το δεύτερο όριο αφορά τη διακυβέρνηση. Το άρθρο 20 στηρίζεται στην ύπαρξη διοικητικών οργάνων που εγκρίνουν, επιβλέπουν και ευθύνονται. Σε έναν αποκεντρωμένο αυτόνομο οργανισμό, όπου οι αποφάσεις λαμβάνονται με ψηφοφορίες κατόχων ψηφιακών κουπονιών ή εκτελούνται αυτόματα από τον κώδικα, το σχήμα αυτό δεν έχει προφανή αποδέκτη. Το τρίτο όριο είναι εδαφικό. Οι κανόνες δικαιοδοσίας του άρθρου 26 στηρίζονται στην εγκατάσταση

⁵³ ENISA (2023), Cybersecurity of AI and Standardisation, σελ. 6.

⁵⁴ Για τη διαχείριση των κινδύνων ασφάλειας των συστημάτων τεχνητής νοημοσύνης βλ. ENISA (2023), Cybersecurity of AI and Standardisation. Ebers, M., Navas, S. (επιμ.) (2020), Algorithms and Law, Cambridge: Cambridge University Press και Finck, M. (2019), Blockchain Regulation and Governance in Europe, Cambridge: Cambridge University Press.

⁵⁵ Ebers, M., Navas, S. (2020), ό.π., σελ. 55.

ή στην κύρια εγκατάσταση της οντότητας⁵⁶, ενώ ένα αποκεντρωμένο πρωτόκολλο δεν είναι εγκατεστημένο πουθενά και ταυτόχρονα λειτουργεί παντού. Τα όρια αυτά δεν σημαίνουν ότι η Οδηγία είναι άχρηστη στο πεδίο που εξετάζουμε. Σημαίνουν ότι η προστασία που παρέχει είναι περιμετρική⁵⁷. Όπως χαρακτηριστικά επισημαίνεται στη θεωρία, στα κατανεμημένα καθολικά «κατανεμημένη» είναι και η ίδια η ευθύνη: η διασπορά της λειτουργίας σε πλήθος κόμβων δεν εξαφανίζει τους νομικούς κινδύνους, αλλά τους κατανέμει σε πρόσωπα, που συχνά αγνοούν την έκθεσή τους, με αποτέλεσμα η εποπτεία και οι ζημιωθέντες να στρέφονται αναγκαστικά προς τους εντοπίσιμους και φερέγγυους κρίκους του συστήματος. Άλλωστε «ο κίνδυνος κατανεμημένης ευθύνης των κατανεμημένων καθολικών υποδηλώνει ότι η συγκεντρωμένη ιδιοκτησία είναι ο πιο πιθανός τρόπος νομικής δομής των κατανεμημένων καθολικών»⁵⁸. Καλύπτει τους κεντριοποιημένους κρίκους γύρω από το αποκεντρωμένο σύστημα, δηλαδή τους παρόχους υποδομών, τις πύλες πρόσβασης και τους διαχειριστές υπηρεσιών, όχι όμως τον πυρήνα του. Η διαπίστωση αυτή, την οποία επιβεβαιώνουν και οι εκθέσεις ωριμότητας του ENISA για τους ψηφιακούς τομείς⁵⁹, θα αποτελέσει βασικό δεδομένο για τις προτάσεις του Κεφαλαίου 6.

4.6. Η σχέση με τα παράλληλα ευρωπαϊκά καθεστώτα

Η NIS2 αποτελεί τον κορμό, όχι όμως το σύνολο του ρυθμιστικού πλέγματος. Γύρω της λειτουργούν τέσσερα τουλάχιστον παράλληλα καθεστώτα με άμεση σημασία για το αντικείμενο της εργασίας. Το πρώτο είναι ο AI Act. Ο Κανονισμός ακολουθεί προσέγγιση βασισμένη στον κίνδυνο και επιβάλλει στα συστήματα υψηλού κινδύνου απαιτήσεις ακρίβειας, στιβαρότητας, δηλαδή ανθεκτικότητας σε σφάλματα και επιθέσεις, και κυβερνοασφάλειας, καθώς και υποχρέωση ανθρώπινης εποπτείας. Οι απαιτήσεις αυτές δεν καταλαμβάνουν κάθε αυτόνομο πράκτορα, καλύπτουν όμως τις περιπτώσεις όπου ο πράκτορας εμπίπτει στους καταλόγους υψηλού κινδύνου και δημιουργούν ένα πρότυπο επιμέλειας με ευρύτερη ακτινοβολία. Το δεύτερο καθεστώς είναι ο Cyber Resilience Act, ο οποίος καλύπτει τα προϊόντα με ψηφιακά στοιχεία και επιβάλλει απαιτήσεις ασφάλειας σε όλο τον κύκλο ζωής του λογισμικού, από τον σχεδιασμό έως τις ενημερώσεις. Το λογισμικό

⁵⁶Άρθρα 26 και 27 της Οδηγίας (ΕΕ) 2022/2555 για τη δικαιοδοσία και την εδαφικότητα, καθώς και για το μητρώο οντοτήτων.

⁵⁷ Για τον καταλογισμό ευθυνών στα κατανεμημένα συστήματα βλ. Zetzsche, D., Buckley, R., Arner, D. (2018), 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain', University of Illinois Law Review, σσ. 1361 επ. Βλ. και Finck, M. (2019), ό.π.

⁵⁸ Zetzsche, D., Buckley, R., Arner, D. (2018), ό.π., σελ. 42.

⁵⁹ENISA (2025), NIS360, έκθεση αξιολόγησης της ωριμότητας και της κρισιμότητας των τομέων υψηλής κρισιμότητας της Οδηγίας NIS2.

ενός πράκτορα ή μιας εφαρμογής έξυπνων συμβάσεων που διατίθεται στην αγορά μπορεί να εμπίπτει στο πεδίο του, με αποτέλεσμα να καλύπτεται έμμεσα και ο κατασκευαστής, που διαφεύγει από τη NIS2. Το τρίτο καθεστώς είναι το ζεύγος DORA και MiCA για τον χρηματοοικονομικό τομέα, το οποίο εξετάστηκε παραπάνω. Το τέταρτο είναι το άρθρο 36 του Data Act, που θεσπίζει ουσιώδεις απαιτήσεις για τις έξυπνες συμβάσεις στις συμφωνίες κοινοχρησίας δεδομένων. Η διάταξη απαιτεί, μεταξύ άλλων, προστασία από σφάλματα και χειραγώγηση, αυστηρούς μηχανισμούς ελέγχου πρόσβασης και δυνατότητα ασφαλούς τερματισμού και διακοπής της εκτέλεσης. Είναι η πρώτη φορά που τεχνικά χαρακτηριστικά των έξυπνων συμβάσεων μετατρέπονται ευθέως σε δεσμευτικές νομικές απαιτήσεις⁶⁰⁶¹. Η συνολική εικόνα είναι εκείνη ενός πυκνού αλλά αποσπασματικού πλέγματος. Κάθε νομοθέτημα καλύπτει ένα τμήμα του φαινομένου από τη δική του σκοπιά, δηλαδή την οντότητα, το σύστημα, το προϊόν ή τη συγκεκριμένη χρήση. Κανένα όμως δεν συλλαμβάνει το φαινόμενο στο σύνολό του, δηλαδή τον αυτόνομο πράκτορα, που συναλλάσσεται πάνω σε αποκεντρωμένη υποδομή. Για το λόγο αυτό, το ζήτημα της ευθύνης, στο οποίο στρέφεται το επόμενο κεφάλαιο, αποκτά ιδιαίτερη βαρύτητα.

⁶⁰ Άρθρο 36 παρ. 1 του Κανονισμού (ΕΕ) 2023/2854. Για τη σύνδεση των τεχνικών εγγυήσεων με την προστασία των συναλλασσομένων βλ. European Law Institute (2022), ό.π.

⁶¹ Άρθρο 36 του Κανονισμού (ΕΕ) 2023/2854 (Data Act), ό.π.

5. Νομική ευθύνη και λογοδοσία των αυτόνομων ψηφιακών οντοτήτων

Το προηγούμενο κεφάλαιο έδειξε ότι το ρυθμιστικό δίκαιο της κυβερνοασφάλειας καλύπτει το φαινόμενο περιμετρικά. Το παρόν κεφάλαιο στρέφεται στο ιδιωτικό δίκαιο και εξετάζει το ερώτημα, που βρίσκεται στον πυρήνα της εργασίας. Ποιος ευθύνεται όταν ένας αυτόνομος πράκτορας συνάπτει ή εκτελεί μια έξυπνη σύμβαση και από τη λειτουργία αυτή προκύπτει ζημία; Η ανάλυση κινείται σε τρία επίπεδα, δηλαδή στη συμβατική ευθύνη, στην εξωσυμβατική ευθύνη και στα ειδικά ζητήματα των αποκεντρωμένων σχημάτων. Σε κάθε επίπεδο αξιολογείται η τυπολογία των βαθμίδων αυτονομίας ως εργαλείο διάγνωσης των σημείων στα οποία τα υφιστάμενα εργαλεία επαρκούν και εκείνων στα οποία αστοχούν.

5.1. Το πρόβλημα του καταλογισμού

Το ιδιωτικό δίκαιο είναι οικοδομημένο πάνω στην έννοια του προσώπου. Μόνο τα φυσικά και τα νομικά πρόσωπα έχουν ικανότητα δικαίου, μόνο αυτά δηλώνουν βούληση και μόνο σε αυτά καταλογίζονται πράξεις και παραλείψεις⁶². Κατά τον Ιγγλεζάκη «ο μηχανισμός με τον οποίο λειτουργεί μια έξυπνη σύμβαση επιτρέπει στους συμβαλλομένους όχι να συγκατατεθούν στην παραγωγή της δήλωσης βουλήσεως από τη σύμβαση ούτε υφίσταται μια σχέση αντιπροσώπευσης μεταξύ συμβαλλόμενου και του λογισμικού της έξυπνης σύμβασης που παράγει δηλώσεις βουλήσεως βάσει προδιαγεγραμμένων εντολών, αλλά η δήλωση βούλησης έχει συντελεσθεί με τη σύναψη της έξυπνης σύμβασης απλώς τα αποτελέσματα παράγονται σε μεταγενέστερο χρόνο»⁶³. Ο αυτόνομος πράκτορας δεν είναι πρόσωπο. Είναι λογισμικό, δηλαδή, από τη σκοπιά του δικαίου, ένα εργαλείο. Η κλασική απάντηση του δικαίου στα εργαλεία είναι απλή. Ό,τι κάνει το εργαλείο καταλογίζεται σε εκείνον, που το χρησιμοποιεί⁶⁴. Η απάντηση αυτή λειτουργεί άψογα όσο το εργαλείο συμπεριφέρεται προβλέψιμα. Αρχίζει όμως να δοκιμάζεται όταν το «εργαλείο» επιλέγει το ίδιο τις ενέργειές του με τρόπο, που ούτε ο κατασκευαστής, ούτε ο χρήστης μπορούν να προβλέψουν στη συγκεκριμένη περίπτωση. Εδώ ακριβώς βρίσκεται η ουσία του προβλήματος. Δεν πρόκειται για κενό δικαίου με την τυπική έννοια, αφού κάποιος κανόνας πάντοτε θα βρεθεί να εφαρμοστεί. Το ουσιαστικό πρόβλημα είναι άλλο. Οι κανόνες του δικαίου των δικαιопραξιών γράφτηκαν με την παραδοχή ότι πίσω από κάθε δήλωση υπάρχει ανθρώπινη επιλογή με προβλέψιμο περιεχόμενο. Όταν την επιλογή αυτή την κάνει πλέον

⁶² Άρθρα 34 και 62 ΑΚ.

⁶³ Ιγγλεζάκης, Ι. (2022), ό.π., σελ. 240-241.

⁶⁴ Για την εργαλειακή αντιμετώπιση των τεχνητών πρακτόρων βλ. Chopra, S., White, L.F. (2011), ό.π., σελ. 5 επ. Βλ. και Turner, J. (2019), Robot Rules: Regulating Artificial Intelligence, Cham: Palgrave Macmillan.

ένα σύστημα προορισμένο να παίρνει αποφάσεις με βάση τις πιθανότητες ορθής εκτέλεσης της σύμβασης, οι κανόνες εξακολουθούν μεν να εφαρμόζονται, η δικαιολογητική τους βάση όμως παύει να ανταποκρίνεται στην πραγματικότητα που ρυθμίζουν.

5.2. Η συμβατική διάσταση

5.2.1. Κατάρτιση της σύμβασης και δήλωση βούλησης

Στις χαμηλές βαθμίδες αυτονομίας η κατάρτιση σύμβασης μέσω αυτοματοποιημένων συστημάτων δεν παρουσιάζει ιδιαίτερο πρόβλημα. Η κρατούσα προσέγγιση δέχεται ότι η δήλωση, που παράγει ένα αυτοματοποιημένο σύστημα καταλογίζεται στον χρήστη του ως δική του δήλωση, διότι αποτελεί εκδήλωση μιας βούλησης, που έχει διαμορφωθεί εκ των προτέρων και έχει αποτυπωθεί στον προγραμματισμό. Το ζήτημα εντάσσεται στην ευρύτερη προβληματική της ηλεκτρονικής δήλωσης βούλησης, την οποία η ελληνική θεωρία επεξεργάστηκε ήδη από την εποχή των πρώτων ηλεκτρονικών συναλλαγών: κρίσιμο είναι αν και υπό ποιες προϋποθέσεις η δήλωση, που σχηματίζεται και διαβιβάζεται με ηλεκτρονικά μέσα, μπορεί να αποδοθεί στο πρόσωπο ως γνήσια εκδήλωση της βούλησής του, ζήτημα, που οξύνεται, όσο το σύστημα μετατρέπεται από απλό δίαυλο διαβίβασης της δήλωσης σε μηχανισμό διαμόρφωσης του περιεχομένου της. Το σχήμα αυτό προϋποθέτει πάντως ότι το περιεχόμενο της δήλωσης παραμένει προβλέψιμο για τον χρήστη⁶⁵, αφού «για να καταρτιστεί μια σύμβαση απαιτείται σύμπτωση των δηλώσεων βουλήσεως, με τις οποίες οι συμβαλλόμενοι συμφωνούν ως προς το επιδιωκόμενο έννομο αποτέλεσμα και τούτο έχει ως συνέπεια ότι τα μέρη δεσμεύονται αμοιβαία από τη ρύθμιση της επιλεχθείσας έννομης σχέσης»⁶⁶. Όποιος ενεργοποιεί μια έξυπνη σύμβαση της Βαθμίδας 0 ή εγκρίνει τη συναλλαγή, που του προτείνει ένα σύστημα της Βαθμίδας 1, δηλώνει βούληση με τον ίδιο τρόπο, που δηλώνει βούληση όποιος χρησιμοποιεί έναν αυτόματο πωλητή. Το σχήμα αυτό αρχίζει να πιέζεται στη Βαθμίδα 2 και δοκιμάζεται σοβαρά στη Βαθμίδα 3. Όταν ο εντολέας έχει ορίσει μόνο έναν γενικό σκοπό και ο πράκτορας επιλέγει μόνος του τον αντισυμβαλλόμενο, το αντικείμενο και το τίμημα, η «βούληση» του εντολέα καλύπτει το αποτέλεσμα μόνο με έναν πολύ αφηρημένο τρόπο. Η θεωρία απαντά εδώ με την κατασκευή μιας γενικής ή πλαισίου βούλησης. Ο εντολέας, δηλαδή, αποδέχεται εκ των προτέρων ως δικές του όλες τις δηλώσεις, που θα παραγάγει ο πράκτορας μέσα στα όρια, που του έχει θέσει. Η κατασκευή αυτή είναι λειτουργική και

⁶⁵ Για την ηλεκτρονική δήλωση βούλησης βλ. Χριστοδούλου, Κ. (2001), Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία, Αθήνα: Αντ. Ν. Σάκκουλας. Βλ. και Γεωργιάδη, Α.Σ. (2019), ό.π.

⁶⁶ Ιγγλεζάκης, Ι. (2022), ό.π., σελ. 239.

προστατεύει τη ασφάλεια των συναλλαγών. Έχει όμως ένα τίμημα. Μετατρέπει τον καταλογισμό σε ανάληψη κινδύνου. Ο εντολέας δεν ευθύνεται πλέον επειδή θέλησε τη συγκεκριμένη δικαιοπραξία, αλλά επειδή θέλησε να αναθέσει τις υποθέσεις του σε ένα σύστημα με απρόβλεπτη συμπεριφορά⁶⁷.

5.2.2. Αντιπροσώπηση και συγγενή εργαλεία

Η φυσική αναλογία, που έρχεται στον νου, είναι η αντιπροσώπηση με το δεδομένο ότι «ορθά απαλείφθηκε από τον Ν. 4961/2022, μετά την κριτική που δέχτηκε κατά τη δημόσια διαβούλευση, η αδικαιολόγητη και άκρως προβληματική πρόβλεψη περί υποχρέωσης αυτοπρόσωπης κατάρτισης του άρθρου 49 παρ.7 του νομοσχεδίου»⁶⁸. Ο πράκτορας μοιάζει να ενεργεί «στο όνομα και για λογαριασμό» του εντολέα του, όπως ο αντιπρόσωπος των άρθρων 211 επ. ΑΚ. Η αναλογία όμως σκοντάφτει σε ένα εννοιολογικό εμπόδιο. Αντιπρόσωπος μπορεί να είναι μόνο πρόσωπο, διότι η αντιπροσώπηση προϋποθέτει ότι ο αντιπρόσωπος προβαίνει ο ίδιος σε δήλωση βούλησης⁶⁹ για λογαριασμό του αντιπροσωπευόμενου. Ο πράκτορας δεν έχει βούληση με τη νομική έννοια και επομένως δεν μπορεί να είναι αντιπρόσωπος. Η ευθεία εφαρμογή των διατάξεων αποκλείεται. Το ερώτημα είναι αν χωρεί αναλογική εφαρμογή ορισμένων λύσεών τους. Η σκέψη αυτή έχει πρακτική αξία κυρίως στο ζήτημα της υπέρβασης των ορίων. Όταν ο πράκτορας της Βαθμίδας 2 ενεργεί έξω από τα όρια, που του έχουν τεθεί, η κατάσταση θυμίζει τον ψευδοαντιπρόσωπο. Η αναλογική αξιοποίηση της λύσης του νόμου θα σήμαινε ότι ο εντολέας δεν δεσμεύεται από τη συναλλαγή που υπερβαίνει τα όρια, εκτός αν την εγκρίνει εκ των υστέρων, ενώ ο καλόπιστος τρίτος προστατεύεται όταν δικαιολογημένα εμπιστεύθηκε την ύπαρξη εξουσίας. Το πρόβλημα είναι ότι στα αποκεντρωμένα περιβάλλοντα ο τρίτος συχνά δεν γνωρίζει καν ότι συναλλάσσεται με πράκτορα και δεν έχει κανέναν τρόπο να ελέγξει τα όρια της «εξουσίας» του. Για το λόγο αυτό, όπως θα προταθεί στο Κεφάλαιο 6, η υποχρέωση γνωστοποίησης της ιδιότητας του πράκτορα και των ορίων του αποτελεί αναγκαίο συμπλήρωμα κάθε λύσης⁷⁰.

⁶⁷ Για τις συναλλαγές που καταρτίζονται από αυτόνομα συστήματα βλ. Bayern, S. (2015), 'The Implications of Modern Business Entity Law for the Regulation of Autonomous Systems', *Stanford Technology Law Review*, 19, σσ. 93 επ. και Fairfield, J. (2014), 'Smart Contracts, Bitcoin Bots, and Consumer Protection', *Washington and Lee Law Review Online*, 71, σσ. 35 επ.

⁶⁸ Λ. Κανέλλος, *Smart Contracts. Νομικές προκλήσεις, σύγχρονες συναλλακτικές πρακτικές και επιχειρηματικές προοπτικές*, [Νομική Βιβλιοθήκη](#), Αθήνα, 2022, σελ. 151.

⁶⁹ Άρθρα 211 επ. ΑΚ. Η άμεση αντιπροσώπηση προϋποθέτει δήλωση βούλησης από πρόσωπο, φυσικό ή νομικό, και για τον λόγο αυτό η ευθεία εφαρμογή της στους τεχνητούς πράκτορες προσκρούει σε εννοιολογικό εμπόδιο.

⁷⁰ Chopra, S., White, L.F. (2011), ό.π. Βλ. και Ebers, M., Navas, S. (2020), ό.π.

5.2.3. Ελαττώματα βούλησης, ερμηνεία και εκπλήρωση

Ανάλογες εντάσεις εμφανίζονται και στα υπόλοιπα κεφάλαια του δικαίου των δικαιιοπραξιών. Στο πεδίο των ελαττωμάτων της βούλησης, η πλάνη προϋποθέτει ασυμφωνία δήλωσης και βούλησης κατά τον χρόνο της δήλωσης. Όταν όμως η «δήλωση» παράγεται από τον πράκτορα, η πλάνη τίνος εξετάζεται; Η λογικά συνεπής απάντηση είναι ότι κρίσιμη παραμένει η σφαίρα του εντολέα⁷¹. Κατά άλλη άποψη «δεν είναι αυτονόητο ότι δεν μπορούν να προκύψουν προβλήματα κατά την εκτέλεση έξυπνων συμβάσεων, αφού μπορεί να υπάρχει σφάλμα στον κώδικα του προγράμματος ή κενό ασφαλείας. Σε τέτοια περίπτωση θα τεθεί ζήτημα εσφαλμένης λειτουργίας του λογισμικού και ευθύνης του κατασκευαστή του λογισμικού»⁷². Το σφάλμα του πράκτορα, είτε οφείλεται σε ελαττωματικά δεδομένα είτε σε αστοχία του μοντέλου, δεν είναι πλάνη του δηλούντος αλλά κίνδυνος της λειτουργίας του συστήματος, τον οποίο κατά κανόνα φέρει εκείνος που το χρησιμοποιεί. Στο πεδίο της εκπλήρωσης, χρήσιμο εργαλείο προσφέρει η έννοια του βοηθού εκπλήρωσης. Όταν ο οφειλέτης χρησιμοποιεί έναν πράκτορα για να εκπληρώσει ενοχή του, είναι εύλογο να ευθύνεται για τις αστοχίες του συστήματος, όπως θα ευθυνόταν για το πταίσμα ενός προσώπου, που θα χρησιμοποιούσε για τον ίδιο σκοπό, κατά την αξιολογική λογική του άρθρου 334 ΑΚ⁷³. Η αναλογία δεν είναι δογματικά καθαρή, αφού το λογισμικό δεν αποτελεί υποκείμενο στο οποίο μπορεί να καταλογιστεί ευθύνη. Οδηγεί όμως σε ένα δίκαιο αποτέλεσμα. Όποιος επεκτείνει τη δραστηριότητά του με τεχνολογικά μέσα δεν πρέπει να βρίσκεται σε καλύτερη θέση από εκείνον που την επεκτείνει με ανθρώπινο προσωπικό⁷⁴, υπό την έννοια ότι όπως ευθύνεται εκείνος για τα πταίσματα του αντιπροσώπου του με τον ίδιο τρόπο θα πρέπει να ευθύνεται ο ίδιος για τις αστοχίες του πράκτορα που χρησιμοποιεί. Άλλωστε «η ζημία που προκαλείται ακόμη και από πλήρως αυτόνομες τεχνολογίες μπορεί γενικά να αναχθεί σε κινδύνους που αποδίδονται σε φυσικά πρόσωπα ή σε υπάρχουσες κατηγορίες νομικών προσώπων και, όπου αυτό δεν ισχύει, οι νέοι νόμοι που απευθύνονται σε άτομα αποτελούν καλύτερη απάντηση από τη δημιουργία μιας νέας κατηγορίας νομικών προσώπων»⁷⁵.

⁷¹ Για τα ελαττώματα της βούλησης στις ηλεκτρονικές δηλώσεις βλ. Χριστοδούλου, Κ. (2001), ό.π.

⁷² Γγγλεζάκης, Ι. (2022), ό.π., σελ. 243.

⁷³ Άρθρο 334 ΑΚ για την ευθύνη από πταίσμα του βοηθού εκπλήρωσης και άρθρο 922 ΑΚ για την ευθύνη του προστήσαντος.

⁷⁴ Για την αξιολογική βάση της ευθύνης για τους βοηθούς βλ. Γεωργιάδη, Α.Σ. (2015), Ενοχικό Δίκαιο, Γενικό Μέρος, 2η έκδοση, Αθήνα: Π.Ν. Σάκκουλας. Expert Group on Liability and New Technologies (New Technologies Formation) (2019), ό.π.

⁷⁵ Expert Group on Liability and New Technologies (New Technologies Formation) (2019), ό.π., σελ. 38.

5.3. Η εξωσυμβατική διάσταση

5.3.1. Η αδικοπρακτική ευθύνη και τα όριά της

Όταν από τη λειτουργία του πράκτορα ζημιώνεται τρίτος, που δεν συνδέεται συμβατικά με τον εντολέα, το ενδιαφέρον μετατοπίζεται στην αδικοπρακτική ευθύνη του άρθρου 914 ΑΚ. Εδώ οι δυσκολίες είναι εντονότερες. Η ευθύνη προϋποθέτει παράνομη και υπαίτια συμπεριφορά, καθώς και αιτιώδη σύνδεσμο με τη ζημία. Στις υψηλές βαθμίδες αυτονομίας και τα τρία στοιχεία θολώνουν. Ποια ακριβώς συμπεριφορά του εντολέα ή του κατασκευαστή είναι παράνομη όταν ο πράκτορας σχεδιάστηκε με επιμέλεια και παρόλα αυτά προκάλεσε ζημία; Πώς θεμελιώνεται υπαιτιότητα για ένα αποτέλεσμα που εξ ορισμού δεν ήταν προβλέψιμο στη συγκεκριμένη του μορφή; Και πώς αποδεικνύει ο ζημιωθείς την αιτιώδη διαδρομή μέσα σε ένα αδιαφανές σύστημα; Η Ομάδα Εμπειρογνομόνων της Επιτροπής είχε εντοπίσει με ακρίβεια τα κενά αυτά και είχε προτείνει, μεταξύ άλλων, αντικειμενική ευθύνη του φορέα εκμετάλλευσης για τις τεχνολογίες αυξημένου κινδύνου και ελαφρύνσεις στο βάρος απόδειξης⁷⁶. Η ευθύνη του προστήσαντος κατά το άρθρο 922 ΑΚ προσφέρει μια χρήσιμη αξιολογική αναλογία, αφού καθιερώνει ευθύνη για ζημίες που προκαλεί ο βοηθός, τον οποίο κάποιος χρησιμοποιεί προς το συμφέρον του. Προσक्रούει όμως στο ίδιο εμπόδιο με την αντιπροσώπευση, δηλαδή στην απαίτηση πταίσματος του προστηθέντος, το οποίο το λογισμικό δεν μπορεί να έχει. Η συζήτηση αυτή απασχολεί έντονα και τη θεωρία. Υποστηρίζεται ότι, όσο αυξάνεται η αυτονομία των συστημάτων, το πταίσμα ως θεμέλιο της ευθύνης χάνει τη λειτουργία του, διότι η ζημία δεν ανάγεται πλέον σε συγκεκριμένη ανθρώπινη αμέλεια αλλά στη συνολική απόφαση να τεθεί σε λειτουργία ένα μη πλήρως προβλέψιμο σύστημα. Για το λόγο αυτό προτείνεται η μετατόπιση προς την ευθύνη από διακινδύνευση, με παράλληλες δικονομικές ελαφρύνσεις για τον ζημιωθέντα⁷⁷.

5.3.2. Η νέα Οδηγία για την ευθύνη λόγω ελαττωματικών προϊόντων

Το σημαντικότερο βήμα του ευρωπαϊού νομοθέτη στο πεδίο αυτό είναι η Οδηγία (ΕΕ) 2024/2853, η οποία αντικαθιστά το καθεστώς του 1985. Οι καινοτομίες της απαντούν σχεδόν σημείο προς σημείο στις δυσκολίες που περιγράφηκαν. Το λογισμικό και επομένως και ο αυτόνομος πράκτορας και ο κώδικας μιας έξυπνης σύμβασης, εντάσσεται ρητά στην έννοια του προϊόντος. Η ελαττωματικότητα κρίνεται με βάση την ασφάλεια, που δικαιούται να αναμένει το κοινό, στην οποία συνυπολογίζονται πλέον και οι απαιτήσεις

⁷⁶Expert Group on Liability and New Technologies (New Technologies Formation) (2019), ό.π.

⁷⁷ Βλ. Wagner, G. (2019), ‘Robot, Inc.: Personhood for Autonomous Systems?’, Fordham Law Review, 88, σσ. 591 επ. Βλ. επίσης Hacker, P. (2023), ‘The European AI Liability Directives’, Computer Law and Security Review, 51 και Expert Group on Liability and New Technologies (New Technologies Formation) (2019), ό.π.

κυβερνοασφάλειας, καθώς και η ικανότητα του προϊόντος να συνεχίζει να μαθαίνει μετά τη διάθεσή του. Ο παραγωγός μπορεί να ευθύνεται και για ελαττώματα, που εμφανίζονται μετά τη διάθεση, εφόσον διατηρεί τον έλεγχο του προϊόντος μέσω ενημερώσεων. Τέλος, ο ζημιωθείς ενισχύεται δικονομικά με υποχρεώσεις αποκάλυψης αποδεικτικών στοιχείων και με μαχητά τεκμήρια ελαττωματικότητας και αιτιώδους συνδέσμου, ιδίως όταν η απόδειξη είναι υπερβολικά δυσχερής λόγω τεχνικής πολυπλοκότητας⁷⁸. Για την πλευρά της υπαίτιας ευθύνης, αντίθετα, η ειδική ευρωπαϊκή πρωτοβουλία ατόνησε. Η πρόταση Οδηγίας για την ευθύνη από τεχνητή νοημοσύνη αποσύρθηκε από την Επιτροπή το 2025⁷⁹. Το αποτέλεσμα είναι ένα ασύμμετρο τοπίο. Η ευθύνη του παραγωγού εκσυγχρονίστηκε ριζικά, ενώ η ευθύνη του χρήστη και του φορέα εκμετάλλευσης παραμένει στα εθνικά δίκαια, με τις αδυναμίες που περιγράφηκαν.

5.4. Η συζήτηση για την «ηλεκτρονική προσωπικότητα»

Απέναντι στις δυσκολίες του καταλογισμού, μια ριζική σκέψη επανέρχεται περιοδικά στη συζήτηση. Αν το πρόβλημα είναι ότι ο πράκτορας δεν είναι πρόσωπο, γιατί να μην τον κάνουμε πρόσωπο; Το Ευρωπαϊκό Κοινοβούλιο είχε ζητήσει από την Επιτροπή, ήδη το 2017, να εξετάσει τη δημιουργία ενός ειδικού νομικού καθεστώτος «ηλεκτρονικού προσώπου» για τα πιο εξελιγμένα αυτόνομα συστήματα⁸⁰. Η πρόταση δέχθηκε έντονη κριτική από μεγάλη μερίδα της επιστημονικής κοινότητας και δεν προχώρησε⁸¹. Η κριτική αυτή είναι, κατά την άποψη, που υιοθετεί η παρούσα εργασία, πειστική για τρεις λόγους⁸². Πρώτον, η νομική προσωπικότητα δεν λύνει το πρόβλημα της ευθύνης αλλά το μεταθέτει. Ένα «ηλεκτρονικό πρόσωπο» χωρίς δική του περιουσία δεν προσφέρει στον ζημιωθέντα

⁷⁸Βλ. άρθρο 4 σημ. 1 της Οδηγίας (ΕΕ) 2024/2853 για την ένταξη του λογισμικού στην έννοια του προϊόντος, άρθρο 7 για την ελαττωματικότητα, στην οποία συνεκτιμώνται και οι απαιτήσεις κυβερνοασφάλειας, καθώς και άρθρα 9 και 10 για την αποκάλυψη αποδεικτικών στοιχείων και τα τεκμήρια που ελαφρύνουν το βάρος απόδειξης του ζημιωθέντος.

⁷⁹Η πρόταση Οδηγίας για την προσαρμογή των κανόνων εξωσυμβατικής αστικής ευθύνης στην τεχνητή νοημοσύνη (AI Liability Directive, COM(2022) 496) περιλήφθηκε στις προς απόσυρση πρωτοβουλίες με το Πρόγραμμα Εργασίας της Ευρωπαϊκής Επιτροπής για το 2025 (Φεβρουάριος 2025), λόγω απουσίας προβλέψιμης συμφωνίας των συννομοθετών.

⁸⁰Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 16ης Φεβρουαρίου 2017 με συστάσεις προς την Επιτροπή σχετικά με ρυθμίσεις αστικού δικαίου στον τομέα της ρομποτικής (2015/2103(INL)), όπου διατυπώθηκε η σκέψη για ένα ειδικό νομικό καθεστώς «ηλεκτρονικού προσώπου» για τα πιο εξελιγμένα αυτόνομα ρομπότ.

⁸¹Βλ. την ανοικτή επιστολή εμπειρογνομόνων της τεχνητής νοημοσύνης και της ρομποτικής προς την Ευρωπαϊκή Επιτροπή (Open Letter to the European Commission on Artificial Intelligence and Robotics, 2018), με την οποία απορρίφθηκε η ιδέα της ηλεκτρονικής προσωπικότητας τόσο για τεχνικούς όσο και για ηθικούς και νομικούς λόγους.

⁸² Βλ. ιδίως Open Letter to the European Commission on Artificial Intelligence and Robotics (2018), ό.π. και Wagner, G. (2019), ό.π. Βλ. και Turner, J. (2019), ό.π.

τίποτα, ενώ ένα ηλεκτρονικό πρόσωπο με περιουσία λειτουργεί απλώς ως ταμείο αποζημίωσης, το οποίο μπορεί να δημιουργηθεί και χωρίς προσωπικότητα, μέσω υποχρεωτικής ασφάλισης ή εγγυητικών κεφαλαίων⁸³. Δεύτερον, η προσωπικότητα δημιουργεί κίνδυνο ηθικής απαλλαγής των πραγματικών συντελεστών, δηλαδή του κατασκευαστή, του παρόχου και του εντολέα, οι οποίοι θα μπορούσαν να κρύβονται πίσω από την ευθύνη του «προσώπου» που δημιούργησαν. Η παρατήρηση ότι τα συστήματα αυτά ενεργούν συχνά και πέρα από τις οδηγίες του φορέα τους δεν αναιρεί το επιχείρημα, αντίθετα το ενισχύει. Ακριβώς επειδή η συμπεριφορά τους δεν είναι πλήρως ελέγξιμη, η ευθύνη πρέπει να παραμένει σε εκείνον, που επέλεξε να θέσει σε λειτουργία ένα τέτοιο σύστημα και όχι να μεταφέρεται σε μια νομική κατασκευή χωρίς πραγματικό υπόστρωμα. Με άλλα λόγια, η μη πλήρης ελεγχσιμότητα του συστήματος δεν συνιστά επιχείρημα υπέρ της αυτονομίας της ευθύνης του, αλλά ακριβώς τον λόγο, για τον οποίο ο καταλογισμός πρέπει να παραμένει στα πρόσωπα, που αποφασίζουν τον σχεδιασμό του και τη θέση του σε λειτουργία. Σε διαφορετική περίπτωση, η ηλεκτρονική προσωπικότητα θα λειτουργούσε ως ασπίδα περιορισμένης ευθύνης χωρίς τις εγγυήσεις κεφαλαίου, οργάνωσης και εποπτείας, που συνοδεύουν τα νομικά πρόσωπα του εταιρικού δικαίου. Άλλωστε «παραμένει, ωστόσο, ασαφές ποια χαρακτηριστικά αποτελούν απαραίτητες προϋποθέσεις για την αναγνώριση της προσωπικότητας και ποια όχι» στα αυτόνομα συστήματα⁸⁴. Τρίτον, το νομικό πρόσωπο του εταιρικού δικαίου λειτουργεί επειδή πίσω του υπάρχουν πάντοτε άνθρωποι, που αποφασίζουν και ελέγχονται. Στη Βαθμίδα 4 της τυπολογίας μας το χαρακτηριστικό αυτό ακριβώς λείπει. Η ορθή κατεύθυνση δεν είναι επομένως η απονομή προσωπικότητας στην οντότητα, αλλά η οργάνωση της ευθύνης των προσώπων, που βρίσκονται γύρω της, σε συνάρτηση με τη βαθμίδα αυτονομίας που επέλεξαν να επιτρέψουν.

5.5. Λογοδοσία στα αποκεντρωμένα σχήματα: το παράδειγμα των DAOs

Η δυσκολότερη περίπτωση είναι εκείνη όπου ούτε εντολέας υπάρχει ούτε αναγνωρίσιμος φορέας εκμετάλλευσης. Οι αποκεντρωμένοι αυτόνομοι οργανισμοί (DAOs) αποτελούν το χαρακτηριστικότερο παράδειγμα. Πρόκειται για σχήματα όπου η διακυβέρνηση ασκείται από τους κατόχους ψηφιακών κουπονιών μέσω ψηφοφοριών και η εκτέλεση των αποφάσεων γίνεται αυτόματα από έξυπνες συμβάσεις. Το ερώτημα της

⁸³ Την κατεύθυνση αυτή είχε υποδείξει ήδη το Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 16ης Φεβρουαρίου 2017, ό.π., με τις προτάσεις του για υποχρεωτική ασφάλιση και εγγυητικό ταμείο αποζημιώσεων.

⁸⁴ Βλ. Wagner, G. (2019), ό.π., σσ. 591 επ.

νομικής τους φύσης έχει απασχολήσει ήδη τα δικαστήρια. Στις Ηνωμένες Πολιτείες, ο Ooki DAO αντιμετωπίστηκε από το δικαστήριο ως ένωση προσώπων χωρίς νομική προσωπικότητα, με συνέπεια την έκθεση των μελών του σε ευθύνη⁸⁵, ενώ η Πολιτεία του Wyoming επέλεξε τον αντίθετο δρόμο και προσέφερε στους DAOs εταιρικό ένδυμα περιορισμένης ευθύνης⁸⁶. Η υπόθεση αξίζει σύντομη αναφορά. Η αμερικανική Επιτροπή Συναλλαγών Παραγώγων (CFTC) στράφηκε το 2022 κατά του Ooki DAO, υποστηρίζοντας ότι μέσω του πρωτοκόλλου προσφέρονταν παρανόμως προϊόντα μόχλευσης χωρίς άδεια και χωρίς διαδικασίες ταυτοποίησης των πελατών. Το δικαστήριο δέχθηκε ότι ο οργανισμός, μολονότι στερείται νομικής προσωπικότητας, μπορεί να εναχθεί ως ένωση προσώπων, έκρινε δε έγκυρη ακόμη και την επίδοση του δικογράφου μέσω του διαδικτυακού συστήματος συνομιλίας του πρωτοκόλλου. Επειδή κανείς δεν εμφανίστηκε να εκπροσωπήσει τον οργανισμό, εκδόθηκε το 2023 ερήμην απόφαση με χρηματική κύρωση και εντολή παύσης της λειτουργίας⁸⁷. Στο ελληνικό δίκαιο, το πλησιέστερο διαθέσιμο σχήμα είναι εκείνο της αστικής εταιρείας χωρίς νομική προσωπικότητα⁸⁸. Η κατάταξη αυτή έχει βαριές συνέπειες, αφού μπορεί να οδηγήσει σε προσωπική ευθύνη προσώπων, που απλώς κατείχαν κουπόνια διακυβέρνησης και ψήφισαν σε μία απόφαση. Το αποτέλεσμα είναι διπλά προβληματικό. Από τη μια πλευρά, οι καλόπιστοι συμμετέχοντες εκτίθενται σε δυσανάλογο κίνδυνο. Από την άλλη, ο ζημιωθείς δεν έχει στην πράξη κανέναν να στραφεί εναντίον του, αφού τα μέλη είναι ψευδώνυμα και διάσπαρτα σε όλο τον κόσμο. Η εμπειρία αυτή ενισχύει το συμπέρασμα ότι το πρόβλημα δεν λύνεται με τα εργαλεία του κοινού δικαίου, αλλά απαιτεί ρυθμιστική παρέμβαση, η οποία θα συνδέει τη δυνατότητα λειτουργίας τέτοιων σχημάτων με ελάχιστες προϋποθέσεις οργάνωσης και λογοδοσίας⁸⁹.

5.6. Ενδιάμεσο συμπέρασμα: η ευθύνη υπό το πρίσμα των βαθμίδων αυτονομίας

⁸⁵CFTC v. Ooki DAO, United States District Court, Northern District of California (2023), όπου ο αποκεντρωμένος αυτόνομος οργανισμός αντιμετωπίστηκε ως ένωση προσώπων χωρίς νομική προσωπικότητα (unincorporated association) και καταδικάστηκε ερήμην.

⁸⁶Βλ. τον νόμο της Πολιτείας του Wyoming των ΗΠΑ για τους αποκεντρωμένους αυτόνομους οργανισμούς (Wyoming Decentralized Autonomous Organization Supplement, 2021), ο οποίος επιτρέπει τη σύσταση DAO με τη μορφή εταιρείας περιορισμένης ευθύνης.

⁸⁷ CFTC v. Ooki DAO, ό.π. Για τη νομική φύση και τη διακυβέρνηση των DAOs βλ. Wright, A. (2021), 'The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges', Stanford Journal of Blockchain Law and Policy, 4.

⁸⁸Βλ. άρθρα 741 επ. ΑΚ για την αστική εταιρεία. Εφόσον μια ένωση προσώπων επιδιώκει κοινό σκοπό με κοινές συνεισφορές χωρίς να έχει τηρηθεί κάποιος εταιρικός τύπος, η κατάταξή της στο σχήμα της αστικής εταιρείας χωρίς νομική προσωπικότητα αποτελεί το πλησιέστερο διαθέσιμο εργαλείο του ελληνικού δικαίου.

⁸⁹ Zetzsche, D., Buckley, R., Arner, D. (2018), ό.π. Βλ. και Wright, A. (2021), ό.π. και Finck, M. (2019), ό.π.

Η ανάλυση του κεφαλαίου αυτού μπορεί να συνοψιστεί με τη βοήθεια της τυπολογίας του Κεφαλαίου 3. Στις Βαθμίδες 0 και 1 τα υφιστάμενα εργαλεία επαρκούν. Η δήλωση βούλησης καταλογίζεται ομαλά στον χρήστη και η ευθύνη ακολουθεί τους γενικούς κανόνες. Στις Βαθμίδες 2 και 3 τα εργαλεία λειτουργούν μόνο με τη βοήθεια κατασκευών, όπως η βούληση ως πλαίσιο, η αναλογία του ψευδοαντιπροσώπου και η αξιολογική επέκταση του βοηθού εκπλήρωσης. Οι κατασκευές αυτές οδηγούν σε ανεκτά αποτελέσματα, μετατρέπουν όμως σιωπηρά την ευθύνη από ευθύνη για πταίσμα σε ευθύνη από διακινδύνευση, χωρίς αυτό να έχει αποφασιστεί ρητά από τον νομοθέτη. Η νέα Οδηγία για τα ελαττωματικά προϊόντα καλύπτει ένα σημαντικό μέρος του κενού από την πλευρά του παραγωγού, αφήνει όμως ακάλυπτη την πλευρά του φορέα εκμετάλλευσης. Στη Βαθμίδα 4, τέλος, τα εργαλεία του ιδιωτικού δικαίου αστοχούν συνολικά, όπως δείχνει το παράδειγμα των DAOs. Η εικόνα αυτή θεμελιώνει το βασικό επιχείρημα του επόμενου κεφαλαίου. Αφού τόσο το ρυθμιστικό δίκαιο όσο και το δίκαιο της ευθύνης κλιμακώνουν de facto την αυστηρότητά τους ανάλογα με την αυτονομία του συστήματος, είναι προτιμότερο η κλιμάκωση αυτή να οργανωθεί ρητά, μέσα από ένα συνεκτικό μοντέλο συμμόρφωσης.

6. Προς ένα μοντέλο νομικής και ρυθμιστικής συμμόρφωσης

Τα προηγούμενα κεφάλαια κατέληξαν σε δύο βασικές διαπιστώσεις. Η πρώτη είναι ότι το ρυθμιστικό δίκαιο της κυβερνοασφάλειας καλύπτει τα οικοσυστήματα των έξυπνων συμβάσεων και των αυτόνομων πρακτόρων περιμετρικά και αποσπασματικά. Η δεύτερη είναι ότι το δίκαιο της ευθύνης λειτουργεί ικανοποιητικά στις χαμηλές βαθμίδες αυτονομίας και αστοχεί στις υψηλές. Το παρόν κεφάλαιο επιχειρεί να μετατρέψει τις διαπιστώσεις αυτές σε μια θετική πρόταση. Προτείνεται ένα μοντέλο συμμόρφωσης με δύο σκέλη. Το πρώτο σκέλος αφορά το τι μπορεί να γίνει ήδη σήμερα, με το ισχύον δίκαιο, από τις οντότητες που αναπτύσσουν ή χρησιμοποιούν τέτοια συστήματα. Το δεύτερο σκέλος αφορά το τι θα έπρεπε να αλλάξει στο ρυθμιστικό πλαίσιο, δηλαδή τις προτάσεις *de lege ferenda*.

6.1. Οι αρχές του μοντέλου

Το προτεινόμενο μοντέλο στηρίζεται σε τέσσερις αρχές. Η πρώτη είναι η αναλογική προς τον κίνδυνο ρύθμιση. Η ένταση των υποχρεώσεων πρέπει να αυξάνεται όσο αυξάνεται η αυτονομία του συστήματος, διότι με την αυτονομία αυξάνεται και ο κίνδυνος. Η αρχή αυτή δεν είναι ξένη προς το ευρωπαϊκό δίκαιο. Αντίθετα, αποτελεί τη λογική τόσο του AI Act, που κλιμακώνει τις απαιτήσεις ανάλογα με τον κίνδυνο του συστήματος, όσο και του άρθρου 21 της NIS2, που απαιτεί μέτρα ανάλογα προς τους κινδύνους. Η δεύτερη αρχή είναι η διατήρηση της δυνατότητας ανθρώπινης παρέμβασης. Όσο ανεβαίνει η βαθμίδα αυτονομίας, τόσο πιο κρίσιμη γίνεται η ύπαρξη ενός αξιόπιστου μηχανισμού διακοπής. Ο ευρωπαίος νομοθέτης έχει ήδη υιοθετήσει τη λογική αυτή δύο φορές, με το άρθρο 36 του Data Act για τις έξυπνες συμβάσεις και με το άρθρο 14 του AI Act για την ανθρώπινη εποπτεία των συστημάτων υψηλού κινδύνου⁹⁰. Η τρίτη αρχή είναι η ανιχνευσιμότητα. Κάθε ενέργεια του συστήματος πρέπει να καταγράφεται με τρόπο, που να επιτρέπει τον εκ των υστέρων έλεγχο, τόσο για εποπτικούς σκοπούς όσο και για την απόδειξη σε περίπτωση διαφοράς⁹¹. Η τέταρτη αρχή είναι η δυνατότητα προσδιορισμού του υπευθύνου. Για κάθε σύστημα που συναλλάσσεται αυτόνομα πρέπει να υπάρχει ένα τουλάχιστον πρόσωπο με πραγματική εξουσία ελέγχου, το οποίο φέρει και την ευθύνη της λειτουργίας του.

⁹⁰ Άρθρο 14 του Κανονισμού (ΕΕ) 2024/1689 (AI Act) για την ανθρώπινη εποπτεία των συστημάτων υψηλού κινδύνου, η οποία πρέπει να επιτρέπει, μεταξύ άλλων, την παρέμβαση στη λειτουργία του συστήματος ή τη διακοπή του.

⁹¹ Βλ. άρθρο 12 του Κανονισμού (ΕΕ) 2024/1689 (AI Act) για την αυτόματη τήρηση αρχείων καταγραφής και άρθρο 15 του ίδιου Κανονισμού για τις απαιτήσεις ακρίβειας, στιβαρότητας και κυβερνοασφάλειας.

6.2. Συμμόρφωση εκ σχεδιασμού στον κύκλο ζωής του συστήματος

Το πρώτο σκέλος του μοντέλου απευθύνεται στις οντότητες και μεταφράζει τις υποχρεώσεις του ισχύοντος δικαίου σε συγκεκριμένα μέτρα ανά φάση του κύκλου ζωής. Στη φάση του σχεδιασμού και της ανάπτυξης, κρίσιμα μέτρα είναι ο ανεξάρτητος έλεγχος του κώδικα των έξυπνων συμβάσεων (audit), η τυπική επαλήθευση των κρίσιμων συναρτήσεων, ο σχεδιασμός των ορίων του πράκτορα ως τεχνικά δεσμευτικών περιορισμών και όχι ως απλών οδηγιών, καθώς και η δοκιμή του συστήματος σε συνθήκες εχθρικής χρήσης, με έμφαση στις επιθέσεις έγχυσης εντολών και στη χειραγώγηση των πηγών δεδομένων. Τα μέτρα αυτά αντιστοιχούν ευθέως στην υποχρέωση ασφάλειας κατά την απόκτηση, ανάπτυξη και συντήρηση των συστημάτων του άρθρου 21 της NIS2 και εξειδικεύονται από τα ευρωπαϊκά πρότυπα για την κυβερνοασφάλεια της τεχνητής νοημοσύνης⁹². Στη φάση της λειτουργίας, το κέντρο βάρους βρίσκεται στην εποπτεία. Απαιτούνται πλήρης καταγραφή των ενεργειών του πράκτορα, όρια συναλλαγών με αυτόματα αναστολή σε περίπτωση υπέρβασης, μηχανισμός άμεσης διακοπής, που δοκιμάζεται περιοδικά και σαφής εσωτερική κατανομή ρόλων, ώστε να είναι πάντοτε γνωστό ποιος άνθρωπος εποπτεύει ποιο σύστημα. Στη φάση, τέλος, του περιστατικού, η οντότητα πρέπει να διαθέτει σχέδιο απόκρισης προσαρμοσμένο στην ιδιαιτερότητα των αυτόνομων συστημάτων, το οποίο θα προβλέπει την άμεση απομόνωση του πράκτορα, τη διάσωση των αρχείων καταγραφής και την τήρηση των προθεσμιών αναφοράς του άρθρου 23 της NIS2. Με αυτόν τον τρόπο, η συμμόρφωση παύει να είναι ένα ζήτημα εγγράφων και γίνεται χαρακτηριστικό της ίδιας της αρχιτεκτονικής του συστήματος. Ένα παράδειγμα κάνει τη λογική αυτή απτή. Πριν τεθεί σε λειτουργία ένας πράκτορας διαχείρισης χαρτοφυλακίου κρυπτοστοιχείων, ο κώδικας των συμβάσεων με τις οποίες αλληλεπιδρά ελέγχεται από ανεξάρτητο ελεγκτή, ο ίδιος ο πράκτορας δοκιμάζεται συστηματικά απέναντι σε επιθέσεις έγχυσης εντολών, τίθενται ανώτατα ημερήσια όρια συναλλαγών που δεν μπορεί να υπερβεί τεχνικά, κάθε ενέργειά του καταγράφεται σε αρχείο που δεν μπορεί να τροποποιηθεί και ο μηχανισμός διακοπής δοκιμάζεται σε τακτά χρονικά διαστήματα⁹³.

6.3. Το κλιμακωτό μοντέλο ανά βαθμίδα αυτονομίας

⁹² ENISA (2023), ό.π. Βλ. και τα σχετικά ευρωπαϊκά πρότυπα για την κυβερνοασφάλεια των συστημάτων τεχνητής νοημοσύνης.

⁹³ Για τους κινδύνους ασφάλειας των εφαρμογών μεγάλων γλωσσικών μοντέλων βλ. OWASP Foundation (2023), OWASP Top 10 for Large Language Model Applications. Βλ. και ENISA (2023), ό.π.

Ο πυρήνας της πρότασης είναι η σύνδεση των μέτρων με την τυπολογία του Κεφαλαίου 3. Η αντιστοίχιση μπορεί να αποτυπωθεί ως εξής.

Στη Βαθμίδα 0 αρκούν τα κλασικά μέτρα ασφάλειας λογισμικού, δηλαδή ο έλεγχος του κώδικα, η ασφαλής ανάπτυξη και η διαχείριση των ευπαθειών. Ο κίνδυνος είναι ο κίνδυνος του σφάλματος, όχι της αυτονομίας.

Στη Βαθμίδα 1 προστίθενται απαιτήσεις διαφάνειας προς τον χρήστη. Εκείνος που εγκρίνει τη συναλλαγή πρέπει να γνωρίζει ότι η πρόταση προέρχεται από σύστημα τεχνητής νοημοσύνης και ποια είναι τα βασικά όρια αξιοπιστίας του.

Στη Βαθμίδα 2 το μοντέλο απαιτεί τεχνικά δεσμευτικά όρια, πλήρη καταγραφή, δοκιμασμένο μηχανισμό διακοπής και ορισμένο φυσικό πρόσωπο ως επόπτη. Η υπέρβαση των ορίων πρέπει να οδηγεί σε αυτόματη αναστολή της λειτουργίας και όχι απλώς σε ειδοποίηση.

Στη Βαθμίδα 3 προστίθενται η υποχρέωση προηγούμενης εκτίμησης επιπτώσεων πριν από τη θέση σε λειτουργία, η περιοδική επαναξιολόγηση του συστήματος όσο αυτό συνεχίζει να προσαρμόζεται, η γνωστοποίηση της ιδιότητας του πράκτορα στους αντισυμβαλλομένους και η οικονομική εξασφάλιση της ευθύνης, ιδίως μέσω ασφάλισης. Στη βαθμίδα αυτή είναι εύλογο να συζητηθεί και η μετάβαση σε αντικειμενική ευθύνη του φορέα εκμετάλλευσης, όπως είχε προτείνει η Ομάδα Εμπειρογνομόνων για τις τεχνολογίες αυξημένου κινδύνου⁹⁴.

Στη Βαθμίδα 4 το μοντέλο καταλήγει σε μια αυστηρή θέση. Η λειτουργία πλήρως αυτόνομων συστημάτων χωρίς κανένα πρόσωπο με εξουσία ελέγχου και χωρίς μηχανισμό διακοπής δεν πρέπει να αντιμετωπίζεται ως αποδεκτή κατάσταση προς ρύθμιση, αλλά ως κατάσταση προς αποτροπή. Η έννομη τάξη δεν μπορεί να ανεχθεί κέντρα λήψης αποφάσεων με έννομες συνέπειες που δεν λογοδοτούν σε κανέναν. Πρακτικά αυτό σημαίνει ότι η πρόσβαση των συστημάτων αυτών στις ρυθμιζόμενες πύλες, δηλαδή στους παρόχους υποδομών, στις πλατφόρμες και στους παρόχους υπηρεσιών κρυπτοστοιχείων, πρέπει να προϋποθέτει την απόδειξη ότι το σύστημα πληροί τα χαρακτηριστικά κατώτερης βαθμίδας.

6.4. Διακυβέρνηση, ταυτότητα και γνωστοποίηση των πρακτόρων

Ένα κρίσιμο συμπλήρωμα του κλιμακωτού μοντέλου αφορά τη διαφάνεια των συναλλαγών. Στο Κεφάλαιο 5 φάνηκε ότι πολλά προβλήματα του δικαίου των δικαιωπραξιών οξύνονται επειδή ο αντισυμβαλλόμενος δεν γνωρίζει ότι απέναντί του

⁹⁴ Expert Group on Liability and New Technologies (New Technologies Formation) (2019), ό.π.

βρίσκεται πράκτορας και δεν μπορεί να ελέγξει τα όρια της εξουσίας του. Για το λόγο αυτό προτείνεται ένα σύστημα ταυτότητας και γνωστοποίησης. Κάθε πράκτορας που συναλλάσσεται αυτόνομα πρέπει να συνδέεται με μια επαληθεύσιμη ταυτότητα, η οποία θα παραπέμπει στο υπεύθυνο πρόσωπο και θα δηλώνει τη βαθμίδα αυτονομίας και τα βασικά όρια λειτουργίας του. Η τεχνολογία που εξετάζουμε προσφέρει η ίδια τα εργαλεία για κάτι τέτοιο, αφού οι κρυπτογραφικές υπογραφές και τα πιστοποιητικά επιτρέπουν τη σύνδεση ενός πορτοφολιού με μια ταυτότητα χωρίς να αποκαλύπτονται περιττά δεδομένα. Η γνωστοποίηση της ιδιότητας του πράκτορα ενισχύει τη συναλλακτική πίστη, διευκολύνει την εφαρμογή των κανόνων για την προστασία του καλόπιστου τρίτου και επιτρέπει στις ρυθμιζόμενες πύλες να εφαρμόζουν το κλιμακωτό μοντέλο, δηλαδή να ελέγχουν τη βαθμίδα πριν επιτρέψουν την πρόσβαση.

6.5. Προτάσεις de lege ferenda

Το δεύτερο σκέλος του μοντέλου απευθύνεται στον νομοθέτη. Οι προτάσεις που ακολουθούν αξιοποιούν κατά το δυνατόν τα υφιστάμενα εργαλεία και απαιτούν στοχευμένες μόνο παρεμβάσεις.

Πρώτη πρόταση: ρητή ένταξη των υπηρεσιών αυτόνομων πρακτόρων στο πεδίο της NIS2. Η επικείμενη αναθεώρηση της Οδηγίας προσφέρει την ευκαιρία να προστεθεί στους τομείς των Παραρτημάτων μια κατηγορία παρόχων υπηρεσιών αυτόνομων πρακτόρων, δηλαδή εκείνων που διαθέτουν ή λειτουργούν πράκτορες ικανούς να καταρτίζουν ή να εκτελούν συναλλαγές. Εναλλακτικά, το ίδιο αποτέλεσμα μπορεί να επιτευχθεί ερμηνευτικά, με καθοδήγηση της Επιτροπής ή της οικείας ομάδας συνεργασίας που θα διευκρινίζει τότε οι υπηρεσίες αυτές εμπίπτουν στις υφιστάμενες κατηγορίες.

Δεύτερη πρόταση: γενίκευση της υποχρέωσης μηχανισμού διακοπής. Το άρθρο 36 του Data Act καθιέρωσε την υποχρέωση ασφαλούς τερματισμού και διακοπής μόνο για τις έξυπνες συμβάσεις των συμφωνιών κοινοχρησίας δεδομένων. Η λογική του όμως έχει γενικότερη αξία. Προτείνεται η καθιέρωση αντίστοιχης οριζόντιας απαίτησης για κάθε έξυπνη σύμβαση και κάθε πράκτορα από τη Βαθμίδα 2 και πάνω, είτε με τροποποίηση του Cyber Resilience Act είτε με αυτοτελή πράξη.

Τρίτη πρόταση: υποχρέωση γνωστοποίησης της ιδιότητας του πράκτορα. Προτείνεται η θέσπιση κανόνα κατά τον οποίο όποιος συναλλάσσεται μέσω αυτόνομου πράκτορα οφείλει να γνωστοποιεί την ιδιότητα αυτή στον αντισυμβαλλόμενο, με τις κατάλληλες συνέπειες στο πεδίο της προστασίας του καλόπιστου τρίτου σε περίπτωση παράλειψης.

Τέταρτη πρόταση: ευθύνη του φορέα εκμετάλλευσης και υποχρεωτική ασφάλιση στις υψηλές βαθμίδες. Μετά την απόσυρση της πρότασης για την ευθύνη από τεχνητή νοημοσύνη, το κενό στην πλευρά του φορέα εκμετάλλευσης παραμένει. Προτείνεται, για τα συστήματα της Βαθμίδας 3 και άνω, καθεστώς αντικειμενικής ευθύνης του προσώπου που θέτει τον πράκτορα σε λειτουργία προς όφελός του, συνοδευόμενο από υποχρεωτική ασφάλιση αστικής ευθύνης. Το σχήμα αυτό δίνει στον ζημιωθέντα έναν δυνητικά φερέγγυο εναγόμενο χωρίς να απαιτεί την απόδειξη πταίσματος μέσα σε ένα αδιαφανές σύστημα.

Πέμπτη πρόταση: νομικό ένδυμα για τους αποκεντρωμένους οργανισμούς. Η εμπειρία των DAOs έδειξε ότι η απουσία νομικής μορφής βλάπτει τόσο τους συμμετέχοντες όσο και τους τρίτους. Προτείνεται η δημιουργία, κατά προτίμηση σε ευρωπαϊκό επίπεδο, μιας νομικής μορφής για τους οργανισμούς αυτούς, η οποία θα παρέχει νομική προσωπικότητα και περιορισμό ευθύνης με αντάλλαγμα ελάχιστες προϋποθέσεις λογοδοσίας, δηλαδή ορισμό εκπροσώπου, δηλωμένη περιουσία, διαφάνεια της διακυβέρνησης και ενσωματωμένο μηχανισμό διακοπής στα κρίσιμα πρωτόκολλα.

Έκτη πρόταση: εποπτικά δοκιμαστήρια για τα αυτόνομα οικοσυστήματα. Τα ρυθμιστικά δοκιμαστήρια, που προβλέπει ο AI Act⁹⁵ μπορούν να αξιοποιηθούν ως χώρος ελεγχόμενης δοκιμής πρακτόρων υψηλών βαθμίδων, ώστε η εποπτική εμπειρία να διαμορφωθεί πριν από τη γενικευμένη διάδοση των συστημάτων και όχι μετά από αυτήν⁹⁶. Ο ίδιος ο Κανονισμός ορίζει άλλωστε τα δοκιμαστήρια ως ελεγχόμενο περιβάλλον ανάπτυξης, εκπαίδευσης, δοκιμής και επικύρωσης των συστημάτων πριν από τη διάθεσή τους στην αγορά, υπό την καθοδήγηση και την εποπτεία των αρμόδιων αρχών, χαρακτηριστικά που ανταποκρίνονται ακριβώς στη λειτουργία, που τους αποδίδεται εδώ⁹⁷.

6.6. Σύνοψη του μοντέλου

Το προτεινόμενο μοντέλο μπορεί να συνοψιστεί σε μία φράση. Η αυτονομία των ψηφιακών οντοτήτων είναι ανεκτή στον βαθμό που παραμένει διαβαθμισμένη, δύναται να εποπτευθεί και είναι υποκείμενο καταλογισμού. Το μοντέλο δεν απαιτεί νέο δογματικό οικοδόμημα

⁹⁵Βλ. άρθρα 57 επ. του Κανονισμού (ΕΕ) 2024/1689 (AI Act) για τα ρυθμιστικά δοκιμαστήρια τεχνητής νοημοσύνης (regulatory sandboxes).

⁹⁶ Για τα ρυθμιστικά δοκιμαστήρια στον χώρο της τεχνητής νοημοσύνης βλ. άρθρα 57 επ. του Κανονισμού (ΕΕ) 2024/1689, ό.π. Για την ανάγκη σταδιακής διαμόρφωσης εποπτικής εμπειρίας βλ. ENISA (2025), NIS360, ό.π.

⁹⁷ Άρθρο 57 του Κανονισμού (ΕΕ) 2024/1689, ιδίως παρ. 5 και 9, κατά τις οποίες τα ρυθμιστικά δοκιμαστήρια ΤΝ παρέχουν ελεγχόμενο περιβάλλον για την ανάπτυξη, την εκπαίδευση, τη δοκιμή και την επικύρωση των συστημάτων πριν από τη διάθεσή τους στην αγορά, υπό την καθοδήγηση και την εποπτεία των αρμόδιων αρχών.

ούτε την απονομή προσωπικότητας στις μηχανές. Απαιτεί τη ρητή οργάνωση μιας κλιμάκωσης, που το δίκαιο ήδη εφαρμόζει σιωπηρά, την ενίσχυσή της με τεχνικά μέσα που η ίδια η τεχνολογία προσφέρει και τη συμπλήρωσή της με στοχευμένες νομοθετικές παρεμβάσεις εκεί όπου τα κενά είναι διαπιστωμένα. Με αυτόν τον τρόπο, η καινοτομία και η ασφάλεια δικαίου παύουν να είναι αντίπαλες επιδιώξεις και γίνονται οι δύο όψεις του ίδιου σχεδιασμού.

7. Συμπεράσματα και προτάσεις για μελλοντική έρευνα

Η παρούσα εργασία εξέτασε τη νομική και ρυθμιστική διάσταση της αλληλεπίδρασης των έξυπνων συμβάσεων με τους αυτόνομους πράκτορες τεχνητής νοημοσύνης, με άξονα την Οδηγία NIS2 και την ελληνική της ενσωμάτωση. Τα συμπεράσματα μπορούν να οργανωθούν γύρω από τα τρία ερευνητικά ερωτήματα που τέθηκαν στην εισαγωγή.

Ως προς το πρώτο ερώτημα, δηλαδή την υπαγωγή στο πεδίο εφαρμογής της NIS2, η απάντηση είναι διπλή. Οι κεντριοποιημένοι κρίκοι της αλυσίδας, δηλαδή οι πάροχοι υπολογιστικού νέφους και κέντρων δεδομένων, οι πάροχοι διαχειριζόμενων υπηρεσιών, οι πλατφόρμες και οι αδειοδοτημένοι πάροχοι υπηρεσιών κρυπτοστοιχείων, καλύπτονται από τη NIS2 ή από τον ειδικότερο DORA, και μέσω αυτών οι απαιτήσεις κυβερνοασφάλειας διαχέονται στο οικοσύστημα. Αντίθετα, ο αποκεντρωμένος πυρήνας του φαινομένου, δηλαδή τα ανοικτά δίκτυα, τα πλήρως αποκεντρωμένα πρωτόκολλα και οι πράκτορες που λειτουργούν πάνω σε αυτά, διαφεύγει από τις κατηγορίες της Οδηγίας. Εντοπίστηκε έτσι ένα κανονιστικό παράδοξο. Όσο μεγαλύτερη είναι η αποκέντρωση, και άρα ο κίνδυνος από την απουσία ελέγχου, τόσο ασθενέστερη είναι η ρυθμιστική κάλυψη.

Ως προς το δεύτερο ερώτημα, δηλαδή την ευθύνη, η ανάλυση έδειξε ότι τα εργαλεία του ιδιωτικού δικαίου λειτουργούν ικανοποιητικά στις χαμηλές βαθμίδες αυτονομίας, όπου η δήλωση και η ζημία ανάγονται ομαλά σε ανθρώπινη επιλογή. Στις μεσαίες βαθμίδες τα ίδια εργαλεία επιβιώνουν μόνο με τη βοήθεια κατασκευών, οι οποίες μετατρέπουν σιωπηρά την ευθύνη για πταίσμα σε ευθύνη από διακινδύνευση. Στις υψηλές βαθμίδες τα εργαλεία αστοχούν, όπως δείχνει με τον πιο παραστατικό τρόπο η περίπτωση των αποκεντρωμένων αυτόνομων οργανισμών. Η νέα Οδηγία για την ευθύνη λόγω ελαττωματικών προϊόντων καλύπτει σημαντικό μέρος του κενού από την πλευρά του παραγωγού, όχι όμως από την πλευρά του φορέα εκμετάλλευσης, ενώ η ιδέα της ηλεκτρονικής προσωπικότητας κρίθηκε ότι μεταθέτει το πρόβλημα αντί να το λύνει.

Ως προς το τρίτο ερώτημα, η εργασία υποστήριξε ότι ένα συνεκτικό μοντέλο συμμόρφωσης είναι εφικτό και σκόπιμο. Το μοντέλο, που προτάθηκε, στηρίζεται στην τυπολογία των πέντε βαθμίδων αυτονομίας και σε τέσσερις αρχές, δηλαδή στην αναλογική προς τον κίνδυνο ρύθμιση, στη διατήρηση της δυνατότητας ανθρώπινης παρέμβασης, στην ανιχνευσιμότητα και στην προσδιορισσιμότητα του υπευθύνου. Στο σκέλος του ισχύοντος δικαίου, το μοντέλο μεταφράζει τις υποχρεώσεις της NIS2 σε συγκεκριμένα μέτρα ανά φάση

του κύκλου ζωής και ανά βαθμίδα. Στο σκέλος των νομοθετικών προτάσεων, εισηγείται τη ρητή ένταξη των υπηρεσιών αυτόνομων πρακτόρων στο πεδίο της Οδηγίας, τη γενίκευση της υποχρέωσης μηχανισμού διακοπής, την υποχρέωση γνωστοποίησης της ιδιότητας του πράκτορα, την αντικειμενική ευθύνη του φορέα εκμετάλλευσης με υποχρεωτική ασφάλιση στις υψηλές βαθμίδες, τη δημιουργία νομικής μορφής για τους αποκεντρωμένους οργανισμούς και την αξιοποίηση των ρυθμιστικών δοκιμαστηρίων.

Η συμβολή της εργασίας έγκειται κυρίως στην τυπολογία των βαθμίδων αυτονομίας ως γέφυρας ανάμεσα στην τεχνολογική πραγματικότητα και στις νομικές κατηγορίες. Η τυπολογία επέτρεψε να φανεί ότι το ερώτημα δεν είναι αν το δίκαιο μπορεί να αντιμετωπίσει τους αυτόνομους πράκτορες, αλλά μέχρι ποια βαθμίδα αυτονομίας μπορεί να τους αντιμετωπίσει με τα υπάρχοντα μέσα και από ποια βαθμίδα και μετά απαιτείται παρέμβαση. Η εργασία έχει βεβαίως όρια. Η ανάλυση περιορίστηκε στο ενωσιακό και το ελληνικό δίκαιο, ενώ το ρυθμιστικό τοπίο μεταβάλλεται ταχύτατα, όπως δείχνουν η προτεινόμενη αναθεώρηση της NIS2 και η συνεχής εξέλιξη της τεχνολογίας των πρακτόρων. Τα συμπεράσματα τελούν επομένως υπό την επιφύλαξη των εξελίξεων.

Η μελλοντική έρευνα μπορεί να κινηθεί σε περισσότερες κατευθύνσεις. Ενδιαφέρον παρουσιάζει, πρώτον, η ποινική διάσταση του φαινομένου, δηλαδή το ερώτημα του καταλογισμού αξιόποινων πράξεων, που τελούνται μέσω αυτόνομων πρακτόρων. Δεύτερον, η διάσταση της προστασίας των δεδομένων, ιδίως η συμβατότητα των αμετάβλητων καταχωρίσεων με τα δικαιώματα διόρθωσης και διαγραφής. Τρίτον, η φορολογική και λογιστική αντιμετώπιση των συναλλαγών, που καταρτίζονται από πράκτορες. Τέταρτον, η ασφαλιστική διάσταση, δηλαδή η διαμόρφωση ενός πλαισίου ασφάλισης κινδύνων και προϊόντων για τις υψηλές βαθμίδες αυτονομίας. Και πέμπτον, η εμπειρική παρακολούθηση της εφαρμογής του Ν. 5160/2024 και του Εθνικού Πλαισίου Απαιτήσεων Κυβερνοασφάλειας στην ελληνική πράξη, καθώς ο πραγματικός έλεγχος κάθε ρυθμιστικού μοντέλου γίνεται πάντοτε στο πεδίο.

8. Βιβλιογραφία

Ελληνόγλωσση

- Γεωργιάδης, Α.Σ. (2015), Ενοχικό Δίκαιο, Γενικό Μέρος, 2η έκδοση, Αθήνα: Π.Ν. Σάκκουλας
- Γεωργιάδης, Α.Σ. (2019), Γενικές Αρχές Αστικού Δικαίου, 5η έκδοση, Αθήνα: Π.Ν. Σάκκουλας
- Ιγγλεζάκης, Ι. (2022), Το δίκαιο της ψηφιακής οικονομίας, Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα
- Καλογεράκης, Γ., Θεοδωράκης, Ν. (2019), «Blockchain: εφαρμογές, προοπτικές και προκλήσεις για το ελληνικό νομικό σύστημα», Δίκαιο Μέσων Ενημέρωσης & Επικοινωνίας (ΔiMEE) 1/2019, σσ. 5-22
- Κανέλλος, Λ. (2020), The GDPR Handbook. Για DPOs, Επιχειρήσεις & Οργανισμούς, Αθήνα: Νομική Βιβλιοθήκη
- Κανέλλος, Λ. (2022), Smart Contracts. Νομικές προκλήσεις, σύγχρονες συναλλακτικές πρακτικές και επιχειρηματικές προοπτικές, Αθήνα: Νομική Βιβλιοθήκη
- Χριστοδούλου, Κ. (2001), Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία, Αθήνα: Αντ. Ν. Σάκκουλας

Ξενόγλωσση

- Bayern, S. (2015), ‘The Implications of Modern Business Entity Law for the Regulation of Autonomous Systems’, Stanford Technology Law Review, 19, σσ. 93 επ.
- Buterin, V. (2014), Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform, Available at: <https://ethereum.org/en/whitepaper/>
- Chopra, S., White, L.F. (2011), A Legal Theory for Autonomous Artificial Agents, Ann Arbor: University of Michigan Press
- De Filippi, P., Wright, A. (2018), Blockchain and the Law: The Rule of Code, Cambridge, MA: Harvard University Press
- DuPont, Q. (2018), ‘Experiments in Algorithmic Governance: A History and Ethnography of The DAO, a Failed Decentralized Autonomous Organization’, σε Campbell-Verduyn, M. (επιμ.), Bitcoin and Beyond, London: Routledge
- Ebers, M., Navas, S. (επιμ.) (2020), Algorithms and Law, Cambridge: Cambridge University Press
- ENISA (2023), Cybersecurity of AI and Standardisation, Available at: <https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation>
- ENISA (2025), ENISA Threat Landscape 2025, Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
- ENISA (2025), NIS360, Available at: <https://www.enisa.europa.eu/publications>

- EU Blockchain Observatory and Forum (2019), Legal and Regulatory Framework of Blockchains and Smart Contracts, Thematic Report
- European Law Institute (2022), ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection, Report of the European Law Institute, Available at: <https://www.europeanlawinstitute.eu>
- Expert Group on Liability and New Technologies (New Technologies Formation) (2019), Liability for Artificial Intelligence and Other Emerging Digital Technologies, Λουξεμβούργο: Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης
- Fairfield, J. (2014), ‘Smart Contracts, Bitcoin Bots, and Consumer Protection’, Washington and Lee Law Review Online, 71, σσ. 35 επ.
- Finck, M. (2019), Blockchain Regulation and Governance in Europe, Cambridge: Cambridge University Press
- Hacker, P. (2023), ‘The European AI Liability Directives’, Computer Law and Security Review, 51
- Marino, B., Juels, A. (2025), ‘Giving AI Agents Access to Cryptocurrency and Smart Contracts Creates New Vectors of AI Harm’, arXiv preprint arXiv:2507.08249, Available at: <https://arxiv.org/abs/2507.08249>
- Mik, E. (2017), ‘Smart Contracts: Terminology, Technical Limitations and Real World Complexity’, Law, Innovation and Technology, 9(2), σσ. 269-300
- Nakamoto, S. (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, Available at: <https://bitcoin.org/bitcoin.pdf>
- Open Letter to the European Commission on Artificial Intelligence and Robotics (2018)
- OWASP Foundation (2023), OWASP Top 10 for Large Language Model Applications
- Russell, S., Norvig, P. (2021), Artificial Intelligence: A Modern Approach, 4th ed., Hoboken: Pearson
- Saeidi, M., Calvert, M., Au, A.W., Sarma, A., Bobba, R.B. (2022), ‘If This Context Then That Concern: Exploring Users’ Concerns with IFTTT Applets’, Proceedings on Privacy Enhancing Technologies, 2022(1), σσ. 166-186, Available at: <https://arxiv.org/pdf/2012.12518>
- Szabo, N. (1997), ‘Formalizing and Securing Relationships on Public Networks’, First Monday, 2(9), Available at: <https://firstmonday.org/ojs/index.php/fm/article/view/548>
- Turner, J. (2019), Robot Rules: Regulating Artificial Intelligence, Cham: Palgrave Macmillan
- Wagner, G. (2019), ‘Robot, Inc.: Personhood for Autonomous Systems?’, Fordham Law Review, 88, σσ. 591 επ.
- Werbach, K., Cornell, N. (2017), ‘Contracts Ex Machina’, Duke Law Journal, 67(2), σσ. 313-382
- Wright, A. (2021), ‘The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges’, Stanford Journal of Blockchain Law and Policy, 4

- Zetzsche, D., Buckley, R., Arner, D. (2018), ‘The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain’, University of Illinois Law Review, σσ. 1361 επ.

Νομολογία

- CFTC v. Ooki DAO, United States District Court, Northern District of California (2023)
- United States v. Eisenberg, United States District Court, Southern District of New York (2023 επ.)

Νομοθεσία

- Αστικός Κώδικας (π.δ. 456/1984, ΦΕΚ Α΄ 164)
- Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (Οδηγία NIS 2), ΕΕ L 333 της 27.12.2022, σ. 80
- Οδηγία (ΕΕ) 2024/2853 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2024, για την ευθύνη λόγω ελαττωματικών προϊόντων
- Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα (DORA)
- Κανονισμός (ΕΕ) 2023/1114 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 31ης Μαΐου 2023, για τις αγορές κρυπτοστοιχείων (MiCA)
- Κανονισμός (ΕΕ) 2023/2854 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2023, για εναρμονισμένους κανόνες σχετικά με τη δίκαιη πρόσβαση σε δεδομένα και τη δίκαιη χρήση τους (Data Act)
- Κανονισμός (ΕΕ) 2024/1689 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουνίου 2024, για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (AI Act)
- Κανονισμός (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία (Cyber Resilience Act)
- Εκτελεστικός Κανονισμός (ΕΕ) 2024/2690 της Επιτροπής, της 17ης Οκτωβρίου 2024, για τον καθορισμό κανόνων εφαρμογής της Οδηγίας (ΕΕ) 2022/2555 όσον αφορά τις τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας
- Ν. 4961/2022 «Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις» (ΦΕΚ Α΄ 146/27.07.2022)
- Ν. 5160/2024 «Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 [...] (Οδηγία NIS 2) και άλλες διατάξεις» (ΦΕΚ Α΄ 195/27.11.2024)
- ΚΥΑ 1689/2025 «Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων» (ΦΕΚ Β΄ 2186/06.05.2025)

- ΚΥΑ 1381/2025 για την Ψηφιακή Πλατφόρμα Εγγραφής Οντοτήτων της Εθνικής Αρχής Κυβερνοασφάλειας (ΦΕΚ Β΄ 463/10.02.2025)
- Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 16ης Φεβρουαρίου 2017 με συστάσεις προς την Επιτροπή σχετικά με ρυθμίσεις αστικού δικαίου στον τομέα της ρομποτικής (2015/2103(INL))
- Πρόταση Οδηγίας για την προσαρμογή των κανόνων εξωσυμβατικής αστικής ευθύνης στην τεχνητή νοημοσύνη (AI Liability Directive), COM(2022) 496
- Πρόταση της Ευρωπαϊκής Επιτροπής της 20ής Ιανουαρίου 2026 για στοχευμένες τροποποιήσεις της Οδηγίας (ΕΕ) 2022/2555 (digital omnibus)
- Wyoming Decentralized Autonomous Organization Supplement (2021)

Ιστοσελίδες

- <https://uk.practicallaw.thomsonreuters.com/w-047-2998> (Thomson Reuters, Practical Law)
- <https://www.sae.org/standards/j3016-taxonomy-definitions-terms-related-driving-automation-systems-road-motor-vehicles> (SAE International, πρότυπο J3016)

«Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν.1599/1986 και τα άρθρα 2,4,6, παρ. 3 του Ν. 1256/1982, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον».