ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2022-2023

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
ΤΟΥ Μάριου Μ. Τσουνιά (Α.Μ.: ΜΔΙ2245)

ΑΥΤΟΜΑΤΙΣΜΟΣ ΚΑΙ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΣΤΟΝ ΕΣΩΤΕΡΙΚΟ ΕΛΕΓΧΟ

AUTOMATION AND ARTIFICIAL INTELLIGENCE IN INTERNAL AUDIT

Επιβλέπουσα
Αναπληρώτρια Καθηγήτρια Ελένη Ρεθυμιωτάκη

Πειραιάς, Μάιος 2024

Ευχαριστίες

Ευχαριστίες σε όλους όσους βοήθησαν με τον δικό τους τρόπο στην προσπάθεια μου για την ολοκλήρωση της διπλωματικής και του μεταπτυχιακού προγράμματος. Τους γονείς μου, τους γονείς της συζύγου μου, την οικογένεια της αδελφής μου, τους συναδέλφους και τους φίλους που στήριξαν την προσπάθεια από το πρώτο λεπτό. Περισσότερο από όλους θέλω να ευχαριστήσω την οικογένεια μου και την αδελφή μου, Στέλα, που μια δύσκολη διαδρομή και με πολλές ατυχείς συγκυρίες, προσέφεραν αβίαστα ότι χρειάστηκε για να φτάσουμε εδώ. Η διαδρομή ήταν μαγική και το αποτέλεσμα τόσο διάχυτο σε φως, όσο και τα φωτεινά πρόσωπά τους σε κάθε στιγμή της.

Στα παιδιά μου για την ανεπιτήδευτη αγάπη τους και στο λιμάνι της ζωής μου, τη σύζυγο μου. Μιχάλη, Χάρη και Αγγελική σας ευχαριστώ για όλα τα λίγα που κάνατε πολλά.

Πίνακας Περιεχομένων

ΠΕΡΙΛΗΨΗ 7

ΚΕΦΑΛΑΙΟ 1. Η ΣΗΜΑΣΙΑ ΤΗΣ ΑΥΤΟΜΑΤΟΠΟΙΗΣΗΣ ΚΑΙ ΤΗΣ ΥΙΟΘΕΤΗΣΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ ΣΤΟΝ ΕΣΩΤΕΡΙΚΟ ΕΛΕΓΧΟ - ΟΡΙΣΜΟΙ 9

1.1 Ορισμός Εσωτερικού Ελέγχου 10

1.2 Τεχνητή Νοημοσύνη 12

1.3 Αυτοματοποίηση Διαδικασιών 13

1.4 ΣΕΕ και Γραμμές Άμυνας 14

1.5 Computer Assisted Audit Techniques (CAATs) 15

1.6 Διαρκής Έλεγχος 16

1.7 Data Analytics και Big Data 17

1.8 Τεχνητή Νοημοσύνη και Αυτοματοποίηση 19

1.9 Προσωπικά Δεδομένα και Έλεγχος 21

ΚΕΦΑΛΑΙΟ 2. ΣΥΣΤΗΜΑ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ ΜΟΝΤΕΛΟ ΤΩΝ ΤΡΙΩΝ ΓΡΑΜΜΩΝ – ΔΙΑΣΦΑΛΙΣΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ, ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΚΑΙ ΕΣΩΤΕΡΙΚΟΣ ΕΛΕΓΧΟΣ 23

2.1 Το ΣΕΕ στο Ελληνικό Δίκαιο 24

2.2 Το ΣΕΕ στο Ευρωπαϊκό Δίκαιο 29

2.3 Η 1η Γραμμή του ΣΕΕ 30

2.4 Η 2η Γραμμή του ΣΕΕ 32

2.5 Η 3η Γραμμή του ΣΕΕ 34

ΚΕΦΑΛΑΙΟ 3. ΩΦΕΛΗ ΚΑΙ ΚΙΝΔΥΝΟΙ ΑΠΟ ΤΗΝ ΑΥΤΟΜΑΤΟΠΟΙΗΣΗ ΣΤΑ ΣΕΕ 36

3.1 Αυτοματοποίηση Επιχειρησιακών Διαδικασιών 37

3.1.1 Κίνδυνος διακυβέρνησης (Governance Risk). 38

3.1.2 Λειτουργικός Κίνδυνος (Operational Risk). 39

3.1.3 Οργανωτικός Κίνδυνος (Organizational Risk). 39

3.1.4 Τεχνολογικός Κίνδυνος (Technological Risk). 40

3.2 Case Study I: Μηχανισμοί Ταυτοποίησης και Περιορισμού Ηλεκτρονικής Απάτης 41

3.3 Case Study II: Μιμητικά Bots 43

3.4 Case Study III: Έγκριση Δανείου και Πιστοληπτική Ικανότητα 46

3.5 Αυτοματοποίηση στον ΕΕ 50

3.6 Διαρκής Παρακολούθηση και Έλεγχος 52

ΚΕΦΑΛΑΙΟ 4. Η ΑΞΙΟΠΟΙΗΣΗ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ ΣΤΟ ΣΥΣΤΗΜΑ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ 56

4.1 Το ΣΕΕ Εφαρμογών ΤΝ 56

4.2 Case Studies: Συστήματα ΤΝ στην 1η και τη 2η γραμμή του ΣΕΕ Πιστωτικών Ιδρυμάτων 58

4.3 Τεχνητή Νοημοσύνη στην 3η Γραμμή – Εσωτερικός Έλεγχος 63

4.4 Case Studies Μηχανισμών Τεχνητής Νοημοσύνης στην 3η Γραμμή 66

4.5 ΤΝ στον Έλεγχο: Απειλή ή Εργαλείο; 68

ΚΕΦΑΛΑΙΟ 5 ΤΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΤΗΣ ΕΕ ΓΙΑ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΚΑΙ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ ΚΑΙ ΤΟΝ ΣΕΒΑΣΜΟ ΤΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΤΟΥ ΑΤΟΜΟΥ 70

5.1 Ελληνική και Ευρωπαϊκή νομοθεσία για την ΤΝ 70

5.2 Ειδικές Ρυθμίσεις για Υψηλού Κινδύνου Συστήματα ΤΝ 74

5.3 ΤΝ και Προσωπικά Δεδομένα 77

5.4 Προσωπικά δεδομένα και ΕΕ 79

ΚΕΦΑΛΑΙΟ 6. Η ΣΥΜΒΟΛΗ ΤΗΣ ΗΘΙΚΗΣ ΚΑΙ ΤΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ 82

6.1 Κώδικες Δεοντολογίας και Αρχές Ηθικής για τους Εσωτερικούς Ελεγκτές 83

6.2 Εφαρμογή και Υιοθέτηση 85

6.2.1 Ακεραιότητα 85

6.2.2 Αντικειμενικότητα 86

6.2.3 Επαγγελματική Επάρκεια 87

6.2.4 Δέουσα Επαγγελματική Επιμέλεια 88

6.2.5 Εμπιστευτικότητα 89

6.3 Κώδικες Δεοντολογίας και Αρχές Ηθικής για την 1η και τη 2η Γραμμή 90

6.4 Ηθική, Τεχνητή Νοημοσύνη και ΕΕ 91

ΚΕΦΑΛΑΙΟ 7. ΣΥΜΠΕΡΑΣΜΑΤΑ 96

ΕΠΙΛΟΓΟΣ 100

ΠΑΡΑΡΤΗΜΑ Ι - ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ 102

ΒΙΒΛΙΟΓΡΑΦΙΑ 103

Νομοθεσία - Αποφάσεις 103

Επιστημονικές Εκδόσεις 105

Διαδικτυακά Άρθρα 106

Ιστοσελίδες 109

On-Line Σεμινάρια – Webinars 111

ΠΕΡΙΛΗΨΗ

Σκοπός της διπλωματικής εργασίας είναι η μελέτη της υιοθέτησης λύσεων αυτοματισμού και τεχνητής νοημοσύνης στα Συστήματα Εσωτερικού Ελέγχου επιχειρήσεων και δημόσιων οργανισμών. Η δομή του συστήματος αποτελείται από τρεις γραμμές άμυνας, τις επιχειρησιακές λειτουργίες για την παραγωγή των αγαθών και την παροχή υπηρεσιών, τη διαχείριση των κινδύνων και τον έλεγχο.

Η κείμενη νομοθεσία αναφορικά με την τεχνητή νοημοσύνη κατευθύνεται πρωτίστως από τον σχετικό Κανονισμό της Ευρωπαϊκής Ένωσης, και τους κανόνες που τίθενται από αυτήν αλλά και δημιουργούνται στις χώρες μέλη αναφορικά με την ανάπτυξη και τη διάθεση συστημάτων που την υιοθετούν. Παράλληλα, τα διεθνή ινστιτούτα ελεγκτών δημιουργούν πρότυπα που ενσωματώνονται σταδιακά στη νομολογία των χωρών μελών προκειμένου να διασφαλίσουν ενιαία και καθολική εφαρμογή.

Αυτοματοποιημένοι μηχανισμοί και συστήματα τεχνητής νοημοσύνης υιοθετούνται και εφαρμόζονται στο σύνολο των δραστηριοτήτων των επιχειρήσεων, καθιστώντας την υλοποίηση, τη χρήση και τον έλεγχο τους επιβεβλημένα. Για το σκοπό αυτό, προσδιορίζονται και επιμετρούνται οι κίνδυνοι από την εφαρμογή σχετικών μηχανισμών και αξιολογείται ο τρόπος ανάπτυξής και «εκπαίδευσής» τους βάσει της αξιοπιστίας των δεδομένων και της μεθοδολογίας που χρησιμοποιούνται.

Οι υλοποιήσεις περιλαμβάνουν λύσεις για την αυτοματοποίηση και τη βελτίωση της ποιότητας της γραμμής παραγωγής (π.χ. ρομποτικά συστήματα, αυτοματοποιημένα κέντρα εξυπηρέτησης πελατών), την παρακολούθηση των κινδύνων, τη συμμόρφωση με τις απαιτήσεις, αποτρεπτικούς μηχανισμούς σε συστήματα ηλεκτρονικής τραπεζικής, ανάλυσης συναλλαγών με τεχνικές data analytics, την αξιολόγηση πιστοληπτικής ικανότητας πελατών, την εγκριτική διαδικασία δανείων καθώς και πιο προηγμένων εφαρμογών που χρησιμοποιούν μηχανική μάθηση και επεξεργασία φυσικής γλώσσας.

Δεδομένου ότι η τεχνητή νοημοσύνη αποτελεί μία πραγματικότητα, έχοντας εισβάλει και βελτιώσει σημαντικά την καθημερινότητα της ανθρώπινης δραστηριότητας, η ηθική διάσταση σχετικά με την αυτοματοποιημένη λήψη αποφάσεων από ένα πληροφοριακό σύστημα που την υιοθετεί αποτελεί σημείο προβληματισμού. Παρότι, ενισχύει σημαντικά την εν λόγω διαδικασία και επεκτείνει τις δυνατότητες της ανθρώπινης νοημοσύνης, δεν πρέπει και δεν θα οδηγήσει στην αντικατάστασή της.

The goal of the diplomatic essay was to study the applications deployed to automate the business processes, while also introducing Artificial Intelligence in the Internal Control Systems implemented by private organizations as well as those of the public sector. The Internal Control System comprises of three lines of defence, namely the business functions for the products and services provided to the customers, the risk management function, and the audit.

The applicable legislative framework with regards to the Artificial Intelligence mainly consists of the European Union Regulation (AI Act), including the rules and the standards which are gradually being created in the member states to establish a regulatory environment for the development and implementation of AI related appliances. Moreover, the international auditing institutes have created standards which may be also incorporated in the local laws of various countries to ensure homogenization and full applicability by all the stakeholders.

The automation of the business processes, including information systems adopting Artificial Intelligence, are applied almost in every aspect of an organization. Consequently, their adoption, their utilization and their evaluation by the audit function deems mandatory. Towards this purpose, the involved and inherent risks should be defined and assessed, including those related with their development and training with reliable and unbiased data and methodology.

The implementations provide for information systems addressed to all the three lines of defence, such as the automation of the production line and the quality management and improvement (e.g. robotics, automated customer care centres), the continuous risk monitoring, the continuous assessment of compliance with the regulatory and the legislative framework, intrusion detection and prevention mechanisms for the Web Banking systems, the analysis of transactions deploying data analytics techniques, the credit risk scoring and evaluation, the automated approval or rejection of a loan application, as well as more sophisticated solutions based on machine learning and natural language processing.

The Artificial Intelligence is a reality and has invaded the human daily activity, thus, affecting several aspects and improving everyday life. The morality beside the possibility for decision-making information systems, based on the analysis performed by the model and the training data provided by the end-user, raises questions that require persuasive responses. It is expected that the deployment of IT systems adopting Artificial Intelligence will enhance and improve the decision-making process and human intelligence without in any case replacing it.

ΚΕΦΑΛΑΙΟ 1. Η ΣΗΜΑΣΙΑ ΤΗΣ ΑΥΤΟΜΑΤΟΠΟΙΗΣΗΣ ΚΑΙ ΤΗΣ ΥΙΟΘΕΤΗΣΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ ΣΤΟΝ ΕΣΩΤΕΡΙΚΟ ΕΛΕΓΧΟ - ΟΡΙΣΜΟΙ

Το επάγγελμα του ελεγκτή και ο έλεγχος έχουν σημαντικό παρελθόν και πλούσια ιστορία. Οι ρίζες του προσδιορίζονται στη Μεσοποταμία, όπου ειδικά σημάδια χρησιμοποιούνταν προκειμένου να καταγράφονται και να επαληθεύονται οι θαλάσσιες μεταφορές εμπορευμάτων και οι οικονομικές συναλλαγές. Ο όρος «audit», προέρχεται από την Λατινική λέξη «auditous» (ακρόαση), που στην αρχαία Ρώμη αφορούσε στην ακρόαση προφορικής συνομιλίας με περιεχόμενο διασταυρούμενο επισήμως από τους συμμετέχοντες. Η έννοια του ελέγχου εξελίχθηκε σημαντικά στο πέρασμα των ετών, κερδίζοντας την αναγνώριση στελεχών και διοικήσεων των επιχειρήσεων, κυρίως λόγω του ότι εκ φύσεως εστιάζει και καλύπτει τις τρέχουσες ανάγκες και τις αλλαγές του παγκόσμιου περιβάλλοντος.

Η Τεχνητή Νοημοσύνη δεν είναι κάτι νέο, αυτό που κομίζει είναι το πραγματικά καινοτόμο για την ανθρώπινη δραστηριότητα. Είναι οι δυνατότητες που προσφέρει και προστίθενται στην υπηρεσία του ατόμου, επεκτείνοντας το φάσμα των δραστηριοτήτων του, επιλύοντας προβλήματα και αίροντας περιορισμούς. Ενδεχομένως να είναι η απάντηση σε πολλά από τα προβλήματα του ατόμου, συμπεριλαμβανομένων και κάποιων που δεν έχουν ακόμα τεθεί.

Η αυτοματοποίηση των διαδικασιών, με ή χωρίς χρήση τεχνητής νοημοσύνης, είναι ένα ακόμα βήμα στην κατεύθυνση της δημιουργίας ενός ελεγχόμενου περιβάλλοντος στις επιχειρήσεις. Η χρήση της τεχνολογίας στις ελεγκτικές πρακτικές (CAATs) υφίσταται αρκετές δεκαετίες, ειδικά μετά την έκρηξη στο χώρο της Πληροφορικής που επέφερε σημαντική μείωση στα κόστη και αύξηση της αξιοπιστίας στην επεξεργασία και στην παραγωγή αποτελεσμάτων.

Η ραγδαία ανάπτυξη στο χώρο των δεδομένων και κυρίως των μεγάλων δεδομένων (“big data”), παράλληλα με την εμφάνιση πληθώρας εργαλείων για την αναζήτηση και την εξόρυξη στοιχείων, ωθεί και μεταβάλει τον τρόπο πραγματοποίησής των ελέγχων. Η δημιουργία αυτοματοποιημένων μηχανισμών επεξεργασίας και εξόρυξης για σκοπούς διαρκούς ελέγχου και παρακολούθησης, αποτελεί τη σύγχρονη πρόκληση για τους ελεγκτές

προκειμένου να εντοπίζονται και να επιμετρούνται, σε πραγματικό χρόνο, κίνδυνοι και παρεκκλίσεις.

Ο Εσωτερικός Έλεγχος (Internal Audit) αποτελεί αναπόσπαστο κομμάτι μίας επιχείρησης προκειμένου να συμμορφωθεί με το νομικό και το κανονιστικό πλαίσιο, να προσαρμοστεί και να υιοθετήσει νέες τεχνολογίες, να βελτιώσει τις λειτουργικές διαδικασίες, το πλαίσιο διακυβέρνησης, να αντιμετωπίσει αποτελεσματικά την απάτη και να περιορίσει τους κινδύνους.

Η ΤΝ και αυτοματοποιημένες διαδικασίες υιοθετούνται από τον έλεγχο αλλά και τις υπόλοιπες μονάδες των επιχειρήσεων και των δημόσιων οργανισμών με ραγδαίους ρυθμούς, καθώς αναγνωρίζονται τα οφέλη τους σε πληθώρα τομέων και δραστηριοτήτων. Βασικοί στόχοι, η απλοποίηση των εσωτερικών διαδικασιών, η μείωση του λειτουργικού κόστους, η βελτίωση της ποιότητας και των υπηρεσιών που προσφέρονται στους πελάτες καθώς και η διαχείριση και ο περιορισμός των κινδύνων που εκτίθεται. Ωστόσο, δημιουργείται το ερώτημα αν αυτή η ψηφιοποίηση του Συστήματος Εσωτερικού Ελέγχου θα βελτιώσει οργανωτικά την ακρίβεια και την αποτελεσματικότητά του, σε σχέση με τις υπάρχουσες γραφειοκρατικές διαδικασίες, ή θα αυξήσει την πολυπλοκότητα και το ανέλεγκτο των διαδικασιών υιοθετώντας τη λογική του αλάθητου;

1.1 Ορισμός Εσωτερικού Ελέγχου

Ο έλεγχος είναι μια ανεξάρτητη, αντικειμενική και συμβουλευτική δραστηριότητα, σχεδιασμένη να προσθέτει αξία και να βελτιώνει τις λειτουργίες της επιχείρησης. Στόχος του είναι να βοηθάει στην επίτευξη των αντικειμενικών σκοπών της, υιοθετώντας μία συστηματική και επαγγελματική προσέγγιση για την αξιολόγηση και τη βελτίωση της αποτελεσματικότητας των διαδικασιών διαχείρισης κινδύνων, των συστημάτων εσωτερικού ελέγχου και της εταιρικής διακυβέρνησης (IIA, 2008).

Οι ελεγκτές (εσωτερικοί και εξωτερικοί) παρέχουν ανεξάρτητη, αντικειμενική και χωρίς προκαταλήψεις υπηρεσίες διασφάλισης αναφορικά με την ορθή λειτουργία των επιχειρησιακών διεργασιών της επιχείρησης[1]. Κατά την άσκηση των καθηκόντων τους

[1] Οι διεργασίες του ελέγχου συχνά αναφέρονται με το ακρωνύμιο GRC – Governance, Risk, Compliance (Διακυβέρνηση, Κίνδυνοι, Συμμόρφωση).

πρέπει να επιδεικνύουν ακεραιότητα, αντικειμενικότητα, επαγγελματισμό, τη γνώση τους επί του ελεγχόμενου αντικειμένου και δεξιότητες ηγεσίας.

Ο έλεγχος των ΣΠ (IT audit) μίας επιχείρησης απαιτεί εξειδικευμένη γνώση λόγω της ιδιαίτερης φύσης του, καθώς εστιάζει στην τεχνολογική υποδομή του οργανισμού, στις εφαρμογές, στα δεδομένα, στις πολιτικές και στις διαδικασίες διαχείρισης για τη συμμόρφωσή τους έναντι αναγνωρισμένων προτύπων και κανονιστικών απαιτήσεων (Information Systems and Control Association - ISACA και Πανεπιστήμιο Harvard).

Στη σύγχρονη εποχή των σημαντικών τεχνολογικών εξελίξεων και των αλυσιδωτών αλλαγών που επέρχονται στον τρόπο λειτουργίας των επιχειρήσεων και στις δραστηριότητές τους, ο ρόλος του ελέγχου ΣΠ έχει αναβαθμιστεί σημαντικά. Η πληθώρα πληροφοριών και δεδομένων που διακινούνται εσωτερικά στις επιχειρήσεις και στο διαδίκτυο, η ανάπτυξη και η αναμενόμενη διάχυση της ΤΝ στις επιχειρηματικές δραστηριότητες καθώς και οι τεχνολογίες υπολογιστικού νέφους (cloud computing) καθιστούν αναγκαία τη διασφάλιση της ασφαλούς και εντός καθορισμένων ορίων λειτουργίας τους, βάσει και των κανονιστικών απαιτήσεων.

Με τους νόμους 4795/2021 (ΦΕΚ Α 62/17.4.2021)[2] και 4972/2022 (ΦΕΚ Α 181 - 23.09.2022), το Ελληνικό κράτος πραγματοποιεί την πρώτη προσπάθεια ρύθμισης του ΣΕΕ και του επαγγέλματος του ελεγκτή[3]. Στους νόμους υιοθετείται ο ορισμός του ελέγχου όπως αποδίδεται από το ΙΙΑ, περιγράφονται τα δομικά στοιχεία του ΣΕΕ συμπεριλαμβανομένων των ρόλων και των αρμοδιοτήτων καθενός εξ αυτών. Παράλληλα, καθορίζονται οι βασικές παράμετροι αναφορικά με την λειτουργία της επιτροπής ελέγχου, καθώς και του ΕΕ μίας επιχείρησης ή ενός δημοσίου οργανισμού από το σχεδιασμό του ετήσιου πλάνου μέχρι και την ετήσια έκθεση που υποβάλλεται στις κανονιστικές αρχές. Τέλος, παραβάλλονται τα απαιτούμενα ελάχιστα προσόντα των ελεγκτών που δραστηριοποιούνται στην Ελληνική επικράτεια, οι αποδεκτές πιστοποιήσεις και τα πρότυπα που οφείλουν να χρησιμοποιούν κατά την άσκηση των καθηκόντων τους.

Αντίστοιχοι ορισμοί δίνονται και από τις εποπτικές αρχές που δραστηριοποιούνται στην Ελλάδα. Ενδεικτικά η Τράπεζα της Ελλάδος (ΤτΕ), στην ΠΔΤΕ2577/9.3.2006, καθορίζει τις

[2] Αφορά στον στενό και στον ευρύτερο δημόσιο τομέα

[3] Άρθρα του Ν.4972 τροποποιήθηκαν το 2023, αναφορικά με τις προϋποθέσεις ένταξης των ελεγκτών στο σχετικό μητρώο του Οικονομικού Επιμελητηρίου Ελλάδος.

βασικές αρχές που θα πρέπει να διέπουν τη λειτουργία της Μονάδας Εσωτερικής Επιθεώρησης[4] και τονίζεται η υποχρέωση να είναι διοικητικά ανεξάρτητη από μονάδες με εκτελεστικές αρμοδιότητες, να αναφέρεται στο Διοικητικό Συμβούλιο (μέσω της Επιτροπής Ελέγχου) και στη Διοίκηση. Ο ρόλος της είναι «*η πραγματοποίηση ελέγχων προκειμένου να διαμορφωθεί αντικειμενική, ανεξάρτητη και τεκμηριωμένη άποψη για την επάρκεια και την αποτελεσματικότητα του ΣΕΕ, σε επίπεδο πιστωτικού ιδρύματος και του ομίλου του οποίου είναι επικεφαλής*» (Κεφάλαιο V, παρ. (α)).

Η επιτροπή Κεφαλαιαγοράς στο άρθρο 16 του Ν.4706/2020, ορίζει τον ΕΕ ως ανεξάρτητη οργανωτική μονάδα εντός της εταιρείας με σκοπό την παρακολούθηση και τη βελτίωση των λειτουργιών της επιχείρησης και των πολιτικών της αναφορικά με το ΣΕΕ. Η Ευρωπαϊκή Κεντρική Τράπεζα (European Central Bank - ΕΚΤ) υιοθετεί τον παραπάνω ορισμό του ΙΙΑ στην Πολιτική Ελέγχου της (Audit Charter), προκειμένου να περιγράψει τις βασικές λειτουργίες, τον ρόλο και τον σκοπό της μονάδας.

1.2 Τεχνητή Νοημοσύνη

Ο όρος Τεχνητή Νοημοσύνη (ΤΝ) ορίζεται με ποικίλους τρόπους από το 1950, μέχρι και σήμερα, οπότε και ο Alan Touring έθεσε το ερώτημα για την ικανότητα σκέψης των μηχανών. Ο McCarthy (1955) προσδιόρισε το πρόβλημα στο «*να μετατρέψουμε μία μηχανή να συμπεριφέρεται με τρόπο που θα χαρακτηρίζονταν ευφυής αν ένας άνθρωπος συμπεριφέρονταν με τον ίδιο τρόπο*». Σε μεταγενέστερο ορισμό ο Minsky (1969) την προσδιορίζει ως «*επιστήμη που κάνει τις μηχανές να κάνουν πράγματα που θα απαιτούσαν ευφυΐα αν αυτά γινόντουσαν από ανθρώπους*».

Ο όρος ΤΝ την δεκαετία του 1990, περίοδος που σημειώνεται σημαντική πρόοδος[5], αναφέρεται στον κλάδο της Πληροφορικής που μελετά την νοήμονα συμπεριφορά και προσπαθεί να αναπτύξει μοντέλα και συστήματα που συμπεριφέρονται κατά αυτόν τον τρόπο (Παναγιωτόπουλος 2000, σελ. 1-20). Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ, 2019) την ορίζει ως σύστημα που βασίζεται σε μηχανές και μπορεί για ένα δεδομένο σύνολο στόχων που καθορίζονται από τον άνθρωπο, να κάνει προβλέψεις,

[4] Παλαιότερη ονομασία της μονάδας ΕΕ
[5] Αναπτύσσονται εξειδικευμένες γλώσσες προγραμματισμού και εργαλεία όπως η Prolog, Clips κ.α.

συστάσεις ή να λάβει αποφάσεις επηρεάζοντας πραγματικά ή εικονικά περιβάλλοντα, ενώ είναι σχεδιασμένο να λειτουργεί με διαφορετικά επίπεδα αυτονομίας.

Τέλος, στον Κανονισμό της EU (2021/0106) η ΤΝ ορίζεται ως λογισμικό που αναπτύσσεται με τη χρήση συγκεκριμένων τεχνικών και προσεγγίσεων (Παράρτημα Ι) και δύναται βάσει προκαθορισμένων από τον άνθρωπο στόχων, να παράγει αποτελέσματα όπως περιεχόμενο, προβλέψεις, συστάσεις/προτάσεις ή ακόμα και αποφάσεις επηρεάζοντας το περιβάλλον που αλληλοεπιδρά.

Κοινό σημείο του συνόλου των δοθέντων ορισμών είναι η ικανότητα μίας μηχανής να αναπαράγει τις γνωστικές λειτουργίες ενός ανθρώπου, όπως η μάθηση, ο σχεδιασμός και η δημιουργικότητα. Είναι η προσπάθεια να καταστήσουμε τις μηχανές ικανές να επιλύουν προβλήματα και να δρουν προς την επίτευξη ενός συγκεκριμένου στόχου με κάποιο βαθμό αυτονομίας.

1.3 Αυτοματοποίηση Διαδικασιών

Η αυτοματοποίηση διαδικασιών, ειδικότερα με χρήση ρομποτικής τεχνολογίας (Robotic Process Automation), αποτελεί το πρώτο βήμα στην κατεύθυνση της υιοθέτησης προηγμένων τεχνολογιών και ΤΝ σε μία επιχείρηση. Ο όρος υιοθετείται για λογισμικά που στηριζόμενα σε πεπερασμένους και σαφώς καθορισμένους κανόνες, εκτελούν κατά κύριο λόγο τυποποιημένες διαδικασίες χωρίς την ανάγκη επίβλεψης από ανθρώπινο παράγοντα. Η χρήση τους συστήνεται σε περιπτώσεις περίπλοκων ενεργειών και πράξεων που απαιτούν την αλληλεπίδραση με πλήθος ΣΠ, έχουν μεγάλη επαναληπτικότητα και σημαντικό φόρτο εργασίας και αποτελούνται από δομημένα δεδομένα (structured data).

Στηρίζονται στη μηχανική αναπαραγωγή της αλληλεπίδρασης του ανθρώπου με τον υπολογιστή, μιμούμενοι ενέργειες που πραγματοποιούνται για την υλοποίηση της εργασίας με χρήση εφαρμογών, όπως την εκτέλεση ερωτημάτων αναζήτησης πληροφοριών, αντιγραφή και επικόλληση δεδομένων και την αλληλεπίδραση με το γραφικό περιβάλλον. Κυριότερο πλεονέκτημά τους είναι οι ελάχιστες απαιτήσεις από την υλικοτεχνική υποδομή που χρησιμοποιούν (hardware).

Η διαφοροποίηση των μηχανισμών για την αυτοματοποίηση διαδικασιών από τα συστήματα ΤΝ έγκειται στη δυνατότητα λήψης αποφάσεων. Τα RPAs στηρίζονται

αποκλειστικά σε πεπερασμένους κανόνες εκτέλεσης συγκεκριμένων πράξεων, χωρίς δυνατότητα διαφοροποίησης από αυτούς. Αντίθετα τα συστήματα ΤΝ, είτε ενσωματώνουν μηχανισμούς αυτό-εκπαίδευσης (self-trained)[6] είτε «εκπαιδεύονται» με δεδομένα επιτρέποντας τη διαφοροποίηση και τη λήψη απόφασης, αναφορικά με τα βήματα που θα ακολουθηθούν από το λογισμικό.

Η υιοθέτησή μηχανισμών RPA έχει ως βασικό στόχο τη βέλτιστη εκμετάλλευση των διαθέσιμων πόρων (ανθρώπινων και τεχνικών), τη βελτιστοποίηση των διαδικασιών και την μείωση του ενεχόμενου λειτουργικού κόστους και κινδύνου. Ωστόσο, η άκριτη και χωρίς κατάλληλες προϋποθέσεις υλοποίησή τους αποδεικνύεται ότι έχει αρνητικές επιπτώσεις τόσο στους εργαζόμενους όσο και στη δυνατότητα επίτευξης των στόχων που τίθενται.

1.4 ΣΕΕ και Γραμμές Άμυνας

Οι επιχειρήσεις χρειάζονται αποτελεσματικές δομές και διαδικασίες για την επίτευξη των στόχων τους και την υποστήριξη ενός ισχυρού πλαισίου διακυβέρνησης και διαχείρισης κινδύνων. Προς τούτο, επιβάλλεται η ανάπτυξη και η υιοθέτηση του Συστήματος Εσωτερικού Ελέγχου (ΣΕΕ), οι δομές του οποίου διευκολύνουν τη μετάβαση της επιχείρησης σε ένα ελεγχόμενο περιβάλλον.

Σύμφωνα με τα διεθνή πρότυπα και την ελληνική νομοθεσία το βασικό μοντέλο του ΣΕΕ είναι αυτό των τριών γραμμών[7]. Η πρώτη αποτελείται από τους επιχειρησιακούς ρόλους που σχετίζονται με τις δραστηριότητες της επιχείρησης, η δεύτερη εστιάζει σε θέματα διαχείρισης κινδύνων και η τρίτη αφορά κυρίως τον ΕΕ. Η αριθμητική διάκριση δεν υποδηλώνει σειρά ως προς την διαδοχικότητα ή την ιεραρχία κατά την ενεργοποίησή τους, καθώς τα τμήματα αυτά λειτουργούν παράλληλα και συμπληρωματικά.

Κοινός στόχος είναι η εγκαθίδρυση ενός αποτελεσματικού μοντέλου λειτουργίας, που οι κίνδυνοι αναγνωρίζονται έγκαιρα και λαμβάνονται υπόψη κατά τη λήψη αποφάσεων, βάσει μίας μελετημένης διαδικασίας που περιλαμβάνει την ανάλυση, τον προγραμματισμό, τις

[6] Με δυνατότητα αυτό-εκπαίδευσης μέσα από την αλληλεπίδραση με τον χειριστή τους και αξιολόγησης της ποιότητας του αποτελέσματος, προκειμένου να αποφεύγονται λάθη σε επόμενες αποφάσεις και να διαφοροποιούν αντίστοιχα τα αποτελέσματα.

[7] Νέα ονομασία του μοντέλου των τριών γραμμών άμυνας, σύμφωνα με τα παγκόσμια πρότυπα του ΙΙΑ. Η ορολογία «πρώτη», «δεύτερη» και «τρίτη» γραμμή διατηρείται για εξοικείωση.

απαιτούμενες ενέργειες, την εποπτεία και τις πιθανές επιπτώσεις. Επιπρόσθετα, με την υλοποίηση των απαραίτητων controls (αυτοματοποιημένων ή διαδικαστικών πρακτικών), ο ενεχόμενος κίνδυνος θα περιορίζεται σε επιθυμητά επίπεδα (risk appetite).

1.5 Computer Assisted Audit Techniques (CAATs)

Η ανάπτυξη των ΣΠ για την αποθήκευση και τη διαχείριση της πληροφορίας μετέβαλε τον παραδοσιακό τρόπο αποθήκευσής της από την έντυπη μορφή σε ηλεκτρονικές βάσεις και αποθήκες δεδομένων[8]. Αντίστοιχη μεταβολή σημειώνεται και στις τεχνικές ελέγχου των σχετικών στοιχείων, καθώς πέρα από την επισκόπηση των αποθηκευμένων σε εφαρμογές εγγράφων και δεδομένων, απαιτείται ανάλυσή για να επιβεβαιωθεί η ορθότητα και η ακρίβεια στην μετάδοσή τους σε άλλα συστήματα. Το περιβάλλον ελέγχου διογκώνεται και περιπλέκεται, λαμβάνοντας υπόψη τους όγκους και την ταχύτητα μετάδοσης των δεδομένων μεταξύ των συστημάτων.

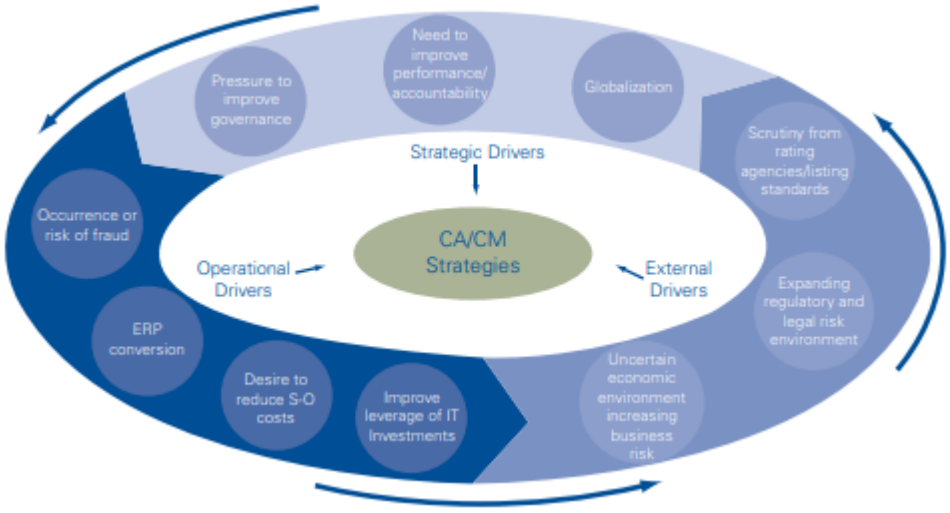
Στο πλαίσιο αυτό, αναπτύσσεται πλήθος λογισμικών που παρέχουν τη δυνατότητα στους ελεγκτές να σαρώσουν (θεωρητικά) άπειρες φορές τα δεδομένα προκειμένου να εντοπίσουν εξαιρέσεις και να αναλύσουν την αιτία για αυτές. Στα CAATs εντάσσονται και οι μηχανισμοί data analytics, που αναλύονται εκτενέστερα στη συνέχεια.

Εν γένει, τα CAATs κατηγοριοποιούνται αναλόγως του βάθους της ανάλυσης που θέλει να εφαρμόσει ο ελεγκτής και τα διαθέσιμα μέσα. Το πρώτο είδος αφορά σε ενσωματωμένους μηχανισμούς ελέγχου[9], που εξετάζουν τις καταχωρούμενες πληροφορίες έναντι συγκεκριμένων κριτηρίων για να διαπιστωθούν εξαιρέσεις, λάθη ή περιπτώσεις απάτης. Ο δεύτερος τύπος αφορά σε μηχανισμούς ανάλυσης των δεδομένων, με χρήση ή χωρίς ΤΝ και εξαγωγή συμπερασμάτων από τους χρήστες – ελεγκτές.

[8] Database και Data Warehouse για την αποθήκευση με δομημένο τρόπο των δεδομένων που αφορούν στη λειτουργία της επιχείρησης μαζί με πληροφορίες που αφορούν στα ίδια τα δεδομένα (data about data – metadata), αθροίσματα και διαστάσεις για ταχεία ανάλυση και ανάκτηση.
[9] Χρησιμοποιείται κυρίως σε μηχανισμούς «διαρκούς ελέγχου».

1.6 Διαρκής Έλεγχος

Ο όρος διαρκής έλεγχος αναφέρεται στην ευθύνη του ελεγκτή να αναλύει και να ελέγχει σε συνεχή βάση την αποτελεσματικότητα και την απόδοση (efficiency και effectiveness) των δικλείδων ασφαλείας (control) που έχουν υλοποιηθεί σε μία επιχείρηση για τον περιορισμό του κινδύνου σε αποδεκτά επίπεδα. Παρατηρείται αυξανόμενη χρήση τέτοιων μηχανισμών λόγω της υιοθέτησης από τις επιχειρήσεις λογισμικού που καλύπτει εξ ολοκλήρου τις επιχειρησιακές διαδικασίες (end-to-end), δημιουργώντας πρόσφορο έδαφος για την υλοποίηση έξυπνων μηχανισμών που διασφαλίζουν την ορθή λειτουργία του.



Εικόνα 1. Παράγοντες που επηρεάζουν τη στρατηγική των CA/CM (πηγή KPMG).

Ο όρος control στα Ελεγκτικά Πρότυπα του IIA ορίζεται ως «*οποιαδήποτε ενέργεια υλοποιούμενη από τη διοίκηση, το συμβούλιο και άλλα όργανα μίας επιχείρησης προκειμένου να διαχειριστούν τον κίνδυνο και να αυξήσουν την πιθανότητα επίτευξης των καθορισμένων αντικειμενικών σκοπών και στόχων. Η διοίκηση είναι υπεύθυνη για την οργάνωση, τον σχεδιασμό και παροχή κατευθυντηρίων οδηγιών με σκοπό την πραγματοποίηση ενεργειών προκειμένου να παράσχει τη διαβεβαίωση ότι οι στόχοι θα επιτευχθούν*» (Πλαίσιο Εφαρμογής ΕΕ σελ.17).

Στόχος του CA είναι η αυτοματοποίηση όλων των στοιχείων, των δεδομένων και των δεικτών που χρησιμοποιούνται από ένα μηχανογραφικό σύστημα, μία επιχειρησιακή διαδικασία, τις συναλλαγές αλλά και τα controls σε συνεχή ή περιοδική βάση, προκειμένου να χρησιμοποιηθούν στους ελέγχους που πραγματοποιούνται. Με τον τρόπο αυτό

ενισχύονται οι δυνατότητες του ΕΕ προκειμένου να διασφαλιστεί η συμμόρφωση με τις πολιτικές, τις διαδικασίες και τις κανονιστικές και εποπτικές απαιτήσεις. Υπό προϋποθέσεις, ενδέχεται να λειτουργούν και ως μηχανισμός έγκαιρης προειδοποίησης για τον εντοπισμό αστοχιών στη λειτουργία των controls, συγκριτικά με τις παραδοσιακές μεθόδους των τακτικών – περιοδικών ελέγχων.

Ο CA δεν πρέπει να συγχέεται με τη διαρκή παρακολούθηση, που αναφέρεται στην ύπαρξη αυτοματοποιημένων μηχανισμών ενημέρωσης αναφορικά με τη λειτουργία των συστημάτων και των controls, σύμφωνα με τις αρχικές προδιαγραφές υλοποίησης. Οι πληροφορίες στην περίπτωση αυτή χρησιμοποιούνται από τα εμπλεκόμενα μέρη για να ενισχύσουν τις δυνατότητες των συστημάτων καθώς και των μηχανισμών ελέγχου χωρίς να επιβαρύνεται η απόδοση και η λειτουργία του συστήματος (KPMG, 2018).

Μεταξύ των δύο υπάρχει κοινό πεδίο αναφορικά με τα κίνητρα υλοποίησής τους. Στρατηγικά και οι δύο τεχνικές στοχεύουν στην ενίσχυση της απόδοσης και στην εγκαθίδρυση ενός περιβάλλοντος επιμερισμού και ανάθεσης της ευθύνης. Από λειτουργικής άποψης έχουν κοινούς στόχους, όπως τον έγκαιρο εντοπισμό των κινδύνων, περιπτώσεων απάτης ή λανθασμένων ενεργειών καθώς και τη βέλτιστη χρήση των διαθέσιμων πόρων, συμπεριλαμβανομένων των ΣΠ.

Η υιοθέτηση CAATs συνδυαστικά με data analytics, συμπεριλαμβανομένης της ΤΝ, βοηθά σημαντικά στην υλοποίηση μηχανισμών CA και υπαγορεύεται από τις αντίστοιχες που πραγματοποιούνται στα ίδια τα ΣΠ των επιχειρήσεων, που μεταβάλλουν σημαντικά το περιβάλλον και τον τρόπο ελέγχου συγκριτικά με το παραδοσιακό μοντέλο.

1.7 Data Analytics και Big Data

Βασικός παράγοντας για την ανάπτυξη των μηχανισμών ΤΝ και την επίτευξη υψηλού βαθμού αυτοματοποίησης των διαδικασιών, αποτελούν τα τεχνολογικά επιτεύγματα στο χώρο της διαχείρισης δεδομένων. Οι εξελίξεις στο πεδίο είναι τόσο σημαντικές ώστε να εγκαθιδρύεται η αίσθηση ότι διανύουμε την περίοδο της 4ης βιομηχανικής επανάστασης.

Η ανάλυση δεδομένων και η δυνατότητα εξαγωγής συμπερασμάτων από παλιές και νέες πηγές για τη λειτουργία συστημάτων, τη λειτουργικότητα των διαδικασιών και τον έλεγχο, ορίζουν την περίμετρο των data analytics. Η αξία των παραπάνω μηχανισμών έγκειται στη

μετατροπή των απλών δεδομένων σε πληροφορίες που αποκαλύπτουν σημαντικά γεγονότα, επιλύουν προβλήματα ή αναδεικνύουν τάσεις. Αντίστοιχα, με την ανάλυση των συμπερασμάτων διαμορφώνουν επιχειρησιακές αποφάσεις, βελτιώνοντας τη διαδικασία λήψης τους και βοηθούν στην ανάπτυξη της επιχείρησης.

Πλέον, υφίστανται αμέτρητες πηγές πληροφοριών πέρα των παραδοσιακών – εγγραφές σε βάσεις, αρχεία κειμένου και υπολογιστικά φύλλα, μη δομημένες πληροφορίες όπως μηνύματα ηλεκτρονικού ταχυδρομείου, αρχεία πολυμέσων, ενώ σε αυτά προστίθενται πληροφορίες που αντλούνται από το διαδίκτυο και από συσκευές που παρακολουθούν και κυρίως καταγράφουν την ανθρώπινη δραστηριότητα. Παράλληλα, αναπτύχθηκαν και εξελίσσονται με ραγδαίο ρυθμό, ΣΠ που ενσωματώνουν με τις απαιτούμενες υπολογιστικές δυνατότητες για την επεξεργασία τους.

Επιπλέον, δημιουργούνται συστήματα αποθήκευσης, ανάκτησης και επεξεργασίας μεγάλων δεδομένων (big data), με ενσωματωμένους αλγορίθμους επεξεργασίας που διασφαλίζουν ταχύτητα και απόδοση. Οι παραδοσιακές βάσεις αντικαθίστανται από πολυσυλλεκτικά συστήματα που λειτουργούν σε υπολογιστικά νέφη (cloud computing) με χρήση τεχνικών κατανεμημένης επεξεργασίας και βελτιστοποίησης των χρησιμοποιούμενων πόρων στην εκτέλεση σύνθετων ερωτημάτων.

Η ύπαρξη κατάλληλων δεδομένων αποτελούσε και αποτελεί τη βάση για την ανάπτυξη της ΤΝ. Η καταλληλόλητά τους εξαρτάται κυρίως από την ποιότητα και από την ποσότητα των πληροφοριών με την οποία εκπαιδεύεται ένα σύστημα ΤΝ, αποτελώντας τους θεμέλιους λίθους της αξιοπιστίας του. Όσο πιο «καθαρά από λάθη» είναι οι διοχετευόμενες σε ένα σύστημα ΤΝ πληροφορίες κατά την εκπαίδευση του αλγορίθμου και την αξιολόγηση των αποτελεσμάτων επεξεργασίας, τόσο αυξάνεται η αξιοπιστία του. Επιπλέον, οι υπολογιστικοί αλγόριθμοι που χρησιμοποιούνται στα εν λόγω συστήματα ενδέχεται να απαιτούν μεγάλους όγκους δεδομένων ώστε να απαλλαγούν από ενδεχόμενα προκατάληψης (bias) αλλά και σφαλμάτων οφειλόμενα σε ακραίες τιμές (outliers) που ο αλγόριθμος διαχειρίζεται λανθασμένα[10].

[10] Οι εφαρμογές Data Analytics συνήθως απορρίπτουν τις ακραίες τιμές, ωστόσο η απόφαση λαμβάνεται από τον αναλυτή.

Εικόνα 2. Τα 7 βήματα για τα data analytics (πηγή Rafeq 2023)

Η ψηφιακή ανάλυση δεδομένων διακρίνεται σε τέσσερις (4) μορφές ανάλογα με την «ερώτηση» που καλείται να απαντήσει. Η πρώτη απαντά στο ερώτημα του τι έχει συμβεί (descriptive analytics), μέσα από την ανάλυση των τάσεων που παρουσιάζονται, ενώ στη δεύτερη διαπιστώνεται το γιατί έχει συμβεί κάποιο γεγονός (diagnostic analytics) και προσδιορίζεται η κύρια αιτία (root cause analysis). Βάσει των στοιχείων και των συμπερασμάτων που έχουν προκύψει από τα προηγούμενα στάδια, στην τρίτη μορφή γίνεται προσπάθεια να προβλεφθεί η πιθανότητα αντίστοιχα γεγονότα να συμβούν στο μέλλον (predictive analysis), αλλά και να καθοριστούν τα επόμενα βήματα βάσει του προσδιορισμού των απαιτούμενων ή πιθανών ενεργειών που προκύπτουν από τους παράγοντες που αξιολογούνται (Cote C. 2021).

1.8 Τεχνητή Νοημοσύνη και Αυτοματοποίηση

Η χρήση της ΤΝ εξαπλώνεται συνεχώς και σε πολλούς τομείς της οικονομικής δραστηριότητας, παράλληλα με το κοινωνικό της αποτύπωμα. Σύμφωνα με διεθνείς μελέτες για τον αντίκτυπο και την πρόοδο της, βρισκόμαστε στο σημείο που πλέον δεν θεωρείται αναδυόμενη τεχνολογία αλλά ώριμη, για την οποία δεν καλούμαστε να αντιμετωπίσουμε υποθετικά σενάρια στο πλαίσιο μιας ερευνητικής δραστηριότητας, αλλά πραγματικές καταστάσεις με θετικές και αρνητικές συνέπειες (Munoko, 2022).

Η ΤΝ προσφέρει δυνατότητες που στηρίζουν και απλοποιούν σημαντικό μέρος των ανθρώπινων δραστηριοτήτων, ενώ περιστασιακά δύναται να τις αντικαταστήσουν. Έχει διεισδύσει σχεδόν σε κάθε τομέα της ανθρώπινης δραστηριότητας: ρομποτική, αυτοκινητοβιομηχανία, ανθρώπινο δυναμικό, ιατρική, γεωργία και αλιεία, εκπαίδευση, ενέργεια, μεταφορές, στην ασφάλεια και σύντομα σε πολλές δημόσιες υπηρεσίες (οι πρώτες υλοποιήσεις τέθηκαν ήδη στη διάθεση του κοινού).

Ενδεικτικές υλοποιήσεις είναι σε συστήματα αυτόνομης οδήγησης, γεωεντοπισμού (geolocation), υπολογισμού θερμοκρασίας, υγρασίας και πίεσης για τα φυτά (γεωργία), προσωποποιημένης πληροφόρησης χρηστών στο διαδίκτυο και σε έξυπνα σπίτια (κατ' επέκταση συνδεδεμένες πόλεις και υποδομές). Στον τομέα της κυβερνοασφάλειας εφαρμόζεται στην ανάλυση δεδομένων που εισρέουν στα συστήματα προστασίας, ώστε αυτά να απαντούν σε τυχόν επιθέσεις βάσει προκαθορισμένων τεχνικών αναγνώρισης και αντιμετώπισης, ενώ στον τομέα της υγείας βρίσκει εφαρμογή στα πεδία της διάγνωσης με την εφαρμογή αλγορίθμων σε απεικονιστικές εξετάσεις και σε επίπεδο πρωτοβάθμιας φροντίδας μέσω σχετικών διαγνωστικών μηχανισμών. Σημαντική αποδείχθηκε η συνεισφορά της στην πανδημία Covid-19 αναφορικά με την ανίχνευση, τη διάγνωση και τον έλεγχο εξάπλωσης, βάσει αναλύσεων σχετικών δεδομένων.

Η ανάπτυξή της αλλάζει τις πρακτικές του ΕΕ που εφαρμόζονται από τις επιχειρήσεις. Ενδεικτικά, στη διεθνή βιβλιογραφία και τις έρευνες που πραγματοποιούνται από τα σχετικά Ινστιτούτα αναγνωρίζονται οι ακόλουθες πρακτικές εφαρμογές:

- Αυτόματη αντιπαραβολή πωλήσεων και παραστατικών (τιμολόγια, αποδείξεις κ.α.).
- Εντοπισμός συναλλαγών με υποψία απάτης.
- Εκτιμήσεις όγκου, πλήθους πωλήσεων και σχετικών στοιχείων, χρησιμοποιώντας αναλυτικά στατιστικά μοντέλα και δεδομένα προηγούμενων περιόδων εμπλουτιζόμενα με τις τρέχουσες τάσεις.
- Αξιολόγηση κινδύνων ευρημάτων του ελέγχου και συνολικά της ελεγχόμενης περιοχής ή διαδικασίας.
- Εκτίμηση των κινδύνων της ελεγχόμενης περιοχής βάσει ιστορικού.
- Ανάλυση των διαδικασιών και εντοπισμός πιθανών αδύναμων σημείων.
- Ψηφιακός έλεγχος εγγράφων, καταγραφή πρακτικών συναντήσεων, δημιουργία περιλήψεων και σύνταξη εκθέσεων.

Η ενσωμάτωση ΤΝ με σκοπό τον υψηλότερο βαθμό αυτοματοποίησης στις διαδικασίες ελέγχου είναι αρκετά περίπλοκη και με υψηλές απαιτήσεις. Η συνεχής διαφοροποίηση του περιβάλλοντος ελέγχου, δημιουργεί αντίστοιχες απαιτήσεις από τα συστήματα που χρησιμοποιούνται. Ωστόσο, οι ανάγκες εγκαθίδρυσης μηχανισμών CA και ενός σύγχρονου ΣΕΕ, παράλληλα με την ανάπτυξη της τεχνολογίας, οδηγούν τις εξελίξεις στην κατεύθυνση αυτή.

Ενδεικτικές περιπτώσεις αυτοματοποίησης αφορούν κυρίως μηχανικές και επαναλαμβανόμενες λειτουργίες, όπως τη δημιουργία μητρώων διαδικασιών για την προτεραιοποίηση και την αξιολόγηση των κινδύνων, την αξιολόγηση των στοιχείων που συλλέγονται διαρκούντος του ελέγχου, την αρχειοθέτηση της τεκμηρίωσης και την αξιολόγηση στοιχείων για την παρακολούθηση της υλοποίησης των διορθωτικών ενεργειών. Σημαντική συνεισφορά υπάρχει στον καθορισμό των στόχων του ελέγχου και την αυτοματοποιημένη επεξεργασία δεδομένων βάσει προκαθορισμένων ντετερμινιστικών σεναρίων.

1.9 Προσωπικά Δεδομένα και Έλεγχος

Οι διεργασίες του ελέγχου ανέκαθεν περιλάμβαναν την επεξεργασία δεδομένων είτε σε έντυπη είτε σε ηλεκτρονική μορφή. Δεδομένου του σύγχρονου τεχνολογικού πλαισίου που τοποθετείται ο έλεγχος, η επεξεργασία σημαντικού όγκου πληροφοριών καθίσταται αναπόφευκτη, μέρος των οποίων ενδεχομένως να αφορούν και προσωπικά δεδομένα πελατών ή και εργαζομένων της επιχείρησης. Ενδεικτικά, κατά τη διερεύνηση περιστατικών απάτης ο ελεγκτής ενδέχεται να χρειαστεί να επισκοπήσει βιντεοληπτικό υλικό[11], σε άλλες να επεξεργαστεί δεδομένα που αφορούν στην επαλήθευση συγκεκριμένων υπολογισμών (reconciliation/reperformance) προκειμένου να επιβεβαιώσουν την αποτελεσματικότητα και την απόδοση των σχετικών controls καθώς και να επισκοπήσει συμβόλαια και συμβάσεις με προμηθευτές ή πελάτες της επιχείρησης, προκειμένου να αποφανθεί για την ορθή εκτέλεσή τους.

[11] Που να απεικονίζονται και άλλοι εργαζόμενοι ή και πελάτες της επιχείρησης.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ 2018), εισήγαγε τις βασικές αρχές που θα πρέπει να τηρούνται σε κάθε περίπτωση επεξεργασίας δεδομένων. Ειδικότερα, στο άρθρο 5 του Κανονισμού αναφέρονται:

- Η αντικειμενικότητα, η νομιμότητα και η διαφάνεια της επεξεργασίας,
- ο περιορισμός του σκοπού,
- η αρχή της ελαχιστοποίησης και της αναλογικότητας,
- η ακρίβεια των δεδομένων και η ανάγκη επικαιροποίησής τους,
- η περιορισμένη διάρκεια τήρησης[12],
- η προστασία της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητάς τους και
- η λογοδοσία - απόδειξη συμμόρφωσης με τον Κανονισμό.

Η εφαρμογή των παραπάνω αρχών κατά την επεξεργασία δεδομένων από τον ΕΕ και τις υπόλοιπες γραμμές άμυνας μίας επιχείρησης είναι αδιαπραγμάτευτη και χωρίς προσαρμογές. Ο τρόπος εφαρμογής τους καθώς και οι ενδεχόμενες παρεκκλίσεις εντός των καθορισμένων από τον νόμο πλαισίων αναλύονται στη συνέχεια.

[12] Σύμφωνα με την πολιτική της επιχείρησης (data retention policy), που εκδίδεται με ευθύνη του Υπευθύνου Προστασίας Δεδομένων.

ΚΕΦΑΛΑΙΟ 2. ΘΕΣΠΙΣΗ ΚΑΙ ΟΡΓΑΝΩΣΗ ΣΥΣΤΗΜΑΤΟΣ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ – ΜΟΝΤΕΛΟ ΤΡΙΩΝ ΓΡΑΜΜΩΝ – ΔΙΑΣΦΑΛΙΣΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ, ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΚΑΙ ΕΣΩΤΕΡΙΚΟΣ ΕΛΕΓΧΟΣ

Το ΣΕΕ των επιχειρήσεων αποσκοπεί στον περιορισμό και τη διαχείριση των κινδύνων διασφαλίζοντας την εύρυθμη λειτουργία και διακυβέρνηση της επιχείρησης και παράλληλα τη συμμόρφωση με το κανονιστικό και το νομοθετικό πλαίσιο. Ο σκοπός αυτός επιτυγχάνεται με τη συμμετοχή του συνόλου των επιχειρησιακών περιοχών, τη σύνθεση των διαφορετικών ρόλων που ανατίθενται και υλοποιούνται από τις τρεις γραμμές που το αποτελούν.

Η διοίκηση βασίζεται στον έλεγχο για την παροχή ανεξάρτητης και αντικειμενικής διασφάλισης καθώς και συμβουλών για όλα τα θέματα συμπεριλαμβανομένης της προώθησης και της διευκόλυνσης της καινοτομίας και της βελτίωσης. Το μοντέλο των τριών γραμμών βοηθά τις επιχειρήσεις στην αναγνώριση των δομών και των διαδικασιών που θα συνεισφέρουν με τον καλύτερο τρόπο στην επίτευξη των στόχων και θα διευκολύνουν την εγκαθίδρυση ισχυρής διακυβέρνησης και επαρκούς διαχείρισης των κινδύνων.

Η ευθύνη της διοίκησης για την επίτευξη των στόχων της επιχείρησης περιλαμβάνει ρόλους της πρώτης και δεύτερης γραμμής[13]. Στην πρώτη, είναι άμεσα συνυφασμένοι με την παράδοση αγαθών και υπηρεσιών στους πελάτες της επιχείρησης, συμπεριλαμβανομένων των υποστηρικτικών λειτουργιών, ενώ στη δεύτερη γραμμή εστιάζουν στη διαχείριση του κινδύνου. Οι δύο πρώτες γραμμές μπορούν να αναμιχθούν ή να διαχωριστούν, ενώ οι ρόλοι της δεύτερης μπορεί να εκτείνονται πέρα από τη διαχείριση κινδύνων, περιλαμβάνοντας και το πλαίσιο διαχείρισης επιχειρηματικών κινδύνων (ERM). Ωστόσο, η ευθύνη για τη διαχείριση του κινδύνου είναι συνυφασμένη με την πρώτη γραμμή και παραμένει στην αρμοδιότητα της διοίκησης.

Ο έλεγχος όντας φύσει ανεξάρτητος, οφείλει να καταλήγει αβίαστα στα συμπεράσματα και στις απαιτούμενες διορθωτικές ενέργειες για τον περιορισμό των κινδύνων που αντιμετωπίζουν οι επιχειρήσεις κατά την λειτουργία τους και στους τομείς δραστηριότητάς τους. Με τον τρόπο αυτό παρέχει ανεξάρτητη και αντικειμενική διασφάλιση και συμβουλές για την επάρκεια και αποτελεσματικότητα της διακυβέρνησης και της διαχείρισης κινδύνων,

[13] Η χρήση του όρου «γραμμή» δεν αντιστοιχεί σε δομικά στοιχεία αλλά σε διαφοροποίηση ρόλων.

μέσω της κατάλληλης εφαρμογής συστηματικών και ενδελεχών διαδικασιών, εμπειρίας και βαθιάς γνώσης. Αναφέρει τα ευρήματά του στη διοίκηση και το ανώτατο διοικητικό όργανο για την προώθηση και διευκόλυνση της συνεχούς βελτίωσης. Παράλληλα, εκτιμά το βαθμό συμμόρφωσης με το εφαρμοστέο κανονιστικό και το νομοθετικό πλαίσιο.

Οι γραμμές εφόσον συνεργάζονται συλλογικά και ευθυγραμμίζονται μεταξύ τους, συμβάλλουν στη δημιουργία και στην προστασία της αξίας. Η ευθυγράμμιση επιτυγχάνεται μέσω της επικοινωνίας, της συμμετοχής και της συνεργασίας, διασφαλίζοντας την αξιοπιστία, τη συνοχή και τη διαφάνεια των πληροφοριών που απαιτούνται για τη λήψη αποφάσεων βάσει της προσέγγισης και της αξιολόγησης των κινδύνων.

Η υιοθέτηση μηχανισμών ΤΝ, η αυτοματοποίηση διαδικασιών και controls, σε όλες τις γραμμές, απαιτεί την αξιολόγηση των ενεχόμενων κινδύνων, την ανάλυση των επιπτώσεων, της προστιθέμενης αξίας για την επιχείρηση και τη διασφάλιση του περιορισμού των κινδύνων στα ανεκτά επίπεδα.

Το ΣΕΕ συνολικά μίας επιχείρησης και κατά συνέπεια και οι μονάδες ΕΕ[14], πρέπει να συμμορφώνονται με την κείμενη νομοθεσία και τις εποπτικές απαιτήσεις που διέπουν τη λειτουργία τους, ανάλογα με τον κλάδο δραστηριότητάς τους. Σημειώνεται, ότι ενώ σε Ευρωπαϊκό επίπεδο έχουν εκδοθεί σχετικά πρότυπα και κώδικες εδώ και αρκετά χρόνια, στην Ελλάδα η σχετική νομοθετική ρύθμιση εκδόθηκε το 2022.

2.1 Το ΣΕΕ στο Ελληνικό Δίκαιο

Ο νόμος 4849/2021 (ΦΕΚ-Α181/23.9.2022), αποτελεί την πρώτη προσπάθεια του Ελληνικού κράτους για τη ρύθμιση του ΣΕΕ αλλά και του επαγγέλματος του ελεγκτή, όντας φυσική συνέχεια του νόμου 4795/2021 (ΦΕΚ62/ 17.4.2021) που αφορούσε στο δημόσιο τομέα. Μέρος των άρθρων του τροποποιήθηκαν νομοθετικά καθώς και με υπουργικές αποφάσεις[15], κυρίως αναφορικά με τα κριτήρια που πρέπει να πληρούνται από τους ελεγκτές προκειμένου να ενταχθούν στο μητρώο που δημιουργήθηκε.

[14] Αποτελώντας ουσιαστικά την 3η γραμμή άμυνας.

[15] Αποτέλεσμα διαβουλεύσεων και συνεργασίας με τα Ελληνικά ινστιτούτα εσωτερικών ελεγκτών και επαγγελματικούς φορείς που δραστηριοποιούνται στον κλάδο με τον Ν. 5027/2023 .

Στους νόμους παρατίθενται βασικές έννοιες και ορισμοί που αφορούν στο επάγγελμα του ελεγκτή και συνολικά του ΣΕΕ που οφείλει να υφίσταται σε κάθε οργανισμό και επιχείρηση (δημοσίου και ιδιωτικού δικαίου). Περιλαμβάνονται οι θεμελιώδεις έννοιες του κινδύνου, της δικλείδας ασφαλείας (control), η διαχείριση κινδύνων και απειλών, το περιβάλλον ελέγχου κ.α. Επίσης, απαριθμούνται ενδεικτικώς και πρότυπα ΕΕ που το σύστημα που εγκαθιδρύεται στις σχετικές επιχειρήσεις θα πρέπει να λαμβάνει υπόψη κατά περίπτωση, με τις όποιες προσαρμογές όπου είναι απαραίτητο και εφικτό[16].

Σκοπός είναι η ενιαία ρύθμιση θεμάτων που αφορούν στο ΣΕΕ και τη λειτουργία των μονάδων ΕΕ στο δημόσιο αλλά και στον ιδιωτικό τομέα, ενισχύοντας με τον τρόπο αυτό τους μηχανισμούς λογοδοσίας και ακεραιότητας. Η εγκαθίδρυσή τους μέσα από ένα νέο ή με την τροποποίηση του υφιστάμενου μοντέλου διακυβέρνησης, αναμένεται να συμβάλλει σημαντικά στην επίτευξη των στόχων των επιχειρήσεων και των δημοσίων οργανισμών βάσει των αρχών της καλής διακυβέρνησης και της χρηστής διοίκησης, σύμφωνα με τα διεθνή ελεγκτικά πρότυπα και τις νομοθετικές προβλέψεις.

Θεσμοθετείται ο διασφαλιστικός και κριτικός ρόλος του ελεγκτή[17], προκειμένου να παρέχει «εύλογη διαβεβαίωση» στην επιχείρηση αναφορικά με την επίτευξη των στόχων, την αποτελεσματικότητα και την απόδοση των επιχειρησιακών λειτουργιών. Ο ρόλος αυτός εντάσσεται πλήρως στο πλέγμα των δραστηριοτήτων, των διαδικασιών και των δικλίδων ελέγχου που υιοθετεί ο φορέας, και συνθέτουν το ΣΕΕ του. Παράλληλα, ο ελεγκτής παρέχει διαβεβαίωση για την αξιοπιστία των δημοσιευόμενων οικονομικών καταστάσεων καθώς και άλλων αναφορών που αποστέλλονται στις εποπτικές αρχές και διασφαλίζει στο μέτρο του δυνατού τη συμμόρφωση με τους νόμους και τους κανονισμούς στο χώρο που δραστηριοποιείται η επιχείρηση.

Ο νόμος περιγράφει διεξοδικά τα δομικά στοιχεία και τη διάρθρωση του ΣΕΕ – τις τρεις γραμμές. Σε αυτές περιλαμβάνονται βασικές λειτουργίες μίας επιχείρησης που σχετίζονται με την διακυβέρνηση, τη διαχείριση κινδύνων και τη συμμόρφωση με το κανονιστικό πλαίσιο, τη διαμόρφωση πολιτικών και κανόνων και τη λειτουργία του ΕΕ. Δίνεται έμφαση

[16] Ενδεικτικά αναφέρονται το COSO (Committee of Sponsoring Organizations of the Treadway Commission), τα πρότυπα IPPF του IIA και το CoBIT που αποτελεί πλαίσιο διακυβέρνησης και διαχείρισης των ΠΣ (ISACA).

[17] Εναρμονισμένος με τα διεθνή πρότυπα

στην ανεξαρτησία της μονάδας ελέγχου και στις αρμοδιότητές της, αυτές της Επιτροπής Ελέγχου και των μονάδων που επιφορτίζονται με ρόλους διαχείρισης κινδύνων, αποτελώντας μέρος του παραπάνω σχήματος.

Ιδιαίτερη μνεία γίνεται στους στόχους των εμπλεκόμενων μονάδων καθώς και στην άσκηση των καθηκόντων τους στο πλαίσιο που έχει τεθεί. Υπογραμμίζεται η ανάγκη παρακολούθησης από τον ΕΕ της υλοποίησης των συστάσεων που έχουν εκδοθεί στο πλαίσιο των ελέγχων, στοχεύοντας στον περιορισμό των κινδύνων, στη βελτίωση των αδυναμιών και στη μείωση του βαθμού έκθεσης της επιχείρησης σε απειλές. Επιπρόσθετα, καθορίζεται η ανάγκη για ετήσιο πρόγραμμα αξιολόγησης και βελτίωσης της ποιότητας της μονάδας ΕΕ, προκειμένου να αποτιμάται ο βαθμός συμμόρφωσής της με τον κανονισμό λειτουργίας του και τα πρότυπα. Τέλος, αναγνωρίζεται η ανάγκη για Κώδικα Δεοντολογίας Εσωτερικών Ελεγκτών στον οποίο να περιλαμβάνονται οι «*αρχές που σχετίζονται με την επαγγελματική πρακτική και τους κανόνες επαγγελματικής συμπεριφοράς και ακεραιότητας που οφείλουν να ακολουθούν, λαμβάνοντας υπόψη τα Διεθνή Πρότυπα για την Επαγγελματική Εφαρμογή του Εσωτερικού Ελέγχου*».

Παρότι δεν γίνεται σαφής αναφορά στη χρήση τεχνικών ΤΝ ή αυτοματοποιημένων μεθόδων ελέγχου, διευκρινίζεται η υποχρεωτική συμμόρφωση με τους κώδικες δεοντολογίας και η υποχρεωτική άσκηση των σχετικών καθηκόντων από πρόσωπα εγγεγραμμένα στο μητρώο. Κατά συνέπεια, η χρήση των παραπάνω μεθόδων αναγνωρίζεται ως επικουρικό εργαλείο κατά τις φάσεις πραγματοποίησης του ελέγχου ή της αξιολόγησης των υφιστάμενων μηχανισμών. Αντίθετα, καθορίζονται οι βασικές αρχές του πλαισίου ελέγχου των ΣΠ μίας επιχείρησης, συμπεριλαμβανομένων όσων υιοθετούν ΤΝ σύμφωνα με τις κανονιστικές απαιτήσεις. Ο έλεγχος λειτουργίας των συστημάτων που χρησιμοποιούνται από τον ΕΕ εμπίπτει στις αρμοδιότητές του, καθώς στο πλαίσιο ελέγχου ποιότητας των παρεχόμενων υπηρεσιών εμπίπτει και ο έλεγχος των υποδομών και των πληροφοριακών συστημάτων που χρησιμοποιούνται από το σύνολο της επιχείρησης.

Σημειώνεται ο ενεργός ρόλος που αναλαμβάνει η τρίτη γραμμή (συνδυαστικά με τις άλλες δύο του ΣΕΕ) αναφορικά με το πλαίσιο διακυβέρνησης της επιχείρησης, μέσα από τον έλεγχό της λειτουργίας και την παροχή διαβεβαίωσης περί της επάρκειας του, με σκοπό την υποστήριξη της επιχείρησης στην επίτευξη των στόχων της. Στο πλαίσιο αυτό εντάσσονται

και οι συστάσεις / διορθωτικά μέτρα που προτείνονται, όπου απαιτείται, από τον ελεγκτή, προκειμένου να απαλειφθούν οι παρεκκλίσεις.

Παράλληλα, μέσα από τις αρμοδιότητες που ανατίθενται μέσω του άρθρου 10 αναφορικά με την «*αξιολόγηση της λειτουργίας, των δραστηριοτήτων και των προγραμμάτων του φορέα βάσει των αρχών της χρηστής δημοσιονομικής διαχείρισης*», η μονάδα ΕΕ και το ΣΕΕ εν γένει καλείται να συμβάλλει στην κοινωνική ευθύνη. Η δραστηριότητα των επιχειρήσεων έχει σημαντικό κοινωνικό αποτύπωμα, συμπεριλαμβανομένου του οικολογικού, για το οποίο ο ΕΕ καλείται να συμβάλει στη μεγιστοποίηση του οφέλους και την ελαχιστοποίηση του αρνητικού κοινωνικού αντικτύπου.

Σημειώνεται ότι τα τελευταία χρόνια, βάσει και των ιδιαιτέρως σημαντικών επιπτώσεων της κλιματικής αλλαγής, εντάχθηκε στις στρατηγικές των επιχειρήσεων αλλά και στους κινδύνους που αντιμετωπίζουν η έννοια του ESG (Environmental, Social, Governance) κινδύνου. Το ΣΕΕ οφείλει να λάβει υπόψη την ικανότητα της επιχείρησης να αντέξει και να διατηρηθεί βιώσιμη στις νέες συνθήκες σε αντιδιαστολή με την ανάγκη αύξησης των δεικτών ανάπτυξης. Παράλληλα, σημειώνεται η ανάγκη χρήσης ή/και παραγωγής προϊόντων και υπηρεσιών με τρόπο κοινωνικά ωφέλιμο, οικονομικά βιώσιμο και περιβαλλοντικά φιλικό. Τέλος το ΣΕΕ θα πρέπει να υποστηρίξει την κυκλική οικονομία και να ευθυγραμμίζεται με τις απαιτήσεις, υποστηρίζοντας ενεργά την ιδέα της ανακύκλωσης και της επανάκτησης των υπαρχόντων πόρων, με γνώμονα την ίδια τη φύση και τις λειτουργίες της σε όλη τη διάρκεια του κύκλου ζωής τους.

Υπογραμμίζεται η αναφορά στην ανάγκη και στην υποχρέωση των εσωτερικών ελεγκτών να εξετάζουν και να αξιολογούν την επάρκεια και την αποτελεσματικότητα του ΣΕΕ έναντι της πρόληψης και της καταπολέμησης της απάτης (εσωτερική και εξωτερική), μέσω της ανίχνευσης και της καταγραφής των σχετικών κινδύνων. Η αναλυτική διερεύνηση ενδέχεται να πραγματοποιηθεί από εξωτερικούς ελεγκτές[18] ή/και το αρμόδιο τμήμα της μονάδας ελέγχου, εφόσον υφίσταται.

Στα άρθρα του νόμου δίνεται έμφαση στην οργάνωση και τη λειτουργία της μονάδας ελέγχου, χωρίς να παραλείπονται οι βασικές αρχές που θα πρέπει να διέπουν τη λειτουργία της μονάδας διαχείρισης κινδύνων, που αποτελεί κομβικό στοιχείο του ΣΕΕ. Συνεπώς

[18] Εφόσον προβλέπεται στο κανονιστικό πλαίσιο

απαιτείται η σύσταση μονάδας με αρμοδιότητες την αναγνώριση και τη διαχείριση των κινδύνων, καθορίζοντας την οργάνωση, τη στελέχωση και τις εν γένει αρμοδιότητές της. Παράλληλα, απαιτείται η δημιουργία μητρώου κινδύνων (Risk Registry), παράλληλα με τη δημιουργία πλαισίου και πολιτικής διαχείρισής τους, που θα καταγράφονται οι αναγνωρισμένοι κίνδυνοι, η αξιολόγησή τους, οι υφιστάμενοι και τυχόν πρόσθετοι μηχανισμοί ελέγχου καθώς και οι υπεύθυνοι διαχείρισής τους[19].

Συμπερασματικά, ο νόμος αν και έπεται σημαντικά της εγκαθίδρυσης ΣΕΕ (και της σχετικής επαγγελματικής κατηγορίας), θέτει τις βάσεις και δημιουργεί το βασικό υπόβαθρο και πλαίσιο εντός των οποίων θα πρέπει να λειτουργούν οι επιχειρήσεις. Το εν λόγω πλαίσιο δεν αποκλίνει από τα ελεγκτικά πρότυπα βάσει των οποίων θα έπρεπε και λειτουργούν οι εμπλεκόμενες μονάδες, διασφαλίζοντας παράλληλα τις εφαρμοζόμενες πρακτικές. Οι αναφορές στην εμπιστευτικότητα των πληροφοριών που διαχειρίζεται το σύνολο των εμπλεκομένων μονάδων και γραμμών αλλά και στον κώδικα δεοντολογίας, εξασφαλίζουν την ευθυγράμμιση με τον ΓΚΠΔ αλλά και τους κανόνες ηθικής που θα πρέπει να διέπουν το επάγγελμα του ελεγκτή.

Ωστόσο, θα πρέπει να σημειωθεί ότι στο διάστημα που μεσολάβησε από την έκδοση του νόμου, ο Κώδικας Δεοντολογίας αντικαταστάθηκε από ένα σύνολο αρχών το οποίο κινείται στο ίδιο πλαίσιο. Ενδεχομένως, οι ευθείες αναφορές στις σχετικές απαιτήσεις και η συσχέτιση του νόμου με αυτές να εγείρουν θέμα επικαιροποίησης. Επίσης, η δημιουργία Μητρώου Ελεγκτών και ο καθορισμός των ελάχιστων απαιτήσεων για τον ελεγκτή, αποσκοπεί στο να εγκαθιδρυθεί ένα κοινώς αποδεκτό πλαίσιο που θα εφαρμοστεί τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Ωστόσο, μετά την αρχική εφαρμογή του[20] δεν έχει επιτευχθεί σε ικανοποιητικό επίπεδο η παρακολούθηση και ο έλεγχος της διαδικασίας, ώστε να μεγιστοποιηθεί βαθμός συμμόρφωσης και να μην ατονήσει οδηγώντας στην πρακτική κατάργηση των μέτρων και την επαναφορά στην προηγούμενη κατάσταση. Επιπλέον, με τις αλλαγές που επήλθαν με την τροποποίηση εντός του 2023 του σχετικού άρθρου, αποφεύχθηκε ο αποκλεισμός ελεγκτών που δεν εναρμονίζονταν πλήρως με τα καθορισμένα

[19] Σύμφωνα με την απαίτηση του νόμου στο μητρώο θα πρέπει να περιλαμβάνονται και οι κίνδυνοι διαφθοράς και απάτης (εσωτερικής και εξωτερικής).

[20] Με σημαντικούς αρωγούς τα ινστιτούτα που δραστηριοποιούνται στην Ελλάδα.

κριτήρια, αλλά ασκούσαν σχετικά καθήκοντα για σημαντικό χρονικό διάστημα πριν την έκδοση της νομοθεσίας.

Τέλος, οι ραγδαίες εξελίξεις στο χώρο της ΤΝ και οι επιπτώσεις που ενδέχεται να έχουν σε μεγάλο μέρος των σχετικών επαγγελμάτων μέσω της αυτοματοποίησης διεργασιών με ενδεχόμενη αντικατάστασή μέρους αυτών από ευφυή συστήματα, καθιστά απαραίτητη την επικαιροποίηση της σχετικής νομοθεσίας. Οι υποχρεώσεις που καθορίζονται τόσο από τη νομοθεσία της ΤΝ αλλά και αυτής για τον ΕΕ οφείλουν να συγκεραστούν προκειμένου να διαλευκανθούν τυχόν ασάφειες και να καθοριστούν επαρκώς ο νέος τρόπος οργάνωσης, τα όρια και κυρίως οι ευθύνες για τις αναλαμβανόμενες αποφάσεις.

2.2 Το ΣΕΕ στο Ευρωπαϊκό Δίκαιο

Σε επίπεδο ΕU δεν έχει υιοθετηθεί Κανονισμός αναφορικά με τον ΕΕ και τις απορρέουσες υποχρεώσεις. Αυτές ρυθμίζονται μέσα από ψηφίσματα του Ευρωπαϊκού Κοινοβουλίου και της Ευρωπαϊκής Επιτροπής αναφορικά με τις αντίστοιχες μονάδες που θα πρέπει να λειτουργούν στα θεσμικά όργανα της Ένωσης. Στους κανονισμούς και τις πολιτικές λειτουργίας που έχουν εκπονηθεί από τις μονάδες αυτές, διαφαίνεται η πλήρης υιοθέτηση και προσαρμογή στα πρότυπα που έχουν εκπονηθεί από τα παγκόσμια ινστιτούτα εσωτερικών ελεγκτών (ΙΙΑ και ISACA αναφορικά με τα ΣΠ). Άλλωστε και η ελληνική νομοθεσία στηρίζεται σε σημαντικό βαθμό σε αυτά, καθώς η καθολικότητά και η παγκόσμια εφαρμογή τους αποτελεί βασικό άξονα ανάπτυξής τους.

Τα πρότυπα παρέχουν δυνατότητα προσαρμογής και εξαιρέσεων, που αναγνωρίζεται και στις σχετικές αποφάσεις της Ένωσης, προκειμένου να καταστούν ελκυστικά και εφαρμόσιμα από όλες τις επιχειρήσεις και τους δημόσιους οργανισμούς που υφίσταται ΣΕΕ και μονάδα ελέγχου. Επιπρόσθετα, η ύπαρξη και η υιοθέτηση του Κώδικα Δεοντολογίας που έχει εκπονηθεί από το ΙΙΑ, επισφραγίζει την καθολική και ενιαία εφαρμογή των απαιτήσεων και των προτύπων από τις αντίστοιχες μονάδες και των τριών γραμμών στους οργανισμούς και τις επιχειρήσεις που λειτουργούν στην Ένωση.

2.3 Η 1η Γραμμή του ΣΕΕ

Η 1η γραμμή του μοντέλου αποτελείται κατά κύριο λόγο από τη διοίκηση και τις επιχειρησιακές περιοχές που ασχολούνται με δραστηριότητες όπως πωλήσεις, επαφή με πελάτες, παράδοση προϊόντων ή/και υπηρεσιών σε αυτούς, καθώς και κάποιες με «διοικητικές» αρμοδιότητες όπως η διαχείριση ανθρώπινων πόρων και κτηριακών υπηρεσιών. Ο ρόλος της στο ΣΕΕ αφορά στη διασφάλιση της ομαλούς λειτουργίας, της εξυπηρέτησης του πελάτη και στην παροχή των υπηρεσιών στο προκαθορισμένο επίπεδο και εντός του περιβάλλοντος κινδύνων που λειτουργεί. Τα controls σε αυτό το επίπεδο σχετίζονται με τον έλεγχο των παραπάνω δραστηριοτήτων, εστιάζοντας στον έγκαιρο εντοπισμό λαθών, υποβάθμισης της ποιότητας των υπηρεσιών που παρέχεται και στην έκθεση σε κινδύνους που δεν είχαν προβλεφθεί ή ξεπερνούν τα καθορισμένα όρια.

Από τη φύση τους οι επιχειρήσεις επιδιώκουν την αυτοματοποίηση των εργασιών τους, για τη διασφάλιση της ποιότητας και της ταχείας εξυπηρέτησης των πελατών τους. Συνεπώς, μεγάλο μέρος των σχετικών μηχανισμών εφαρμόζονται σε υπηρεσίες και διαδικασίες της πρώτης γραμμής. Ιστορικά, η αυτοματοποίηση εφαρμόστηκε πρωτίστως στις βιομηχανικές γραμμές παραγωγής κάθε λογής αγαθών, από τρόφιμα, micro-chips για υπολογιστές και φορητές συσκευές μέχρι οχήματα και τη βαριά βιομηχανία. Ως βασικοί στόχοι αναγνωρίζονται η αύξηση του ρυθμού παραγωγής και η τυποποίηση του τελικού αποτελέσματος, παράλληλα με την ποιοτική βελτίωσή του, και σε κάθε περίπτωση η διασφάλιση και ο έλεγχος των πρώτων υλών, της διαδικασίας παραγωγής και ο έγκαιρος εντοπισμός πιθανών προβληματικών προϊόντων.

Πρόσφατο παράδειγμα αυτοματοποίησης χειροκίνητης διαδικασίας της 1ης γραμμής σε ΠΙ, είναι η χρήση ρομποτικών συστημάτων για την παραλαβή, την ψηφιοποίηση[21] και την αρχειοθέτηση εγγράφων πιστοποίησης του πελάτη. Τα εν λόγω συστήματα αναλαμβάνουν και τον επιπρόσθετο ρόλο της εξακρίβωσης της συνάφειας και της γνησιότητας των στοιχείων, βάσει των ενσωματωμένων μηχανισμών. Ενδεικτικά για τις ταυτότητες πραγματοποιούνται αναζητήσεις σε κεντρική βάση ώστε να διαπιστωθεί αν έχει δηλωθεί ως κλαπείσα ή απολεσθείσα, ελέγχεται η αυθεντικότητα της βάσει των controls που

[21] Συχνά τα έγγραφα παραλαμβάνονται ψηφιοποιημένα (scanned) ή μέσα από ψηφιακές πλατφόρμες όπως το e-Gov.gr

ενσωματώνονται σε αυτές. Για το σκοπό αυτό και την «καταχώρηση» των αναγραφόμενων δεδομένων[22] στα συστήματα της επιχείρησης, οι εν λόγω μηχανισμοί συνδυάζονται και με έξυπνους αλγορίθμους για να αποφευχθούν διπλοεγγραφές αλλά και περιπτώσεις ψευδών καταχωρήσεων.

Παράλληλα, ολοένα και περισσότερα ΠΙ ενσωματώνουν μηχανισμούς ΤΝ σε διάφορες φάσεις των διαδικασιών τους. Η έγκριση ενός δανείου πλέον στηρίζεται σε σημαντικό ποσοστό στην επεξεργασία δεδομένων από τα ΣΠ των Τραπεζών και άλλων επιχειρήσεων αναζητώντας στοιχεία που συνδυαστικά θα οδηγήσουν σε αποφάσεις χαμηλού ρίσκου. Πρόσφατα διάφορες επιχειρήσεις και Τράπεζες υιοθέτησαν μηχανισμούς που επιτρέπουν την επεξεργασία των αξιολογήσεων που καταχωρούνται για ξενοδοχειακές επιχειρήσεις σε πλατφόρμες κρατήσεων (ανωνυμοποιημένες), ώστε να έχουν επιπρόσθετους τρόπους αξιολόγησης των υπηρεσιών που παρέχει η επιχείρηση που αιτείται τη χρηματοδότηση.

Η ενσωμάτωση μηχανισμών ΤΝ στις καθημερινές εργασίες των επιχειρήσεων συνδυαστικά με την υιοθέτηση των νέων τεχνολογιών, αναμένεται να μειώσει σημαντικά το λειτουργικό κόστος τους. Από σχετική έρευνα της Juniper Research για τον τραπεζικό κλάδο (ΣΕΠΕ, 2023), τα οικονομικά οφέλη υπολογίζονται σε περίπου $900 εκατ. μέχρι το 2028, λόγω εξοικονόμησης χρόνου κατά την εκτέλεση βασικών τραπεζικών λειτουργιών. Το σχετικό όφελος ωστόσο αντισταθμίζεται από τις αυξημένες απαιτήσεις για υπηρεσίες ηλεκτρονικής πιστοποίησης του πελάτη (κατά ~34% μέχρι το 2028, πηγή ΣΕΠΕ 2023) και από τις επενδύσεις για την περαιτέρω ενίσχυση των ψηφιακών τεχνολογιών.

Η υλοποίηση και η σταδιακή εφαρμογή ολοκληρωμένων ΣΠ που ενσωματώνουν μηχανισμούς ανάλυσης των δυναμικών δεδομένων που τροφοδοτούνται και των συνθηκών που διαμορφώνονται αποτελεί προτεραιότητα και ανάγκη των επιχειρήσεων. Ο βαθμός διείσδυσης των παραπάνω τεχνολογιών αναμένεται ισχυρός, καθώς οι μέχρι τώρα μελέτες έχουν επαρκώς αποδείξει ότι συμβάλλουν σημαντικά στη μείωση των λαθών – χειριστικών ή κατασκευαστικών, τη μείωση των κινδύνων που ενέχονται στη διαδικασία και αντίστοιχα αυτών που αναλαμβάνει η επιχείρηση.

[22] Χρησιμοποιώντας προηγμένους μηχανισμούς OCR (Optical Character Recognition) για την τυποποιημένη δομή που έχουν τα εν λόγω έγγραφα και τα metadata τους.

Η επαναληπτικότητα των διαδικασιών αυτών επιτρέπει την εκτίμησή των κινδύνων αρχικά κατά την φάση της υλοποίησης και μετέπειτα σε περιοδική βάση συνδυαστικά με τις αλλαγές που πραγματοποιούνται. Στο στάδιο αυτό υλοποιούνται τα ενσωματωμένα controls, που ανιχνεύουν σε διαρκή βάση αποκλίσεις ή παράτυπες ενέργειες τη στιγμή εμφάνισής τους. Ο εμπλουτισμός τους απαιτείται για την επίτευξη του εξυπηρετούμενου σκοπού.

Το ερώτημα είναι αν η αυξημένη χρήση μηχανισμών ΤΝ επηρεάζει ή απειλεί τις θέσεις εργασίας της 1ης γραμμής. Εύκολη απάντηση δεν υφίσταται και προκύπτει από την ανάλυση των ιστορικών στοιχείων. Στο παρελθόν η χρήση υψηλού βαθμού αυτοματοποίησης και μηχανολογικών υλοποιήσεων, οδήγησε σε ανάπτυξη της παραγωγής και σε σημαντικές εργασιακές αλλαγές. Ο εργασιακός χώρος είναι σε θέση να απορροφά τις σχετικές κρίσεις μέσα από την εκπαίδευση των στελεχών του στις νεοεισερχόμενες τεχνολογίες. Οι αρχικοί κραδασμοί και οι απώλειες που σαφέστατα θα εμφανιστούν, θα πρέπει να μετατραπούν σε ευκαιρίες μετασχηματισμού των επιχειρήσεων και των εργαζομένων, στο πλαίσιο ενός ολοκληρωμένου σχεδίου που εκπονεί η επιχείρηση.

2.4 Η 2η Γραμμή του ΣΕΕ

Η βασική αρμοδιότητα της 2ης γραμμής είναι η υποστήριξη στη διαχείριση των κινδύνων, και έγκειται στην παροχή συμπληρωματικής εμπειρίας, υποστήριξης, παρακολούθησης και διαχείρισης των προκλήσεων. Επιπλέον, είναι υπεύθυνη για τον προσδιορισμό των εσωτερικών και των εξωτερικών κινδύνων που προκύπτουν από το περιβάλλον που δραστηριοποιείται η επιχείρηση.

Για τα ΠΙ το ασταθές χρηματοοικονομικό περιβάλλον, το επίπεδο ανεργίας και ανάπτυξης στη χώρα που δραστηριοποιούνται καθώς και άλλου είδους γεωπολιτικές κρίσεις αποτελούν κινδύνους προς προσδιορισμό και επιμέτρηση. Στο πλαίσιο αυτό πραγματοποιούνται ασκήσεις βάσει προκαθορισμένων σεναρίων για συγκεκριμένους δείκτες, και αξιολογείται η επίπτωση σε αυτούς (ρευστότητα, πιστωτικός κίνδυνος κ.α.), προκειμένου να προσδιοριστούν τα απαραίτητα μέτρα για τον περιορισμό των κινδύνων σε ανεκτά επίπεδα σύμφωνα με το risk appetite που έχει καθοριστεί.

Οι εξωτερικοί κίνδυνοι που αντιμετωπίζουν οι επιχειρήσεις και ιδιαίτερα τα ΠΙ συνδέονται άμεσα με εξωτερικές απάτες και επιθέσεις με στόχο να βλάψουν τις επιχειρησιακές διαδικασίες. Οι περιπτώσεις αυτές ακολουθούν τις εξελίξεις στον χώρο της τεχνολογίας, αλλάζοντας συνεχώς μορφή και απειλώντας σε συνεχή βάση τη λειτουργία τους (π.χ. επιθέσεις Distributed Denial of Service - DDoS) ή τους πελάτες και τις καταθέσεις τους (π.χ. phishing για την υποκλοπή των χαρακτηριστικών εισόδου στα εναλλακτικά δίκτυα, ATM skimming με την αντιγραφή καρτών και την ανάληψη χρηματικών ποσών). Παράλληλα, δεν έχουν εξαλειφθεί περιπτώσεις που πελάτες παρέχουν ψευδή στοιχεία πιστοποίησης, με σκοπό την πρόσβαση σε λογαριασμούς καταθέσεων τρίτων ή αιτούμενοι δάνεια που δεν αποπληρώνονται.

Ο κίνδυνος εσωτερικής απάτης είναι άρρηκτα συνδεδεμένος με τις αδυναμίες των διαδικασιών και των ΣΠ που χρησιμοποιούν οι επιχειρήσεις. Αφορούν σε προβλήματα του μοντέλου λειτουργίας μίας επιχειρησιακής περιοχής, γίνονται αντικείμενο εκμετάλλευσης από το προσωπικό και οδηγούν σε οικονομική ή λειτουργική ζημία ή έχουν αντίκτυπο σε μη μετρήσιμα στοιχεία όπως η φήμη της. Η διαρροή προσωπικών δεδομένων πελατών ή της λίστας των πελατών πέρα από τη οικονομική ζημία που θα επιφέρει, θα έχει σημαντικό αντίκτυπο και στη δημόσια εικόνα της επιχείρησης.

Η ΤΝ και η αυτοματοποίηση διαδικασιών βρίσκουν πρόσφορο έδαφος στο πεδίο δράσης της 2ης γραμμής. Χρησιμοποιούνται για την επιμέτρηση των κινδύνων και την πρόβλεψη του αντίκτυπου αναλόγως των παραμέτρων, που δεν θα ήταν εφικτή χωρίς τις προηγμένες τεχνικές ανάλυσης δεδομένων και την ΤΝ. Η εναλλαγή και η προσαρμογή των παραμέτρων, βάσει ιστορικών στοιχείων που τροφοδοτούνται τα εν λόγω συστήματα, επιτρέπουν την πραγματοποίηση απαιτητικών και περίπλοκων βραχυπρόθεσμων και μακροπρόθεσμών προβλέψεων, ακόμη και πέρα της πενταετίας. Στα ΠΙ σειρά τέτοιων στοιχείων υπολογίζονται για τον πιστωτικό κίνδυνο[23], τον λειτουργικό κίνδυνο καθώς και για θέματα ρευστότητας[24].

Η ανάπτυξη, η εφαρμογή και η συνεχής βελτίωση των πρακτικών διαχείρισης κινδύνων (συμπεριλαμβανομένων των controls) σε επίπεδο διαδικασιών, συστημάτων και επιχείρησης

[23] Πιθανότητα αθέτησης, αναγνώρισης μη εξυπηρετούμενων δανείων, συστήματα έγκαιρης προειδοποίησης για μη εξυπηρετούμενα δάνεια, απώλειες σε περίπτωση αθέτησης.
[24] Άμεση απαίτηση υπολοίπων από λογαριασμούς καταθέσεων, παράγωγα, ομόλογα κ.α.

περιλαμβάνονται στις αρμοδιότητές της 2ης γραμμής. Οι πρακτικές οφείλουν να συμμορφώνονται με την επιχειρησιακή στρατηγική και τα καθορισμένα επίπεδα risk appetite/tolerance. Οι μηχανισμοί ΤΝ και αυτοματοποίησης συνεισφέρουν ουσιαστικά μέσα από την εγκαθίδρυση ενός περιβάλλοντος CM, αξιολόγησης της επάρκειας των controls και προσδιορισμού των απαιτούμενων διορθωτικών ενεργειών. Επιπλέον, στις υποχρεώσεις της 2ης γραμμής εντάσσονται ο καθορισμός και η, ενδεχομένως, αυτοματοποιημένη παρακολούθηση της επίτευξης των στόχων διαχείρισης κινδύνων, όπως:

- συμμόρφωση με νόμους και κανονισμούς,
- αποδεκτή ηθική συμπεριφορά,
- controls,
- ασφάλεια πληροφοριών και της τεχνολογίας,
- βιωσιμότητα, και διασφάλιση ποιότητας.

Οι αναλύσεις που πραγματοποιούνται από τις εμπλεκόμενες μονάδες αποτυπώνονται σε εκθέσεις που υποβάλλονται στη διοίκηση της επιχείρησης και αποτυπώνουν με σαφήνεια την επάρκεια και την αποτελεσματικότητα της διαχείρισης κινδύνων, συμπεριλαμβανομένων των controls, καθώς και τις ενέργειες που απαιτούνται ή είναι σε εξέλιξη από τις επιχειρησιακές μονάδες των δύο πρώτων γραμμών για τον περιορισμό τους.

2.5 Η 3η Γραμμή του ΣΕΕ

Ο ρόλος της 3ης γραμμής[25] είναι να παρέχει ανεξάρτητη και αντικειμενική διασφάλιση συμπεριλαμβανομένων συμβουλών για την επάρκεια και την αποτελεσματικότητα της διακυβέρνησης και της διαχείρισης των κινδύνων που εκτίθεται η επιχείρηση. Σε ορισμένες περιπτώσεις επιφορτίζεται με την εποπτεία, τον έλεγχο, την έρευνα, την αξιολόγηση λειτουργιών καθώς και την αποκατάστασή τους[26]. Τα ευρήματα αναφέρονται στην διοίκηση[27] ώστε να διασφαλίζεται η προώθηση των απαιτούμενων μέτρων έναντι των κινδύνων που εκτίθεται η επιχείρηση αλλά και η διασφάλιση της συνεχούς βελτίωσής του.

[25] Εσωτερικός έλεγχος ή άλλη αρμόδια μονάδα που έχουν ανατεθεί τα σχετικά καθήκοντα.
[26] Οι εν λόγω λειτουργίες ενδέχεται να είναι ανεξάρτητες μονάδες ή εσωτερικά στην μονάδα ΕΕ.
[27] Ή/Και στο ανώτατο διοικητικό όργανο της επιχείρησης.

Ο εσωτερικός σε σχέση με τον εξωτερικό έλεγχο διαφέρουν στο αντικείμενο (τι ελέγχεται), στο υποκείμενο (ως τα πρόσωπα που τον διενεργούν και τα προσόντα τους), καθώς επίσης στις διαδικασίες και στις τεχνικές του. Ειδικότερα, οι εξωτερικοί έλεγχοι διακρίνονται σε αυτούς που πραγματοποιούνται κατ' απαίτηση του κανονιστικού πλαισίου και της σχετικής νομοθεσίας, σε αυτούς των εποπτικών αρχών και σε όσους αιτείται η επιχείρηση.

Οι έλεγχοι που πραγματοποιούνται στα ΠΙ ανά τριετία από εξωτερικούς ελεγκτές για την αξιολόγηση της συμμόρφωσής με τις απαιτήσεις της ΠΔΤΕ 2577 ή ο έλεγχος των οικονομικών καταστάσεων μίας επιχείρησης από ορκωτούς ελεγκτές[28], αποτελούν παραδείγματα εξωτερικών ελέγχων. Επίσης, εταιρίες εισηγμένες στο Χρηματιστήριο της Νέας Υόρκης οφείλουν να έχουν καταγεγραμμένα τα controls για την ασφαλή χρηματοοικονομική διαχείριση, να αυτοαξιολογούνται και να πιστοποιούνται ετησίως για την επάρκεια τους ο διευθύνων σύμβουλος, ο οικονομικός διευθυντής και ο εξωτερικός ελεγκτής. Επίσης, επιβάλλεται να διενεργούν ετησίως δοκιμές αξιολόγησης του ΣΕΕ της εταιρείας, που θα διαφέρουν ανάλογα με τη σημαντικότητα της ελεγχόμενης διαδικασίας (section 404 – SOX 2002).

Οι έλεγχοι από την ΤτΕ, την επιτροπή κεφαλαιαγοράς ή οποιαδήποτε άλλη αρχή σε εποπτευόμενη δημόσια ή ιδιωτική επιχείρηση, εντάσσονται στην δεύτερη κατηγορία και έχουν σκοπό τη διερεύνηση συμβάντων και την αξιολόγηση της λειτουργίας της επιχείρησης ως προς μία ή περισσότερες δραστηριότητες. Στην κατηγορία αυτή εντάσσονται οι εποπτικοί έλεγχοι από αρχές της EU, στο πλαίσιο των αρμοδιοτήτων τους και σε συνεργασία με τις τοπικές αρχές[29]. Τέλος, ένας οργανισμός στο πλαίσιο λήψης πιστοποιήσεων σύμφωνα με κάποιο πρότυπο ISO[30] ελέγχεται απαραίτητα προ της πιστοποίησης.

[28] Αναλόγως του μεγέθους της εταιρίας όπως ορίζεται στον Ν.4336/2015 και τα άρθ.1 και 2 του Ν.4308/2014.

[29] Όπως ο Single Supervisory Mechanism (SSM), για την εποπτεία στο τραπεζικό σύστημα της EU, σε συνεργασία με τις τοπικές κεντρικές τράπεζες.

[30] 9001 σύστημα ποιότητας, 27001 ασφάλεια ΠΣ, 20001 παροχή υπηρεσιών πληροφορικής

ΚΕΦΑΛΑΙΟ 3. ΩΦΕΛΗ ΚΑΙ ΚΙΝΔΥΝΟΙ ΑΠΟ ΤΗΝ ΑΥΤΟΜΑΤΟΠΟΙΗΣΗ ΣΤΑ ΣΕΕ

Η χρήση αυτοματοποιημένων συστημάτων εστιάζει στην παραγωγή αγαθών και στην παροχή υπηρεσιών από τις επιχειρήσεις, την υλοποίηση αντίστοιχων controls για τον έλεγχο, είτε ως μέρος της εφαρμοζόμενης ολοκληρωμένης λύσης, είτε ως ξεχωριστά συστήματα και εφαρμογές. Τα τελευταία δύνανται να παρέμβουν στη διαδικασία εφόσον διαπιστώνονται αποκλίσεις από τα καθορισμένα επίπεδα, να παράγουν αναφορές σφαλμάτων (exception reports) και να αποστέλλουν αυτοματοποιημένα ειδοποιήσεις για την ανάληψη και την υλοποίηση ενεργειών από τους εμπλεκόμενους. Η χρήση τους δεν περιορίζεται στην 1η και τη 2η γραμμή αλλά επεκτείνεται πλέον και στον έλεγχο.

Οι πρώτοι αυτοματισμοί αφορούσαν ρομποτικούς μηχανισμούς στις γραμμές παραγωγής αγαθών και ελέγχου ποιότητας του αποτελέσματος στο τέλος τους ή/και σε κάθε στάδιο της. Ο βαθμός παρέμβασής τους εξαρτάται από τη χρήση, ενώ σε σημαντικό μέρος αυτών ο ανθρώπινος παράγοντας εξακολουθεί να λαμβάνει την τελική απόφαση.

Η πλέον διαδεδομένη αυτοματοποιημένη λύση για την παροχή υπηρεσιών είναι τα bots που χρησιμοποιούνται κυρίως σε μηχανισμούς υποστήριξης χρηστών και πελατών της επιχείρησης[31]. Οι τεχνολογικές εξελίξεις, ωστόσο, βοηθούν στην περαιτέρω δημιουργία μηχανισμών και τεχνικών που βρίσκουν εφαρμογή σε ολοένα και περισσότερα πεδία, συμπεριλαμβανομένων περίπλοκων και απαιτητικών διαδικασιών όπως η διαχείριση αιτημάτων δανείων, δημιουργίας τραπεζικής σχέσης με το άνοιγμα λογαριασμού και την ταυτοποίηση του πελάτη ή ακόμα και την έγκριση πραγματοποίησης συναλλαγής μέσω ηλεκτρονικής τραπεζικής.

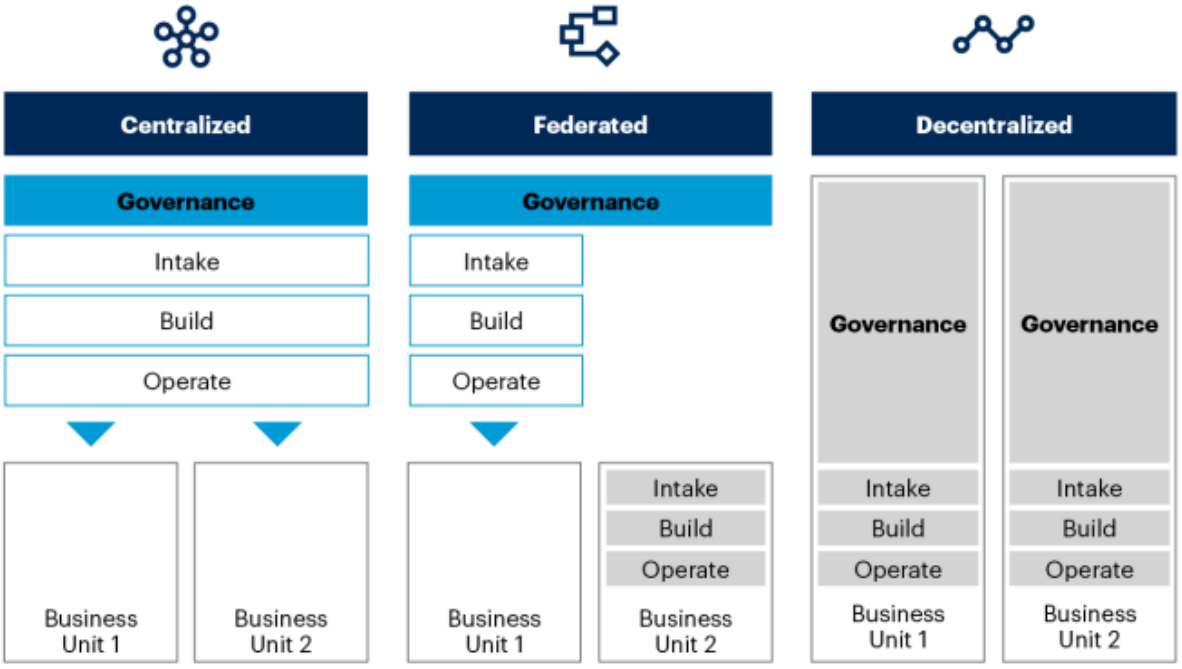
Η λειτουργία των controls στις περιπτώσεις αυτές στοχεύει στη διασφάλιση ότι η συναλλαγή ή η υπηρεσία που παρέχεται στον πελάτη συμφωνεί με τα πρότυπα και τα καθορισμένα επίπεδα. Η παρεμβατικότητά τους στη διαδικασία καθορίζεται από τη χρήση και ενδέχεται να οδηγούν στην απόρριψη της συναλλαγής, στη μη παροχή της υπηρεσίας, στην έγκρισή της είτε στην προώθησή της στο επόμενο επίπεδο διαχείρισης.

[31] Αποτέλεσαν την απαρχή των αυτοματοποιημένων μηχανισμών παροχής υπηρεσιών σε πελάτες.

3.1 Αυτοματοποίηση Επιχειρησιακών Διαδικασιών

Στην προσπάθεια μεγιστοποίησης του οφέλους που προκύπτει από την υιοθέτηση σύγχρονων τεχνολογιών σε καθημερινές εργασίες, μείωσης του λειτουργικού κόστους και επίτευξης των ποιοτικών στόχων που έχουν τεθεί, η αυτοματοποίηση μέρους των υπηρεσιών που παρέχονται στους πελάτες και εσωτερικών λειτουργιών/διεργασιών αποτελεί μονόδρομο για τις σύγχρονες επιχειρήσεις. Για τη διασφάλιση της διαχείρισης των κινδύνων, η εκάστοτε επιχείρηση οφείλει να σχεδιάζει, να υλοποιεί, να παρακολουθεί και να αξιολογεί τα κατάλληλα controls που θα διέπουν την αυτοματοποιημένη διαδικασία. Βασικός στόχος είναι ο περιορισμός των ενεχόμενων κινδύνων σε αποδεκτά πλαίσια, χωρίς να τίθενται εμπόδια στην υλοποίηση και στην αποκόμιση του προσδοκώμενου οφέλους.

Για την επιλογή της κατάλληλης μεθόδου, πρέπει να αξιολογείται το συνολικό φάσμα των κινδύνων που ενέχονται στη διαδικασία. Η διαχείριση των κινδύνων εξαρτάται σε σημαντικό βαθμό και από το επιχειρησιακό μοντέλο που θα επιλέξει η επιχείρηση: κεντροποιημένο, ενοποιημένο ή αποκεντρωμένο (Gartner, 2021).



Εικόνα 4. Οι τρεις τύποι των λειτουργικών μοντέλων RPAs (πηγή Gartner / Deloitte)

Στην πρώτη μέθοδο, ορίζεται ένα κεντρικό σημείο/μονάδα που έχει την ευθύνη τυποποίησης των διαδικασιών και των πολιτικών και συντονισμού του συνόλου των επιχειρησιακών μονάδων. Στην περίπτωση αυτή η εποπτεία των μηχανισμών, η διαχείριση

κινδύνων και ο έλεγχος πραγματοποιείται κεντρικά, βοηθώντας σημαντικά στην αύξηση του επιπέδου ασφαλείας και τη βελτιστοποίηση των τεχνικών υλοποιήσεων[32]. Αντίστοιχα, στο αποκεντρωμένο μοντέλο, ελλείψει κεντρικής διαχείρισης, κάθε επιχειρησιακή μονάδα ενθαρρύνεται και δύναται να υλοποιήσει σχετικά συστήματα και αυτοματοποιήσεις, βάσει του δικού της πλαισίου λειτουργίας, των αναγκών της, των προτύπων που ακολουθεί και των απαιτήσεων για τη διαχείριση των κινδύνων που προκύπτουν. Στο υβριδικό μοντέλο, το πλαίσιο καθορίζεται σε κεντρικό επίπεδο και καλύπτει το σύνολο της επιχείρησης, ωστόσο οι ειδικοί σε επίπεδο επιχειρησιακής μονάδας θα καθορίσουν και θα υλοποιήσουν τα σχετικά συστήματα.

Εν γένει, από την πρακτική εφαρμογή των ρομποτικών συστημάτων σε επιχειρησιακές διαδικασίες, προκύπτει η ανάγκη περιορισμού των κινδύνων που ελλοχεύουν από την υλοποίησή τους. Οι μηχανισμοί ελέγχου που θα υλοποιηθούν θα πρέπει να επιλεγούν κατάλληλα προκειμένου να μην αυξηθούν τα επίπεδα κινδύνου που εκτίθεται συνολικά η επιχείρηση αλλά και να μην διαταραχθεί η διαχείρισή τους. Παράλληλα, θέτουν πλήθος προκλήσεων για τον ΕΕ, καθώς απαιτούν εξειδίκευση, τεχνικές γνώσεις και εις βάθος ανάλυση.

3.1.1 Κίνδυνος διακυβέρνησης (Governance Risk).

Ο κίνδυνος διακυβέρνησης αφορά στην έλλειψη controls της απόδοσης και της λειτουργίας των αυτοματοποιημένων λύσεων που υιοθετούνται κεντρικά και τοπικά[33], καθώς και όσων έχουν μπει σε λειτουργία. Παράλληλα, η ύπαρξη τεχνικών που παρακάμπτουν τους μηχανισμούς ελέγχου, ευκαιριακά ή συστηματικά, θα πρέπει να αντιμετωπίζονται κατά τις φάσεις σχεδιασμού και υλοποίησης.

Η διαχείριση των κινδύνων που σχετίζονται με την παρακολούθηση και τη συνολική λειτουργία των controls και των αυτοματοποιημένων λύσεων είναι κρίσιμη, καθώς ενδέχεται να οδηγήσει είτε στην αποτυχία τους είτε τελικά στη μη συμμόρφωση με τις απαιτήσεις και τους κανονισμούς της επιχείρησης και του νομοθετικού πλαισίου.

[32] Ασφάλεια προσβάσεων, συμμόρφωση με εσωτερικές διαδικασίες, το κανονιστικό και νομοθετικό πλαίσιο, ελλείψεις ή παραλείψεις στις τεχνικές υλοποιήσεις κ.α.
[33] Μηχανισμοί που αναπτύσσονται στο πλαίσιο μίας επιχειρησιακής μονάδας.

3.1.2 Λειτουργικός Κίνδυνος (Operational Risk).

Η γενική προσέγγιση στην αυτοματοποίηση διαδικασιών έγκειται στην υλοποίησή της σε μικρότερης κλίμακας υπό-διαδικασίες, που με τη σειρά τους αποτελούν μέρος μίας ευρύτερης ροής εργασιών. Η απευθείας εφαρμογή της σε μεγάλης κλίμακας διεργασίες ενέχει τον κίνδυνο συνολικής αποτυχίας του εγχειρήματος ή/και εκπτώσεων στα απαραίτητα controls προκειμένου να επιτευχθεί η ορθή διαχείριση και παρακολούθηση.

Παράλληλα, θα πρέπει να διασφαλιστεί η διαχείριση των μελλοντικών αλλαγών, που εν γένει δεν είναι εύκολο να υλοποιηθούν με άμεσο τρόπο σε περίπλοκες ενοποιημένες ροές. Στις περισσότερες περιπτώσεις, το εγχείρημα αποτυγχάνει καθώς δημιουργούνται προβλήματα στη λειτουργία του μηχανισμού. Χαρακτηριστικό παράδειγμα αποτελούν τα bots που χρησιμοποιούνται για την επικοινωνία του πελάτη με την επιχείρηση και την παροχή υποστήριξης. Η υλοποίηση ενός μηχανισμού που καλύπτει το σύνολο των πιθανών ερωτημάτων του χρήστη μίας υπηρεσίας ενδέχεται να απαιτεί υψηλότερο κόστος συντήρησης και μεγαλύτερη εξειδίκευση για την υποστήριξη και την προσαρμογή σε ενδεχόμενη αλλαγή. Ωστόσο, η κατάτμηση της υπηρεσίας σε μικρότερα τμήματα διευκολύνει την υποστήριξη, τη μεταβολή των υφιστάμενων μηχανισμών και τη μελλοντική επέκτασή μέσω των αλλαγών σε αυτούς, την κατάργηση κάποιου ή/και την προσθήκη νέων.

Η επάρκεια των controls και η επικοινωνία μεταξύ των εμπλεκόμενων επιχειρησιακών μονάδων αποτελούν αναπόσπαστα τμήματα του ΣΕΕ που διέπει την αυτοματοποιημένη διαδικασία. Υπερβολικά μεγάλο πλήθος, μέσα από πολλαπλά στάδια ελέγχου και προκειμένου να καλύψουν τις ανάγκες πολλαπλών επιχειρησιακών μονάδων, έχει τελικά αντίκτυπο στην ίδια τη λειτουργία και στην απόδοση. Ενδεικτικά η παραγωγή πολλαπλών εξαιρέσεων ή η ενημέρωση και η λήψη εγκρίσεων σε μεγάλο πλήθος σταδίων της διαδικασίας, προξενούν τελικώς συνεχείς διακοπές και καθυστέρηση στην ολοκλήρωσή της.

3.1.3 Οργανωτικός Κίνδυνος (Organizational Risk).

Οι επιφορτισμένες μονάδες με τον έλεγχο των αυτοματοποιημένων διαδικασιών οφείλουν να διαθέτουν επαρκείς πόρους για την εκτέλεση των καθηκόντων που τους έχουν ανατεθεί, ώστε να μην δημιουργούνται κενά ή λάθος προτεραιοποιήσεις στη διαχείριση των

κινδύνων. Παράλληλα, η επαρκής εκπαίδευση και εξειδίκευση αποτελεί σημαντικό παράγοντα για την επιτυχία του εγχειρήματος για το σύνολο των εμπλεκομένων μερών. Η συχνότητα, ο βαθμός και ο τρόπος παρέμβασης καθενός από τα εμπλεκόμενα μέρη θα πρέπει να έχει οριστεί στις διαδικασίες και στο πλαίσιο διακυβέρνησης.

Οι παραπάνω οργανωτικές απαιτήσεις αποτελούν και την απάντηση στη διαχείριση πλεονάζοντος προσωπικού που προκύπτει μετά την αυτοματοποίηση των διαδικασιών. Η κατάλληλη εκπαίδευση και χρησιμοποίησή του με πιο ελεγκτικό ρόλο προκειμένου να διασφαλιστεί η ορθή λειτουργία της αυτοματοποιημένης διαδικασίας είναι κομβικής σημασίας, καθώς πρόκειται συνήθως για πόρους με σημαντική εξειδίκευση και γνώση του αντικειμένου.

3.1.4 Τεχνολογικός Κίνδυνος (Technological Risk).

Η άκριτη υιοθέτηση των νέων τεχνολογιών ενδέχεται να θέσει στο περιθώριο την υλοποίηση controls, που σε πολλές περιπτώσεις είναι κρίσιμα για τη βιωσιμότητα και την ορθή λειτουργία της διαδικασίας. Επιπλέον, η δημιουργία «τοπικών» μονάδων πληροφορικής (shadow IT) με αυτόνομη λειτουργία και χωρίς να υιοθετούν τις επίσημες διαδικασίες της επιχείρησης ή παρακάμπτοντας τα υφιστάμενα controls, αποτελεί σημαντικό τεχνολογικό κίνδυνο που χρήζει μέτρων περιορισμού και αντιμετώπισης[34].

Θεμελιώδες σημείο αποτελεί και η διαχείριση των εγγενών κινδύνων που προκύπτουν από τις τεχνικές υλοποιήσεις. Οι εν λόγω μηχανισμοί είναι σχεδιασμένοι ώστε να λειτουργούν κατά κύριο λόγο χωρίς την ανθρώπινη παρέμβαση. Για τον σκοπό αυτό αποδίδονται σημαντικά δικαιώματα πρόσβασης στα συστήματα ακόμα και σε επίπεδο διαχειριστή σταθμών εργασίας, δικτυακών πόρων ή και διακομιστών (servers), καθιστώντας τα επισφαλή και αντικείμενο εκμετάλλευσης για εσωτερικές απάτες ή επιθέσεις από εξωτερικούς παράγοντες. Τεχνικές όπως αυτές του ελάχιστου και απαραίτητου δικαιώματος (least privilege, need-to-have, need-to-know) και η συχνή επισκόπηση των ημερολογίων του συστήματος αποτελούν προτιμητέες λύσεις.

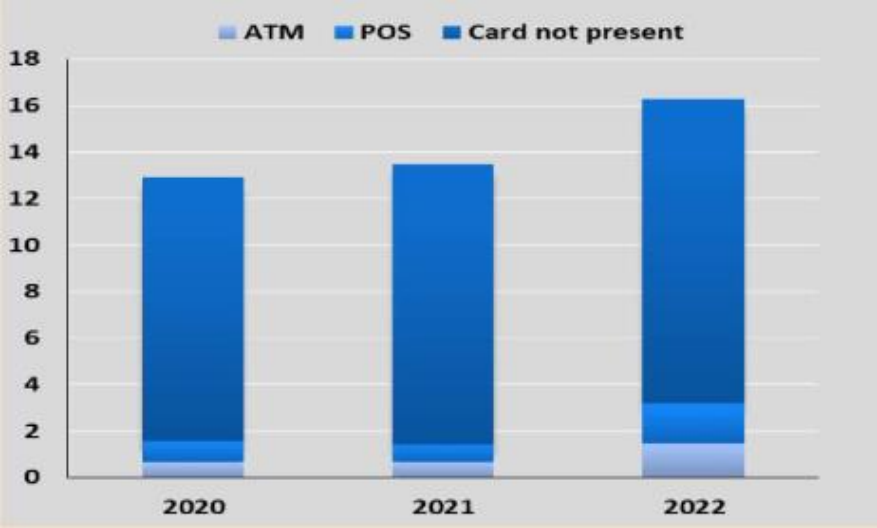
[34] Η παράκαμψη υφιστάμενων controls αποτελεί τον κυριότερο τύπο εκούσιας ή ακούσιας εσωτερικής απάτης με σημαντικό πλήθος περιστατικών να σημειώνονται ετησίως.

Επιπλέον, η καταγραφή των ενεργειών και η συχνή επισκόπηση των αντίστοιχων ημερολογίων θα πρέπει να διασφαλιστεί. Λόγω του σημαντικού όγκου πληροφοριών που περιέχουν, η χρήση data analytics αποτελεί μονόδρομο, προκειμένου να προσδιορίζονται με ευκολότερο τρόπο μοτίβα που δεν ανταποκρίνονται στην κανονική διαδικασία, ενέργειες που δεν ταιριάζουν στην αναμενόμενη συμπεριφορά του ή παραβιάσεις ασφαλείας. Ενδεχόμενη ενσωμάτωση αντίστοιχων τεχνικών στα υλοποιημένα controls, με παράλληλη ενημέρωση των αρμοδίων μονάδων και παραγωγή exception reports ενισχύει σημαντικά το ΣΕΕ.

3.2 Case Study I: Μηχανισμοί Ταυτοποίησης και Περιορισμού Ηλεκτρονικής Απάτης

Η ταυτοποίηση των προσώπων που συναλλάσσονται για λογαριασμό τους ή εκ μέρους των επιχειρήσεων που εκπροσωπούν, αποδεικνύεται ιδιαίτερα απαιτητική. Στον όρο συναλλαγή δεν περιλαμβάνονται μόνο ενχρήματες αλλά κάθε πράξη ή ενέργεια ενός προσώπου στο πλαίσιο των καθημερινών δραστηριοτήτων. Ενδεικτικά, ο όρος περιλαμβάνει συναλλαγές σε συστήματα ηλεκτρονικής τραπεζικής, ηλεκτρονικού εμπορίου, σε POS, αυτόματη εξόφληση οφειλών και η κατάθεση δικαιολογητικών και εντύπων σε φυσική ή ηλεκτρονική μορφή.

Κοινό χαρακτηριστικό τους είναι η αναγκαιότητα ταυτοποίησης του προσώπου που τις διενεργεί. Παλαιότερα, η επίδειξη ενός εντύπου ταυτοπροσωπίας (π.χ. διαβατήριο, αστυνομική ταυτότητα) ήταν επαρκής. Ωστόσο, η ανάπτυξη της τεχνολογίας πέρα από τα οφέλη της στους τομείς της ταχύτητας και της ποιότητας της εξυπηρέτησης, εγκυμονεί κινδύνους για την αξιοπιστία της διαδικασίας, καθώς παρουσιάζεται σημαντική αύξηση των περιπτώσεων πλαστοπροσωπίας, σε συνδυασμό με τη χρήση φαινομενικά αξιόπιστων εγγράφων. Παράλληλα, η χρήση ηλεκτρονικών μέσων για την πραγματοποίηση συναλλαγών έχει αυξήσει σημαντικά και τις περιπτώσεις υποκλοπής των χαρακτηριστικών σύνδεσης (credentials) που χρησιμοποιούνται για την ταυτοποίηση των συναλλασσόμενων.



Εικόνα 5. Αριθμός συναλλαγών περιστατικών απάτης ανά τύπο συναλλαγής-σε χιλ. (πηγή ΤτΕ)

Σε απάντηση των παραπάνω προκλήσεων, υλοποιούνται κατάλληλα «εκπαιδευμένα» αυτόματα bots που αναγνωρίζουν το είδος του εγγράφου και αναζητούν τα ενσωματωμένα (με τη μορφή είτε μέτα-δεδομένων[35] είτε ταινιών ασφαλείας) χαρακτηριστικά γνησιότητάς. Επιπλέον, ενδέχεται οι φωτογραφίες του προσώπου που ενσωματώνονται στα έντυπα ταυτοποίησης να συγκριθούν με την εικόνα που αποστέλλει ο συναλλασσόμενος[36], με χρήση αλγορίθμων ΤΝ (face recognition). Εμπόδιο στην αξιοπιστία της διαδικασίας αποτελεί η παλαιότητα του εγγράφου καθώς και η ποιότητα ψηφιοποίησης.

Με χρήση OCR τεχνικών διαβάζεται κείμενο σε συγκεκριμένα σημεία του εντύπου, προκειμένου να γίνει αντιπαραβολή με δεδομένα που περιέχονται ήδη στα συστήματα της επιχείρησης ή παρέχονται από εξωτερικές πηγές[37] και να διαπιστωθεί η γνησιότητα τους. Σε περίπτωση σφαλμάτων η συναλλαγή απορρίπτεται και ο συναλλασσόμενος καλείται να υποβάλλει εκ νέου τα στοιχεία ή να παρουσιαστεί αυτοπροσώπως.

Η αυτοματοποίηση των παραπάνω διαδικασιών, καθώς και των μηχανισμών ελέγχου που τη διέπουν, βοηθά σημαντικά στην εξοικονόμηση χρόνου αλλά και στην αξιοπιστία του αποτελέσματος. Εφόσον, η απόφαση δεν είναι εφικτό να ληφθεί από τον αυτοματοποιημένο

[35] Σε έγγραφα που έχουν εκδοθεί και υποβληθεί ψηφιακά

[36] Εφαρμόζεται κυρίως σε περιπτώσεις δημιουργίας σχέσης – άνοιγμα καταθετικού λογαριασμού – μέσω υπηρεσιών ηλεκτρονικής τραπεζικής, ενώ παράλληλα πραγματοποιείται βίντεο-κλήση.

[37] Ενδεικτικά, βάσεις δεδομένων με κλαπείσες ή απολεσθείσες ταυτότητες, στοιχεία από την ΑΑΔΕ για ΑΦΜ, το Γενικό Εμπορικό Μητρώο κ.α.

μηχανισμό, κατατάσσονται ως εξαιρέσεις και τα απαιτούμενα στοιχεία επαναξιολογούνται (ενδεχομένως και σε φυσική μορφή). Παράλληλα, η αξιοπιστία των controls είναι αυξημένη και ο περιοδικός έλεγχος συνδυαστικά με την επικαιροποίηση και προσαρμογή/εναρμόνισή τους με τις τρέχουσες απαιτήσεις, βοηθά στην περαιτέρω βελτίωσή.

Αυτοματοποιημένοι μηχανισμοί ταυτοποίησης έχουν εισέλθει και στις ηλεκτρονικές υπηρεσίες. Ο παραδοσιακός τρόπος που στηρίζονταν στο ονόματος χρήστη και τον κωδικό πρόσβασης (username και password) που παρείχε ο συναλλασσόμενος προκειμένου να αυθεντικοποιηθεί δεν είναι πλέον επαρκής. Αντικαθίσταται από προηγμένους μηχανισμούς δύο ή/και περισσότερων παραγόντων (two ή multi-factor authentication mechanisms), με την αποστολή επιπρόσθετων κωδικών στους χρήστες[38]. Τα εφαρμοζόμενα controls αφορούν κυρίως στην ασφάλεια του μέσου που χρησιμοποιείται, σε όρους εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Το μέσο θα πρέπει να διασφαλίζει την εμπιστευτικότητα της πληροφορίας που διακινείται[39], την ακεραιότητά του – παράδοση του πλήρους κωδικού και της συνεχούς διαθεσιμότητας του μέσου αποφεύγοντας διακοπές λειτουργίας. Τυχόν δυσλειτουργίες ή διαρροές θα πρέπει να εντοπίζονται και να διορθώνονται άμεσα.

3.3 Case Study II: Μιμητικά Bots

Σημαντικό ρόλο στην αυτοματοποίηση διαδικασιών διαδραματίζουν οι μηχανισμοί μίμησης της ανθρώπινης δραστηριότητας (bots). Οι εν λόγω εφαρμογές, με κατάλληλη παραμετροποίηση και προγραμματισμό, πραγματοποιούν επαναλαμβανόμενες και τυποποιημένες ενέργειες αντίστοιχες με αυτές ενός ανθρώπου, όπως να διαλέγονται με χρήστες μίας εφαρμογής και να υλοποιήσουν τυποποιημένες ακολουθίας ενεργειών (π.χ. καταχώρηση στοιχείων από ψηφιοποιημένα έγγραφα).

Στην πρώτη περίπτωση τα bots είναι προγράμματα που πραγματοποιούν προκαθορισμένες ενέργειες βάσει των προγραμματιστικών εντολών (μακροεντολές[40]), που περιλαμβάνουν το σύνολο των προς υλοποίηση ενεργειών. Κυρίως αφορά στην καταχώρηση τιμών σε μία εφαρμογή, που λαμβάνει ως δεδομένα εισόδου κάποιο ψηφιοποιημένο έγγραφο

[38] Μηνύματα κειμένου, Viber, βιομετρική ταυτοποίηση, ή/και email
[39] Στην περίπτωση αυτή τον κωδικό μίας χρήσης – One-Time-Password (OTP)
[40] Πολλαπλά στιγμιότυπα της οθόνης ενός χρήστη που λαμβάνουν τη μορφή βίντεο.

όπως τιμολόγια, φόρμες συμπληρωμένες από πελάτες, έγγραφα πιστοποίησης (ταυτότητες, διαβατήρια και φορολογικές δηλώσεις). Το bot εκτός της απλής καταχώρησης, υλοποιεί και πιο σύνθετες ενέργειες όπως επιπρόσθετους υπολογισμούς, καταχωρήσεις σε πολλαπλές οθόνες και την εκκίνηση άλλων διεργασιών, μιμούμενη σε σημαντικό βαθμό αυτή της ανθρώπινης δραστηριότητας.

Προϋπόθεση είναι η σύνδεση στις εφαρμογές που χρησιμοποιούνται με τρόπο αντίστοιχο του πραγματικού χρήστη και με κατάλληλα δικαιώματα. Πέρα από την παρακολούθηση των ενεργειών που υλοποιούνται και των παραχωρημένων δικαιωμάτων πρόσβασης[41], η απόδοσή μέσα από την αξιολόγηση του βαθμού ολοκλήρωσης των απαιτούμενων ενεργειών εντός προκαθορισμένου χρόνου, αποτελεί βασικό control. Η διαχείριση αλλαγών αποτελεί κομβικό σημείο, καθώς μεταβολές στις εφαρμογές και τα συστήματα που χρησιμοποιούνται από τα bots χωρίς την ενημέρωσή του λογισμικού τους, ενδέχεται να δημιουργήσουν δυσλειτουργίες, θέτοντας σε κίνδυνο την επιτυχή ολοκλήρωση των εργασιών. Επίσης, ο έλεγχος της τεκμηρίωσής τους οφείλει να είναι συνεχής και να λαμβάνονται οι κατάλληλες εγκρίσεις πριν προωθηθούν στο περιβάλλον παραγωγής, μετά την επιτυχή ολοκλήρωση των απαραίτητων δοκιμών.

Ο ρόλος του ΕΕ στις περιπτώσεις αυτές αφορά στην επισκόπηση της ορθής και αποδοτικής λειτουργίας των παραπάνω controls. Σε ενδεχόμενη έλλειψή τους ο ελεγκτής πρέπει να αναλύσει τα διαθέσιμα δεδομένα, προκειμένου να αξιολογήσει την απόδοση και την ορθή λειτουργία των bots. Οι αδυναμίες που θα προκύψουν σε ότι αφορά τους ελεγκτικούς μηχανισμούς και στην ίδια τη λειτουργία τους θα πρέπει να διορθωθούν άμεσα, για τον περιορισμό των μελλοντικών επιπτώσεων τους.

Τα bots που αναλαμβάνουν την εξυπηρέτηση και τη διαχείριση των αιτημάτων των πελατών αποτελούν σημαντικό κρίκο στην αλυσίδα των υπηρεσιών που προσφέρει η επιχείρηση. Η ακρίβεια των απαντήσεων που δίνονται είναι άμεση συνάρτηση των δεδομένων που έχουν φορτωθεί σε αυτό και της ορθότητας στην ανίχνευση των ερωτήσεων που υποβάλλονται. Τα συστήματα αυτά συναντώνται με τη μορφή τυποποιημένων ερωτήσεων που προσφέρονται έτοιμες στον τελικό χρήστη και επιλέγονται προς υποβολή

[41] Για να αποφευχθεί η χρήση τους σε παράνομες και χωρίς δυνατότητα εντοπισμού ενέργειες.

από αυτόν[42] ή με τη μορφή ανοικτού κειμένου όπου ο χρήστης πληκτρολογεί το ερώτημα και το bot αναζητά σε αυτό λέξεις κλειδιά προκειμένου να αποκριθεί.

Οι απαντήσεις προκύπτουν από τη βάση δεδομένων του συστήματος, και επιλέγονται από το bot βάσει του βήματος (αριθμός ερωτήσεων) που βρίσκεται ο χρήστης και τις λέξεις που έχει ανιχνεύσει στο ερώτημά του. Η δομή τους είναι δενδρική και σε κάθε ερώτηση το σύστημα είτε προχωράει στο επόμενο βήμα (κατεβαίνοντας ένα επίπεδο στο δένδρο) είτε κινείται οριζόντια προκειμένου να επιλέξει το κατάλληλο μονοπάτι. Στα τελικά φύλλα του δένδρου βρίσκονται οι λύσεις για τα θέματα που υποβάλλονται, ενώ σε περίπτωση αδυναμίας απόκρισης προτείνεται η επικοινωνία με φυσικό εκπρόσωπο ή επανεκκίνηση της διαδικασίας με πιο σαφείς ερωτήσεις. Με την ανάπτυξη και την υιοθέτηση ΤΝ[43], βελτιώνεται η αξιοπιστία και η ακρίβεια των απαντήσεων που παρέχονται, συναρτήσει της εκπαίδευσης του μοντέλου και της αξιολόγησης του πελάτη για την εμπειρία και το βαθμό ικανοποίησης από τη δοθείσα λύση.

Παράλληλα, με την ΤΝ μειώνεται σημαντικά ο αριθμός των αιτημάτων που τελικώς οδηγούνται στο τηλεφωνικό κέντρο της επιχείρησης (agents). Ωστόσο, απαιτούνται πιο εξελιγμένα και με μεγαλύτερη ακρίβεια controls προκειμένου να διασφαλιστεί η ορθή και αξιόπιστη λειτουργία τους. Η επιμέτρηση της απόδοσης γίνεται βάσει μεγεθών όπως ο αριθμός των ερωτήσεων που απαντήθηκαν ορθά ή δεν απαντήθηκαν[44], η αξιολόγηση του πελάτη - χρήστη της υπηρεσίας και το πλήθος αυτών που εγκατέλειψαν μη ικανοποιημένοι την προσπάθεια χωρίς αυτή να ολοκληρωθεί, διαχωρίζοντας όσους βρήκαν την απάντηση σε προγενέστερο του τελικού στάδιο.

Τα παραπάνω στατιστικά στοιχεία χρησιμοποιούνται κυρίως από τις δύο πρώτες γραμμές, σε συνδυασμό με τις δυνατότητες που προσφέρουν τα data analytics για μεγαλύτερη εμβάθυνση σε συγκεκριμένα σημεία των δεδομένων που προκύπτουν από την διαδικασία (ειδικά για τις εξαιρέσεις) και τις απαντήσεις των πελατών. Από τις αναλύσεις προκύπτουν βελτιώσεις στις απαντήσεις που φορτώνονται στο σύστημα και για τον ίδιο τον μηχανισμό (στην περίπτωση της ΤΝ στην εκπαίδευσή του, συμπεριλαμβανομένου και του

[42] Αποτελεί την πρώτη γενιά αυτών των συστημάτων που χρησιμοποιούνται ακόμα από πλήθος επιχειρήσεων στο διαδίκτυο.

[43] Ενδεικτικά το ChatGPT που μπορεί να ενσωματωθεί στα αντίστοιχα συστήματα της επιχείρησης.

[44] Με αποτέλεσμα ο πελάτης να οδηγηθεί σε τηλεφωνικό κέντρο ή στην υποβολή γραπτού αιτήματος

self-learning). Η ορθή διαχείριση αλλαγών θα διασφαλίσει την ακεραιότητα και τη διαθεσιμότητά του συστήματος σε όλο τον κύκλο ζωής του. Ο ρόλος του ελέγχου πέρα από την επισκόπηση των υφιστάμενων controls, περιλαμβάνει την ανάλυση του τρόπου εκπαίδευσης των συστημάτων ώστε να γίνουν αποτελεσματικότερα και με μεγαλύτερη ακρίβεια. Επιπρόσθετα σημεία αφορούν στην επισκόπηση των δοκιμών που πραγματοποιήθηκαν και την αξιολόγηση της αξιοπιστίας των αποτελεσμάτων συνδυαστικά με τις διορθωτικές ενέργειες, η περιοδικότητα των αλλαγών και η συνάφεια με την τρέχουσα κατάσταση.

3.4 Case Study III: Έγκριση Δανείου και Πιστοληπτική Ικανότητα

Ο όρος πιστοληπτική ικανότητα (credit rating - CR) αναφέρεται στην αξιοπιστία και στην φερεγγυότητα ενός ΦΠ, μιας επιχείρησης ή και μιας χώρας στην αποπληρωμή των χρεών της. Η εν λόγω αξιολόγηση υπολογίζει για λογαριασμό του δανειστή την πιθανότητα ο δανειολήπτης να ανταποκριθεί στις υποχρεώσεις χωρίς τον κίνδυνο αθέτησης ή πτώχευσης. Σημειώνεται ότι βάσει του Ν.4972/2022[45], η αξιολόγηση της πιστοληπτικής ικανότητας ΦΠ και ΝΠ πραγματοποιείται υποχρεωτικώς και έναντι του Ελληνικού Δημοσίου (άρθρο 51, παρ. 1), με αρμοδιότητα παραγωγής και χορήγησης της βαθμολόγησης από την Ανεξάρτητη Αρχή Πιστοληπτικής Αξιολόγησης που συστάθηκε με τον ίδιο νόμο.

Ο υπολογισμός του CR ενός πελάτη ΠΙ, αποτελεί μία από τις πρώτες και σχεδόν πλήρως αυτοματοποιημένες διεργασίες στον τραπεζικό τομέα, ειδικά για τα ΦΠ. Συνδέεται με την εκτίμηση της πιθανότητας εμφάνισης ασυνέπειας στις υποχρεώσεις του[46] μέσα στον προκαθορισμένο χρονικό ορίζοντα πρόβλεψης (συνήθως δώδεκα μήνες) και αποτελεί το πρώτο βήμα στη διαδικασία έγκρισης ή απόρριψης ενός αιτήματος δανειοδότησης. Η εγκριτική διαδικασία έχει αυτοματοποιηθεί σε σημαντικό βαθμό, στη λογική της τμηματοποίησης.

Η βάση για την αξιολόγηση του υποψηφίου δανειολήπτη εξαρτάται σε σημαντικό βαθμό από την πληρότητα, την επάρκεια και την ποιότητα των στοιχείων που συλλέγει το ΠΙ κατά

[45] Όπως τροποποιήθηκε με τον Ν.5046/2023.

[46] Όπως αυτή ορίζεται από την ΕΚΤ στους σχετικούς κανονισμούς και εξειδικεύεται από τα ΠΙ.

την υποβολή της αίτησης, προκειμένου να διασφαλιστεί η ορθότητα του υπολογισμού και να εντοπιστούν ενδεχόμενα απάτης. Επιπλέον, λαμβάνεται υπόψη και η συναλλακτική συμπεριφορά του βάσει των στοιχείων της αίτησης καθώς και αυτών που τηρούνται στο ΠΙ[47].

Το στατιστικό μοντέλο που εφαρμόζεται για την κατηγοριοποίηση του πελάτη σε σχέση με τον αναλαμβανόμενο πιστωτικό κίνδυνο αξιολογεί σειρά παραμέτρων για φυσικά και νομικά πρόσωπα, όπως η ικανότητα αποπληρωμής του πιστούχου βάσει των καθαρών του εσόδων, του καθαρού διαθέσιμου εισοδήματος, τις εύλογες δαπάνες διαβίωσης κ.α. Ειδικά για τα ΝΠ, τα εν λόγω κριτήρια εμπλουτίζονται με επιπρόσθετους πυλώνες, όπως η αξιολόγηση της πιθανότητας απάτης, δημογραφικών στοιχείων που προκύπτουν από τα μοντέλα βαθμολόγησης του CR, στοιχείων από εξωτερικές πηγές[48], του επιχειρηματικού σχεδίου (οργανωτική δομή, επιχειρηματικό μοντέλο), των εξασφαλίσεων που δίνονται από την επιχείρηση για το δάνειο κ.α.[49]. Σημαντικά ποιοτικά στοιχεία στην διαδικασία είναι η κατάσταση του κλάδου δραστηριότητας της επιχείρησης, η αξιολόγηση των πηγών αποπληρωμής του δανείου, των πραγματικών αναγκών της επιχείρησης, και τυχόν άλλων δεσμεύσεών της όπως και των χαρακτηριστικών του αιτούμενου δανείου σε σχέση με την οικονομική κατάσταση της.

Στα ΦΠ οι εν λόγω υπολογισμοί πραγματοποιούνται αυτόματα από εξειδικευμένα συστήματα που εκκινούν με το αίτημα του δανείου και αφορούν κυρίως σε στατιστικά δεδομένα που συλλέγονται από εσωτερικές και εξωτερικές πηγές. Αναλόγως του αποτελέσματος και της κατάταξης, η αίτηση προωθείται για έγκριση ή απορρίπτεται. Για τις επιχειρήσεις, τουλάχιστον για τις μεσαίες και μεγάλες εξ αυτών, η διαδικασία δεν έχει πλήρως αυτοματοποιηθεί. Τα αίτια έγκεινται στην υποχρέωση να αξιολογούνται και επιπρόσθετα στοιχεία πέραν όσων προκύπτουν με χρήση στατιστικών μεθόδων, για τα οποία η αυτόματη διαδικασία δεν δύναται να εφαρμοστεί.

[47] Άλλα ενεργά και μη ενεργά προϊόντα - δάνεια, πιστωτικές κάρτες, όρια χρηματοδότησης, κεφάλαια κίνησης, καταθέσεις, εξασφαλίσεις κ.α. Για τα μη ενεργά πραγματοποιείται ανάλυση των ιστορικών τους στοιχείων, όπως καθυστερήσεις, έγκαιρη αποπληρωμή, ρυθμίσεις κ.α.

[48] Κατά κύριο λόγο το στατιστικό μοντέλο της Τειρεσίας (Credit Bureau Score) ειδικά για τα ΝΠ.

[49] Δείκτης LTV – Loan-to-Value, ποσό του δανείου ως ποσοστό της αξίας των εξασφαλίσεων.

Η αυτοματοποιημένη εγκριτική διαδικασία ενός δανειακού αιτήματος πραγματοποιείται στη βάση προκαθορισμένων κριτηρίων και προϋποθέσεων[50] και αφορά κυρίως ΦΠ και περιπτώσεις που ο πιστωτικός κίνδυνος που εκτίθεται το ΠΙ εκτιμάται ως χαμηλός[51]. Ο πελάτης ενημερώνεται για την αυτοματοποιημένη επεξεργασία των στοιχείων του και παρέχει τη συγκατάθεσή του κατ' απαίτηση του ΓΚΠΔ και οδηγίας της ΕU ενώ μη λήψη της ενδέχεται να οδηγήσει σε απόρριψη του αιτήματος ή διαβίβασή του στο αρμόδιο εγκριτικό κλιμάκιο με ενδεχόμενη καθυστέρηση. Τα δεδομένα που λαμβάνονται υπόψη δεν θα πρέπει να προέρχονται αποκλειστικά από εξωτερικές πηγές αλλά και από τα ΠΣ του ΠΙ, βάσει τυποποιημένων μεθόδων (Οδηγία 36/ΕU παρ. 70). Ο πελάτης έχει επιπρόσθετα το δικαίωμα εναντίωσης στην απόφαση που λαμβάνει το σύστημα και του κοινοποιείται από το ΠΙ, για ενδεχόμενη επανεξέταση του αιτήματος, χωρίς την παρέμβαση του αυτοματοποιημένου μηχανισμού.

Η εγκριτική διαδικασία ενός δανείου και ο υπολογισμός του αναλαμβανόμενου πιστωτικού κινδύνου από την πλευρά του ΠΙ είναι ιδιαιτέρως περίπλοκη διαδικασία και κρίσιμη για την οικονομική ευημερία των δανειοληπτών και τη χρηματοδότηση της οικονομίας. Η αυτοματοποίηση με τη χρήση στατιστικών μεθόδων και εφαρμογή σύνθετων υπολογισμών στα δεδομένα συναλλακτικής συμπεριφοράς αλλά και στα οικονομικά στοιχεία του υποψηφίου δανειολήπτη, επιταχύνει τη διαδικασία σε όφελος του πελάτη και διασφαλίζει σε ικανοποιητικό βαθμό το ΠΙ. Οι εν λόγω μηχανισμοί δεν αποτελούν ωστόσο μόνο παράδειγμα επιτυχημένης αυτοματοποίησης[52], αλλά και επιτυχούς ενσωμάτωσης μίας πρώτης μορφής ΤΝ σε καθημερινά συστήματα, με χρήση μεγάλων δεδομένων και κυρίως τη δυνατότητα του συστήματος να λαμβάνει αποφάσεις, χωρίς απαραίτητα ανθρώπινη παρέμβαση.

Ο Κανονισμός για την ΤΝ αναφέρει τα συστήματα CR ως συστήματα «υψηλού κινδύνου»[53], με την εξαίρεση αυτών που χρησιμοποιούνται από μικρούς προμηθευτές και για

[50] Τα κριτήρια που εφαρμόζονται για την αυτοματοποιημένη έγκριση των δανείων ενδέχεται να διαφέρουν μεταξύ των ΠΙ, ωστόσο οι βασικές αρχές παραμένουν κοινές προκειμένου να περιοριστεί ο πιστωτικός κίνδυνος που αναλαμβάνουν.

[51] Βάσει στατιστικών στοιχείων και του credit risk appetite

[52] Έστω και αν αυτή έχει επιτευχθεί μερικώς για τις περιπτώσεις ΦΠ και μικρών επιχειρήσεων.

[53] Παράρτημα ΙΙΙ, παρ. 5b *"systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use;"*

ιδία χρήση. Κατά συνέπεια, οι μηχανισμοί που έχουν υλοποιηθεί τόσο από ΠΙ όσο και από επιχειρήσεις που παρέχουν δάνεια σε πελάτες τους (π.χ. εταιρίες ηλεκτρονικών ειδών)[54] θα πρέπει να αξιολογηθούν σύμφωνα με τις νέες απαιτήσεις.

Η διασφάλιση της αβίαστης και μη μεροληπτικής συμπεριφοράς του μηχανισμού εξαρτάται από τα δεδομένα που χρησιμοποιούνται για την εκπαίδευση του μοντέλου. Οι απαιτήσεις καθορίζουν ότι θα πρέπει να προέρχονται από ιστορικά στοιχεία του ΠΙ και να έχουν συλλεγεί με αμερόληπτο τρόπο. Για παράδειγμα, η εκπαίδευση του αυτόματου μηχανισμού μόνο με στοιχεία αιτήσεων που έχουν απορριφθεί ή εγκριθεί, για δάνεια μικρού ή πολύ μεγάλου ύψους, για συγκεκριμένους σκοπούς όπως η αγορά καταναλωτικών αγαθών ή στεγαστικών δανείων, ή από συγκεκριμένες κατηγορίες δανειοληπτών ενδέχεται να οδηγήσει το αποτέλεσμα προς μία συγκεκριμένη κατεύθυνση.

Η εγκριτική διαδικασία διέπεται από πλήθος controls συμπεριλαμβανομένων των παραγόμενων αναφορών για τη λειτουργία του μηχανισμού. Η ύπαρξη ακραίων συμπεριφορών (π.χ. σημαντικό πλήθος απορρίψεων ή εγκρίσεων) και αποκλίσεων από τα καθιερωμένα αποτελούν ενδείξεις αναθεώρησης του μηχανισμού. Η απόδοσή του, βάσει της ταχύτητας εκτέλεσης και του πλήθος αμφισβητήσεων – λαμβάνοντας υπόψη τυχόν παράπονα πελατών που η έκβαση του δανείου αποδείχθηκε λανθασμένη, συγκαταλέγονται στην αξιολόγηση. Η μονάδα διαχείρισης κινδύνων, μέσα από την μελέτη του αναλαμβανόμενου πιστωτικού κινδύνου και την ανάλυση της εξέλιξης των δανειακών προϊόντων[55] εισηγείται διορθώσεις (αναθεώρηση μοντέλων, προσαρμογές στην πιστωτική πολιτική, επικαιροποίηση δεδομένων) και αξιολογεί την επάρκεια του μηχανισμού. Το τελευταίο αποτελεί κοινό στόχο με τον ΕΕ συνδυαστικά με την περιοδική αξιολόγηση της απόδοσης των παραπάνω controls βάσει των στόχων της επιχείρησης.

Συμπερασματικά, η αυτοματοποιημένη εγκριτική διαδικασία ενός αιτήματος δανειολήπτη εκκινώντας από τη συμπλήρωση του αιτήματος μέχρι και την έγκριση ή την απόρριψη, ωφελεί την επιχείρηση και τον πελάτη καθώς βελτιώνει την εμπειρία του και την αξιοπιστία του αποτελέσματος, μειώνει τον απαιτούμενο χρόνο και τον λειτουργικό

[54] Δεν συμπεριλαμβάνονται οι δόσεις με χρήση πιστωτικών καρτών καθώς στην περίπτωση αυτή το δάνειο εξακολουθεί να δίνεται από το ΠΙ – εκδότη της κάρτας που αναλαμβάνει και τον κίνδυνο.

[55] Σημαντικά στοιχεία είναι η ύπαρξη πλήθους δανείων που δεν εξυπηρετούνται σε σύντομο χρονικό διάστημα ή εντός οριζόμενου από την πολιτική δωδεκαμήνου.

κίνδυνο. Παράλληλα, με την καθολική χρήση ΤΝ στους εν λόγω μηχανισμούς, η επιχείρηση ωφελείται στη διαχείριση του αναλαμβανόμενου κινδύνου και στην αξιοποίηση ευκαιριών πιστωτικής επέκτασης.

Δεδομένου ότι το αίτημα ενός δανείου υποβάλλεται για την κάλυψη πραγματικών, ενδεχομένως κρίσιμων, αναγκών ενός ΦΠ ή μίας επιχείρησης, η ηθική διάσταση πίσω από την αυτοματοποιημένη έγκριση δεν πρέπει να αμελείται. Σε αρκετές περιπτώσεις τα υποκειμενικά κριτήρια δεν αποτυπώνονται επαρκώς ή με τρόπο αντιληπτό από έναν αλγόριθμο, οδηγώντας τελικώς σε απόρριψη. Το δικαίωμα εναντίωσης και επανεξέτασης του αποτελέσματος καθίσταται ιδιαίτερα χρήσιμο, αρκεί να πραγματοποιείται από ανθρώπινο παράγοντα και όχι από τον ίδιο αλγόριθμο.

3.5 Αυτοματοποίηση στον ΕΕ

Λαμβάνοντας υπόψη την πρόοδο του τεχνολογικού τομέα και ειδικότερα σε αυτόν της αυτοματοποίησης των διαδικασιών, η υιοθέτηση αντίστοιχων μηχανισμών από τον ΕΕ μοιάζει αναπόφευκτη και υποχρεωτική. Παράλληλα, θα προετοιμάσει το έδαφος για τις μελλοντικές εξελίξεις αποφεύγοντας τον κίνδυνο να καταστεί ο έλεγχος ουραγός αυτών στο επίπεδο της επιχείρησης. Τα αποτελέσματα των δημοσιοποιημένων μελετών σε περιπτώσεις που συμβαδίζουν με την σύγχρονη τεχνολογία, δείχνουν ότι βιώνουν ήδη τα οφέλη της επιλογής τους.

Η αυτοματοποίηση διαδικασιών στον ΕΕ ξεκινά από απλά, συνεχώς επαναλαμβανόμενα (καθημερινά ενδεχομένως) βήματα. Η πλήρης ή μερική αυτοματοποίηση ελεγκτικών βημάτων αποτελεί το πρώτο πεδίο εφαρμογής, όπως η εξόρυξη δεδομένων από μεγάλα datasets σε αρχεία για περαιτέρω επεξεργασία και εξαγωγή συμπερασμάτων (Pundman and others 2018) . Οι διαδικασίες αυτές δεν αφορούν μόνο τη διενέργεια των ελέγχων[56] αλλά και τα δεδομένα που τροφοδοτούν την αξιολόγηση των κινδύνων σε μία περιοχή. Η τελευταία εκτελείται από μονάδες με χαμηλό επίπεδο αυτοματισμού σε ετήσια βάση, λαμβάνοντας υπόψη πληροφορίες από εσωτερικές και εξωτερικές πηγές, όπως το κανονιστικό πλαίσιο, τις αλλαγές στις διαδικασίες και στις πολιτικές της επιχείρησης, τη στρατηγική της κ.ο.κ. Βάσει

[56] Δεδομένα που θα εξαχθούν από βάσεις και υποδομές big data για την παραγωγή συμπερασμάτων μετά την κατάλληλη επεξεργασία (data manipulation) στο σύνολο ή σε δείγμα τους.

αυτών αξιολογείται η φύση των κινδύνων που εκτίθεται κάθε επιχειρησιακή διαδικασία, η κατάλληλη επιμέτρηση[57] και η κρισιμότητά της διαδικασίας για τη λειτουργία της επιχείρησης[58].

Ωστόσο, η υιοθέτηση προηγμένων ρομποτικών τεχνολογιών αυτοματοποιεί τη συλλογή των απαραίτητων στοιχείων σε πραγματικό χρόνο, οδηγώντας σε συνεχή διαδικασία αξιολόγησης των κινδύνων. Συνεπώς καθίστανται εφικτοί ο δυναμικός προγραμματισμός, η διενέργεια στοχευμένων ελέγχων σε σημαντικές για την επιχείρηση περιοχές και η ποιοτική βελτίωση, οδηγώντας στην επίτευξη του σημαντικότερου στόχου του ΕΕ, την προσθήκη αξίας στην επιχείρηση.

Η χρήση bots αποδεικνύεται χρήσιμη κατά την υλοποίηση των ελέγχων και αναλόγως του τύπου τους, οι ακόλουθες δραστηριότητες απλοποιούνται σημαντικά:

- Επαληθεύσεις και σύγκριση καταστάσεων (π.χ. λογιστικών) βάσει προκαθορισμένων κριτηρίων. Ειδικότερα με την εφαρμογή NLP, οι ενέργειες τους προσομοιώνουν σε σημαντικό βαθμό αυτές ενός ελεγκτή.
- Μοντελοποίηση των δεδομένων και προβολή (visualization) χρήσιμων πληροφοριών.
- Επιλογή αντιπροσωπευτικού δείγματος από το σύνολο του πληθυσμού για περαιτέρω ανάλυση και προβολή των αποτελεσμάτων στο σύνολο του (extrapolation).
- Αθροίσεις σύνθετων δεδομένων.
- Αναζητήσεις ενδείξεων απάτης και έγκαιρη ενημέρωση/ειδοποίηση των εμπλεκομένων.
- Επισκόπηση και ανάλυση ημερολογίων κινήσεων, παραμετροποίησης συστημάτων και εφαρμογών, τιμολογίων και αποδείξεων, δεδομένων που προέρχονται από διαφορετικά συστήματα κ.α.
- Παρακολούθηση υλοποίησης διορθωτικών ενεργειών και το κλείσιμο του ελέγχου. Τα bots λαμβάνουν, επεξεργάζονται και αρχειοθετούν τις απαντήσεις των ελεγχόμενων μονάδων και τη συγκέντρωση των αποδεικτικών στοιχείων.

[57] Η επιμέτρηση του κινδύνου στηρίζεται στον υπολογισμό της πιθανότητας εμφάνισης και του αντίκτυπου που θα έχει στην επιχειρησιακή λειτουργία (impact * likelihood)

[58] Στον υπολογισμό της κρισιμότητας υπεισέρχονται επιπρόσθετα κριτήρια, όπως ο ελεγκτικός κύκλος, αλλαγές στη διαδικασία, ο βαθμός εξάρτησής της από ΣΠ, κανονιστικές απαιτήσεις, ενδείξεις ή υποθέσεις απάτης κ.α.

Η χρήση της παραπάνω τεχνολογίας οφείλει να διέπεται από αυστηρούς κανόνες, προκειμένου να διασφαλιστεί η αποτελεσματικότητα και η εναρμόνιση με τους επιδιωκόμενους σκοπούς. Η πολυπλοκότητα και ο απαιτούμενος προϋπολογισμός υλοποίησης πρέπει να λαμβάνονται υπόψη κατά τον σχεδιασμό, ώστε να αποφευχθούν τυχόν ανατροπές και εκπτώσεις στο τελικό αποτέλεσμα, και να διατηρηθούν τα κόστη σε λογικά επίπεδα. Η τεκμηρίωση των αποτελεσμάτων, των φάσεων υλοποίησης και συνολικά του έργου συνεισφέρει σημαντικά ειδικά όταν η ανάπτυξη πραγματοποιείται από τρίτο μέρος, στην κατανόηση του αποτελέσματος και στη διασφάλιση επίτευξης του προσδοκώμενου οφέλους. Οι δοκιμές λειτουργίας και χρήσης των συστημάτων, θα πρέπει να πραγματοποιούνται με ποιοτικά δεδομένα και βάσει προκαθορισμένων σεναρίων για να επιτευχθεί ο απαιτούμενος βαθμός ακρίβειας.

Θέματα ασφάλειας των προσβάσεων στις πληροφορίες των ελέγχων, λαμβάνοντας υπόψη ότι σχεδόν στο σύνολό τους είναι εμπιστευτικής φύσης, πρέπει να επιλύονται με αποτελεσματικό τρόπο. Η διαθεσιμότητα και η επιχειρησιακή συνέχεια των εμπλεκόμενων μηχανισμών πρέπει να διασφαλιστεί, λαμβάνοντας υπόψη και την αυξανόμενη εξάρτηση που έχουν οι μονάδες ΕΕ από τα συστήματα αυτά.

Στα σημαντικότερα κέρδη από την εφαρμογή αυτοματοποιημένων τεχνικών ανάλυσης δεδομένων συμπεριλαμβανομένων και των ρομποτικών, συγκαταλέγονται η ταχύτερη και αποδοτικότερη υλοποίηση χρονοβόρων ελεγκτικών βημάτων, ο περιορισμός των λαθών και η δυνατότητα διενέργειας προβλέψεων χρησιμοποιώντας τα μέτα-δεδομένα και πληροφορίες που προκύπτουν από υφιστάμενα αποδεικτικά στοιχεία.

3.6 Διαρκής Παρακολούθηση και Έλεγχος

Οι όροι της διαρκούς παρακολούθησης (CM) και ελέγχου (CA) είναι συνυφασμένοι με την έννοια της αυτοματοποίησης και υλοποιούνται παράλληλα και αλληλένδετα[59] (KPMG 2018). Η δομική διαφορά τους έγκειται στις γραμμές που τα υλοποιούν και αφορούν, όπου στο CM είναι οι επιχειρησιακές μονάδες (1η και 2η γραμμή) ενώ στον CA είναι η 3η γραμμή (Deloitte 2018).

[59] Συχνά θεωρούνται παραλλαγές του ίδιου θέματος.

Στο CM οι αρμόδιες μονάδες επισκοπούν διαρκώς τις επιχειρησιακές διαδικασίες προκειμένου συμμορφώνονται με αυτές και να προτείνουν βελτιώσεις σε περιπτώσεις αποκλίσεων από τα καθορισμένα επίπεδα λειτουργίας και απόδοσης. Τα πλεονεκτήματά του συνοψίζονται στη διαρκή αξιολόγηση της απόδοσης και βελτίωση των υλοποιημένων controls και διαδικασιών, στον έγκαιρο εντοπισμό σημείων κινδύνου, στη διασφάλιση της συμμόρφωσης με ηθικά και κανονιστικά πρότυπα, στη λήψη αποφάσεων βάσει των κινδύνων και στην υιοθέτηση νέων τεχνολογιών.

Στο CA ο έλεγχος συλλέγει τα απαραίτητα δεδομένα σε συνεχή βάση ώστε να πραγματοποιούνται και να τεκμηριώνονται οι έλεγχοι, διασφαλίζοντας τη συμμόρφωση με πολιτικές και τις διαδικασίες της επιχείρησης με αποδοτικό τρόπο και χαμηλότερα κόστη. Παράλληλα, διευκολύνεται η μετάβαση από περιστασιακούς ή ελέγχους βάσει κυκλικότητας[60] σε συνεχείς και διαρκείς. Το ετήσιο πλάνο από στατικό, αποκτά τη δυνατότητα συνεχούς προσαρμογής στις δυναμικές συνθήκες της επιχείρησης και προσανατολίζεται στους κινδύνους που αντιμετωπίζει στις δραστηριότητές της. Η μείωση του κόστους μέσα από την υιοθέτηση και ορθή χρήση των νέων τεχνολογιών και των δυνατοτήτων της πληροφορικής βρίσκει πρόσφορο έδαφος.

Μία εφαρμογή τους είναι στην παρακολούθηση συναλλαγών (π.χ. τραπεζικών, λογιστικών, παραγγελιών, παραδόσεων κ.α.) μέσω ανάλυσης δεδομένων. Οι εξαιρέσεις και οι παρεκκλίσεις εντοπίζονται άμεσα και με ταυτόχρονη ενημέρωση των ενδιαφερόμενων μερών προκειμένου να προσδιοριστούν και να υλοποιηθούν διορθωτικές ενέργειες. Ο κίνδυνος εσωτερικής απάτης μειώνεται δραστικά λόγω της κουλτούρας που δημιουργείται σταδιακά μέσα στην επιχείρηση καθώς οι παρεκκλίσεις δεν περνούν απαρατήρητες και εντοπίζονται έγκαιρα. Σύμφωνα με τις μελέτες, στις επιχειρήσεις του κλάδου των μεταφορών τα δρομολόγια που εκτελούνται με πληρότητα κάτω από το 60% είναι ιδιαίτερα ζημιογόνα και απαιτούνται συγχωνεύσεις και αλλαγές, προκειμένου να επιτευχθεί το επιθυμητό επίπεδο στον δείκτη πληρότητας. Μετά την εφαρμογή μηχανισμών συνεχούς ελέγχου της πληρότητας και εν γένει των δρομολογίων, παρατηρήθηκε μείωση κόστους που στις περισσότερες περιπτώσεις ξεπερνούσε το 50%.

[60] Στην κατάρτιση του ετήσιου πλάνου λαμβάνονται υπόψη σημαντικά συμβάντα και η κυκλικότητα των ελέγχων (σε έτη) ώστε να διασφαλίζεται ότι κρίσιμες περιοχές έχουν ελεγχθεί τουλάχιστον μία φορά εντός του κύκλου.

Η παρακολούθηση συναλλαγών, η διασταύρωση και ο συνδυασμός τους με αντίστοιχα γεγονότα άλλων εφαρμογών (π.χ. ταμειακές συναλλαγές συσχετιζόμενες με αντίστοιχες λογιστικές) σε ΠΙ συμβάλλει στον περιορισμό της εσωτερικής απάτης, την ενίσχυση του ΣΕΕ και του πλαισίου διαχείρισης κινδύνων. Για τον έλεγχο, η ανάλυση δεδομένων συναλλαγών όχι σε δειγματοληπτική βάση αλλά στο σύνολο του πληθυσμού με χρήση data analytics, αλλάζει τον τρόπο πραγματοποίησης ελέγχων αφού υλοποιείται σε πραγματικό χρόνο μετατρέποντας την παραπάνω συνήθως περιοδική διαδικασία σε συνεχή. Επιπλέον, η ολιστική προσέγγιση και ανάλυση του πληθυσμού μέσω data analytics, βοηθά στον εντοπισμό τμηματικά εκτελούμενων συναλλαγών με στόχο να υπερκεραστούν οι περιορισμοί που τίθενται από πολιτικές, διαδικασίες και το κανονιστικό πλαίσιο.

Ενδεικτικά, μέσω τμηματικής εκτέλεσης συναλλαγών σε μετρητά παρακάμπτονται οι εγκριτικοί μηχανισμοί και η δυνατότητα παρακολούθησής τους όπως απαιτείται από την ΤτΕ με σκοπό τον έλεγχο των μετρητών που τίθενται σε κυκλοφορία εντός ΕU και για σκοπούς AML/CFT (ΕΤΠΘ 281/17.3.2009). Χρησιμοποιώντας τα δεδομένα των ημερολογίων των ΣΠ και των υποδομών μίας επιχείρησης, συνδυαστικά με στοιχεία του ανθρώπινου δυναμικού, εντοπίζονται περιπτώσεις όπου προσωπικό σε άδεια εισέρχεται στα συστήματα της και πραγματοποιεί συναλλαγές ή παρέχει εγκρίσεις. Παράλληλα, προσδιορίζονται μη εξουσιοδοτημένες προσβάσεις και πολλαπλές συνδέσεις με χρήση του ίδιου λογαριασμού σε σταθμούς εργασίας και εφαρμογές[61].

Η υιοθέτηση και πρακτική εφαρμογή μηχανισμών CM και CA από τις αρμόδιες επιχειρησιακές μονάδες έχει προχωρήσει σημαντικά, λόγω χρήσης data analytics και μοντέλων που επιτρέπουν τη διαχείριση μεγάλου όγκου πληροφοριών από διαφορετικά συστήματα και ανεξάρτητα της μορφής της πληροφορίας. Εφαλτήρια για τη μετάβαση σε ένα συνεχώς ελεγχόμενο περιβάλλον αποτελούν η ανάγκη για μείωση του λειτουργικού κόστους, η εναρμόνιση με το κανονιστικό περιβάλλον και κυρίως ο περιορισμός των κινδύνων σε ανεκτά και διαχειρίσιμα επίπεδα.

Πρωταρχικό μέλημα των επιχειρήσεων είναι να επισκοπήσουν το κανονιστικό και το νομοθετικό πλαίσιο που οφείλουν να εναρμονιστούν, να αποκτήσουν γνώση των

[61] Ο διαμοιρασμός των χαρακτηριστικών σύνδεσης μεταξύ πολλών χρηστών (password sharing) είναι εκ των κυριότερων παραβιάσεων πολιτικών και διαδικασιών μίας επιχείρησης.

απαιτήσεων για controls, να εφαρμόσουν τους αυτοματοποιημένους μηχανισμούς και τελικώς να προχωρήσουν σε βελτιώσεις στο λειτουργικό περιβάλλον. Τα συνήθη προβλήματα αφορούν στη διάθεση των απαραίτητων πόρων και στις αυξημένες απαιτήσεις μηχανογραφικών υλοποιήσεων, που αντισταθμίζονται επαρκώς από τα οφέλη και την εγκαθίδρυση ενός περιβάλλοντος αντικειμενικότητας, συμμόρφωσης με τους επιχειρησιακούς κανόνες, μειωμένου λειτουργικού κόστους, εντοπισμού και επίλυσης των όποιων εξαιρέσεων σε πραγματικό χρόνο.

ΚΕΦΑΛΑΙΟ 4. Η ΑΞΙΟΠΟΙΗΣΗ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ ΣΤΟ ΣΥΣΤΗΜΑ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ

Η εφαρμογή της ΤΝ επεκτείνεται συνεχώς σε ολοένα και περισσότερα πεδία, από τη στοχοθεσία των πωλήσεων και του δυνητικού πελατολογίου, μέχρι τον υπολογισμό του βαθμού καταλληλόλητας και του κινδύνου των υποψηφίων πελάτη ή και προμηθευτών για τη σύναψη σχέσης με μία επιχείρηση (συμπεριλαμβανομένων των ΠΙ). Η πληθώρα δεδομένων και η ποικιλία των σύγχρονων ΣΠ που τα χρησιμοποιούν και τα παρέχουν, δημιουργούν ένα σύνθετο περιβάλλον και περιπλέκουν τόσο τα controls που υλοποιούνται από τις δύο πρώτες γραμμές, όσο και τους περιοδικούς ελέγχους της 3ης.

Παρότι σε αρκετούς τομείς της ανθρώπινης δραστηριότητας η ΤΝ βρίσκεται στα πρώτα στάδια εφαρμογής της, η υιοθέτησή από τον ΕΕ ξεκίνησε αρκετά χρόνια πριν, απόρροια των αντίστοιχων πρακτικών που εφαρμόστηκαν από τις δύο πρώτες γραμμές του ΣΕΕ. Δίπλα στις παραδοσιακές πρακτικές ανάλυσης δεδομένων, τοποθετούνται πλέον τεχνολογίες όπως μοντέλα πρόβλεψης, αυτοματοποίησης διαδικασιών με χρήση ρομποτικών μηχανισμών και παραγωγής νέων δεδομένων και γνώσης με την χρήση υφιστάμενων πληροφοριών (Cognitive Intelligence - CI).

Η υιοθέτηση της ΤΝ από το σύνολο των γραμμών του ΣΕΕ αναμένεται να έχει θετικό αντίκτυπο σε θέματα ποιότητας των ελέγχων που πραγματοποιούνται από κάθε εμπλεκόμενο μέρος, τον περιορισμό των κινδύνων που εκτίθεται η επιχείρηση και στη βελτίωση του βαθμού επίγνωσης των παραπάνω κινδύνων από την επιχείρηση. Η έλλειψη αυτοματοποιημένων μεθόδων και μηχανισμών, επηρεάζει αρνητικά τη χρήση από τον έλεγχο τεχνικών που στηρίζονται στην ΤΝ, εξαιτίας της δυσκολίας μετατροπής και μεταγλώττισης χειροκίνητων διεργασιών σε δεδομένα επεξεργάσιμα από ένα σύστημα ΤΝ.

4.1 Το ΣΕΕ Εφαρμογών ΤΝ

Η αξιοπιστία των αποτελεσμάτων της επεξεργασίας πληροφοριών μέσω ΤΝ αλλά και η λειτουργία των ΣΠ, εξαρτάται σημαντικά από την ποιότητα των δεδομένων τροφοδότησης. Ο έλεγχός τους δεν περιορίζεται στην ανάλυση του τρόπου λειτουργίας και των παραδοσιακών ICT κινδύνων που αντιμετωπίζουν, αλλά και στον «κίνδυνο δεδομένων»

(data risk) και στα controls που τον περιορίζουν. Ο όρος αναφέρεται στον κίνδυνο που εκτίθεται η επιχείρηση λαμβάνοντας αποφάσεις βάσει μη αξιόπιστων στοιχείων ή αποτελεσμάτων επεξεργασίας δεδομένων αμφιβόλου ποιότητας/μη κατάλληλων. Χαμηλής ποιότητας δεδομένα, κατευθυνόμενα, μη ανεξάρτητα, που δεν αντανακλούν την πραγματικότητα, επηρεάζουν το τελικό αποτέλεσμα και θέτουν σε κίνδυνο την ακρίβεια και την ακεραιότητα του αποτελέσματος.

Επιπρόσθετα, ο έλεγχος εστιάζει στα μέτρα για τη συμμόρφωση με το κανονιστικό και νομικό πλαίσιο καθώς και με τους κανονισμούς ιδιωτικότητας. Θέματα ηθικής που ενδέχεται να αφορούν στα «εκπαιδευτικά» δεδομένα των μοντέλων, οφείλουν να εξεταστούν πριν τη χρήση.

Κατά την ανάπτυξη και την υλοποίηση των μοντέλων λήψης αποφάσεων με ΤΝ, ελέγχεται ο καθορισμός των παραμέτρων και η βαρύτητα καθεμίας. Σημαντικό ρόλο παίζουν και οι κανονιστικές απαιτήσεις αλλά και η ηθική πίσω από την απόφαση που λαμβάνεται[62]. Το νομοθετικό πλαίσιο απαγορεύει πώληση και προώθηση προϊόντων σε ανηλίκους, ενώ αντίστοιχα η πώληση συγκεκριμένων μακροπρόθεσμων ή περίπλοκων προϊόντων σε ηλικιωμένους δεν είναι ηθικά αποδεκτή λόγω δυσκολίας κατανόησης των όρων και των προϋποθέσεων. Αντίστοιχα, υφίσταται ο κίνδυνος αποκλεισμού πελατών, μέσω αποφάσεων για δάνεια και τους υπολογισμούς για το CR με άμεση επίπτωση στην καθημερινότητά τους. Η αυστηρώς ελεγχόμενη πρόσβαση στα μοντέλα και στους υπολογισμούς που πραγματοποιούνται θα πρέπει να επιβεβαιώνεται για την αποφυγή υποβάθμισης απόδοσης και αξιοπιστίας του αποτελέσματος.

Βασικό στοιχείο ελέγχου είναι η ύπαρξη επιχειρησιακής στρατηγικής για την ΤΝ, που θα καθορίζει τους στόχους, τα αναμενόμενα αποτελέσματα από τη χρήση και τον τρόπο επίτευξης τους, συμμορφώνεται με το εφαρμοζόμενο ρυθμιστικό, κανονιστικό και νομικό πλαίσιο και ευθυγραμμίζεται με το risk appetite της επιχείρησης. Ειδικά για το τελευταίο, πρέπει να διασφαλίζεται ότι δεν εκτίθεται η επιχείρηση σε νέους κινδύνους ή δεν αυξάνεται το επίπεδο όσων έχουν ήδη αναγνωριστεί (και περιοριστεί μέσω των εφαρμοζόμενων controls). Τέλος, μέσω του μοντέλου διακυβέρνησης που υιοθετείται πρέπει να καθορίζεται

[62] Ενδεικτικά η ηλικία του πελάτη σε έναν αλγόριθμο ΤΝ διασταυρούμενων πωλήσεων χρηματοοικονομικών προϊόντων

ο τρόπος παρακολούθησης της προόδου υλοποίησης και αξιολόγησης των αποτελεσμάτων σε κάθε στάδιο υλοποίησης, προκειμένου να εντοπίζονται και να επιλύονται έγκαιρα τυχόν προβλήματα.

Το σύνολο των παραπάνω controls (π.χ. στρατηγική χρήσης και εφαρμογής, περιορισμοί για τα δεδομένα «εκπαίδευσης» του μοντέλου) εφαρμόζεται και σε συστήματα ML, καθώς υιοθετούν ΤΝ για την πραγματοποίηση των υπολογισμών. Ο έλεγχος εστιάζει στα εφαρμοζόμενα controls κατά την ανατροφοδότηση των αποτελεσμάτων στο μοντέλο ΤΝ, καθώς αυτό θα καθορίσει με τη σειρά του τις επόμενες επεξεργασίες και το βαθμό ανεξαρτησίας. Ακόμα και σε περιπτώσεις που δεν διαπιστώνονται αποκλίσεις κατά την αρχική εκπαίδευση του μοντέλου, η ανατροφοδότηση με μη αντικειμενικό τρόπο[63], αρκεί για να μεταβληθεί ο τρόπος λειτουργίας του. Ενδεικτικά, αν σε έναν αυτοματοποιημένο εγκριτικό μηχανισμό δανειακών προϊόντων εισάγονται μόνο αποφάσεις εγκρίσεων ή απορρίψεων για μια συγκεκριμένη κατηγορία πελατών (π.χ. κάτοικοι μίας περιοχής), επηρεάζεται η λειτουργία του σε μελλοντική βάση, παρά την αρχική εκπαίδευση του μοντέλου με αντιπροσωπευτικά δεδομένα για το σύνολο του δυνητικού πελατολογίου.

Η υιοθέτηση του νέου Ευρωπαϊκού Κανονισμού για την ΤΝ αναμένεται να ενισχύσει σημαντικά τον έλεγχο τους. Ο καθορισμός ενιαίου πλαισίου για την αξιολόγηση των κινδύνων, την κατηγοριοποίηση των συστημάτων και την υιοθέτηση ενιαίων βασικών κανόνων και controls κατά την υλοποίηση και τη χρήση, θα συμβάλλει σημαντικά στο ΣΕΕ. Επιπλέον, θα επέλθει ισορροπία μεταξύ της εξυπηρέτησης των επιχειρησιακών απαιτήσεων και της προστασίας των συμφερόντων και των δικαιωμάτων των πελατών, γεγονός που δεν είναι θέσφατο στη σημερινή κατάσταση.

4.2 Case Studies: Συστήματα ΤΝ στην 1η και τη 2η γραμμή του ΣΕΕ Πιστωτικών Ιδρυμάτων

Η υιοθέτηση ΤΝ σε controls συστημάτων ενός ΠΙ έχει ιδιαίτερη αξία στη διασφάλιση των συναλλαγών, καθώς συνεισφέρει στον έγκαιρο εντοπισμό των υπόπτων και την εφαρμογή κατάλληλων μέτρων με γνώμονα τον κίνδυνο. Οι αυτόματα πραγματοποιούμενες ενέργειες, περιλαμβάνουν παραγωγή ειδοποιήσεων σε πραγματικό χρόνο, έγκριση ή

[63] Μη-ορθά ή δεδομένα που επηρεάζουν το αποτέλεσμα

απόρριψη της συναλλαγής, αποστολή αιτήματος για τη λήψη επιπρόσθετης επιβεβαίωσης και καταγραφή της προκειμένου να επεξεργασθεί σε μεταγενέστερο χρόνο. Η ανάπτυξη νέων στατιστικών μεθόδων μοντελοποίησης συνδυαστικά με την ολοένα αυξανόμενη διαθεσιμότητα (αξιόπιστων και μη) δεδομένων, ανοίγει νέους ορίζοντες πρακτικής εφαρμογής.

Στα συστήματα προστασίας συναλλαγών που πραγματοποιούνται μέσω ηλεκτρονικής τραπεζικής (Web και Mobile Banking), «ευφυείς» μηχανισμοί προστασίας με χρήση ΤΝ προστατεύουν την υποδομή από επιθέσεις που έχουν ως στόχο να πλήξουν τη διαθεσιμότητα της και την ακεραιότητα και την εμπιστευτικότητα τραπεζικών λογαριασμών και δεδομένων πελατών (DoS, intrusions, κ.α.). Η ΤΝ στα «τείχη προστασίας» (firewalls) και στους μηχανισμούς αποτροπής και εντοπισμού διεισδύσεων, αναλύει τη συμπεριφορά των επιτιθέμενων βάσει ιστορικού και δεδομένων που συλλέγονται καθ' όλη την διάρκεια της επίθεσης, ενεργοποιώντας τις απαιτούμενες ενέργειες αποτροπής για την προστασία της υποδομής (συμπεριλαμβανομένης της απενεργοποίησής της). Η λήψη αποφάσεων, στηρίζεται σε προκαθορισμένους αλγορίθμους ΤΝ και στατιστική ανάλυση του αντικτύπου σε πραγματικό χρόνο, συνδυαστικά με καθορισμένα σενάρια που έχουν «φορτωθεί» στα συστήματα. Επιπλέον, περιλαμβάνουν δυνατότητες μάθησης μέσω ανατροφοδότησης[64], που πραγματοποιείται σε κάθε επίθεση που δέχονται ανεξαρτήτως αποτελέσματος (απόκρουση επίθεση ή πλήγμα στην υποδομή).

Η ΤτΕ (ΠΔΤΕ-2577/2006) έχει εντάξει στο ΣΕΕ την ύπαρξη μηχανισμού ανάλυσης του συναλλακτικού προφίλ για την προστασία των πελατών στις συναλλαγές ηλεκτρονικής τραπεζικής από επιτήδειους για την πραγματοποίηση απάτης. Η χρήση μεθόδων phishing για την υποκλοπή των χαρακτηριστικών σύνδεσης (credentials) στα συστήματα ηλεκτρονικής τραπεζικής[65], έχει οδηγήσει σε αλματώδη αύξηση του σχετικού δείκτη τα τελευταία χρόνια. Ο Ν.5019/2023 περιορίζει την ευθύνη των καταθετών (ΦΠ και ΝΠ) που διενεργούν πράξεις πληρωμής (διάθεση, μεταβίβαση, ανάληψη χρηματικών ποσών) σε περίπτωση που πέσουν θύματα σχετικής απάτης, θέτοντας χρηματικό όριο ύψους € 1.000

[64] Τα στοιχεία συλλέγονται αυτόματα από το ίδιο το σύστημα, από άλλα ή από τους διαχειριστές.
[65] Και πιο προηγμένες τεχνικές όπως vishing και sim swapping

(για βαριά αμέλεια) και θεσπίζοντας περιπτώσεις περιορισμού της ευθύνης όπως π.χ. όταν δεν υφίσταται πρόθεση ή δόλος για τις ζημίες που έχει υποστεί.

Η σημαντικότερη διάταξη, που οδήγησε τα ΠΙ να βελτιώσουν τα υφιστάμενα συστήματά τους εφαρμόζοντας ΤΝ, καταλογίζει την ευθύνη στον καταθέτη για όλες τις ζημίες από το phishing, αν ο πάροχος υπηρεσιών πληρωμών εφαρμόζει μέτρα ασφαλείας, υπέρτερα των απαιτούμενων, για την ισχυρή ταυτοποίηση των συναλλαγών (π.χ. τηλεφωνική επιβεβαίωση) που μπορούν να προκαλέσουν ζημία άνω του ορίου. Επιπλέον, καταλογίζεται ευθύνη στον καταθέτη για τη ζημία, εφόσον αποδειχθεί ότι δολίως αθέτησε τις υποχρεώσεις που προβλέπονται για τους χρήστες υπηρεσιών πληρωμών, όπως η άμεση ειδοποίηση του ΠΙ για απώλεια πιστωτικής κάρτας (PSD2, 2018).

Τα ΠΙ προκειμένου να εναρμονιστούν με τις απαιτήσεις, αναβάθμισαν τα εμπλεκόμενα συστήματα ενσωματώνοντας ΤΝ, ώστε να εντοπίζουν ηλεκτρονικές διευθύνσεις και χαρακτηριστικά φορητών συσκευών από τις οποίες συνδέεται ο χρήστης και βάσει κριτηρίων να παρεμποδίζουν τη συναλλαγή (π.χ. η σύνδεση από χώρες με απαγόρευση συναλλαγών, μη δηλωθείσα συσκευή στο ΠΙ). Παράλληλα, μέσω σεναρίων διαπιστώνονται έγκαιρα ενέργειες που δεν ταιριάζουν στο συναλλακτικό προφίλ του πελάτη ή ακολουθούν μοτίβα που αντιστοιχούν σε απάτη, όπως η πραγματοποίηση πολλαπλών εμβασμάτων σε άλλους λογαριασμούς, ανεξαρτήτως προορισμού, από πελάτη που χρησιμοποιεί την υπηρεσία ηλεκτρονικής τραπεζικής σχεδόν αποκλειστικά για πληρωμές λογαριασμών[66]. Αντίστοιχα, η πραγματοποίηση συναλλαγών αμέσως μετά την αλλαγή κωδικού πρόσβασης ή/και συσκευής, ενεργοποιεί τους μηχανισμούς ζητώντας την εκ νέου αυθεντικοποίησή του (μέσω εφαρμογής ή καλώντας το τηλεφωνικό κέντρο) προκειμένου να επιβεβαιώσει τη συναλλαγή.

Βασική αρχή λειτουργίας των παραπάνω μηχανισμών είναι η κατάρτιση συναλλακτικού προφίλ για τον πελάτη, βάσει του ιστορικού που συλλέγεται. Οι πραγματοποιούμενες κινήσεις αντιπαρατίθενται με αυτό, με την ταυτοποίηση και την αξιολόγηση των χαρακτηριστικών της σύνδεσής του (π.χ. ανεπιτυχείς προσπάθειες σύνδεσης) και επιλέγεται

[66] Το ποσό κάθε συναλλαγής ενδέχεται να μη συνυπολογιστεί καθώς πολλαπλές χαμηλόποσες συναλλαγές παρατηρούνται συχνά σε περιπτώσεις απάτης.

το καταλληλότερο μέτρο – απόρριψη, αποδοχή, αίτημα παροχής επιπρόσθετου κωδικού ασφαλείας μέσω email, παραγωγή ειδοποίησης για ενδεχόμενη απάτη.

Στο συναλλακτικό προφίλ του πελάτη στηρίζονται και τα συστήματα AML/CFT, συνδυαστικά με τη γνώση του πελάτη από την πλευρά του ΠΙ, μέσα από τη διαδικασία "Know-Your-Customer" (KYC) και την περιοδική λήψη βασικών στοιχείων πιστοποίησης (ΑΔΤ, ΑΦΜ, διευθύνσεις κατοικίας και εργασίας κ.α.) συνοδεία των σχετικών εντύπων πιστοποίησης τους (Ν.4557/2018). Η 1η γραμμή του ΣΕΕ έχει την ευθύνη πιστοποίησης των πελατών, ενώ η 2η γραμμή καθορίζει τα σενάρια για τον εντοπισμό συναλλαγών και εμπλεκόμενων προσώπων. Σημειώνεται ότι βάσει της σχετικής νομοθεσίας τα ΠΙ υποχρεώνονται να διακόψουν τη σχέση με πελάτες ενεχόμενους με αντίστοιχες πράξεις όσο και να τους αναφέρουν Αρχή Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες.

Οι αλγόριθμοι που υιοθετούνται στηρίζονται στην εντατική και σε πραγματικό χρόνο ανάλυση των συναλλαγών που πραγματοποιούνται σχετικά με την προέλευσή τους, τα προσωπικά στοιχεία του πελάτη, λίστες ατόμων που εμπλέκονται σε παράνομες ενέργειες ή και χωρών που έχουν καταδικαστεί για σχετικές πράξεις και εφόσον ταυτοποιηθούν ως ύποπτες δεν πραγματοποιούνται. Σε δεύτερο χρόνο αναλύονται βάσει σεναρίων και συγκρίνονται με το συναλλακτικό προφίλ του πελάτη, προκειμένου να χαρακτηριστούν κατάλληλα όσες ενέχουν σημαντικό κίνδυνο AML/CFT και να αυξηθεί ανάλογα το επίπεδο κινδύνου του Πελάτη προκειμένου να εφαρμοστούν μέτρα δέουσας επιμέλειας σε επόμενες συναλλαγές. Επιπλέον, καθορίζονται όρια, που εφόσον ξεπεραστούν, επιβάλλονται από το ΠΙ κυρώσεις στον πελάτη, όπως μείωση του χρηματικού ορίων συναλλαγών, εντατική παρακολούθηση, διακοπή σχέσης και αναφορά του.

Λόγω των υφιστάμενων ελλείψεων στα συστήματα των ΠΙ αναφορικά με τα δεδομένα πιστοποίησης του πελάτη[67], η εις βάθος ανάλυση απαιτεί την εκτέλεση πολλαπλών κανόνων βάσει σεναρίων ΤΝ που αντιπαρέρχονται τα προβλήματα ποιότητας για να καταλήξουν σε ασφαλή συμπεράσματα. Παράλληλα δημιουργούνται κανόνες που εξετάζουν το συναλλακτικό αποτύπωμα του πελάτη σε διάφορες περιόδους (ημερήσια/

[67] Μειούμενες με ταχείς ρυθμούς μέσω της ηλεκτρονικής πιστοποίησης και των στοιχείων που αντλούνται από ψηφιακές πύλες (π.χ. e-Gov.gr).

εβδομαδιαία/μηνιαία). Τα αποτελέσματα συνθέτουν ένα είδους score που εκτιμάται βάσει προκαθορισμένων ορίων που προκύπτουν από την ανάλυση του συνόλου των πελατών, προκειμένου να εκτιμηθεί ο κίνδυνος για τον συγκεκριμένο. Παράλληλα, η αξιολόγηση των αποτελεσμάτων ανατροφοδοτείται περιοδικά (ή/και σε συχνή βάση) στο σύστημα ώστε να μειωθεί ο όγκος των false-positive περιπτώσεων καθώς και για την εκπαίδευση του αλγορίθμου.

Στα ΠΙ ο κίνδυνος εσωτερικής απάτης περιλαμβάνει ενέργειες που πραγματοποιούνται από το Προσωπικό του, και δεν συμμορφώνονται με τις εσωτερικές οδηγίες και πολιτικές, το κανονιστικό και το νομικό πλαίσιο. Η αρμοδιότητα εντοπισμού και αντιμετώπισής της ανήκει σε εξειδικευμένο όργανο κατάλληλα στελεχωμένο, που στις περισσότερες περιπτώσεις ανήκει ή κατ' ελάχιστον συνεργάζεται στενά με την μονάδα ΕΕ (ΠΔΤΕ2577, 2006) και τις μονάδες διαχείρισης κινδύνων. Το έργο τους διευκολύνεται από την υιοθέτηση μηχανισμών ΤΝ και ανάλυσης δεδομένων, με σκοπό τον έγκαιρο εντοπισμό της, των εμπλεκομένων, τον προσδιορισμό του τρόπου πραγματοποίησής της, τη συλλογή των αποδεικτικών στοιχείων, τον καθορισμό των νομικών προεκτάσεων και την εκτίμηση της ζημίας που προκλήθηκε.

Η δημιουργία σεναρίων για τις αναλύσεις δεδομένων αποτελεί την βάση της παραπάνω διαδικασίας. Οι πληροφορίες ποικίλουν και περιλαμβάνουν ημερολόγια των συστημάτων που χρησιμοποιούνται (π.χ. logs από συστήματα απομακρυσμένης πρόσβασης, ημερολόγια συστήματος ηλεκτρονικού ταχυδρομείου)[68] και συναλλαγές που πραγματοποιήθηκαν. Η ανάλυση τους εστιάζει στον εντοπισμό μη συμβατών συναλλαγών και ενεργειών που συνδυαστικά απλώνονται σε μία ευρύτερη γκάμα ΣΠ (π.χ. απομακρυσμένη διενέργεια συναλλαγών, με χρήση τερματικών άλλων λειτουργών).

Η συνεισφορά της ΤΝ, συνίσταται στις αυξημένες δυνατότητες που προσφέρει για τη συνδυαστική ανάλυση μεγάλου όγκου δεδομένων και για τον προσδιορισμό μη προφανών συσχετίσεων μεταξύ διαφορετικών τύπων δεδομένων (π.χ. δομημένων και μη). Παράλληλα, καθίσταται εφικτός ο εντοπισμός συγκεκριμένων μοτίβων συναλλαγών και ενεργειών σε μία πληθώρα συστημάτων τα ημερολόγια των οποίων δεν είναι απολύτως συμβατά ως προς

[68] Περιλαμβάνουν βασικές πληροφορίες των ανταλλασσόμενων μηνυμάτων (π.χ. αποστολείς, παραλήπτες, θέμα, ονομασίες attachments κ.α.) και σε καμία περίπτωση το περιεχόμενο του μηνύματος και επισυναπτόμενων αρχείων.

τη μορφή τους. Η εκτίμηση και η προσωπική κρίση του ελεγκτή θα επιβεβαιώσουν την αποτελεσματικότητα του συστήματος και θα κατευθύνουν την έρευνα προς άλλες πτυχές της. Επιπλέον, συνεισφέρει σημαντικά στην ταχύτατη επεξεργασία των δεδομένων, ενδεχομένως και σε πραγματικό χρόνο, παράγοντας κρίσιμος στη διερεύνηση υποθέσεων απάτης.

Παράλληλα, πέρα από τον καταλογισμό ευθυνών και ενδεχομένως πειθαρχικών ποινών, ορισμένες μη συμβατές ενέργειες λειτουργών της επιχείρησης ενδέχεται να έχουν ακούσιο χαρακτήρα και να οφείλονται σε αδυναμίες της διαδικασίας, των ΣΠ και των controls. Ο έγκαιρος εντοπισμός και η τεκμηριωμένη ανάλυση των παραπάνω περιπτώσεων μέσω ΤΝ, οδηγεί σε διορθωτικά μέτρα περιορισμού των κινδύνων, καθιστώντας την ΤΝ αρωγό τόσο του ΕΕ όσο και της 2ης γραμμής.

4.3 Τεχνητή Νοημοσύνη στην 3η Γραμμή – Εσωτερικός Έλεγχος

Η αναγκαία προσαρμογή του ελεγκτή στις νέες απαιτήσεις προϋποθέτει την κατανόηση του τρόπου λειτουργίας της ΤΝ καθώς και των αλλαγών που επιφέρει ή έχουν ήδη επέλθει στο ΣΕΕ. Η ΤΝ εισβάλει σε όλες της φάσεις ενός ελέγχου από το σχεδιασμό μέχρι και το κλείσιμο/ολοκλήρωσή του με την αρχειοθέτηση της σχετικής τεκμηρίωσης των αποδεικτικών στοιχείων.

Στη φάση του σχεδιασμού μέσω ΤΝ καταγράφονται πρακτικά των συναντήσεων για την κατανόηση του χώρου και αναλύονται με τη χρήση τεχνικών NLP και αναγνώρισης φωνής. Αντίστοιχα μέσω ML και data analytics γίνεται αξιολόγηση των κινδύνων στο σύνολο της περιοχής, δομικό στοιχείο στην πραγματοποίηση ενός ελέγχου. Σε δεύτερη φάση απαιτείται η εκτίμηση των controls, που παραδοσιακά πραγματοποιούνταν με την επισκόπηση των πολιτικών και των διαδικασιών της περιοχής, συναντήσεις με τους εμπλεκόμενους και χειροκίνητες δοκιμές[69]. Η ΤΝ συστηματοποιεί και εντατικοποιεί τους παραπάνω ελέγχους, ψηφιοποιεί τη διεργασία και βοηθά στην ανάλυση των διαδικασιών και στον εντοπισμό ενδεχόμενων προβληματικών σημείων.

[69] Μέσω παρατήρησης, επισκόπησης εγγράφων, επανεκτέλεσης διαδικασιών κ.α.

Ο θετικός αντίκτυπος των μηχανισμών ΤΝ και των data analytics στην κύρια φάση του ελέγχου κρίνεται σημαντικός, καθώς καθίσταται εφικτή η ανάλυση των δεδομένων και η αντιπαραβολή τους με το σύνολο των πρωτογενών στοιχείων (π.χ. λογιστικές εγγραφές-παραστατικά τιμολογίων). Επιπλέον, μέσα από τη στατιστική ανάλυση πραγματοποιούνται προβλέψεις[70] που συγκρινόμενες με τις πραγματικές ενέργειες εντοπίζουν αδυναμίες στο σχεδιασμό και την υλοποίηση μίας διαδικασίας, ενώ παράλληλα διευκολύνει τον εντοπισμό συναλλαγών με υποψία απάτης. Τέλος, η σύνταξη της αναφοράς διευκολύνεται καθώς πραγματοποιούμενη με χρήση εργαλείων ΤΝ, συμπεριλαμβανομένης της εκτίμησης του κινδύνου κάθε ευρήματος, τη συνολική αξιολόγηση και γνώμης βάσει αυτού.

Με την ΤΝ λύνονται περίπλοκα και απαιτητικά προβλήματα της καθημερινότητας των ελεγκτών, σε σημαντικά μικρότερο χρόνο και σε μεγαλύτερη έκταση. Ωστόσο, η υιοθέτησή στις καθημερινές εργασίες μίας επιχείρησης, συμπεριλαμβανομένου του εσωτερικού ελέγχου μοιάζει με «δαμόκλειο σπάθη»[71]. Προσφέρει εντυπωσιακές δυνατότητες, που ανοίγουν μεγαλύτερους ορίζοντες στις δυνατότητες του ελέγχου, μέσα από τους ταχύτατους και σχετικά αξιόπιστους αλγορίθμους επεξεργασίας δεδομένων. Ωστόσο, οι ελεγκτές πέρα από τη χρήση νοημοσύνης – με διαφορετική προσέγγιση από τα ΣΠ – χρησιμοποιούν συναισθήματα και προσωπική κρίση για να φτάσουν σε συμπεράσματα, κάτι που στην παρούσα φάση δεν προσφέρεται από τα υπολογιστικά συστήματα (Ramachandran, 2019). Η έλλειψη καλής γνώσης για τη χρήση της μπορεί να οδηγήσει στην υιοθέτησή της εξαιτίας πιέσεων από την αγορά και ανταγωνισμού, ενώ οι απαιτήσεις προστασίας των προσωπικών δεδομένων έναντι ενδεχόμενων παραβιάσεων εσκεμμένων ή ακούσιων δεν θα πρέπει να αμελούνται. Η ασφάλεια των ΣΠ που επεξεργάζονται τα δεδομένα είναι θεμελιώδης προκειμένου να μην αυξάνεται ο κίνδυνος διαρροής.

Η άγνοια γύρω από τις δυνατότητες της ΤΝ ενδέχεται να οδηγήσει σε ακούσια ή και εκούσια λάθη των ελεγκτών κατά την εφαρμογή της. Η παρακολούθηση των δραστηριοτήτων που πραγματοποιούνται από αυτή σε συνδυασμό με τον διαχωρισμό

[70] Για τον όγκο των πωλήσεων, το είδος, την αναγκαιότητα πραγματοποίησης παραγγελιών και την ποσότητά τους κ.α.

[71] Σύμφωνα με την Ελληνική μυθολογία ο βασιλιάς Διονύσιος που παραχώρησε την εξουσία για μία ημέρα στον αυλοκόλακα Δαμοκλή, είχε κρεμασμένο ένα μεγάλο ξίφος στηριζόμενο σε τρίχες αλόγου για να του θυμίζει τον καθημερινό κίνδυνο για τη ζωή του όταν ελάμβανε μεγάλες αποφάσεις.

καθηκόντων αποτελούν κύριες πρακτικές προκειμένου να αποφευχθούν και να περιοριστούν γεγονότα με, ενδεχομένως, καταστροφικές συνέπειες για τον έλεγχο και το ΣΕΕ της επιχείρησης. Η επιλογή των δεδομένων «εκπαίδευσης» των εν λόγω συστημάτων πρέπει να διασφαλίζουν την ιδιωτικότητα των εμπλεκομένων και παράλληλα την αξιοπιστία των αποτελεσμάτων. Η αντικειμενικότητα και η ανεξαρτησία επιλογής, διαδραματίζει κύριο ρόλο στην ποιότητα του αποτελέσματος, και οι έλεγχοι των controls που αφορούν στην ποιότητα και στην καταλληλότητά τους πρέπει να ενταχθούν στον αρχικό σχεδιασμό. Βασικός στόχος είναι η διασφάλιση της αξιοπιστίας και της αποτελεσματικότητας των controls, στο βαθμό που στηρίζονται σε αντίστοιχα δεδομένα, στο πλαίσιο των αυξανόμενων, τα τελευταία χρόνια, κανονιστικών απαιτήσεων, ιδιαιτέρως στο τραπεζικό σύστημα[72].

Τα τελευταία χρόνια αναπτύσσονται συστήματα ανάλυσης των εκφράσεων του προσώπου, του τρόπου ομιλίας και των λεγομένων ενός υπόπτου για κάποια απάτη, με τα οποία εφοδιάζονται ολοένα και περισσότερα τμήματα καταπολέμησής της (οι μηχανισμοί αυτοί εντάσσονται στα συστήματα ML με ανατροφοδότηση συμπερασμάτων). Η απόλυτη εμπιστοσύνη σε αυτά, ενδέχεται να έχει ολέθριες συνέπειες για την αξιοπιστία των συμπερασμάτων καθώς η ανθρώπινη επαφή που είναι σημαντικό κομμάτι της διαδικασίας παρακάμπτεται, ενώ παράλληλα εγείρονται και σημαντικά θέματα ηθικής.

Η αυτοματοποιημένη επεξεργασία και παραγωγή σημαντικού όγκου δεδομένων της ελεγκτικής διαδικασίας θέτει σε κίνδυνο την ανθρώπινη διάσταση του ελέγχου. Η διερεύνηση μίας απάτης είναι μία πολυσύνθετη διαδικασία, που ο ανθρώπινος παράγοντας και κυρίως η κρίση έχουν καθοριστικό ρόλο. Για το τελικό συμπέρασμα απαιτείται η έγγραφη αλλά και προφορική δήλωση των ενεχομένων, από όπου προκύπτουν και υποθέσεις που στην παρούσα φάση δύσκολα μπορεί να επεξεργαστεί ένα σύστημα ΤΝ. Ο χειρισμός τέτοιων συστημάτων απαιτεί εξειδικευμένες γνώσεις που δεν διαθέτει το σύνολο των ελεγκτών. Η διαχείρισή τους και η ανάθεση καθηκόντων που σχετίζονται με το γνωσιακό τους υπόβαθρο θα πρέπει να αποτελεί κύριο μέλημα.

[72] Base's BCBS239 και US Dodd-Frank Wall Street Reform ad Consumer Protection Act αναφορικά με τον «κίνδυνο δεδομένων» (data risk).

4.4 Case Studies Μηχανισμών Τεχνητής Νοημοσύνης στην 3η Γραμμή

Οι προηγμένες αναλύσεις δεδομένων αποτελούν σημαντικό εργαλείο του ΕΕ όχι μόνο τον εντοπισμό εξαιρέσεων και παραβατικών συμπεριφορών, αλλά και για την πραγματοποίηση προβλέψεων και την εικονοποίηση των αποτελεσμάτων. Η χρήση στατιστικής και μοντελοποίησης δεδομένων με τη χρήση σύγχρονων εργαλείων βελτιώνει σημαντικά την ακρίβεια που επιτυγχάνεται στις αναλύσεις και προσθέτει ένα κομβικό βέλος στην φαρέτρα του ελεγκτή προκειμένου να γίνει αποδοτικότερη η καθημερινή εργασία του. Στα εν λόγω εργαλεία προστίθενται τα συστήματα CI, συμπεριλαμβανομένων των μηχανισμών αναγνώρισης και παραγωγής φυσικής γλώσσας[73] καθώς και ML με τα οποία βελτιώνονται οι δυνατότητες προβλέψεων από τα συστήματα ανάλυσης δεδομένων καθώς και η ίδια η λειτουργία τους (αυτό-μάθηση) βάσει των στοιχείων που τροφοδοτούνται.

Το ChatGPT αποτελεί την πρώτη εφαρμογή ΤΝ ευρείας χρήσης που πλήθος επιχειρήσεων σπεύδει να υιοθετήσει, καθώς προσφέρεται τόσο με τη μορφή αλγοριθμικής επεξεργασίας των δεδομένων που εισάγονται[74], όσο και για χρήση βάσει της «εκπαίδευσης» που έχει πραγματοποιηθεί από την κατασκευάστρια εταιρία. Στην πρώτη περίπτωση οι απαντήσεις εξαρτώνται αποκλειστικά από την εκπαίδευση της εφαρμογής από την επιχείρηση, καθώς αυτό αποτελεί αποκλειστική ευθύνη της, ενώ στη δεύτερη, οι απαντήσεις προκύπτουν από τα στοιχεία και τα δεδομένα που έχουν φορτωθεί στον αλγόριθμο από την εταιρία[75]. Σε κάθε περίπτωση, ο μηχανισμός εκπαιδεύεται και από την ανατροφοδότησή του χρήστη που αξιολογεί το αποτέλεσμα.

Σημαντικό πλήθος μονάδων ΕΕ και ελεγκτών κάνουν χρήση της ελεύθερης πλατφόρμας προκειμένου να καθορίσουν τα ελεγκτικά βήματα που θα χρησιμοποιήσουν. Τα παραγόμενα αποτελέσματα[76] κρίνονται σχετικώς αξιόπιστα καθώς οι προτεινόμενες ελεγκτικές διαδικασίες στηριζόντουσαν σε διεθνή πρότυπα και μεθόδους, με τα οποία έχει

[73] Natural Language Generation και Processing - μηχανισμοί που παρέχουν την δυνατότητα στα ΣΠ να παράγουν και κατανοήσουν τη φυσική γλώσσα. Ενδεικτικές εφαρμογές, είναι η Cortana των Microsoft Windows, η Siri της Apple και η Google Assistant για φορητές συσκευές.

[74] Δεδομένα φυσικής γλώσσας καθώς ο χρήστης διαλέγεται με τον μηχανισμό μέσω ερωτήσεων, που διαμορφώνονται βάσει των αποτελεσμάτων του αλγορίθμου και των απαντήσεων του χρήστη.

[75] Σύμφωνα με την OpenAI η εκπαίδευση του μηχανισμού πραγματοποιήθηκε με χρήση ~4 δις εγγραφών διαθέσιμες στο Διαδίκτυο.

[76] Όπως επιβεβαιώθηκε στις δοκιμές που πραγματοποιήθηκαν για την διπλωματικής εργασία.

εκπαιδευτεί ο αλγόριθμος, όπως και από τους τελικούς χρήστες. Ωστόσο, απαιτούν περαιτέρω επεξεργασία προκειμένου να προσαρμοστούν στις ανάγκες της επιχείρησης καθώς και του ελεγκτικού έργου που πρόκειται να πραγματοποιηθεί, καθώς το μέγεθος, οι δραστηριότητες και η δομή μίας επιχείρησης δεν είναι εφικτό για λόγους εμπιστευτικότητας να εισαχθούν στον αλγόριθμο αλλά λαμβάνονται υπόψη κατά την επεξεργασία του αποτελέσματος από τον ελεγκτή.

Στην περίπτωση χρήσης του εργαλείου αποκλειστικά από την επιχείρηση, τα εν λόγω στοιχεία αποτελούν αναπόσπαστο μέρος των δεδομένων εισόδου και εκπαίδευσης του μηχανισμού. Επιπλέον, στη βάση αποκλειστικής χρήσης του εργαλείου επιπρόσθετα δεδομένα όπως χαρακτηριστικά από απάτες[77], αποτελέσματα προηγούμενων ελέγχων, η επάρκεια του ΣΕΕ στην περιοχή, τα υλοποιημένα controls, εισάγονται στην «εκπαιδευτική» διαδικασία του αλγορίθμου. Το αποτέλεσμα θα είναι σαφέστατα βελτιωμένο ως προς τον προσανατολισμό και την προσαρμογή τους στις ανάγκες της επιχείρησης.

Η άκριτη αποδοχή από τον ελεγκτή (κατά την υιοθέτηση, χρήση ή και την εφαρμογή) των συμπερασμάτων σχετικών εργαλείων, ενδέχεται να επηρεάσει την απαιτητή κριτική σκέψη στην άσκηση των καθηκόντων του και τελικώς την ανεξαρτησία και την ακεραιότητά του. Σημαντικό ρόλο διαδραματίζει ο τρόπος εκπαίδευσης του αλγορίθμου που είναι άρρηκτα συνυφασμένος με την ποιότητα των δεδομένων και την αντικειμενικότητα στην επιλογή τους. Παράλληλα, η αξιολόγηση των συμπερασμάτων βάσει των πραγματικών συνθηκών, της κατάστασης της επιχείρησης και του στρατηγικού σχεδιασμού της, διασφαλίζουν το αποτέλεσμα. Τέλος, η συνεχής ανατροφοδότηση και επικαιροποίηση των δεδομένων που στηρίζεται ο αλγόριθμος, όπως νέων προτύπων και ερμηνειών, νέων ελεγκτικών βημάτων στην παγκόσμια βιβλιογραφία και των αποτελεσμάτων των ελέγχων που πραγματοποιήθηκαν, συντελούν στην αύξηση της αξιοπιστίας και στην επέκταση του πεδίου εφαρμογής όπως στην αξιολόγηση του ελεγκτικού περιβάλλοντος, στην αξιολόγηση και διαχείριση των κινδύνων και στην αξιολόγηση της συμμόρφωσης με το κανονιστικό πλαίσιο.

[77] Όπως η ζημιά που προκλήθηκε, το χρονικό εύρος, ο αριθμός των εμπλεκομένων προσώπων.

4.5 ΤΝ στον Έλεγχο: Απειλή ή Εργαλείο;

Η χρήση εφαρμογών ΤΝ αυξάνει την ποιότητα του αποτελέσματος που διασφαλίζουν οι ισχύοντες κανόνες και η συμμετοχή του ελεγκτή σε κάθε στάδιο της επεξεργασίας. Η ΤΝ δεν υιοθετείται αβασάνιστα και αβίαστα αλλά εφαρμόζεται κατά την κρίση του ελεγκτή για την ενδυνάμωση και την αύξηση της αξιοπιστίας του αποτελέσματος. Τα όποια λάθη πρέπει να εντοπίζονται και να καθίστανται ευδιάκριτα, επιτρέποντας τη συστηματική και έγκαιρη διόρθωσή τους. Παράλληλα βελτιώνεται σημαντικά ο απαιτούμενος χρόνος[78] για την υλοποίηση των εργασιών, μειώνοντας αντίστοιχα τα κόστη που αφορούν στην υλοποίηση του ελέγχου. Επιπλέον, διευκολύνεται ο προγραμματισμός των ελέγχων και η εστίαση σε περιοχές υψηλού κινδύνου καθώς και η συνεχής επιμέτρηση του κινδύνου με χρήση μηχανισμών ανάλυσης δεδομένων.

Το σημαντικότερο πλεονέκτημα που προστίθεται με την ΤΝ σχετίζεται με τον βασικό σκοπό του ΕΕ, που είναι να προσδίδει αξία στην επιχείρηση. Η δυνατότητα πραγματοποίησης ελέγχων στο σύνολο του πληθυσμού και όχι σε δείγμα[79], μεγιστοποιεί την αντίληψη της κατάστασης της επιχείρησης και παράλληλα ενισχύει το βαθμό διασφάλισης που παρέχεται στη διοίκηση. Επίσης, διευκολύνεται η μετάβαση στο μοντέλο του CA, εξασφαλίζοντας ότι πολύτιμες πληροφορίες για τη λειτουργία της επιχείρησης, τα χρήσιμα συμπεράσματα που προκύπτουν από τις αναλύσεις και αξιόπιστες αναφορές θα αποστέλλονται στα διοικητικά όργανα της.

Σε καμία περίπτωση δεν αποτελεί θέσφατο ότι η χρήση ΤΝ επιλύει το σύνολο των προβλημάτων που αντιμετωπίζει ο ΕΕ και το ΣΕΕ γενικότερα. Τα αποτελέσματα που προκύπτουν από τις αναλύσεις και την εφαρμογή της θα πρέπει να αξιολογούνται από τους ελεγκτές. Η έννοια του κινδύνου είναι αντικειμενικό στοιχείο, αλλά η αξιολόγησή του παραμένει υποκειμενική. Οι ενδείξεις για μία απάτη μπορεί να προκύπτουν από την επεξεργασία των δεδομένων, η μετατροπή τους όμως σε αποδείξεις και η συνολική

[78] Οι έρευνες δείχνουν μείωση ~90% του απαιτούμενου χρόνου ελέγχου σε περιοχές που εφαρμόζονται μηχανισμοί data analytics ή υιοθετείται ΤΝ.

[79] Δειγματοληπτικός έλεγχος: επιλογή δείγματος από το σύνολο του πληθυσμού με χρήση στατιστικών μεθόδων για τη διασφάλιση αντιπροσωπευτικότητας και της δυνατότητας προβολής των αποτελεσμάτων στο σύνολο (extrapolation).

αξιολόγηση των εμπλεκομένων καθώς και του βαθμού εμπλοκής τους παραμένει ευθύνη του ελεγκτή.

Επίσης, η αξιοπιστία των αποτελεσμάτων που προκύπτουν από την εφαρμογή ΤΝ και τις αναλύσεις δεδομένων είναι ικανοποιητικός αλλά σε καμία περίπτωση δεν είναι ο απόλυτος. Η επιλογή αυτών προς επεξεργασία καθώς και η «εκπαίδευση» του λογισμικού ιδίως για συστήματα ML παραμένουν στο πεδίο ευθύνης του ελεγκτή. Τα δύο στοιχεία αυτά αποτελούν καθοριστικούς παράγοντες στη διαμόρφωση αξιόπιστων αποτελεσμάτων, καθώς η ΤΝ χαρακτηρίζεται ως μη αντικειμενική μέθοδος λήψης αποφάσεων (non-bias) στη βάση ότι το αποτέλεσμα έχει υψηλή εξάρτηση από τα δεδομένα εισόδου.

Τέλος, η εκπαίδευση των ελεγκτών και συνολικά του ΕΕ σε σχέση με τη χρήση των νέων τεχνολογιών αποτελεί κομβικό σημείο για την επιτυχία του εγχειρήματος. Οι παραδοσιακές ελεγκτικές πρακτικές δεν μπαίνουν στο περιθώριο, αλλά μετασχηματίζονται προκειμένου να προσαρμοστούν στις σύγχρονες απαιτήσεις. Η ανάγκη πολύωρων χειροκίνητων αναζητήσεων για πιθανές εξαιρέσεις σε τιμολόγια, πραγματοποιείται πλέον με πιο στοχευμένο τρόπο βάσει της επεξεργασίας που προηγείται. Η βαρύτητα των τριών βασικών φάσεων του ελέγχου (προετοιμασία – ελεγκτική εργασία – συγγραφή αναφοράς), αλλάζει σημαντικά (π.χ. η προετοιμασία από 30% πλέον φτάνει στο 50% του ελεγκτικού χρόνου).

Το συμπέρασμα αναφορικά με την ενσωμάτωση ΤΝ στον ΕΕ προκύπτει εκ πρώτης όψεως μάλλον αβίαστα: δεν συνιστά απειλή, αλλά ένα πολύτιμο εργαλείο, που με ορθή χρήση και υλοποίηση σύμφωνα με τις ανάγκες μπορεί να δείξει (σ)το μέλλον. Τα προβλήματα και οι σκέψεις που συνοδεύουν τη χρήση ΤΝ σε κάθε έκφανση της ανθρώπινης δραστηριότητας δεν απουσιάζουν από την εφαρμογή της στον ΕΕ. Με τη λήψη κατάλληλων μέτρων, δύναται να περιοριστούν και η υιοθέτηση της ΤΝ να ενδυναμώσει το αποτέλεσμα, συνιστώντας μέσο που θα μειώσει τους πόρους για την πραγματοποίηση ελέγχων, θα αυξήσει την αποτελεσματικότητά του και θα μεγιστοποιήσει την προστιθέμενη αξία στην επιχείρηση.

ΚΕΦΑΛΑΙΟ 5 ΤΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΤΗΣ ΕΕ ΓΙΑ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΚΑΙ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ ΚΑΙ ΤΟΝ ΣΕΒΑΣΜΟ ΤΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΤΟΥ ΑΤΟΜΟΥ

Η ΕU μέσω των αρμοδίων οργάνων της ψήφισε τον Μάρτιο 2024 τον Κανονισμό που αφορά στη χρήση της ΤΝ σε συστήματα και εφαρμογές που τίθενται σε κυκλοφορία ή αναπτύσσονται στους κόλπους της, με σταδιακή εφαρμογή του μέχρι την 1η Αυγούστου 2026. Ο εν λόγω κανονισμός θα τεθεί σε ισχύ ταυτόχρονα και στα 27 κράτη-μέλη με δεσμευτικό χαρακτήρα[80].

Σε αυτόν τίθενται κανόνες για την κυκλοφορία στην ενιαία αγορά, την παροχή υπηρεσιών και τη χρήση της ΤΝ από όσους δραστηριοποιούνται στο χώρο στα κράτη μέλη, είτε στην παραγωγή ή στη διακίνηση των εν λόγω συστημάτων[81]. Συνεπώς, στο πεδίο εφαρμογής εμπίπτουν οι πάροχοι, χρήστες, εισαγωγείς, διανομείς και πωλητές εξοπλισμού που υιοθετούν μηχανισμούς ΤΝ.

Παράλληλα, καθορίζονται απαγορεύσεις και απαιτήσεις από τα συστήματα, βάσει της κατηγορίας κινδύνου που θα ενταχθούν κατά την αξιολόγησή τους, εφόσον χρησιμοποιούνται ή αναπτύσσονται από επιχειρήσεις εντός ΕU. Βασικός στόχος είναι η διάθεσή στην αγορά και χρήση συστημάτων ΤΝ που πληρούν συγκεκριμένες προδιαγραφές ασφαλείας και εναρμονίζονται με τις θεμελιώδεις αρχές και τις αξίες της Ένωσης. Η ΤΝ αναγνωρίζεται ως «οικογένεια τεχνολογιών», γρήγορα αναπτυσσόμενη και με θετικό οικονομικό και κοινωνικό αντίκτυπο σε όλο το φάσμα της βιομηχανίας και των κοινωνικών δραστηριοτήτων.

5.1 Ελληνική και Ευρωπαϊκή νομοθεσία για την ΤΝ

Ο Κανονισμός προορίζεται να αποτελέσει μέρος μίας ευρύτερης δέσμης μέτρων για την ανάπτυξη και τη χρήση της ΤΝ, καθορίζοντας την αλληλεπίδρασή και την εναρμόνισή του

[80] Δεν απαιτείται συγκεκριμένη νομοθεσία σε τοπικό επίπεδο, χωρία να απαγορεύεται, ενώ τέθηκε σε εφαρμογή από την 1η Αυγούστου 2024.

[81] Συμπεριλαμβανομένων αυτών που παράγονται σε τρίτες χώρες και κυκλοφορούν εντός της ΕU, εφόσον τα αποτελέσματα του συστήματος θα χρησιμοποιούνται εντός της Ένωσης.

με υφιστάμενους κανονισμούς και νομοθετικές ρυθμίσεις που αφορούν ή προσεγγίζουν σε κάποιο βαθμό ανάλογα θέματα υπό διαφορετική οπτική γωνία[82].

Ευθυγραμμίζεται με τον Χάρτη Θεμελιωδών Δικαιωμάτων της EU (ΧΘΔΕΕ) και ειδικότερα την προστασία των προσωπικών δεδομένων, λειτουργώντας επικουρικά στον σχετικό Κανονισμό, καθώς και με τη Συνθήκη για τη Λειτουργία της Ένωσης (άρθρα 114 και 16). Παράλληλα, συμπληρώνει την ισχύουσα ευρωπαϊκή νομοθεσία για την αποφυγή διακρίσεων που ενδέχεται να προκύψουν από κινδύνους αλγοριθμικής διάκρισης (ιδίως σε ότι αφορά στα σύνολα δεδομένων που χρησιμοποιούνται)[83].

Βασική αρχή είναι η διαχείριση των κινδύνων που απορρέουν από τα συστήματα που ενσωματώνουν μηχανισμούς ΤΝ. Προς τούτο, οργανώνει επίπεδα ρυθμιστικής παρέμβασης ανάλογα με το επίπεδο κινδύνου που αναγνωρίζεται σε αυτά. Συνεπώς, η κυκλοφορία ενός προϊόντος που υιοθετεί ΤΝ εντός EU[84] απαιτεί την αξιολόγησή του σύμφωνα με προκαθορισμένα κριτήρια. Αναλόγως της αξιολόγησης («μη αποδεκτού», «Υψηλού», «μεσαίου» και «χαμηλού» κινδύνου), καθορίζεται το πλαίσιο ανάπτυξης και προσδιορίζονται τα μέτρα που θα εφαρμοστούν κατά την κυκλοφορία του συστήματος, ώστε να συμμορφώνεται με τις απαιτήσεις.

Εικόνα 3. Κατηγοριοποίηση συστημάτων ΤΝ σύμφωνα με τον Ευρωπαϊκό Κανονισμό (πηγή Sisodia 2023)

[82] Ενδεικτικά ο κανονισμός για το CR των πελατών ΠΙ βάσει συναλλακτικής συμπεριφοράς και οικονομικής κατάστασης (Οδηγία 2013/36/EU).

[83] Αναμένονται αλλαγές και σε πλήθος άλλων Κανονισμών, οδηγιών και νόμων της EU μέρος όπως αναφέρονται στο τελευταίο τμήμα της πρότασης Κανονισμού.

[84] Ανεξαρτήτως αν έχει παραχθεί/αναπτυχθεί εντός ή εκτός EU - η αξιολόγηση πρέπει να γίνεται από τους εισαγωγείς ή/και τους εμπόρους – παρόχους.

Κάθε κράτος-μέλος θα ορίσει ή θα δημιουργήσει κανονιστική Αρχή, υπεύθυνη για την δημιουργία και υλοποίηση των απαιτούμενων διαδικασιών αξιολόγησης, ανάθεσης αρμοδιοτήτων και ενημέρωσης των μερών που θα αξιολογούν τη συμμόρφωση καθώς και την παρακολούθησή τους. Οι αξιολογητές οφείλουν να έχουν αντίστοιχα τις δικές τους εσωτερικές διαδικασίες βάσει των οποίων θα πραγματοποιήσουν την εκτίμηση και να εξασκούν με τον μέγιστο επαγγελματισμό τα καθήκοντά τους[85].

Ο Κανονισμός θέτει τους όρους αξιολόγησης από την Αρχή και τις απαιτήσεις για τον συντονισμό μεταξύ των εμπλεκόμενων μερών στην εκτίμηση του βαθμού συμμόρφωσης των συστημάτων. Καθορίζει τις απαιτήσεις για την παραχώρηση της πιστοποίησης αλλά και τυχόν εξαιρέσεις αναφορικά με περιπτώσεις που απαιτείται η επείγουσα παραχώρησή της, προκειμένου το σύστημα να ενταχθεί άμεσα στην αγορά. Επιπλέον, περιλαμβάνονται προβλέψεις για την διακυβέρνηση του εγχειρήματος καθορισμού κανόνων για την διάθεση στην αγορά και την ανάπτυξη συστημάτων ΤΝ εντός της ΕU και καθορίζονται μέτρα ανάπτυξης και υποστήριξης της καινοτομίας, με προτεραιότητα στις μικρές και τις μικρομεσαίες επιχειρήσεις.

Εν γένει, ο Κανονισμός στοχεύει μέσα από το ρυθμισμένο περιβάλλον που θα δημιουργηθεί και τις αλλαγές που θα επιφέρει σε ένα σύνολο τομέων[86] να προσδώσει ένα ανταγωνιστικό πλεονέκτημα στην ΕU και να υποστηρίξει την κοινωνική συνοχή. Παράλληλα θα παράσχει ασφάλεια δικαίου για την διευκόλυνση των επενδύσεων και της καινοτομίας στον τομέα της ΤΝ και την ανάπτυξη ενιαίας αγοράς για νόμιμα ασφαλή και αξιόπιστα συστήματα, προλαμβάνοντας ενδεχομένως τον κατακερματισμό της.

Εν αναμονή του νόμου με τον οποίο θα ενσωματωθούν οι απαιτήσεις του Ευρωπαϊκού Κανονισμού στην ελληνική νομοθεσία και θα εξειδικευθούν περαιτέρω οι διατάξεις του, παραμένει σε ισχύ ο Ν.4961/2022[87]. Το νομοθέτημα είχε ως στόχο την ανάπτυξη των σχετικών τεχνολογιών σε συνάρτηση με τις εξελίξεις στον τομέα της Πληροφορικής και την αξιοποίησή τους με θεμιτό και αξιόπιστο τρόπο στον δημόσιο και στον ιδιωτικό τομέα.

[85] Αντίστοιχες υποχρεώσεις ισχύουν και για τυχόν sub-contractors που ανατίθεται το σύνολο ή μέρος της διαδικασίας.

[86] Πρόβλεψη, βελτιστοποίηση των λειτουργιών κ.α.

[87] Στηρίζεται εν πολλοίς στη Λευκή Βίβλο για την ΤΝ του 2020, που αντικαταστάθηκε από τον Κανονισμό.

Λειτουργεί παράλληλα και σχεδόν συμπληρωματικά με τον ΓΚΠΔ, καθώς όπως ρητώς ορίζεται «*δεν θίγει τα δικαιώματα και τις υποχρεώσεις που απορρέουν από τον Κανονισμό αλλά και από το Ν.4624/2019, όπως ισχύει*».

Οι διατάξεις του καθορίζουν τις υποχρεώσεις τόσο των φορέων του δημοσίου όσο και των ιδιωτικών επιχειρήσεων αναφορικά με τη χρήση συστημάτων ΤΝ, συμπεριλαμβανομένης της παροχής πληροφόρησης αναφορικά με τις παραμέτρους λειτουργίας, τις αποφάσεις που λαμβάνονται, τα τεχνικά χαρακτηριστικά των συστημάτων καθώς και την ανάπτυξή τους σύμφωνα με την ισχύουσα νομοθεσία για τα προσωπικά δεδομένα. Επιπλέον, συστήνεται η τήρηση μητρώου συστημάτων ΤΝ καθώς και η εκπόνηση αλγοριθμικής εκτίμησης αντικτύπου (στους δημόσιους φορείς), προκειμένου να καθοριστούν μεταξύ άλλων ο σκοπός του συστήματος, οι δυνατότητες και οι παράμετροι λειτουργίας, το είδος των αποφάσεων και των πράξεων, οι κίνδυνοι που ελλοχεύουν από τη χρήση και το όφελος για το κοινωνικό σύνολο[88].

Κωδικοποιούνται διατάξεις που αφορούν στις ιδιωτικές επιχειρήσεις, για επιμέρους χρήσεις ΤΝ σε συστήματα επιλογής, πρόσληψης ή αξιολόγησης προσωπικού και τη δεοντολογική χρήση δεδομένων σε συστήματα ΤΝ. Τέλος, συστήνεται Συντονιστική Επιτροπή για την ΤΝ με σκοπό την κατάρτιση Εθνικής Στρατηγικής και, γενικότερα, την χάραξη πολιτικής γύρω από την ΤΝ και Επιτροπή για την εποπτεία της στρατηγικής, που μεριμνά για την υλοποίηση, τον συντονισμό των αρμοδίων φορέων και την μέριμνα για την εφαρμογή της.

Δεδομένης της ψήφισης του Κανονισμού, ο νόμος κρίνεται ως προπαρασκευαστικός των αλλαγών που επέρχονται. Στη λογική αυτή, εντάσσονται οι ρυθμίσεις για την ασφαλή χρήση της ΤΝ και τη ψηφιακή αναβάθμιση των δημόσιων και ιδιωτικών φορέων. Παράλληλα, ορίζεται ως προϋπόθεση συστημάτων ΤΝ, η δυνατότητα απόδειξης της νομιμότητας χρήσης τους, ενώ τα προβλεπόμενα πρόστιμα και οι κυρώσεις επιβάλλουν την έγκαιρη συμμόρφωση με το θεσμικό πλαίσιο. Άλλωστε οι διατάξεις του νέου Ευρωπαϊκού Κανονισμού, προβλέπουν και επεκτείνουν αυτές του ελληνικού νόμου και του θεσμικού πλαισίου που προϋπήρχε.

[88] Τα στοιχεία που αναφέρονται περιλαμβάνονται στο σύνολο τους και στον νέο Κανονισμό της EU

Σημειώνεται ότι πέρα των όσων ορίζονται για την ΤΝ, ο νόμος θεσπίζει το νομοθετικό πλαίσιο για το διαδίκτυο των πραγμάτων (Internet of Things - IoT), τη θεσμική ενίσχυση της ασφάλειας πληροφοριών και της προστασίας προσωπικών δεδομένων, την παροχή ταχυδρομικών υπηρεσιών με τη χρήση Συστημάτων μη Επανδρωμένων Αεροσκαφών (ΣμηΕΑ), τις τεχνολογίες κατανεμημένου καθολικού (ΤΚΚ), τα έξυπνα συμβόλαια και τις τρισδιάστατες εκτυπώσεις. Ο αντίκτυπος του δεν περιορίζεται στο ψηφιακό μετασχηματισμό του δημοσίου τομέα, αλλά επεκτείνεται και στην ψηφιακή οικονομία και τις συναλλαγές.

5.2 Ειδικές Ρυθμίσεις για Υψηλού Κινδύνου Συστήματα ΤΝ

Δομικό στοιχείο του Κανονισμού για την ΤΝ αποτελεί η αξιολόγηση των συστημάτων για τους κινδύνους που απορρέουν από αυτά, προκειμένου να καθοριστεί και το απαιτούμενο επίπεδο ρυθμιστικής παρέμβασης. Στο πλαίσιο αυτό, ορίζονται κριτήρια αξιολόγησης που αφορούν στη χρήση των εν λόγω συστημάτων (αντίκτυπος και αποτέλεσμα), ο σκοπός και το εύρος χρήσης ΤΝ σε αυτό. Τα κριτήρια εξειδικεύονται στις διάφορες κατηγορίες εξετάζοντας τον βαθμό αυτονομίας τους στη λήψη αποφάσεων, τη χρήση ειδικών δεδομένων (π.χ. βιομετρικά), τη συμμόρφωση με τους κανόνες της ΕΕ και τα δικαιώματα του ατόμου.

Για τις δύο πρώτες κατηγορίες αξιολόγησης («μη αποδεκτού» και «υψηλού κίνδυνου») υφίστανται ειδικές απαιτήσεις, που δεν καθορίζονται μόνο από τον νέο Κανονισμό αλλά και από προηγούμενες αποφάσεις των ευρωπαϊκών οργάνων, αναφορικά με την χρήση ρομποτικών μηχανισμών και αυτοματοποιημένων συστημάτων. Πέρα από τις ειδικές κατηγορίες χρήσης όπως απαριθμούνται στο Παράρτημά του και εντάσσουν αυτόματα τα συστήματα σε κάποια από αυτές, υφίστανται και υποχρεώσεις προκειμένου να επιτραπεί η κυκλοφορία εντός ΕΕ. Ειδικότερα για τα συστήματα με αξιολόγηση κινδύνου:

- «μη αποδεκτού»: δεν επιτρέπεται η κυκλοφορία τους, εκτός και αν ληφθούν μέτρα μείωσης του υφιστάμενου κινδύνου.
- «υψηλού»: θα τίθενται σε λειτουργία υπό την προϋπόθεση ότι ο κίνδυνος που ενέχει η χρήση τους είναι μικρότερος από τον αντίκτυπο που θα είχε η απαγόρευση

κυκλοφορίας τους στην αγορά. Αφορά συστήματα για την ασφάλεια[89], την υγεία και τα θεμελιώδη δικαιώματα των ατόμων, όσα εμπίπτουν στον Κανονισμό ασφαλείας της EU (παιχνίδια, ιατροτεχνολογικά προϊόντα) και τα αυτόνομα συστήματα ΤΝ προοριζόμενα για χρήση σε συγκεκριμένους τομείς της οικονομικής και της ανθρώπινης δραστηριότητας (π.χ. μετανάστευση, υποδομές ζωτικής σημασίας, επιβολή του νόμου, εκπαίδευση, εργασία κ.α.), όπως απαριθμούνται σε Παράρτημα του Κανονισμού.

- «μεσαίου» και «χαμηλού»: για τη μελλοντική συμμόρφωσή τους με τις απαιτήσεις του Κανονισμού, οι πάροχοι ενθαρρύνονται να υιοθετήσουν, εθελοντικά, κώδικες συμπεριφοράς ή να συμμορφωθούν με τις απαιτήσεις των συστημάτων υψηλού κινδύνου, κυρίως αναφορικά με τη δημιουργία τεχνικών προδιαγραφών και λύσεων σύμφωνα με τον σκοπό τους.

Συνεπώς, η ύπαρξη αναλυτικής τεκμηρίωσης των εφαρμοζόμενων μοντέλων αλλά και των αυτοματοποιημένων μηχανισμών συνεχούς ελέγχου και παρακολούθησης των κινδύνων θεωρούνται εκ των ουκ άνευ, καθ' όλη τη διάρκεια ζωής των εν λόγω συστημάτων. Για την διασφάλιση της διαφάνειας απαιτείται τεκμηρίωση του συνόλου των δεδομένων εισόδου και εξόδου με έμφαση στον τρόπο χρήσης των τελευταίων (άρθρο 15 – Accuracy, Robustness and Cybersecurity).

Στο πλαίσιο αυτό, η χρήση συστημάτων ΤΝ από τις μονάδες που αποτελούν το ΣΕΕ μιας επιχείρησης, απαιτεί το σύστημα διαχείρισης των κινδύνων (βάσει και των σχετικών απαιτήσεων που εισάγει ο Κανονισμός), να:

- Προσδιορίζει και να αναλύει τους τρέχοντες και τους προβλέψιμους κινδύνους.
- Εκτιμά και να αξιολογεί τους κινδύνους που προκύπτουν από τη χρήση του σύμφωνα με τον προκαθορισμένο σκοπό.
- Αξιολογεί τα δεδομένα που συλλέγονται.
- Υιοθετεί μέτρα διαχείρισης και περιορισμού των κινδύνων σε αποδεκτά επίπεδα[90].

[89] Ειδικά αν χρησιμοποιείται ως στοιχείο ασφαλείας ενός προϊόντος ή περιέχουν κάποιο σχετικό τμήμα.

[90] Περιορισμός του εναπομένοντος κινδύνου (residual risk) σε αποδεκτά επίπεδα σύμφωνα με το risk appetite που έχει καθοριστεί μετά την κυκλοφορία του προϊόντος και τη χρήση του σύμφωνα με τον σκοπό του, καθώς και ενδεχόμενη μη ορθή χρήση που δύναται να προβλεφθεί.

- Τηρούνται ημερολόγια χρήσης (logs) του συστήματος για ικανό χρονικό διάστημα με σκοπό την έγκαιρη διάγνωση και διερεύνηση τυχόν μη καθορισμένων συμπεριφορών του συστήματος. Τα καταγραφόμενα στοιχεία περιλαμβάνουν την ημερομηνία και την ώρα χρήσης, την βάση δεδομένων αναφοράς με την οποία αξιολογήθηκε το σύστημα και τα δεδομένα ταυτοποίησης.
- Λαμβάνονται αντίγραφα ασφαλείας (resilience).
- Υπάρχουν μηχανισμοί προστασίας του από δεδομένα που ενδέχεται να επηρεάσουν την λειτουργία, τα δεδομένα εισόδου και τις ροές επεξεργασίας του.

Σημειώνεται ότι η επίβλεψη της λειτουργίας του συστήματος από τον ανθρώπινο παράγοντα επιβάλλεται από τον Κανονισμό και εξειδικεύοντας τις απαιτήσεις (άρθρο 14-Human Oversight). Η ανθρώπινη επίβλεψη και διαχείριση θα πρέπει να διασφαλίζει την παρέμβαση που απαιτείται, τη δυνατότητα διόρθωσης και ερμηνείας των αποτελεσμάτων και τη δυνατότητα απόφασης για τα διάφορα στάδια επεξεργασίας και παρέμβασης στην λειτουργία του, συμπεριλαμβανομένης της διακοπής της[91].

Η αυτοματοποιημένη εκτέλεση του συστήματος και ανατροφοδότησή του με δεδομένα εξόδου χωρίς την ανθρώπινη παρέμβαση, κυρίως στη διαδικασία λήψης αποφάσεων και εκπαίδευσής του, δεν θα πρέπει πραγματοποιείται χωρίς επίβλεψη ("unattended") και κυρίως να οδηγεί σε προαποφασισμένα αποτελέσματα. Τέλος, στο πλαίσιο των αρμοδιοτήτων τους οι μηχανισμοί αυτοί θα πρέπει να καλύπτονται από το συστήματα διαχείρισης ποιότητας και ενδεχομένως μετά την ψήφιση και τη σταδιακή εφαρμογή του Κανονισμού να ενημερώνονται σχετικώς και οι τοπικές αρχές.

Καθώς η ΤΝ μπαίνει στη ζωή των ελεγκτών και των μονάδων διαχείρισης κινδύνων, διευκολύνοντας την καθημερινή εργασία, βοηθώντας σημαντικά στην αναγνώριση των κινδύνων και της τρωτότητας μιας επιχείρησης και φυσικά στην αντιμετώπισή τους, οι διατάξεις του Κανονισμού υποχρεώνουν τις μονάδες ελέγχου, να διασφαλίζουν την εναρμόνιση των επιχειρήσεων με τις απαιτήσεις του, ειδικά για συστήματα υψηλού κινδύνου.

Ο μη καθολικός ενδεχομένως ορισμός της ΤΝ, η ανάγκη αναδρομικής αξιολόγησης των υφιστάμενων συστημάτων, συμπεριλαμβανομένων τυχόν εξαιρέσεων και η πλήρης και

[91] Ύπαρξη "Stop" πλήκτρου ή άλλου χειροκίνητου τερματισμού.

διαφανής ενημέρωση για τις δυνατότητες και τις ευκαιρίες που προκύπτουν, αποτελούν μέρος των σημαντικότερων προκλήσεων στην εφαρμογή του Κανονισμού. Ο έλεγχος σε αυτή τη φάση οφείλει να αξιολογήσει τα υφιστάμενα συστήματα, για τυχόν υποκρύπτοντα θέματα, συμπεριλαμβανομένων και των αυτοματοποιήσεων, καθώς παρά την απλότητα στην υλοποίηση τους, η μη υποχρεωτική επιτήρησή από τον ανθρώπινο παράγοντα και η χρήση δεδομένων εξόδου ενδέχεται να ενέχει σημαντικούς κινδύνους.

5.3 ΤΝ και Προσωπικά Δεδομένα

Τα σύγχρονα συστήματα ΤΝ στηρίζουν τις αναλύσεις και τα συμπεράσματά τους στα δεδομένα που τροφοδοτούνται. Άλλωστε από γεννήσεως της ΤΝ υπήρχε ισχυρή εξάρτηση μεταξύ της ανάπτυξης της και κυρίως της αξιοπιστίας των αποτελεσμάτων της με τα δεδομένα εισόδου. Αρχικώς ήταν οι αποκαλούμενοι πίνακες γεγονότων (fact-tables) που απαιτούνταν από τα πρώιμα συστήματα ΤΝ για ανάλυση γεγονότων και παραγωγή αποτελεσμάτων βάσει ασαφούς λογικής (fuzzy logic), που όσο περισσότερα και πλήρη δεδομένα περιείχαν οδηγούσαν σε ακριβέστερα αποτελέσματα. Πλέον, οι πίνακες περιορισμένου μεγέθους και πληροφοριών αντικαθίστανται από δομές *«μεγάλων δεδομένων»* με περίσσεια απαιτούμενων πληροφοριών προς ανάλυση και διενέργεια προβλέψεων.

Αυτή ακριβώς η υπέρ-πληθώρα και υψηλή διαθεσιμότητα δεδομένων και πληροφοριών, σχεδόν για κάθε τομέα της ανθρώπινης δραστηριότητας, εγκυμονεί σημαντικούς κινδύνους. Ενδεικτικά, δεδομένα κίνησης που καταγράφονται από έξυπνες συσκευές (wearables, έξυπνα τηλέφωνα και GPS οχημάτων) μπορούν πλέον να συνδυαστούν με όσα συγκεντρώνονται από άλλες πηγές, να τύχουν επεξεργασίας και να παραχθούν αποτελέσματα που αφορούν το υποκείμενο χωρίς να είναι απαραίτητα εν γνώσει του.

Από εκεί απορρέει το ερώτημα αν η προέλευση και ενδεχομένως η νομιμότητας της επεξεργασίας των προσωπικών δεδομένων θυσιάζονται στον βωμό των ακριβέστερων συμπερασμάτων και της προσωποποίησής τους από συστήματα που υιοθετούν ΤΝ. Η χρησιμότητά τους παραμένει άγνωστη στο ευρύ κοινό, ενώ παράλληλα οι εταιρίες που αναπτύσσουν σχετικά συστήματα είτε αποκρύπτουν επιμελώς τις απαιτήσεις τους είτε προσφέρουν δελεαστικούς τρόπους για τη λήψη συγκατάθεσης για την παραχώρησή τους.

Ο ΓΚΠΔ θέτει αρχές και κατευθύνσεις αναφορικά με την νομιμότητα της επεξεργασίας και καθορίζει επακριβώς τα δικαιώματα του υποκειμένου. Παράλληλα, διαχωρίζει τα προσωπικά από τα δεδομένα ειδικών κατηγοριών (π.χ. υγείας, φυλετικής προέλευσης). Ο διαχωρισμός και ορισμός τους είναι κρίσιμος, προκειμένου το υποκείμενο να μην γίνεται αντικείμενο εκμετάλλευσης και επειδή τα συστήματα ΤΝ στηρίζονται σε αυτά για την παραγωγή ακριβέστερων και προσωποποιημένων αποτελεσμάτων.

Κρίνεται απαραίτητη η ύπαρξη πλαισίου διακυβέρνησης των δεδομένων που θα χρησιμοποιηθούν για την εκπαίδευση, την ανάπτυξη και την επικύρωση των υπολογιστικών μοντέλων που χρησιμοποιούνται από τους μηχανισμούς ΤΝ. Μέσω αυτού θα διασφαλίζεται η ποιότητα των δεδομένων, η αβίαστη χρήση και η ευθυγράμμισή τους με τον σκοπό και τις συνθήκες χρήσης του συστήματος.

Η χρήση προσωπικών δεδομένων σε διάφορες εφαρμογές ΤΝ έχει αποδειχθεί ιδιαίτερα σημαντική για τη λειτουργία τους όπως στις υπό ανάπτυξη εφαρμογές απονομής δικαιοσύνης που ανατροφοδοτούνται με αυτά των αποφάσεων των δικαστηρίων και τα χαρακτηριστικά των υποδίκων. Παράλληλα, σε ευρείας χρήσης εφαρμογές όπως αυτές που παρακολουθούν και μελετούν την καθημερινή μας δραστηριότητα, δεδομένα ειδικών ή όχι κατηγοριών (π.χ. θέματα υγείας, ύψος, βάρος) συλλέγονται και αποτελούν αντικείμενο επεξεργασίας ή περιλαμβάνονται στα δεδομένα εισόδου σχετικών μηχανισμών. Για παράδειγμα στα συστήματα μελέτης και ρύθμισης σε πραγματικό χρόνο της κίνησης των οχημάτων στους δρόμους των μεγαλουπόλεων, αριθμοί κυκλοφορίας, φωτογραφίες και βίντεο που ενδέχεται να περιλαμβάνονται και εικόνες των οδηγών και των επιβαινόντων χρησιμοποιούνται χωρίς ενδεχομένως την απαιτούμενη μέριμνα[92].

Αντίθετα, υπογραμμίζεται η αξία και η σημασία που ενδέχεται να έχουν κάποια εξ αυτών για σκοπούς πρόληψης ή καταστολής. Στις ιατρικές έρευνες τα φυλετικά στοιχεία ενδέχεται να διαδραματίζουν καταλυτικό ρόλο στην πρόγνωση εξάπλωσης, στην αποτελεσματικότητα της θεραπείας και στα συμπεράσματα στον γενικό πληθυσμό. Επιπλέον, «ηλεκτρονικά» προσωπικά δεδομένα όπως η διαδικτυακή διεύθυνση (IP address)

[92] Ενδέχεται να εμπίπτουν στη διαφύλαξη του δημόσιου συμφέροντος ή να διαφύλαξη ζωτικού συμφέροντος του υποκειμένου.

είναι ιδιαίτερα χρήσιμα για την ανάπτυξη αποτελεσματικών μηχανισμών προστασίας σε πραγματικό χρόνο.

Οι προϋποθέσεις που αναφέρονται στον Κανονισμό αναφορικά με τη βάση της νομιμότητας της επεξεργασίας των προσωπικών δεδομένων, εξακολουθούν να ισχύουν και στα συστήματα ΤΝ. Κατά συνέπεια θα πρέπει να λαμβάνεται η συγκατάθεση του υποκειμένου ή να εξετάζονται οι υπόλοιπες προϋποθέσεις όπως η εκτέλεση σύμβασης που το υποκείμενο είναι συμβαλλόμενο μέρος (π.χ. παροχή δανείου από ΠΙ), η εκπλήρωση υποχρεώσεων που απορρέουν από τον νόμο, η ικανοποίηση έννομου συμφέροντος κ.α. Ειδικά για τη συγκατάθεση, το υποκείμενο οφείλει να έχει πλήρη επίγνωση των όρων και του αντίκτυπου που έχει η επεξεργασία των προσωπικών δεδομένων του, να δίνεται επί συγκεκριμένου σκοπού και να γνωρίζει τα δικαιώματά όπως απορρέουν από τον Κανονισμό. Σε κάθε περίπτωση η ενημέρωση είναι υποχρεωτική ακόμα και αν τα δεδομένα δεν συλλέγονται από το υποκείμενο (άρθρο 14).

Η ΤΝ και τα οφέλη της δεν αποτελούν δικαιολογία για την παραβίαση των κανονισμών που αφορούν στην προστασία των δεδομένων αλλά και των δικαιωμάτων του ατόμου. Ενδεχομένως να είναι μία απειλή, ειδικά εάν αποκτώνται εν αγνοία του προσώπου (πλήρη ή μερική) ή στον τρόπο χρήσης των αποτελεσμάτων της επεξεργασίας. Αντισταθμιστικά προτείνεται η χρήση τεχνικών ψευδωνυμοποίησης ή ανωνυμοποίησης και η εφαρμογή των αρχών ελαχιστοποίησης και του καθορισμένου σκοπού της επεξεργασίας. Άλλωστε ο σεβασμός στα δικαιώματα του ανθρώπου καθώς και στις απαιτήσεις του ΓΚΠΔ περιλαμβάνονται τόσο στον εν ισχύ ελληνικό νόμο για την ΤΝ όσο και στον σχετικό Ευρωπαϊκό Κανονισμό.

5.4 Προσωπικά δεδομένα και ΕΕ

Οι απαιτήσεις του ΓΚΠΔ ισχύουν στο ακέραιο για τον ΕΕ, οι αρχές του αποτελούν σημεία-κλειδιά για τη διασφάλιση της ορθότητας και της νομιμότητας των επεξεργασιών που πραγματοποιούνται από τους ελεγκτές. Επιπλέον, στον κώδικα δεοντολογίας των ελεγκτών υπογραμμίζεται ο ρόλος του στη διαφύλαξη της εμπιστευτικότητας των επεξεργαζόμενων στοιχείων για το σύνολο της επιχείρησης.

Ειδικότερα, σε σχέση και με τις βασικές αρχές του ΓΚΠΔ και την επεξεργασία δεδομένων από ελεγκτές, απαιτείται ο σαφής καθορισμός του σκοπού της επεξεργασίας και η λήψη συγκατάθεσης του υποκειμένου[93] (π.χ. αποδοχή χρήσης καμερών στο περιβάλλον εργασίας). Πέρα από τη διασφάλιση της διαφάνειας, είναι απαραίτητος ο έλεγχος συμβατότητας του σκοπού και η εφαρμογή της αρχή της ελαχιστοποίησης, ώστε να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία. Η παραπάνω αρχή καθίσταται βασικός γνώμονας επεξεργασίας, συνδυαστικά με την αναζήτηση ενδεχομένως ηπιότερων μέσων για την επίτευξη του σκοπού της. Απαραίτητη είναι και η διασφάλιση της ακρίβειας σε όλες τις φάσεις επεξεργασίας και η εφαρμογή πολιτικής διατήρησης των δεδομένων για πεπερασμένο χρονικό διάστημα σύμφωνα με τις σχετικές πολιτικές της επιχείρησης.

Για τα δεδομένα που διαχειρίζεται ο έλεγχος θα πρέπει να λαμβάνονται υπόψη και τυχόν κανονιστικές απαιτήσεις που αφορούν στην τήρησή τους. Ενδεικτικά, η τεκμηρίωση που συγκεντρώνεται κατά τους τακτικούς ελέγχους διαφυλάσσεται σύμφωνα με τις απαιτήσεις της πολιτικής της επιχείρησης και συναρτήσει του ελεγκτικού κύκλου, ενώ σε διερευνήσεις απάτης το χρονικό διάστημα τήρησης προκύπτει από την κείμενη νομοθεσία και σε καμία περίπτωση δεν θα πρέπει να διαγράφονται πριν την τελεσιδικία της υπόθεσης[94].

Σημειώνεται ότι στην Ελληνική νομοθεσία αναφορικά με το ΣΕΕ και τις μονάδες ελέγχου, υπογραμμίζεται η «*πλήρης και απρόσκοπτη πρόσβαση σε όλα τα φυσικά στοιχεία και αρχεία του φορέα, που είναι αναγκαία κατά την εκτέλεση των καθηκόντων τους και συνεργάζονται με τους εργαζόμενους σε αυτόν, στο μέτρο που είναι απαραίτητο για την υλοποίηση του έργου τους*» (Άρθρο 22[Ε]) με την επιφύλαξη των περιορισμών που τίθενται από τους Ευρωπαϊκούς Κανονισμούς. Παράλληλα, τεκμηριώνεται η εχεμύθεια και η εμπιστευτικότητα των δεδομένων και των στοιχείων που περιέρχονται σε γνώση των ελεγκτών κατά την άσκηση των καθηκόντων τους.

Η χρήση μηχανισμών ΤΝ ή και αυτοματοποιημένης επεξεργασίας, ειδικά αν συνοδεύεται από ψευδωνυμοποίηση ή ανωνυμοποίηση των δεδομένων αποτελούν σημαντικά εργαλεία που διασφαλίζουν συμμόρφωση με τις απαιτήσεις. Η πρόσβαση σε

[93] Συνήθως μέσω της σύμβασης που υπογράφουν οι εργαζόμενοι, οι πελάτες και οι προμηθευτές διατυπώνονται οι απαιτήσεις επεξεργασίας με απλό και κατανοητό τρόπο.

[94] Εφόσον υφίσταται αγωγή προς ή από τους ενεχόμενους στην απάτη.

προσωπικά ή/και σε «ειδικά» δεδομένα[95], θα πρέπει να αποφεύγεται και σε κάθε περίπτωση να είναι ενήμερος ο Υπεύθυνος Προστασίας, παρέχοντας όπου είναι απαραίτητο σχετική εξουσιοδότηση. Η ύπαρξη μηχανισμών ασφαλείας, που θα διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα τους[96], εφαρμόζοντας στο ακέραιο τα privacy-by-design και privacy-by-default.

Ο έλεγχος δεν υπερβαίνει τις απαιτήσεις του ΓΚΠΔ, αλλά ασκεί τα καθήκοντα που του έχουν ανατεθεί συμμορφούμενος με τις διατάξεις τους. Διερευνά την πληρότητα και την ποιότητα των στοιχείων, εστιάζει στις επεξεργασίες που παρουσιάζουν υψηλό κίνδυνο για τα δικαιώματα[97], προτείνει ενέργειες βελτίωσης στην κατεύθυνση της προστασίας των δεδομένων των εργαζομένων, των πελατών και των προμηθευτών της επιχείρησης. Παρακάμψεις ή υπερβάσεις θέτουν σε κίνδυνο όχι μόνο την εμπιστευτικότητα και την ακεραιότητα των δεδομένων από μη εξουσιοδοτημένες επεξεργασίες αλλά τον ίδιο τον σκοπό του ελέγχου, για το σύνολο των γραμμών αμύνης.

[95] Ειδικές κατηγορίες δεδομένων όπως ιατρικά, φυλετικής ή εθνικής καταγωγής, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, βιομετρικά και γενετικά, δεδομένα υγείας κ.α.
[96] Τρίπτυχο Confidentiality – Integrity – Availability (CIA), αναπόσπαστο δομικό στοιχείο λειτουργίας των ΣΠ.
[97] Συμπεριλαμβανομένων των δεδομένων που χρησιμοποιούνται κατά το ελεγκτικό έργο.

ΚΕΦΑΛΑΙΟ 6. Η ΣΥΜΒΟΛΗ ΤΗΣ ΗΘΙΚΗΣ ΚΑΙ ΤΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ

Η ΤΝ αποτελεί μία πραγματικότητα έχοντας περάσει ήδη στην καθημερινότητα της ανθρώπινης δραστηριότητας, ενώ αναμένεται να ενισχύσει σημαντικά τη λήψη των αποφάσεων και την ανθρώπινη νοημοσύνη, χωρίς να οδηγήσει στην αντικατάστασή της. Παρότι τα τεχνολογικά επιτεύγματα και η ανάπτυξη συγκεκριμένων κλάδων της Πληροφορικής[98] βοηθούν στην κατεύθυνση ανάπτυξης συστημάτων που προσομοιώνουν ανθρώπινες δραστηριότητες με κάποιο βαθμό αυτονομίας, ανθρώπινης κίνησης, παρουσίασης συναισθημάτων και χειρισμού αντικειμένων, είναι κοινώς αποδεκτό ότι δεν είναι εφικτή η αντικατάσταση του ανθρώπινου νου. Άλλωστε, πώς θα αντικατασταθεί ο ανθρώπινος νους όταν ακόμα δεν έχει εξηγηθεί πλήρως ο τρόπος λειτουργίας του;

Παρότι σημαντικό μέρος των καθημερινώς χρησιμοποιούμενων συσκευών και των συστημάτων ενσωματώνει σχετικούς μηχανισμούς, σε πόσες περιπτώσεις η ανθρώπινη παρέμβαση είναι απαιτητή; Για παράδειγμα στα συστήματα αυτόνομης οδήγησης, μετά από σημαντικό αριθμό ατυχημάτων ενσωματώθηκε η οδηγία για την απενεργοποίηση του μηχανισμού σε περίπτωση που τα χέρια του οδηγού απομακρυνθούν από το τιμόνι. Επιπλέον, κατά πόσο οι αποφάσεις που λαμβάνονται από τα συστήματα ΤΝ αφήνουν περιθώριο στο χρήστη για την τελική απόφαση ή με έμμεσο τρόπο αποφασίζουν αυτά για εκείνον; Ο Κανονισμός απαντά στον ορισμό της ΤΝ αφήνοντας το περιθώριο *«κάποιου βαθμού αυτονομίας»* αλλά και με την υποχρέωση ανθρώπινης επίβλεψης και παρέμβασης στη λήψη αποφάσεων.

Τα νέα παγκόσμια ελεγκτικά πρότυπα του ΙΙΑ καθορίζουν τη λειτουργία του ΕΕ και προσεγγίζουν τον τρόπο επικοινωνίας με τη διοίκηση της επιχείρησης, διατηρώντας την ηθική ακεραιότητα και την ποιότητα στην καθημερινή εργασία, παρέχοντας ξεκάθαρη καθοδήγηση στους ελεγκτές (εξωτερικούς και εσωτερικούς) σε στρατηγικό και σε λειτουργικό επίπεδο. Σημαντική διαφοροποίηση από την προηγούμενη έκδοση, είναι η απαίτηση για επαυξημένη διαφάνεια για το έργο που επιτελεί η μονάδα ΕΕ της επιχείρησης. Τέλος, αυστηροποιείται η υποχρέωση συμμόρφωσης με τις ηθικές αρχές, που αντικαθιστούν

[98] Συστήματα διαχείρισης μεγάλων δεδομένων, νευρωνικά δίκτυα, στατιστικές και μαθηματικές αναλύσεις, μηχανική μάθηση κ.α.

τον «Κώδικα Δεοντολογίας», όπως υπογραμμίζεται και από τη χρήση της αγγλικής λέξης «must» που χρησιμοποιείται κατά την περιγραφή τους.

Οι ηθικές αρχές και οι απαιτήσεις των προτύπων εφαρμόζονται στο ακέραιο για τους εξωτερικούς και τους εσωτερικούς ελεγκτές. Η διάκριση εσωτερικού και εξωτερικού ελέγχου, έγκειται στη διαφορετική φιλοσοφία και χαρακτήρα (προληπτικός και κατασταλτικός αντίστοιχα) και τη με εξαρτημένη σχέση εργασίας με τον ελεγχόμενο καθώς ανήκουν σε επιχειρήσεις ανεξάρτητες από την ελεγχόμενη εταιρία για τον εξωτερικό σε αντίθεση με τον εσωτερικό που αμείβεται απευθείας από την επιχείρηση, κάτι που ενδεχομένως να θωρηθεί ότι δεν συνάδει με την ανεξάρτητη έκφρασή του[99]. Την άποψη αυτή επιτείνουν φαινόμενα πλημμελούς άσκησης καθηκόντων λόγω της κακώς εννοούμενης συναδελφικότητας και της υπαλληλικής σχέσης και μετριάζονται από τις σχετικές αρχές ηθικής.

Για τον περιορισμό των παραπάνω κινδύνων, καθορίζεται ένα ελάχιστο επίπεδο προσόντων και απαιτήσεων για τους ασκούντες το επάγγελμα του ελεγκτή, σχετικώς διαφοροποιημένα μεταξύ των εξωτερικών και των εσωτερικών. Στη χώρα μας, για παράδειγμα, απαιτούνται για τους ορκωτούς ελεγκτές ελάχιστος χρόνος ελεγκτικής εμπειρίας και επιτυχής εξέταση σε σειρά μαθημάτων, που διενεργούνται από το Σώμα Ορκωτών Λογιστών (ΣΟΕΛ), συνδυαστικά και με την κτήση τίτλου πιστοποίησης εγκεκριμένου ελεγκτή λογιστή (π.χ. CPA, ACA, ACCA, κ.λπ.). Επίσης, ο πρόσφατος νόμος έθεσε συγκεκριμένα κριτήρια προϋπηρεσίας, πιστοποίησης και σπουδών για τους ασκούντες το επάγγελμα του ελεγκτή προκειμένου να εγγραφούν στο σχετικό μητρώο[100].

6.1 Κώδικες Δεοντολογίας και Αρχές Ηθικής για τους Εσωτερικούς Ελεγκτές

Το ΙΙΑ κατά την πρόσφατη αναθεώρηση των παγκόσμιων προτύπων για την υιοθέτηση του ΣΕΕ στις επιχειρήσεις, προχώρησε στην αντικατάσταση του Κώδικα Δεοντολογίας με μία σειρά αρχών ηθικής που θα πρέπει να τηρεί το σύνολο των εμπλεκομένων στο μοντέλο διακυβέρνησης του ελέγχου και σε κάθε περίπτωση οι εσωτερικοί ελεγκτές. Ειδικότερα,

[99] Δεν αποτελούν τον γενικό κανόνα, καθώς στο σύνολο των επιχειρήσεων υφίστανται κανόνες ανεξαρτησίας και έλεγχος από τα εποπτικά όργανα.

[100] Ενδεικτικά ελάχιστη προϋπηρεσία 5 ετών, παρακολούθηση εισαγωγικών σεμιναρίων, ελεγκτικές πιστοποιήσεις, ελάχιστο επίπεδο σπουδών.

οφείλουν να συμμορφώνονται με πέντε βασικές αρχές καθώς και με τα standards που καθορίζονται για αυτές, ενώ προτείνονται και τρόποι υλοποίησης και επιμέτρησης του βαθμού συμμόρφωσης με αυτά.

Εικόνα 6. Βασικές αρχές εσωτερικού ελεγκτή (πηγή ΙΙΑ 2023)

Η συμμόρφωση με τις αρχές και τα πρότυπα που περικλείονται εγκαθιδρύει την εμπιστοσύνη στο επάγγελμα και τις υπηρεσίες του ελεγκτή, δημιουργώντας μία ηθική κουλτούρα στον ΕΕ. Παράλληλα, αποτελεί τη βάση για τη δημιουργία κλίματος αξιοπιστίας γύρω από τη δουλειά αλλά και την κρίση των ελεγκτών. Η συμμόρφωση με τις παραπάνω αρχές αλλά και συνολικά τα πρότυπα του ΙΙΑ απαιτείται ακόμα και όταν υπάρχουν επιπρόσθετοι κανόνες ηθικής και απαιτήσεις που επιβάλλονται από το νομικό πλαίσιο και τις πολιτικές/πρακτικές της επιχείρησης.

Η διοίκηση της μονάδας ΕΕ διασφαλίζει τη συμμόρφωση των πολιτικών, των διαδικασιών και των πρακτικών που εφαρμόζονται από τους ελεγκτές σε σχέση με τις παραπάνω αρχές. Τυχόν αποκλίσεις πρέπει να καταγραφούν και να αιτιολογηθούν κατάλληλα, εφόσον έχει εξαντληθεί κάθε δυνατότητα υιοθέτησης και υλοποίησης εναλλακτικών λύσεων προκειμένου να ευθυγραμμιστεί η λειτουργία της μονάδας με τα διεθνή πρότυπα. Στο πλαίσιο αυτό οι δημόσιοι φορείς έχουν εξειδικεύσει και προσαρμόσει τον κώδικα δεοντολογίας του ΙΙΑ. Η Εθνική Αρχή Διαφάνειας έχει εκδώσει σχετικό κώδικα

(Ιανουάριος 2021), που στη συνέχεια υιοθετήθηκε από σειρά άλλων φορέων[101]. Ο εν λόγω Κώδικας λειτουργεί επικουρικά και συνδυαστικά με άλλους που θεσπίζονται από το ελληνικό κράτος και διέπουν την άσκηση καθηκόντων του προσωπικού του δημοσίου και του ευρύτερου δημόσιου τομέα. Παράλληλα, με την επικαιροποίηση των διεθνών προτύπων οι εν λόγω κώδικες οφείλουν να αναθεωρηθούν και να προσαρμοστούν αντίστοιχα μέχρι και την ημερομηνία εφαρμογής τους[102], δεδομένου ότι βασικός πυλώνας της αναθεώρησης των προτύπων ήταν και η εφαρμογή τους στον δημόσιο τομέα, με τις ελάχιστες δυνατές προσαρμογές και τροποποιήσεις, ώστε να επιτευχθεί η καθολική εφαρμογή από το σύνολο των ενδιαφερόμενων και εμπλεκόμενων μερών.

6.2 Εφαρμογή και Υιοθέτηση

Τα διεθνή ελεγκτικά πρότυπα ορίζουν τις παραπάνω αρχές, αναλύουν τις απαιτήσεις και παράλληλα προτείνουν τρόπους για την εφαρμογή τους από τους ελεγκτές. Επιπλέον, παρέχονται μέθοδοι ώστε να μπορέσει η επιχείρηση να εφαρμόσει τις απαιτήσεις και να επιμετρήσει τον βαθμό συμμόρφωσής.

6.2.1 Ακεραιότητα

Ο ελεγκτής οφείλει να επιδεικνύει ακεραιότητα στη συμπεριφορά του και να ενεργεί με ειλικρίνεια και επαγγελματικό θάρρος. Οφείλουν να είναι αξιόπιστοι, ακριβείς, ξεκάθαροι και ανοικτοί κερδίζοντας τον σεβασμό σε κάθε επαγγελματική σχέση και επικοινωνία, ειδικά σε περιπτώσεις που εκφράζουν αντίθετη άποψη και οπτική σε σχέση με την πεποίθηση του ελεγχόμενου. Είναι υποχρέωση των ελεγκτών να παρουσιάζουν όλα τα σημαντικά γεγονότα που τους γνωστοποιούνται ή ανακαλύπτουν κατά τη διενέργεια των ελέγχων, ιδιαίτερα όταν η μη αποκάλυψή τους ενδέχεται να επηρεάσει τη δυνατότητα της επιχείρησης να λαμβάνει στρατηγικές αποφάσεις.

Παράλληλα, οι ελεγκτές πρέπει να δρουν και να συμπεριφέρονται σύμφωνα και με το νομικό και ηθικό πλαίσιο που έχει δημιουργηθεί στην επιχείρηση, να προωθούν τη σχετική κουλτούρα και να αναγνωρίζουν αντίθετες συμπεριφορές, υπό την προϋπόθεση ότι έχουν

[101] Ενδεικτικά Υπουργείο Ανάπτυξης, Πανεπιστήμια, Γενική Επιθεώρηση κ.ο.κ.
[102] Σύμφωνα με το IIA η εφαρμογή ξεκινά ένα έτος μετά τη δημοσίευσή τους, τον Ιανουάριο 2025.

άρτια γνώση και παράλληλα πλήρη κατανόησή του. Ενδεικτικά αναφέρονται το νομοθετικό πλαίσιο που ισχύει (πέραν των κανόνων και των πολιτικών των επιχειρήσεων) για εργαζομένους σε εταιρίες παροχής επενδυτικών υπηρεσιών (ΕΠΕΥ), εταιρίες αθλητικού στοιχηματισμού, δημοπρασιών και εισπρακτικές, καθώς και στα ΠΙ.

Προϋπόθεση των παραπάνω είναι και η ύπαρξη ενός σχετικού κώδικα δεοντολογίας και ηθικής, στηριζόμενο σε καταγεγραμμένες και ευρέως γνωστές πολιτικές και διαδικασίες. Οι εν λόγω διαδικασίες συνδυαστικά με τους αντικειμενικούς στόχους που έχουν εκ των προτέρων τεθεί από την επιχείρηση, είναι αυτές που θα προάγουν τις αξίες και την ηθική συμπεριφορά, βάζοντας τις βάσεις για τη δημιουργία αντίστοιχης κουλτούρας. Τα στοιχεία αυτά αποτελούν αντικείμενο ελέγχου (επιμέρους αλλά και συνολικά), αναφορικά με την καθολική εφαρμογή τους από τους εργαζόμενους της επιχείρησης.

Η αρμοδιότητα τήρησης και εφαρμογής ανήκει στον επικεφαλής του ΕΕ χωρίς να είναι άμοιροι ευθυνών οι ελεγκτές. Η συνεχής επιμόρφωση σε θέματα ηθικής βοηθά στη δημιουργία κουλτούρας και επίγνωσης καθώς και στην εξάσκηση πρακτικών που ενισχύουν την ειλικρινή και αξιόπιστη επικοινωνία, διασφαλίζοντας ότι θα ληφθούν οι σωστές αποφάσεις σε περίπτωση πραγματικών γεγονότων. Η καθοδήγηση και η έγκαιρη διαπίστωση τυχόν περιστατικών που ενδέχεται να δοκιμάσουν την ακεραιότητα και την αξιοπιστία των ελεγκτών, απαιτείται από τα πρώτα στάδια του ελεγκτικού έργου.

6.2.2 Αντικειμενικότητα

Οι ελεγκτές πρέπει να τηρούν αμερόληπτη στάση κατά την άσκηση των καθηκόντων τους και στη λήψη των αποφάσεων, που οφείλουν να έχουν αντικειμενική βάση ώστε να μην διακυβεύεται ο σκοπός του ελέγχου, η ανεξαρτησία του και να εκπληρώνονται με τον καλύτερο τρόπο τα ανατεθέντα καθήκοντα. Η επαγγελματική ατομική αμεροληψία οφείλει να στηρίζεται στη λήψη αποφάσεων βάσει ισορροπημένων κρίσεων και πραγματικών γεγονότων σε όλες τις καταστάσεις καθώς και στη δυνατότητα αναγνώρισης ενδεχόμενων προκαταλήψεων.

Συνεπώς, πρέπει να είναι σε θέση να αναγνωρίζουν, να αποφεύγουν και να περιορίζουν τις συνθήκες που ενδέχεται να επηρεάσουν την κρίση και την αντικειμενικότητά τους, όπως η αποδοχή δώρων, ανταμοιβών ή εξυπηρετήσεων και καταστάσεις σύγκρουσης

συμφερόντων. Ενδεικτικά, η πραγματοποίηση ελέγχου σε περιοχή που κατέχαν θέση ευθύνης[103] ή σε ΣΠ που συμμετείχαν στην ανάπτυξή τους, σε περιοχές που στο πλαίσιο των καθηκόντων του ΕΕ προσέφεραν συμβουλευτικές υπηρεσίες ή υπηρετούν συγγενικά πρόσωπα.

Σε περιπτώσεις που αναγνωρίζουν ότι επηρεάζεται η αντικειμενικότητά τους οφείλουν να ενημερώνουν έγκαιρα τα ενδιαφερόμενα μέρη. Με ευθύνη του επικεφαλής του ΕΕ καθορίζονται οι επόμενες ενέργειες προκειμένου να περιοριστούν οι συνέπειες (π.χ. αλλαγή της σύνθεσης της ομάδας, συνέχιση του ελέγχου χωρίς αλλαγές αλλά με εντατικότερη παρακολούθηση, αναβολή του ελέγχου, εξωτερική ανάθεση κ.α.). Πέρα από την ευθύνη και την επιμέλεια των ελεγκτών κατά την άσκηση των καθηκόντων τους. η ύπαρξη μεθοδολογιών και πολιτικών που αναγνωρίζουν ανάλογες συνθήκες και καθορίζουν τον τρόπο δράσης κρίνονται απαραίτητες[104].

6.2.3 Επαγγελματική Επάρκεια

Οι ελεγκτές οφείλουν να έχουν τις απαραίτητες γνώσεις, ικανότητες και δυνατότητες ώστε να φέρνουν εις πέρας τα έργα που τους ανατίθενται και σε κάθε περίπτωση να γνωρίζουν τις απαιτήσεις των προτύπων. Η εμπλοκή τους πρέπει να πραγματοποιείται μόνο σε έργα για τα οποία διαθέτουν σχετική γνώση. Παράλληλα με ευθύνη των προϊσταμένων τους αλλά και των ιδίων οφείλουν να αναπτύσσουν περαιτέρω την επάρκεια και τις ικανότητες τους μέσα από συνεχή εκπαιδευτικά προγράμματα.

Η ανάπτυξη επιτυγχάνεται μέσα από την επικοινωνία και τη συνεργασία με τα υπόλοιπα τμήματα όλων των γραμμών που συνθέτουν το ΣΕΕ της επιχείρησης, με παράλληλα οφέλη για τις άλλες δύο γραμμές, αλλά και τη συνεχή εκπαίδευσή τους σε θέματα που αντιμετωπίζουν στην καθημερινότητά τους. Οι περιοχές που θα πρέπει να επικεντρώνονται περιλαμβάνουν τους κινδύνους, την αναγνώριση και την αντιμετώπιση της απάτης, τα εργαλεία και τις τεχνικές για την ανάλυση και την αξιολόγηση των δεδομένων, τον αντίκτυπο από ενδεχόμενες απειλές που προκύπτουν από τις οικονομικές,

[103] Τα διεθνή πρότυπα καθορίζουν ελάχιστο διάστημα 12 μηνών

[104] Ενδεικτικά εργαλεία που υιοθετούνται ευρέως είναι οι πολιτικές σύγκρουσης συμφερόντων (αναφορά ετησίως περιοχών που παρατηρούνται συγκρούσεις), ανάθεση ελέγχων σε τρίτους, διαδικασίες αναφοράς τυχόν δώρων βάσει προκαθορισμένου ορίου.

οργανωτικές, περιβαλλοντικές, πολιτικές, νομικές και κοινωνικές συνθήκες στις οποίες λειτουργεί η επιχείρηση. Επιπλέον, είναι απαραίτητη η γνώση των τρεχουσών νομικών και κανονιστικών απαιτήσεων στο περιβάλλον δραστηριοποίησης της επιχείρησης. Το σύστημα διαχείρισης και αξιολόγησης ποιότητας της μονάδας ΕΕ, οφείλει να αναγνωρίζει περιοχές που χρήζουν περαιτέρω βελτίωσης και να καθορίζει τον τρόπο διαχείρισης και αντιμετώπισής τους.

6.2.4 Δέουσα Επαγγελματική Επιμέλεια

Οι ελεγκτές οφείλουν να ασκούν τα καθήκοντά τους, από το σχεδιασμό μέχρι και την υλοποίηση του ελέγχου, με τη δέουσα επαγγελματική επιμέλεια. Η συμμόρφωση με τα πρότυπα, η ανάλυση και προσαρμογή στη φύση, τις απαιτήσεις και τις συνθήκες του ελεγκτικού έργου καθώς και η κριτική σκέψη για την αξιολόγηση των πληροφοριών που συλλέγονται αποτελούν βασικά σημεία που αποδεικνύουν επαγγελματισμό.

Οφείλουν να σχεδιάζουν και πραγματοποιούν τον έλεγχο σύμφωνα με τα διεθνή πρότυπα και τη μεθοδολογία που έχει υιοθετηθεί και τεκμηριωθεί από την αντίστοιχη μονάδα της επιχείρησης[105]. Τα αποτελέσματα των υπηρεσιών τους κοινοποιούνται, χωρίς εκπτώσεις, στην ελεγχόμενη περιοχή και στα αρμόδια διοικητικά όργανα. Αντίστοιχα θα πρέπει να λαμβάνονται υπόψη και να εφαρμόζονται στις ελεγκτικές διαδικασίες και τυχόν απαιτήσεις από άλλες πηγές, όπως το νομικό και κανονιστικό πλαίσιο ενώ στον κανονισμό πρέπει να προβλέπονται περιπτώσεις που πρακτικές αντιτίθεται στα ελεγκτικά πρότυπα. Τέλος, τυχόν αδυναμίες συμμόρφωσης του ελεγκτή με κάποια από τις παραπάνω απαιτήσεις θα πρέπει να κοινοποιείται και να τεκμηριώνεται επαρκώς από τον επικεφαλής της μονάδας ΕΕ.

Στο πλαίσιο των καθηκόντων τους, οι ελεγκτές αξιολογούν τη στρατηγική και τους αντικειμενικούς στόχους της επιχείρησης καθώς και τα σημεία ενδιαφέροντος που υποδεικνύονται από τους ελεγχόμενους[106], συνδυαστικά με τα controls και τις διαδικασίες σε

[105] Το σύνολο των μεθοδολογιών μίας επιχείρησης πρέπει να είναι σαφώς τεκμηριωμένο και να συμμορφώνεται στο μέγιστο βαθμό με τα διεθνή πρότυπα.

[106] Τα σημεία που υποδεικνύονται δεν θα πρέπει να είναι αποκλειστικά το αντικείμενο του ελέγχου, αλλά μετά από αξιολόγηση να αποτελούν σημεία εστίασης.

περιοχές όπως η διακυβέρνηση του οργανισμού και η διαχείριση κινδύνων[107]. Για την επίτευξη των παραπάνω σκοπών, η συνεχής παρακολούθηση και προσαρμογή με τα διεθνή ελεγκτικά πρότυπα, με τις κανονιστικές και νομικές απαιτήσεις είναι το ελάχιστο απαιτητό, προκειμένου να πραγματοποιούνται έγκαιρα οι αναγκαίες προσαρμογές. Αντίστοιχα, τα παραπάνω σημεία πρέπει να λαμβάνονται υπόψη κατά τον σχεδιασμό του ελεγκτικού έργου, διασφαλίζοντας την νομική βάση αλλά και την ουσία του. Σε δεύτερο χρόνο, το σύστημα διαχείρισης ποιότητας παρακολουθεί για τυχόν εξαιρέσεις και καθορίζει τις απαιτούμενες ενέργειες.

Αντίστοιχα οι ελεγκτές οφείλουν να πραγματοποιούν τον έλεγχο με κριτική σκέψη, να αξιολογούν τα στοιχεία και τις πληροφορίες που συλλέγουν για την αξιοπιστία τους και να είναι ειλικρινείς στα θέματα που αναδεικνύουν καθώς και στα ερωτήματα που θέτουν. Σε περίπτωση που δεν διαθέτουν επαρκή στοιχεία για τη λήψη απόφασης, πρέπει να αναζητούνται επιπρόσθετες πληροφορίες προκειμένου να διασφαλιστεί το αποτέλεσμα.

6.2.5 Εμπιστευτικότητα

Οι ελεγκτές οφείλουν να ασκούν τα καθήκοντα τους με εμπιστευτικότητα προστατεύοντας το τελικό αποτέλεσμα του έργου τους. Οι ελεγκτές θεωρούνται στα διεθνή πρότυπα ως θεματοφύλακες της εμπιστευτικότητας, λαμβάνοντας υπόψη και τον όγκο αλλά και την αξία των πληροφοριών που έρχονται σε επαφή και αξιολογούν κατά την άσκηση των καθηκόντων τους. Στα δεδομένα αυτά περιλαμβάνονται και τυχόν προφορικές επικοινωνίες, πέραν των ψηφιακών ή των γραπτών στοιχείων που συλλέγουν, και προκύπτουν από επίσημες ή/και ανεπίσημες συναντήσεις. Οι παραπάνω πληροφορίες χρησιμοποιούνται σύμφωνα με τις πολιτικές και τις διαδικασίες της επιχείρησης και σε εναρμόνιση με το κανονιστικό και το νομικό πλαίσιο, και σε καμία περίπτωση για ίδιον όφελος ή σε αντίθεση με την ηθική διάσταση και απαιτήσεις.

Η σημασία της εμπιστευτικότητας των πληροφοριών που συλλέγονται κατά τη διάρκεια του ελεγκτικού έργου, υποδεικνύεται από τις ενδεχόμενες συνέπειες από τυχόν αποκάλυψή

[107] Πιθανά λάθη και ο κίνδυνος για απάτες ή μη συμμόρφωση με το νομικό και το κανονιστικό πλαίσιο οφείλουν να λαμβάνονται υπόψη σε κάθε στάδιο και στην αξιολόγηση.

τους[108]. Αντίστοιχης σημασίας είναι και η ύπαρξη πολιτικών και διαδικασιών για τη διαχείρισή τους, συμπεριλαμβανομένων της διαβαθμισμένης χρήσης, αποθήκευσης και καταστροφής τους[109]. Τα απαιτούμενα μέτρα είναι τόσο τεχνικά (π.χ. κρυπτογράφηση, χρήση κωδικών ασφαλείας) όσο και διαδικαστικά (π.χ. ο τρόπος καταστροφής εγγράφων, ο χρόνος τήρησής τους, η υποχρέωση μη αποκάλυψης).

6.3 Κώδικες Δεοντολογίας και Αρχές Ηθικής για την 1η και τη 2η Γραμμή

Σε αντίθεση με τα ισχύοντα για τους ελεγκτές, δεν έχουν δημιουργηθεί διεθνή πρότυπα για τις άλλες δύο γραμμές του ΣΕΕ. Οι κανόνες ηθικής και συμπεριφοράς καθορίζονται από το νομικό και κανονιστικό πλαίσιο που διέπει τις εργασίες και τα καθήκοντα καθενός από τα εμπλεκόμενα μέρη. Παράλληλα, αναφορικά με τον ελεγκτικό τους ρόλο εξακολουθούν να ισχύουν οι βασικές αρχές των ελεγκτών, όντας υπεύθυνοι για τον καθημερινό έλεγχο των συναλλαγών, την ανάλυσή τους για τον εντοπισμό λαθών ή και ενδεχομένως παραβατικών συμπεριφορών.

Οι αρχές της ακεραιότητας, της αντικειμενικότητας και της εμπιστευτικότητας αποτελούν αναπόσπαστα κομμάτια των κανόνων ηθικής που απαιτούνται στην άσκηση οποιουδήποτε επαγγέλματος. Περιλαμβάνονται άλλωστε, με εμφατικό τρόπο στην πλειοψηφία των περιπτώσεων, σχεδόν σε κάθε κώδικα δεοντολογίας που εκδίδεται από κάποιο δημόσιο οργανισμό και στις πολιτικές των επιχειρήσεων[110]. Παράλληλα, είναι αναπόσπαστο μέρος των συμβάσεων που υπογράφουν οι εργαζόμενοι κατά την πρόσληψή τους αλλά και των κανόνων δεοντολογίας[111] που υφίστανται σε τέτοιους οργανισμούς. Η ισχύς των εν λόγω κανόνων διασφαλίζεται και από τις Συλλογικές Συμβάσεις Εργασίας, που με τη σειρά τους σε αρκετές περιπτώσεις περιλαμβάνουν προβλέψεις ηθικής συμπεριφοράς.

[108] Πρόστιμα από τις κανονιστικές αρχές, φήμη για την επιχείρηση, παραβίαση των νόμων και του κανονιστικού πλαισίου, προσωπικές συνέπειες για τους εργαζόμενους κ.α.

[109] Είτε με το πέρας του ελεγκτικού έργου είτε μετά από καθορισμένο χρονικό διάστημα.

[110] Στα ΠΙ αποτελούν τμήμα των πολιτικών που εκδίδονται και εφαρμόζονται σε όλους τους τομείς δραστηριότητας.

[111] Συχνά αναφερόμενοι και ως «Οργανισμός Προσωπικού»

Σε σχέση με την επαγγελματική επάρκεια και επιμέλεια των επιφορτισμένων με ελεγκτικά καθήκοντα εργαζομένων στις άλλες δύο γραμμές του ΣΕΕ, διαπιστώνεται, βάσει των εφαρμοζόμενων πρακτικών, ότι υπάρχει πρόσφορο έδαφος για την υιοθέτηση και εφαρμογή τους. Η εκπαίδευση των στελεχών και η συνεχής παρακολούθηση των εξελίξεων και των μεταβολών που πραγματοποιούνται στο χώρο ευθύνης τους αποτελεί αναπόσπαστο κομμάτι.

Η αυτοματοποίηση των διαδικασιών καθώς και η χρήση ΤΝ στην καθημερινότητα των δύο πρώτων γραμμών, βοηθά στη διασφάλιση του αποτελέσματος και τη μείωση λαθών και παραλείψεων. Παράλληλα, αυξάνει σε κάποιο βαθμό τον κίνδυνο κατάχρησής για σκοπούς διάφορους από την αρχικό, και ενδεχομένως για κακόβουλες δραστηριότητες. Η υπευθυνότητα, η επαρκής εκπαίδευση και το σύστημα αξιών των στελεχών σε αυτές τις γραμμές, που έχουν την καθημερινή επαφή με τον πελάτη, την αρμοδιότητα διαχείρισης και εντοπισμού των κινδύνων αποτελούν εχέγγυα πρόληψης και έγκαιρης διάγνωσης, ενδεχομένως και καταστολής σχετικών φαινομένων. Παράλληλα, συμβάλλουν σημαντικά και αποτελούν εργαλεία περαιτέρω μείωσης των εγγενών και υπολειπόμενου κινδύνου.

Τα ζητήματα ευθύνης που προκύπτουν από την έλλειψη ικανότητας αυτοκαθορισμού των εν λόγω συστημάτων, οφείλουν να επιλυθούν από τις εταιρίες ανάπτυξης και από τους τελικούς χρήστες, υπεύθυνους τελικώς για την ορθή χρήση. Ο Κανονισμός για την ΤΝ, παρά τη σημαντική καθυστέρηση στην έγκρισή του και το χρονικό περιθώριο των δύο ετών για την πλήρη υιοθέτησή του, κινείται προς την σωστή κατεύθυνση αναφορικά με την ρύθμιση της στην ΕΕ. Με ανθρωποκεντρική προσέγγισή και σεβασμό στα θεμελιώδη δικαιώματα του ανθρώπου και τις αρχές της Ένωσης καθορίζει κανόνες ώστε να αποτελέσει μία τεχνολογία που θα δουλεύει για τους ανθρώπους από τους ανθρώπους.

6.4 Ηθική, Τεχνητή Νοημοσύνη και ΕΕ

Τα σημαντικά οφέλη που αποκομίζει ο ΕΕ και ο ίδιος ελεγκτής από την υιοθέτηση ΤΝ στη διαδικασία περιλαμβάνουν την εξοικονόμηση χρόνου, την ταχύτατη ανάλυση δεδομένων, τα αυξημένα επίπεδα αξιοπιστίας και ακρίβειας και τη δυνατότητα εμβάθυνσης στις επιχειρησιακές διαδικασίες, επιτρέποντας την παροχή ακριβέστερων και ποιοτικότερων ελεγκτικών υπηρεσιών. Στις έρευνες που πραγματοποιούνται αναδεικνύεται η πεποίθηση

ότι περίπου το 50% των ελέγχων πρέπει να πραγματοποιείται με χρήση ή αποκλειστικά μέσω συστημάτων ΤΝ.

Ωστόσο, καθώς προκύπτουν ολοένα και περισσότερα οφέλη από την εφαρμογή ΤΝ στην ελεγκτική διαδικασία, ξεκινά η συζήτηση αναφορικά με τις εκούσιες ή ακούσιες συνέπειες που μπορεί να έχει στο επάγγελμα του ελεγκτή. Για το σκοπό αυτό διεξάγονται συζητήσεις με σκοπό τη διερεύνηση των ηθικών επιπτώσεων από τη χρήση των αναδυόμενων τεχνολογιών σχετικών με την ΤΝ, δεδομένων των έμφυτων χαρακτηριστικών, της φύσης και των σκοπών της. Παρότι οι λεπτομερείς συνέπειες ενδέχεται να εμφανιστούν μετά από μεγάλο χρονικό διάστημα χρήσης και εφαρμογής τους σε μεγαλύτερο εύρος εργασιών, η αναγνώριση των κινδύνων στη φάση αρχικής υλοποίησης κρίνεται απαραίτητη δεδομένης της συνεχώς αυξανόμενης χρήσης περίπλοκων αλγορίθμων σε αυτά, σε συνδυασμό με τα βεβιασμένα συμπεράσματα και προσεγγίσεις αναφορικά με τη λειτουργία τους[112].

Οι βασικές αξίες που αναλύθηκαν πρωτύτερα ισχύουν και βρίσκουν εφαρμογή σε ελέγχους που πραγματοποιούνται με χρήση ΤΝ, με υπαρκτό, ωστόσο, το ενδεχόμενο να επηρεαστούν σημαντικά. Πώς ο ελεγκτής θα αποδείξει τη δέουσα επαγγελματική επάρκεια όταν έχει να αντιμετωπίσει έναν αλγόριθμο μη επαρκώς εξηγημένο ή/και κατανοητό; Πώς θα ελεγχθεί το οργανωτικό πλαίσιο και η διακυβέρνηση μίας επιχείρησης όταν η ΤΝ προξενεί αλλαγές σε αυτά με ταχύτατο ρυθμό; Κατά πόσο έχει γίνει συνειδητό ότι η αλλαγή που προκαλείται από την ΤΝ (θα πρέπει να) περιορίζεται στις επιμέρους εργασίες της ελεγκτικής διαδικασίας και όχι στο ίδιο το επάγγελμα του ελεγκτή; Επιπλέον, υφίσταται ο κίνδυνος ο ελεγκτής να δείξει υπερβάλλουσα εμπιστοσύνη στα αποτελέσματα του συστήματος, αφομοιώνοντας άκριτα τα συμπεράσματά του. Η θεμελιώδης αρχή της αλγοριθμικής επεξεργασίας «*ο αλγόριθμος είναι τόσο καλός όσο τα δεδομένα που χρησιμοποιεί*» βρίσκει σε κάθε περίπτωση εφαρμογή.

Η δυνατότητα των μηχανισμών αυτών να εμφανίζουν ψήγματα ευφυίας, μετατρέπουν τη θεώρηση των ελεγκτών για τα ΣΠ από «λογισμικό που πράττει» σε «σκεπτόμενο». Λαμβάνοντας υπόψη ότι οι εν λόγω εφαρμογές δεν έχουν συναισθηματική νοημοσύνη[113], ενδέχεται να υπάρξουν προβλήματα σε θέματα ασφάλειας και προστασίας, προξενώντας

[112] Όπως «τα συστήματα είναι πάντα σωστά», «συμπεριφέρονται με τον επιθυμητό τρόπο» «οι διαφοροποιήσεις γίνονται άμεσα αντιληπτές».

[113] Ενδεικτικά να έχουν πλήρη κατανόηση, αυτοέλεγχο, συνείδηση και κίνητρο των πράξεων τους.

άνευ λόγου κακό. Οι υπολογισμοί και οι πράξεις τους στηρίζονται σε στοιχεία, που ίσως να εγείρουν θέματα ιδιωτικότητας, εμπιστευτικότητας και προστασίας τους[114]. Ειδικότερα σε περιπτώσεις συστημάτων ML, ενδέχεται το υποκείμενο των δεδομένων να μην ξέρει τι πραγματικά γνωρίζουν οι ελεγκτές για αυτόν. Ο σκοπός αλλά και η διάρκεια τήρησης των δεδομένων αναδεικνύονται σε σημαντικά ζητήματα ηθικής. Επιπλέον, η αυτοματοποιημένη αξιολόγηση της εμπλοκής ενός προσώπου σε μία υπόθεση απάτης, ενδέχεται να οδηγήσει σε λανθασμένα συμπεράσματα απεμπολώντας την κριτική σκέψη και ικανότητα που διέπουν τον ελεγκτή.

Η αδιαμφισβήτητη δυνατότητα ταχείας επίλυσης περίπλοκων προβλημάτων και λήψης αποφάσεων, εγείρει θέματα διαφάνειας[115] για την ίδια την τεχνολογία και για τα τεχνουργημάτων της, λόγω της πολυπλοκότητας υπολογισμών και του καθορισμού των δεδομένων που οδήγησαν στα συμπεράσματα. Παράλληλα, ενδέχεται η ΤΝ να καταστεί μη προσβάσιμη, λόγω αδυναμίας τεχνικής κατανόησης και του ισχυρού (υπό δημιουργία) κανονιστικού πλαισίου, δεδομένου ότι τα υφιστάμενα πρότυπα αδυνατούν να καλύψουν όλες τις πτυχές της.

Τα σημαντικότερα ζητήματα ηθικής που τίθενται από την εφαρμογή της ΤΝ στον ΕΕ αφορούν στην εμπιστοσύνη και στη δυνατότητα απόδοσης ευθύνης (accountability). Η εμπιστοσύνη θεμελιώνεται στη δυνατότητα πρόβλεψης, στις εξαρτήσεις, στην αξιοπιστία, στην ευρωστία, στην κατανόηση, στην αποκλειστικότητα του σκοπού, στη χρησιμότητα και στην εξοικείωση του χρήστη με τα συστήματα αυτά. Ωστόσο, η συνεχής χρήση τους ενδέχεται να αποπροσανατολίσει τον ελεγκτή από τον πραγματικό στόχο, επικεντρώνοντας την προσοχή του στα αυτοματοποιημένα συμπεράσματα του μηχανισμού παρότι υφίστανται μη-αυτοματοποιημένες ενδείξεις για το αντίθετο. Το φαινόμενο είναι πιο έντονο σε περιπτώσεις νέων ελεγκτών που δεν έχουν την εμπειρία αλλά και το επίπεδο κριτικής σκέψης να διαχωρίσουν το σφάλμα στον υπολογισμό.

Η απόδοση της ευθύνης ειδικά για συστήματα επαυξημένης ή αυτόνομης ΤΝ, εντάσσεται στο πλαίσιο της αξιολόγησης προκειμένου να απαντηθεί το σχετικό ερώτημα

[114] Φαινόμενα όπως η επιμονή ανεύρεσης των απαιτούμενων δεδομένων χωρίς την απαραίτητη γνώση του υποκειμένου και σε περιπτώσεις αλλαγής του σκοπού.

[115] Σύμφωνα με Wright (2011) η διαφάνεια «*είναι απαραίτητη προϋπόθεση για την εμπιστοσύνη του κοινού σε κάποια τεχνολογία και τυχόν έλλειψή της στην πράξη μειώνει την υποστήριξη σε αυτήν*».

για αποφάσεις της ΤΝ σε περιπτώσεις μη νόμιμων ενεργειών. Αντίστοιχα, ο ελεγκτής θεωρείται υπεύθυνος σε περίπτωση αστοχίας λόγω λανθασμένων αποφάσεων, δημιουργώντας εύλογα ερωτήματα για την ευθύνη εφόσον οι σχετικές αποφάσεις έχουν ληφθεί αυτόνομα από το σύστημα ή χωρίς κατανόηση από τον ίδιο.

Παράλληλα, η άκριτη χρήση των συστημάτων ΤΝ στην ελεγκτική διαδικασία θέτει θέματα εκπαίδευσης και απόκτησης των απαραίτητων δεξιοτήτων. Οι παραδοσιακοί ορκωτοί ελεγκτές θα αντικατασταθούν από επιστήμονες των δεδομένων ή οι πρώτοι οφείλουν να αποκτήσουν επιπλέον δεξιότητες προκειμένου να ανταπεξέλθουν στα καθήκοντά τους; Είναι δεδομένο ότι θα δημιουργηθούν ανισότητες, οι οποίες πρέπει να αναγνωριστούν και να επιλυθούν άμεσα. Η αυτοματοποίηση αντικαθιστά την παραδοσιακή επαφή των νέων ελεγκτών με βασικά τμήματα της διαδικασίας να εκτελούνται από μηχανισμούς, δημιουργώντας θέματα ανάπτυξης και εξέλιξης των ελεγκτών. Ακόμα και η επαφή με τον ελεγχόμενο και τις πρακτικές του στρεβλώνονται με την υπερβολική χρήση των εν λόγω μηχανισμών, αποστερώντας από την ελεγκτική διαδικασία σημαντικά στοιχεία που προκύπτουν μέσα από την ανθρώπινη επαφή (isolation).

Ο ελεγκτής δεν πρέπει να απεμπολήσει την εμπιστοσύνη του στην τεχνολογία και στις επερχόμενες αλλαγές στον τρόπο άσκησης των καθηκόντων. Αντίθετα, θα πρέπει να αγκαλιάσει την τεχνολογική εξέλιξη και τις βελτιώσεις που κομίζει η ΤΝ, θεωρώντας ότι συμπληρώνουν την επαγγελματική του κρίση δείχνοντας υψηλό επίπεδο κριτικής σκέψης, ειδικά στα μελλοντικά στάδια μετάβασης από την υποβοηθούμενη στην αυτόνομη ΤΝ. Η χρήση της είναι επιβεβλημένη λόγω των σημαντικών πλεονεκτημάτων που προσφέρει, αλλά θα πρέπει να είναι και λελογισμένη προκειμένου να μην διακυβευτεί η σημαντικότερη αρχή της ανεξαρτησίας του ελέγχου, έναντι της εξάρτησης από τα τεχνουργήματα της.

Συμπερασματικά, η ευθυγράμμιση του Κανονισμού με τον ΧΘΔΕΕ και τις σχετικές συνθήκες, είναι ένα πρώτο βήμα για την οργάνωση των αξιών που θα δομηθεί η κοινωνία και τον καθορισμό του ρόλου που θα έχουν οι νέες τεχνολογίες. Οι βασικές απαιτήσεις που καταγράφονται από τις διεπιστημονικές ομάδες της EU για τον σκοπό αυτό[116] υιοθετούνται σε σημαντικό βαθμό στον κανονισμό. Ο έλεγχος θα πρέπει να διασφαλίσει την

[116] (1) Ανθρώπινη υπηρεσία και επίβλεψη, (2) τεχνική ευρωστία και ασφάλεια, (3) απόρρητο και διακυβέρνηση δεδομένων, (4) διαφάνεια, (5) ποικιλομορφία, μη διάκριση και δικαιοσύνη, (6) κοινωνική και περιβαλλοντική ευημερία και (7) λογοδοσία

ευθυγράμμιση συστημάτων ΤΝ που αναπτύσσονται ή υιοθετούνται ώστε παράλληλα με τις αρχές «*privacy by design και default*» που εισήχθησαν από τον ΓΚΠΔ να υπάρξουν και οι αρχές «*ethics by design και default*».

ΚΕΦΑΛΑΙΟ 7. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η έννοια της ΤΝ από καταβολής αναφέρονταν στην ανάπτυξη μηχανισμών, τεχνικών και ΣΠ που θα μιμούνται την ανθρώπινη μάθηση και συμπεριφορά, αναπτύσσοντας «λογική σκέψη» για τη λήψη αποφάσεων[117]. Ο εν εξελίξει διάλογος στη διεθνή κοινότητα αναφορικά με την ΤΝ, τις επιπτώσεις, την επίδραση στην ανθρώπινη δραστηριότητα καθώς και στα δικαιώματα του ατόμου, προβληματίζει το σύνολο των εμπλεκομένων στο ΣΕΕ, και κυρίως τους ελεγκτές. Η ραγδαία ανάπτυξη της ΤΝ και των επιμέρους τομέων της (π.χ. ML, NLP, CI), λόγω των ισχυρών πλεονεκτημάτων που προσφέρουν, οδηγεί στην υιοθέτηση αντίστοιχων μηχανισμών από αυξανόμενο αριθμό επιχειρήσεων.

Οι εξελίξεις αυτές αλλάζουν σημαντικά το πεδίο εφαρμογής των controls και την ίδια τη φύση των εργασιών. Διαδικαστικές και χειροκίνητες εργασίες, πλέον πραγματοποιούνται με συνεχή ροή και περίσσεια ακρίβεια από αυτοματοποιημένα συστήματα, βάσει εντολών και σχετικού προγραμματισμού. Μηχανικά συστήματα αντικαθιστούν τον ανθρώπινο παράγοντα στην παροχή βοήθειας σε τηλεφωνικά κέντρα, στην άμεση απάντηση ερωτημάτων που υποβάλλονται σε ιστότοπους, τον υπολογισμό κρίσιμων μεγεθών και παραμέτρων για τη λήψη αποφάσεων (π.χ. CR και έγκριση δανείων).

Παράλληλα, ολοένα και περισσότερες «έξυπνες συσκευές» αφομοιώνονται στην καθημερινή δραστηριότητα των ανθρώπων. Μεταξύ αυτών, ρολόγια και bands που μετρούν βασικές παραμέτρους της φυσικής κατάστασης του ατόμου, κινητά και έξυπνες συσκευές που επικοινωνούν μέσα από το IoT, αυτόνομα και διασυνδεδεμένα οχήματα που ρυθμίζουν την κίνηση και την κυκλοφορία και πλήθος άλλων εφαρμογών με βασικό στόχο τη διευκόλυνση του ατόμου.

Το υφιστάμενο ελεγκτικό τοπίο αλλάζει μορφή και ταυτόχρονα αυξάνονται οι απαιτήσεις. Αρχικά, θα πρέπει να αφουγκραστεί τις απαιτήσεις των καιρών, να βελτιωθεί με αντίστοιχο τρόπο και να προσαρμοστεί στη σύγχρονη εποχή ώστε να προσδιοριστούν, να επιμετρηθούν και να αντιμετωπιστούν κατάλληλα οι νέοι κίνδυνοι. Οι τελευταίοι σχετίζονται με το σχεδιασμό του μοντέλου, την ανάπτυξη και την εφαρμογή νέων στις δύο

[117] Ενδεικτικά συστήματα ασαφούς λογικής «fuzzy logic" που προσπαθούσαν να προσομοιώσουν τον τρόπο σκέψης, τη λογική πίσω από τις αποφάσεις που λαμβάνει ο ανθρώπινος εγκέφαλος.

πρώτες γραμμές άμυνας, το σχεδιασμό των εφαρμοζόμενων controls[118] και καταλήγουν στην ανάγκη συμμόρφωσης με το υφιστάμενο ή το νέο κανονιστικό πλαίσιο που δημιουργείται, την κείμενη νομοθεσία και τους ευρωπαϊκούς κανονισμούς.

Ο ρόλος της ΤΝ στις δύο πρώτες γραμμές απαλλάσσεται σταδιακά από τον αποδοθέντα «βοηθητικό» χαρακτήρα, στη βάση των εργασιών που εξυπηρετούσε καθώς σταδιακά μετατρέπεται σε επαυξημένη ή και αυτόνομη, αποκτώντας ευφυΐα σε συνδυασμό με τον αναλυτικό τρόπο εκτέλεσης και επεξεργασίας εργασιών. Συνεπώς, οι επιχειρήσεις πρέπει να κατανοήσουν το αναγκαίο προς εφαρμογή επίπεδο ΤΝ, να αναγνωρίσουν τις τρέχουσες δυνατότητες σύμφωνα με τις απαιτήσεις και να αποφασίσουν βάσει των εγγενών πλεονεκτημάτων και των περιορισμών κάθε λύσης, λαμβάνοντας υπόψη και τον αντίκτυπο που μπορεί να έχει σε θέματα ηθικής.

Στον έλεγχο η ΤΝ χρησιμοποιείται, προς ώρας, κυρίως στη χρήση εξειδικευμένων λογισμικών, που με την «κατάλληλη» εκπαίδευση, αναλύουν μεγάλους όγκους δομημένων (και μη) δεδομένων και εξάγουν συμπεράσματα με μοντελοποιημένο τρόπο. Παράλληλα, τα τελευταία χρόνια υιοθετούνται όλο και περισσότερο συστήματα ανάλυσης φωνής και εικόνας, μηχανές αναζήτησης και συστήματα GenAI όπως το ChatGPT, βοηθώντας στην πραγματοποίηση και στον σχεδιασμό του ελέγχου[119]. Υλικοτεχνικός εξοπλισμός με ενσωματωμένη ΤΝ (π.χ. drones, διασυνδεμένες συσκευές μέσα από το IoT) χρησιμοποιείται στην υλοποίηση ελεγκτικών έργων υψηλών απαιτήσεων (π.χ. έλεγχος αποθέματος). Η μετάβαση από την αναλυτική στην ενστικτώδη (στη λογική της κατανόησης εννοιών από ένα σύστημα) ΤΝ από τον έλεγχο είναι το επόμενο στάδιο, ενώ τα πρώτα βήματα στην κατεύθυνση αυτή είναι σε εξέλιξη.

Η χρήση ΤΝ από τους ελεγκτές είναι συνυφασμένη με τη δυνατότητα ανάλυσης μεγάλων δεδομένων με σκοπό την ελαχιστοποίηση του απαιτούμενου χρόνου, των χρησιμοποιούμενων πόρων και την κάλυψη του μεγαλύτερου δυνατού μέρους του πληθυσμού ή μεγιστοποιώντας το εξεταζόμενο δείγμα. Βασικός στόχος παραμένει και η δυνατόν μεγαλύτερη κατανόηση των δεδομένων, των περιγραφόμενων γεγονότων, ο εντοπισμός και η επεξήγηση τυχόν «ανωμαλιών» ή μίας ασυνήθιστης αλληλουχίας

[118] Συμπεριλαμβανομένων του ανασχεδιασμού ή την κατάργηση υφιστάμενων.

[119] Δημοσιεύσεις ελεγκτικών εταιριών, του ΙΙΑ και μονάδων ΕΕ σημαντικών ΠΙ, αναδεικνύουν τη χρησιμότητα του GenAI στην κατάρτιση ελεγκτικών βημάτων και στο σχεδιασμό του ελέγχου.

γεγονότων που ενέχει κινδύνους για τη λειτουργία του οργανισμού. Παράλληλα, μηχανισμοί ΤΝ χρησιμοποιούνται και για την ανάλυση εγγράφων και μη δομημένων δεδομένων, συμπεριλαμβανομένης της επεξεργασίας φυσικής γλώσσας.

Τα θέματα που αντιμετωπίζονται στην εφαρμογή της ΤΝ από τους ελεγκτές δεν διαφέρουν σημαντικά από αυτά σε άλλες υλοποιήσεις. Η επιλογή αυτών που θα χρησιμοποιηθούν, η προσβασιμότητά και η αξιοπιστία τους συνθέτουν τα σημεία κλειδιά για τη διασφάλιση του αποτελέσματος. Παράλληλα, η ανεπαρκής δοκιμή των στοιχείων και των αλγορίθμων ενδέχεται να έχει επίπτωση και στα αποτελέσματα του ίδιου του ελέγχου, σε συνάρτηση με τα όποια λάθη δεν εντοπιστούν κατά την ανάπτυξή του.

Σε κάθε περίπτωση ο ΕΕ οφείλει να προσδιορίσει και να επιμετρήσει τα βραχυπρόθεσμα και τα μακροπρόθεσμα οφέλη που αναμένει να αποκομίσει από τη χρήση ΤΝ στις μεθόδους του. Σε κάθε στάδιο θα πρέπει να προσδιοριστεί το είδος της εφαρμόσιμης ΤΝ (ενδεικτικά predictive analysis, RPA, NLP) από την αρχική θεώρηση του ελέγχου, το σχεδιασμό και την υλοποίηση μέχρι και την παραγωγή της αναφοράς.

Η χρήση ΤΝ σε μία περιοχή που αντιμετωπίζει σε συνεχή βάση θέματα και διλήμματα ηθικής, θα πρέπει να λαμβάνει υπόψη και τις βασικές αρχές της. Η διαφάνεια, η δικαιοσύνη, η απουσία προαιρέσεων, η υπευθυνότητα, η ιδιωτικότητα, η εμπιστοσύνη, η βιωσιμότητα και αξιοπρέπεια συγκαταλέγονται στα ελάχιστα απαιτούμενα για τη χρήση και την ανάπτυξη αντίστοιχων μηχανισμών. Η διαχείριση των σχετικών κινδύνων, που αποτελεί ευθύνη και των τριών γραμμών, θα πρέπει να στηρίζεται στη εγκαθίδρυση μίας σχέσης εμπιστοσύνης μεταξύ των εμπλεκόμενων μερών. Παράλληλα, σημείο εστίασης αποτελούν η διαδικασία και το πλαίσιο ανάπτυξης, η δοκιμή και η αξιολόγηση των αποτελεσμάτων τους σε όλο τον κύκλο ανάπτυξης και διαχείρισης αλλαγών στις αντίστοιχες εφαρμογές. Και σε κάθε περίπτωση, τα ίδια τα άτομα οφείλουν να επιλύουν τυχόν ηθικά διλήμματα που ενδέχεται να επηρεάσουν το τελικό αποτέλεσμα.

Είναι προφανές ότι η βελτίωση της ποιότητας των ελέγχων και συνολικά του έργου των ελεγκτών, περνάει μέσα από την εφαρμογή σε ευρεία κλίμακα της ΤΝ. Οι διάφορες μορφές της σε σχέση με τον ρόλο της και την τεχνολογία που υιοθετείται προσδίδουν σημαντικά πλεονεκτήματα στους ελεγκτές. Αποτελεί παράλληλα και σημαντικό πονοκέφαλο, για την κατανόηση από μη ειδικούς, προκειμένου να μην μετατραπεί σε μαύρο κουτί με άγνωστο περιεχόμενο. Η διαφάνεια αποτελεί απαρέγκλιτη αρχή του ελέγχου και περικλείει το

σύνολο των εργασιών που τον αφορούν. Η σύγκλιση ανάμεσα στους δύο κόσμους (τεχνολογικό και ελεγκτικό), είναι το συστατικό που προσδίδει προστιθέμενη αξία στην επιχείρηση και στον ελεγκτικό χώρο. Επιπλέον, συμβιβάζει την ηθική των αποφάσεων που καλούνται να λάβουν οι ελεγκτές βάσει των αποτελεσμάτων της ανάλυσης με χρήση ΤΝ και παράλληλα θα αποτρέψει παρεκκλίσεις από τις αξίες της εμπιστευτικότητας και της ακεραιότητας διασφαλίζοντας την αρχή της ευθύνης και της απαρέγκλιτης τήρησης των απαιτήσεων.

ΕΠΙΛΟΓΟΣ

Η ΤΝ παρότι δεν αποτελεί μία καινούργια τεχνολογία, συγκαταλέγονταν, λανθασμένα ίσως στις ανερχόμενες, γνωρίζει πρωτοφανή ανάπτυξη τα τελευταία χρόνια και αναμένεται να εξελιχθεί έτι περαιτέρω την επόμενη δεκαετία. Τα σημαντικά επιτεύγματα των υπολογιστικών συστημάτων, στη διαθεσιμότητα των δεδομένων και στις ανάγκες της ανθρώπινης δραστηριότητας αποτελούν το άρμα που σέρνει τις εξελίξεις στον τομέα. Οι μηχανισμοί ΤΝ αλλάζουν μορφή και αποκτούν προηγμένη ευφυΐα. Παύουν να αποτελούν συστήματα ειδικού σκοπού, εξειδικευμένα σε ένα μόνο αντικείμενο π.χ. να παίζουν σκάκι όπως ο "Deep Blue" με τον οποίο αναμετρήθηκε ο Κασπάρωφ (1997). Πλέον μπορούν να αναλύσουν, βάσει προγραμματισμού, μεγάλη ποικιλία καταστάσεων, να απαντήσουν σε πολλαπλές ερωτήσεις και να λάβουν αποφάσεις είτε αυτόνομα είτε σε συνεργασία με τον άνθρωπο.

Ο έλεγχος αποτελεί πεδίο εφαρμογής της ΤΝ, με τη μορφή των συστημάτων που υιοθετούνται στις δραστηριότητές του, αλλά και δράσης προκειμένου να διασφαλιστεί η ορθή λειτουργία τους. Αυτός ο διττός ρόλος καθιστά αναγκαία την προσαρμογή και την παρακολούθηση των εξελίξεων στο χώρο και ταυτόχρονα αλλάζει το τοπίο που δραστηριοποιείται. Είναι υποχρέωση η κατανόηση των περίπλοκων αυτών αλγορίθμων, στη λογική των συνεργιών με τους επιστήμονες του χώρου, αλλά και ανεξάρτητα στη βάση των αρχών και του κώδικα δεοντολογίας που διέπει τα καθήκοντά του. Η αυτοματοποίηση μέρους ή του συνόλου των διαδικασιών επιβάλλεται από την ανάγκη ανακατανομής των διαθέσιμων πόρων και την αντιμετώπιση των ποικίλων κινδύνων που αντιμετωπίζουν οι σύγχρονες επιχειρήσεις.

Το κανονιστικό και το νομοθετικό πλαίσιο γύρω από την ΤΝ είναι υπό διαμόρφωση, μετά και την έκδοση του σχετικού Κανονισμού, σε συνέχεια πλήθους οδηγιών και προτάσεων που έχουν διατυπωθεί τα τελευταία χρόνια. Παράλληλα, όλο και περισσότερες έρευνες και δημοσιεύσεις που παρουσιάζονται, υπογραμμίζουν την ανάγκη υιοθέτησης της ΤΝ στις καθημερινές εργασίες διαφόρων κλάδων – μεταξύ αυτών και των ελεγκτών – αλλά και ρύθμισής της προκειμένου να διασφαλιστούν θέσεις εργασίας και η εφαρμογή της σύμφωνα με τις ανάγκες. Οι οργανισμοί και οι ενώσεις των ελεγκτών σε παγκόσμιο επίπεδο, διατυπώνουν απόψεις και μελετούν τις εξελίξεις προετοιμάζοντας το έδαφος ή

προσδιορίζοντας το πεδίο εφαρμογής της, προκειμένου να έχουν άμεση αντίδραση με την έκδοση των σχετικών κανονισμών.

Ωστόσο, οι διαχρονικές αξίες του ΕΕ όπως η ακεραιότητα, η αντικειμενικότητα, η επαγγελματική επάρκεια, η δέουσα επιμέλεια και η εμπιστευτικότητα είναι αυτές που συνδυαστικά με την ανεξαρτησία του θα διασφαλίσουν την ομαλή μετάβαση στη νέα εποχή. Η ηθικότητα του ελεγκτή δεν δύναται να προγραμματιστεί καθώς οι μηχανισμοί ΤΝ δεν διαθέτουν συνείδηση. Μπορούν να προσομοιάσουν την ελεγκτική εργασία, να αξιολογήσουν τα δεδομένα, να προσδιορίσουν αποκλίσεις, να εντοπίσουν παραβατικές συμπεριφορές, να διακρίνουν αλλαγές σε εκφράσεις ή σε καταστάσεις αλλά δεν είναι και ενδεχομένως δεν θα πρέπει να είναι και στο μέλλον σε θέση να λάβουν αποφάσεις. Η εξάρτησή τους από τα δεδομένα που τροφοδοτούνται αλλά και από την ηθική που διακρίνει τον τρόπο προγραμματισμού τους αποτελούν ανασταλτικούς παράγοντες σε αυτό.

Όσο πιο σημαντικός είναι ο ρόλος που δίνεται στην ΤΝ τόσο μεγαλύτερος είναι και ο κίνδυνος οι δικλείδες ασφαλείας που έχουν υλοποιηθεί να αποδειχθούν ανεπαρκείς και να αποτύχουν τελικά στο σκοπό τους για τη διαφύλαξη ενός αγαθού, μίας υπηρεσίας ή μίας διαδικασίας από λάθη και παραλείψεις. Ο ελεγκτής οφείλει να αξιολογεί το ρόλο που έχει ανατεθεί σε ένα σύστημα ΤΝ, τις τρέχουσες δυνατότητες έναντι των εφαρμοζόμενων και την ευφυΐα που απαιτείται για την εκτέλεσης της διεργασίας. Οι ελεγκτικοί στόχοι πλέον μεταβάλλονται ώστε να συμπεριλάβουν την αξιολόγηση επίτευξης τόσο του τεχνολογικού και πρακτικού σκοπού που οδήγησαν στην ανάγκη υλοποίησης ενός συστήματος ΤΝ όσο και του ηθικού σκοπού ώστε να είναι αποδεκτό από τους χρήστες και την κοινωνία.

Στο νέο αυτό περιβάλλον υποκρύπτεται μία σειρά σημαντικών ερωτημάτων που θα έρχονται στην επιφάνεια σταδιακά, ακολουθώντας τις εξελίξεις και προσαρμοζόμενοι σε αυτές. Έννοιες όπως εμπιστοσύνη και ευθύνη στη λήψη αποφάσεων θα αποκτούν ολοένα και περισσότερη αξία. Η ηθική πίσω από αποφάσεις που λαμβάνονται με αυτοματοποιημένο τρόπο αποτελεί τον ακρογωνιαίο λίθο για την εγκυρότητα και την εφαρμογή της. Η ΤΝ είναι σαν την μόδα, αλλάζει συνεχώς αλλά παραμένει πάντα εδώ, κάνοντας τη ρήση του Thomas Jefferson επίκαιρη *"In matters of style, swim with the current; in matters of principle stand like a rock"*.

ΠΑΡΑΡΤΗΜΑ Ι - ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

EU	Ευρωπαϊκή Ένωση (European Union)
ΕΕ	Εσωτερικός Έλεγχος
ΣΠ	Συστήματα Πληροφορικής
ΣΕΕ	Σύστημα Εσωτερικού Ελέγχου
ΙΙΑ	Ινστιτούτο Εσωτερικών Ελεγκτών
ΕΚΤ	Ευρωπαϊκή Κεντρική Τράπεζα
ΟΟΣΑ	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
CAATs	Τεχνικές ελέγχου με χρήση Πληροφοριακών Συστημάτων - Computer Assisted Audit Techniques
CA/ΔΕ	Continuous Auditing / Διαρκής Έλεγχος
ΜΕΕ	Μητρώο Εσωτερικών Ελεγκτών
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
ΧΘΔΕΕ	Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης
ΤτΕ	Τράπεζα της Ελλάδος
ΠΙ	Πιστωτικό Ίδρυμα
CI	Γνωστική Νοημοσύνη - Cognitive Intelligence
ML	Μηχανική Μάθηση - Machine Learning
NLP	Επεξεργασία Φυσικής Γλώσσας - Natural Language Processing
RPA	Αυτοματοποίηση Διαδικασιών με χρήση Ρομποτικής Τεχνολογίας - Robotics Process Automation
CR	Αξιολόγηση Πιστωτικού Κινδύνου Credit Rating
ΑΑΔΕ	Ανεξάρτητη Αρχή Δημοσίων Εσόδων
ΦΠ	Φυσικό Πρόσωπο - Ιδιώτης
ΝΠ	Νομικό Πρόσωπο - Επιχείρηση
AML	Καταπολέμηση Ξεπλύματος Βρώμικου Χρήματος – Anti-Money Laundering
CFT	Καταπολέμηση Χρηματοδότησης της Τρομοκρατίας – Counterfeit Terrorism Financing
CM/ΔΠ	Continuous Monitoring / Διαρκής Παρακολούθηση

ΒΙΒΛΙΟΓΡΑΦΙΑ

Νομοθεσία - Αποφάσεις

Νόμος 4972/2022 (ΦΕΚ 181/23.09.2022) 'Εταιρική διακυβέρνηση των Ανωνύμων Εταιρειών του Δημοσίου και των λοιπών θυγατρικών της Ελληνικής Εταιρείας Συμμετοχών και Περιουσίας, διαχείριση συμμετοχών του Δημοσίου σε ανώνυμες εταιρείες και ρυθμίσεις για την Ελληνική Εταιρεία Συμμετοχών και Περιουσίας, αξιολόγηση της έναντι του Δημοσίου φερεγγυότητας και πιστοληπτικής ικανότητας φυσικών και νομικών προσώπων και σύσταση Ανεξάρτητης Αρχής Πιστοληπτικής Αξιολόγησης, ίδρυση και λειτουργία Κεντρικού Μητρώου Πιστώσεων, Συμπληρωματικός Κρατικός Προϋπολογισμός οικονομικού έτους 2022 και λοιπές διατάξεις οικονομικού και αναπτυξιακού χαρακτήρα'.

Νόμος 4961/2022 (ΦΕΚ 146/27.7.2022). 'Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις'.

Τράπεζα της Ελλάδος (2022) 'ΠΕΕ 209/19.7.2022 Υιοθέτηση των αναθεωρημένων κατευθυντήριων γραμμών της Ευρωπαϊκής Αρχής Τραπεζών (EBA/GL/2021/03) σχετικά με την αναφορά μείζονων συμβάντων δυνάμει της αναθεωρημένης οδηγίας για τις υπηρεσίες πληρωμών (2015/2366/ΕΕ)'.

Ευρωπαϊκή Επιτροπή (2021), 2021/0106 , 'Proposal for a regulation of the European parliament and of the council laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts'. Διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 [Ημερομηνία πρόσβασης 20.10.2023]

Νόμος 4795/2021 (ΦΕΚ 62/17.4.2021), 'Σύστημα Εσωτερικού Ελέγχου του Δημόσιου Τομέα, Σύμβουλος Ακεραιότητας στη δημόσια διοίκηση και άλλες διατάξεις για τη δημόσια διοίκηση και την τοπική αυτοδιοίκηση'.

Νόμος 4849/2021 (ΦΕΚ 207/5.11.2021) Αναμόρφωση και εκσυγχρονισμός του ρυθμιστικού πλαισίου οργάνωσης και λειτουργίας του υπαίθριου εμπορίου, ρυθμίσεις για την άσκηση ψυχαγωγικών δραστηριοτήτων και την απλούστευση πλαισίου δραστηριοτήτων στην εκπαίδευση, βελτιώσεις στην επιμελητηριακή νομοθεσία, άλλες διατάξεις του Υπουργείου Ανάπτυξης και Επενδύσεων και λοιπές επείγουσες διατάξεις.

Νόμος 5027/2023 (ΦΕΚ 48/2.3.2023) Σύστημα Καινοτομίας στον δημόσιο τομέα - Ρυθμίσεις Γενικής Γραμματείας Ανθρωπίνου Δυναμικού Δημοσίου Τομέα - Ρυθμίσεις για τη λειτουργία των Ο.Τ.Α. α' και β' βαθμού και των αποκεντρωμένων διοικήσεων και για την ευζωία των ζώων συντροφιάς - Λοιπές επείγουσες ρυθμίσεις του Υπουργείου Εσωτερικών και άλλες διατάξεις.

Τράπεζα της Ελλάδος (2021), 'ΕΤΠΘ 188/26-4-2021 Τροποποίηση της απόφασης της Επιτροπής Τραπεζικών και Πιστωτικών Θεμάτων 281/5/17-3-2009 «Πρόληψη της

χρησιμοποίησης των εποπτευομένων από την Τράπεζα της Ελλάδος πιστωτικών ιδρυμάτων και χρηματοπιστωτικών οργανισμών για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας»'

European Banking Authority – EBA (2021) 'EBA/GL/2021/03 Revised guidelines on major incident reporting under PSD2'.

Νόμος 4706/2020 (ΦΕΚ 136/17.7.2020). 'Εταιρική διακυβέρνηση ανωνύμων εταιρειών, σύγχρονη αγορά κεφαλαίου, ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας (ΕΕ) 2017/828 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, μέτρα προς εφαρμογή του Κανονισμού (ΕΕ) 2017/1131 και άλλες διατάξεις'.

Νόμος 4557/2018 (ΦΕΚ 139/30.7.2018) «Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας (ενσωμάτωση της Οδηγίας 2015/849/ΕΕ) και άλλες διατάξεις»

Νόμος 4537/2018 (ΦΕΚ 84/15.5.2018) Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2015/2366/ΕΕ για τις υπηρεσίες πληρωμών και άλλες διατάξεις

Ευρωπαϊκή Ένωση (2016) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679 [Ημερομηνία πρόσβασης 20.10.2023]

Ευρωπαϊκό Κοινοβούλιο, 'Οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2015 σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 2002/65/ΕΚ, 2009/110/ΕΚ και 2013/36/ΕΕ και του κανονισμού (ΕΕ) αριθ. 1093/2010 και την κατάργηση της οδηγίας 2007/64/ΕΚ (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)'. Διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32015L2366 [Ημερομηνία πρόσβασης 20.10.2023]

Ευρωπαϊκή Επιτροπή (2013), 'Οδηγία 36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms'. Διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0036 [Ημερομηνία πρόσβασης 20.10.2023]

Τράπεζα της Ελλάδος (2009), 'ΕΤΠΘ 281/17.3.2009 Απόφαση της Επιτροπής Τραπεζικών και Πιστωτικών Θεμάτων «Πρόληψη της χρησιμοποίησης των εποπτευόμενων από την Τράπεζα της Ελλάδος πιστωτικών ιδρυμάτων και χρηματοπιστωτικών οργανισμών για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας»'.

Τράπεζα της Ελλάδος (2009), 'Ενδεικτική τυπολογία ασυνήθων ή ύποπτων συναλλαγών κατά την έννοια των παραγράφων 13-14 του άρθρου 4 του ν. 3691/2008'.

Ευρωπαϊκό Κοινοβούλιο (2009), 'Κανονισμός (ΕΚ) αριθ. 1060/2009 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 16ης Σεπτεμβρίου 2009 για τους οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας'.

Ευρωπαϊκή Ένωση (2007) 'Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση Ενοποιημένη απόδοση της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης Πρωτόκολλα Παραρτήματα της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης Δηλώσεις οι οποίες προσαρτώνται στην τελική πράξη της διακυβερνητικής διάσκεψης η οποία υιοθέτησε τη Συνθήκη της Λισαβώνας που υπογράφηκε στις 13 Δεκεμβρίου 2007'. Διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A12016ME%2FTXT [Ημερομηνία πρόσβασης 20.10.2023]

Τράπεζα της Ελλάδος, Πράξη Διοικητή 2577/9.3.2006 (2006) 'Πλαίσιο αρχών λειτουργίας και κριτηρίων αξιολόγησης της οργάνωσης και των Συστημάτων Εσωτερικού Ελέγχου των πιστωτικών και χρηματοδοτικών ιδρυμάτων και σχετικές αρμοδιότητες των διοικητικών τους οργάνων.' Ανακτήθηκε από https://www.bankofgreece.gr/RelatedDocuments/%CE%A0%CE%94.%CE%A4%CE%95_2577-9.3.2006_%CE%A0%CE%BB%CE%B1%CE%AF%CF%83%CE%B9%CE%BF_%CE%B1%CF%81%CF%87%CF%8E%CE%BD_%CE%BB%CE%B5%CE%B9%CF%84%CE%BF%CF%85%CF%81%CE%B3%CE%AF%CE%B1%CF%82_%CE%BA%CE%B1%CE%B9_%CE%BA%CF%81%CE%B9%CF%84%CE%B7%CF%81%CE%AF%CF%89%CE%BD_%CE%B1%CE%BE%CE%B9%CE%BF%CE%BB%CF%8C%CE%B3%CE%B7%CF%83%CE%B7%CF%82_%CF%84%CF%89%CE%BD_%CE%A3%CE%95%CE%95.pdf [Ημερομηνία πρόσβασης 18.1.2024]

Επιστημονικές Εκδόσεις

Ελληνικό Ινστιτούτο Εσωτερικών Ελεγκτών (2023), 'Σεμινάριο Data Analytics' [Ημερομηνία διενέργειας 18-20.10.2023].

Ρεθυμιωτάκη Ε., 'Η ρύθμιση της τεχνητής νοημοσύνης ως πρόκληση για την Ευρωπαϊκή Ένωση', Έκτο και Έβδομο μάθημα, σημειώσεις μαθήματος Κανονισμοί και οδηγίες στην Ευρωπαϊκή Ένωση: Ηθική, αποδοχή, νομιμότητα 2022-2023, Πανεπιστήμιο Πειραιά ΠΜΣ «Δίκαιο και Τεχνολογίες Πληροφορικής και Επικοινωνιών»

European Banking Authority (2020), 'EBA report on big data and advanced analytics', EBA/REP/2020/01, Διαθέσιμο στο https://www.eba.europa.eu/sites/default/files/document_library/Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf [Ημερομηνία πρόσβασης 27.10.2023]

Ελληνικό Ινστιτούτο Εσωτερικών Ελεγκτών (2008), 'Το πλαίσιο επαγγελματικής εφαρμογής του Εσωτερικού Ελέγχου, εναρμονισμένο με τα διεθνή πρότυπα και τον Κώδικα Δεοντολογίας του Institute of Internal Auditors (IIA)'

Παναγιωτόπουλος, Θ. (2000) Λογικός Προγραμματισμός και Τεχνητή Νοημοσύνη Πανεπιστήμιο Πειραιά

Παναγιωτόπουλος, Θ. (2000) Ευφυή Συστήματα, Πανεπιστήμιο Πειραιά

Διαδικτυακά Άρθρα

Joffe E., Karp D. και Newcomer S. (2024) 'AIs bright future in audit, risk and compliance', *Auditboard,* διαθέσιμο στο https://www.auditboard.com/resources/ebook/ai-s-bright-future-in-audit-risk-and-compliance/ [Ημερομηνία πρόσβασης 11.3. 2024]

Muraleedhara P. (2024), 'The need for AI-powered cybersecurity to tackle AI-driven cyberattacks', *ISACA*, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/the-need-for-ai-powered-cybersecurity-to-tackle-ai-driven-cyberattacks [Ημερομηνία πρόσβασης 23.4.2024]

Prasad V. (2024), 'Cybersecurity risk of AI-based applications demystified', *ISACA Journal*, *Τεύχος 2/2024*, σελίδες 1-3, διαθέσιμο στο https://www.isaca.org/resources/isaca-journal/issues/2024/volume-2/cybersecurity-risk-of-ai-based-applications-demystified [Ημερομηνία πρόσβασης 23.4.2024]

Bhatia P. (2024), 'How will AI impact our jobs in digital trust', *ISACA,* διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/how-will-ai-impact-our-jobs-in-digital-trust-fields [Ημερομηνία πρόσβασης 23.4.2024]

DeWeese K. (2024), 'Get grounded with AI', *ISACA,* διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/get-grounded-in-ai [Ημερομηνία πρόσβασης 28.3.2024]

Piazzi D. (2024), 'A proposed high-level approach to AI audit', *ISACA Journal*, *Τεύχος 2/2024*, σελίδες 1-4, διαθέσιμο στο https://www.isaca.org/resources/isaca-journal/issues/2024/volume-2/a-proposed-high-level-approach-to-ai-audit [Ημερομηνία πρόσβασης 23.4.2024]

Karp D. (2024), 'How AI is transforming audit, risk and compliance', *ISACA,* διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/how-ai-is-transforming-audit-risk-and-compliance [Ημερομηνία πρόσβασης 24.3.2024]

Lyons S. (2024). 'Anticipating a scandal: Is AI a ticking time bomb for companies?', *Internal Audit 360*, διαθέσιμο στο https://internalaudit360.com/anticipating-a-scandal-is-ai-a-ticking-bomb-for-companies/ [Ημερομηνία πρόσβασης 1.3.2024]

Cassidy B. και Hittner R. (2024). 'Demystifying AI and its algorithms: What internal auditors need to know?', *Internal Audit 360*, διαθέσιμο στο https://internalaudit360.com/demystifying-ai-and-its-algorithms-what-internal-auditors-need-to-know [Ημερομηνία πρόσβασης 1.3.2024]

Carmichael M. (2023), 'Key considerations for developing organizational generative AI policies', *ISACA*, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-44/key-considerations-for-developing-organizational-generative-ai-policies [Ημερομηνία πρόσβασης 17.11.2023]

Rafeq A. (2023), 'Seven steps to Empowerment with data analytics', *ISACA*, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-34/seven-steps-to-empowerment-with-data-analytics [Ημερομηνία πρόσβασης 1.10.2023]

Φραγκούλη Ν. (2023), 'Η τεχνητή νοημοσύνη φέρνει εξοικονόμηση κόστους $900 εκατ. στις Τράπεζες', *Σύνδεσμος Επιχειρήσεων Πληροφορικής & Επικοινωνιών Ελλάδος*, διαθέσιμο στο https://www.sepe.gr/tehnologia-pliroforiki/anaduomenes-tehnologies/22359165/i-tehniti-noimosuni-fernei-exoikonomisi-kostous-900-ekat-stis-trapezes/ [Ημερομηνία πρόσβασης 17.11.2023]

Diogo Reis L.C. (2023), 'ChatGPT and IT auditing: Opportunities, threats and challenges', *ISACA*, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/chatgpt-and-it-auditing-opportunities-threats-and-challenges [Ημερομηνία πρόσβασης 1.10.2023]

Jaleel A. (2023), 'ChatGPT and leveraging artificial intelligence in auditing', *ISACA*, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/chatgpt-and-leveraging-artificial-intelligence-in-auditing [Ημερομηνία πρόσβασης 1.10.2023]

Sisodia J. (2023), 'Understanding the EU AI Act', *ISACA*, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/industry-news/2023/understanding-the-eu-ai-act [Ημερομηνία πρόσβασης 1.10.2023]

Geldenhuys F. και Silvo G. (2022) 'Seven things to know before automating IT General Control audits', *ISACA*, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/industry-news/2022/seven-things-to-know-before-automating-it-general-control-audits [Ημερομηνία πρόσβασης 27.10.2023]

Scarpino J. (2022), 'Evaluating Ethical Challenges in AI and ML', *ISACA Journal*, Τεύχος 4/2022, σελίδες 27-31. Διαθέσιμο στο https://www.isaca.org/resources/isaca-journal/issues/2022/volume-4/evaluating-ethical-challenges-in-ai-and-ml [Ημερομηνία πρόσβασης 27.10.2023]

Munoko I. (2022), 'Implementing Artificial Intelligence: Capabilities and risk', *ISACA Journal, Τεύχος 4/2022*, σελίδες 1-9. Διαθέσιμο στο https://www.isaca.org/resources/isaca-journal/issues/2022/volume-4/implementing-artificial-intelligence-capabilities-and-risk [Ημερομηνία πρόσβασης 1.10.2023]

Pearce G. (2022), 'Focal points for auditable and explainable AI', *ISACA Journal, Τεύχος 4/2022*, σελίδες 1-17, διαθέσιμο στο https://www.isaca.org/resources/isaca-journal/issues/2022/volume-4/focal-points-for-auditable-and-explainable-ai [Ημερομηνία πρόσβασης 1.10.2023]

Menon S. (2021), 'How Can AI Drive Audits', *ISACA Journal*, *Τεύχος 4/2021*, σελίδες 1-9, διαθέσιμο στο https://www.isaca.org/resources/isaca-journal/issues/2021/volume-4/how-can-ai-drive-audits [Ημερομηνία πρόσβασης 1.10.2023]

Shinde B. (2021), 'Artificial Intelligence Adoption in Internal Audit Processes', *ISACA Journal*, *Τεύχος 4/2021*, σελίδες 1-4, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-40/artificial-intelligence-adoption-in-internal-audit-processes [Ημερομηνία πρόσβασης 1.10.2023]

Wang J. (2021) 'The ethics of Artificial Intelligence', *ISACA*, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/the-ethics-of-artificial-intelligence [Ημερομηνία πρόσβασης 27.10.2023]

Lloyd K. (2021) 'Establishing Artificial Intelligence governance: Tips for CIOs', *ISACA*, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/industry-news/2021/establishing-artificial-intelligence-governance-tips-for-cios [Ημερομηνία πρόσβασης 1.10.2023]

Cote C. (2021) '4 Types of data analytics to improve decision-making', *Harvard Business School Online*, διαθέσιμο στο https://online.hbs.edu/blog/post/types-of-data-analysis?c1=GAW_CM_NW&source=INTL_CLIMB_PMAX&cr2=content___-___international___-___climb___-___pmax&kw=climb&cr5=&cr6=&cr7=c&utm_campaign=content___-___international___-___climb___-___pmax&utm_term=climb&gad_source=1&gclid=CjwKCAjwrcKxBhBMEiwAIVF8rCFfHqHZ9Gk4L08pT3zGJ0puitHbnhThY4jmOnMcCdWXlm6h8c1NIhoCV0gQAvD_BwE [Ημερομηνία πρόσβασης 15.11.2023]

Toor H. (2020), 'Robotic Process Automation for Internal Audit', *ISACA Journal*, *Τεύχος 5/2022*, σελίδες 1-3, διαθέσιμο στο https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/robotic-process-automation-for-internal-audit [Ημερομηνία πρόσβασης 27.10.2023]

Munoko I. (2020) 'The ethical implications of using artificial intelligence in auditing', *Journal of business ethics*, σελίδες 1-26, διαθέσιμο στο https://www.academia.edu/53323579/The_Ethical_Implications_of_Using_Artificial_Intelligence_in_Auditing?sm=b [Ημερομηνία πρόσβασης 28.2.2024]

Sutaria N. (2020), 'Artificial Intelligence impact on auditing emerging technologies', *ISACA Journal*, *Τεύχος 6/2020*, σελίδες 1-6, διαθέσιμο στο https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/artificial-intelligences-impact-on-auditing-emerging-technologies [Ημερομηνία πρόσβασης 27.10.2023]

Sutaria N. (2020), 'Artificial Intelligence regulations gaining traction', *ISACA*, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/artificial-intelligence-regulations-gaining-traction [Ημερομηνία πρόσβασης 1.10.2023]

Ahmed H. (2020), 'Auditing guidelines for Artificial Intelligence', *ISACA Journal*, *Τεύχος 26/2020*, σελίδες 1-5, διαθέσιμο στο https://www.isaca.org/resources/news-and-

trends/newsletters/atisaca/2020/volume-26/auditing-guidelines-for-artificial-intelligence [Ημερομηνία πρόσβασης 1.10.2023]

Wlosinski L. (2020), 'Understanding and managing the Artificial Intelligence threat', *ISACA Journal*, *Τεύχος 1/2020* σελίδες 1-9, διαθέσιμο στο https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/understanding-and-managing-the-artificial-intelligence-threat [Ημερομηνία πρόσβασης 1.10.2023]

Bizarro P, Crum E. και Nix J. (2019), 'The Intelligent Audit', *ISACA Journal*, *Τεύχος 6/2019* σελίδες 1-12, διαθέσιμο στο https://www.isaca.org/resources/isaca-journal/issues/2019/volume-6/the-intelligent-audit [Ημερομηνία πρόσβασης 1.10.2023]

Priyadarshi G, 'Inherent risk in adopting RPA and opportunities for internal audit departments', *ISACA Journal, Τεύχος 6/2019*, σελίδες 50-52, διαθέσιμο στο https://www.isaca.org/resources/isaca-journal/issues/2019/volume-6/inherent-risk-in-adopting-rpa-and-opportunities-for-internal-audit-departments [Ημερομηνία πρόσβασης 1.10.2023].

Ramachandran R. (2019), 'Artificial Intelligence: A Damocles sword', *ISACA*, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/artificial-intelligence-a-damocles-sword [Ημερομηνία πρόσβασης 1.10.2023]

Villanueva L. (2019), 'Ethical considerations of Artificial Intelligence', *ISACA*, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/ethical-considerations-of-artificial-intelligence [Ημερομηνία πρόσβασης 1.10.2023]

Pearce G. (2019), 'Data Auditing: Building Trust in Artificial Intelligence', *ISACA Journal*, *Τεύχος 6/2019*, διαθέσιμο στο https://www.isaca.org/resources/isaca-journal/issues/2019/volume-6/data-auditing-building-trust-in-artificial-intelligence [Ημερομηνία πρόσβασης 15.11.2023]

Cassels W., Traub J, Alvero K. και Fernandez J. (2019), 'The pain of automation: Internal audit functions face real-world challenges amid optimistic environment', *ISACA Journal*, *Τεύχος 4/2019*, σελίδες 14-18, διαθέσιμο στο https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/the-pain-of-automation [Ημερομηνία πρόσβασης 24.10.2023]

Marks L. (2018), 'Leveraging Artificial Intelligence', *ISACA*, διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/leveraging-artificial-intelligence [Ημερομηνία πρόσβασης 1.10.2023]

Peters I. (2017), 'Data Analytics: Is it time to take the first step?', *Chartered Institute of Internal Auditors*, διαθέσιμο στο https://www.iia.org.uk/media/1689102/0906-iia-data-analytics-5-4-17-v4.pdf [Ημερομηνία πρόσβαση 24.10.2023]

Ιστοσελίδες

PriceWaterhouseCoopers (2024), 'Implementing the IIA's new Global Internal Audit Standards'. Διαθέσιμο στο https://www.pwc.com/gx/en/services/audit-assurance/internal-audit/new-global-internal-audit-standards.html [Ημερομηνία πρόσβασης 11.3.2024].

The Institute of Internal Auditors IIA Global (2023), 'Το μοντέλο των τριών γραμμών του IIA Global, Επικαιροποίηση του μοντέλου των τριών γραμμών άμυνας', διαθέσιμο στο https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-greek.pdf [Ημερομηνία πρόσβασης 10.11.2023]

ISACA (2023), 'How business leaders can responsibly embrace generative AI', ISACA. Διαθέσιμο στο https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/how-business-leaders-can-responsibly-embrace-generative-ai [Ημερομηνία πρόσβασης 26.12.2023].

ISACA (2023), 'AI policies are low, use is high, and adversaries are taking advantage, says new AI study', *ISACA*, διαθέσιμο στο https://www.isaca.org/about-us/newsroom/press-releases/2023/ai-policies-are-low-use-is-high-and-adversaries-are-taking-advantage-says-new-ai-study [Ημερομηνία πρόσβασης 17.11.2023].

Ζιαμπάρας Δ. (2023), 'Προστασία Καταθέτη από ηλεκτρονική απάτη', διαθέσιμο στο https://ziamparas.gr/ηλεκτρονικό-έγκλημα/νεοσ-νομοσ-2023-για-ευθυνη-τραπεζασ-στην-η/ [Ημερομηνία πρόσβασης 28.1.2024].

Oracle India (2023), 'What is data analytics', διαθέσιμο στο https://www.oracle.com/in/business-analytics/data-analytics/ [Ημερομηνία πρόσβασης 27.10.2023]

Lawspot (2023), 'Ηλεκτρονικές απάτες και ευθύνη τραπεζών: Τι προβλέπει η τελική διάταξη για μη εγκεκριμένες πράξεις πληρωμής (phishing)', διαθέσιμο στο https://www.lawspot.gr/nomika-nea/ilektronikes-apates-kai-eythyni-trapezon-ti-provlepei-i-teliki-diataxi-gia-mi [Ημερομηνία πρόσβασης 18.1.2024]

Ευρετήριο Οικονομικών Όρων (2023), 'Πιστοληπτική ικανότητα / Διαβάθμιση (Credit rating)', διαθέσιμο στο https://euretirio.com/pistoliptiki-ikanotita/ [Ημερομηνία πρόσβασης 27.12.2023]

Lawspot (2022), 'Δημοσιεύθηκε ο νόμος για τις ψηφιακές συμβάσεις (Ν. 4967/2022)'. Διαθέσιμο στο https://www.lawspot.gr/nomika-nea/dimosieythike-o-nomos-gia-tis-psifiakes-symvaseis-n-4967-2022 [Ημερομηνία πρόσβασης 26.12.2023]

ISACA (2020), 'Implementing Robotic Process Automation (RPA) – Trends in RPA adoption, uses and implementation challenges', *ISACA*. Διαθέσιμο στο www.isaca.org [Ημερομηνία πρόσβασης 27.10.2023]

ICAP AE (2019), 'Μεθοδολογία Απόδοσης Αξιολογήσεων Πιστοληπτικής Ικανότητας', διαθέσιμο στο https://dir.icap.gr/mailimages/icap.gr/ratings_analytics/ICAP%20A.E.Μεθοδολογία_Απόδοσης

_Αξιολογήσεων_Πιστοληπτικής_Ικανότητας_Σεπτέμβριος2019.pdf [Ημερομηνία πρόσβασης 27.12.2023]

Deloitte (2018), 'Adopting automation in Internal Audit – Using Robotic Process Automation and cognitive intelligence to fortify the third-line of defence'. Διαθέσιμο στο https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/adopting-robotic-process-automation-in-internal-audit.pdf [Ημερομηνία πρόσβασης 27.10.2023]

Deloitte (2018), 'Continuous Monitoring and Continuous Auditing: From idea to implementation', διαθέσιμο στο https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-aers-continuous-monitoring-and-continuous-auditing-whitepaper-102910.pdf [Ημερομηνία πρόσβασης 27.10.2023]

Gartner (2021), 'RPA operating models: Internal control risk implications for internal auditors', διαθέσιμο στο https://www.gartner.com/document/3999912?ref=solrAll&refval=382636870& [Ημερομηνία πρόσβασης 27.10.2023]

Ernst & Young (2019), 'Κανονισμός ΕΕ 2019/1150: Νέοι κανόνες για τις επιγραμμικές πλατφόρμες'. Διαθέσιμο στο https://www.ey.com/el_gr/tax/tax-alerts/neoi-kanones-gia-tis-epigrammikes-platformes [Ημερομηνία πρόσβασης 26.12.2023]

KPMG (2018), 'Continuous auditing and continuous monitoring: Transforming internal audit and management monitoring to create value', διαθέσιμο στο https://assets.kpmg.com/content/dam/kpmg/kz/pdf/cacm-brochure.pdf [Ημερομηνία πρόσβασης 25.1.2024]

Data Consulting (2017), 'Applying data analytics to internal audit', διαθέσιμο στο www.dataconsulting.co.uk/applying-data-analytics-to-internal-audit/ [Ημερομηνία πρόσβασης 10.2.2024]

European Central Bank (2016), 'ECB Audit Charter, διαθέσιμο στο https://www.ecb.europa.eu/ecb/pdf/orga/ecbauditcharter.en.pdf [Ημερομηνία πρόσβασης 25.1.2024]

Tax Heaven (2016), 'Υποχρεωτικός έλεγχος από ορκωτούς ελεγκτές και σε μικρότερες επιχειρήσεις'. Διαθέσιμο στο https://www.taxheaven.gr/news/30918/ypoxrewtikos-elegxos-apo-orkwtoys-elegktes-kai-se-mikroteres-epixeirhseis [Ημερομηνία πρόσβασης 25.11.2023]

On-Line Σεμινάρια – Webinars

Fang V. (2023), 'Audit Practitioner's Guide to Machine Learning', ISACA Webinar, διαθέσιμο στο https://store.isaca.org/s/community-event?id=a334w000005JoduAAC [Ημερομηνία πρόσβασης 23.12.2023]