



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Πρόγραμμα Μεταπτυχιακών Σπουδών
«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»
Ακαδημαϊκό έτος 2023-2024

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της Παναγιώτας Δ. Κουβουτσάκη (Α.Μ.:2219)

Η ΕΠΙΔΡΑΣΗ ΤΩΝ ΠΟΛΙΤΙΚΩΝ ΚΑΠΟΛΕΜΗΣΗΣ ΤΗΣ ΝΟΜΙΜΟΠΟΙΗΣΗΣ
ΕΣΟΔΩΝ ΑΠΟ ΠΑΡΑΝΟΜΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΣΤΑ ΠΡΟΣΩΠΙΚΑ
ΔΕΔΟΜΕΝΑ

THE IMPACT OF ANTI-MONEY LAUNDERING POLICIES ON DATA PROTECTION

Επιβλέπουσα Καθηγήτρια:

Ευαγγελία (Λίλιαν) Μήτρου

Πειραιάς, Δεκέμβριος 2024

Κατάλογος Περιεχομένων

ΕΙΣΑΓΩΓΗ.....	7
ΚΕΦΑΛΑΙΟ 1.....	9
ΕΠΙΣΚΟΠΗΣΗ ΤΟΥ ΚΑΝΟΝΙΣΤΙΚΟΥ ΠΛΑΙΣΙΟΥ ΤΗΣ ΕΕ	9
1.1. Ιστορική Αναδρομή	9
1.2.1 Η 1 ^η Οδηγία	10
1.2.2. Η 2 ^η Οδηγία	11
1.2.3. Η 3 ^η Οδηγία	12
1.2.4 Η Τέταρτη Οδηγία	14
1.2.5 Η Πέμπτη Οδηγία	15
1.2.6 Η Οδηγία 2018/1673	16
1.2.7 AML Package.....	16
ΚΕΦΑΛΑΙΟ 2.....	23
ΕΡΓΑΛΕΙΑ ΣΥΜΜΟΡΦΩΣΗΣ ΓΙΑ ΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΗΣ ΝΟΜΙΜΟΠΟΙΗΣΗΣ ΕΣΟΔΩΝ ΑΠΟ ΠΑΡΑΝΟΜΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	23
2.1.Προσέγγιση Βάσει Κινδύνου- Risk-Based Approach - RBA)	23
2.2 Η διαδικασία Γνώρισε Τον Πελάτη Σου (ΚΥC)	27
2.3. Δέουσα Επιμέλεια (Due Diligence).....	28
2.3.2 Οι Κατηγορίες Δέουσας Επιμέλειας	30
ΚΕΦΑΛΑΙΟ 3.....	34
Η ΣΥΣΧΕΤΙΣΗ ΜΕΤΑΞΥ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΜΕΤΡΩΝ ΓΙΑ ΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΗΣ ΝΟΜΙΜΟΠΟΙΗΣΗΣ ΕΣΟΔΩΝ ΑΠΟ ΠΑΡΑΝΟΜΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ.....	34
3.1. Εισαγωγή.....	34
3.2. Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ).....	35
3.3. Οι αρχές του ΓΚΠΔ.....	36

3.3.1 Επί της αρχής του περιορισμού του σκοπού	36
3.3.2. Η αρχή της ακρίβειας των δεδομένων	38
3.3.3. Η αρχή της ελαχιστοποίησης των δεδομένων και του περιορισμού της αποθήκευσης	41
3.3.4. Ο περιορισμός της αποθήκευσης	44
3.3.5 Η αρχή της ακεραιότητας και εμπιστευτικότητας	47
3.4. Νομική Βάση Επεξεργασίας.....	50
ΚΕΦΑΛΑΙΟ 4.....	54
ΟΙ ΠΕΡΙΟΡΙΣΜΟΙ ΣΤΑ ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ.....	54
4.1. Περιορισμοί στο πλαίσιο της Καταπολέμησης της Νομιμοποίησης εσόδων από παράνομες δραστηριότητες	54
4.2 Περιορισμοί στο όνομα της εθνικής ασφάλειας	57
4.2. Το δικαίωμα ενημέρωσης.....	58
4.3. Το δικαίωμα πρόσβασης.....	61
ΚΕΦΑΛΑΙΟ 5:.....	66
ΔΙΑΣΥΝΟΡΙΑΚΕΣ ΜΕΤΑΦΟΡΕΣ ΔΕΔΟΜΕΝΩΝ	66
5.1. Το Νομικό Πλαίσιο για τις Διαβιβάσεις Δεδομένων	66
5.2. Το ισχύον Νομοθετικό Πλαίσιο.....	68
5.3 Το νέο Νομοθετικό Πλαίσιο	70
ΚΕΦΑΛΑΙΟ 6.....	76
Η ΥΠΟΘΕΣΗ ΤΟΥ ΠΡΑΓΜΑΤΙΚΟΥ ΔΙΚΑΙΟΥΧΟΥ	76
6.1. Εννοιολογική Προσέγγιση.....	76
6.2. Η Περίφημη Απόφαση WM και Sonim SA κατά Εμπορικού Μητρώου του Λουξεμβούργου.....	78
6.2.1. Το Ιστορικό των συνεκδικαζόμενων υποθέσεων	78
6.2.2. Η πρόταση του Εισαγγελέα	80
6.2.3. Η Απόφαση του Δικαστηρίου	82
6.3. Μετά την Απόφαση.....	86
6.4. Η Νομοθετική Μεταρρύθμιση	89

ΚΕΦΑΛΑΙΟ 7.....	94
Η ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΟΙ ΣΥΝΕΠΕΙΕΣ ΤΗΣ ΕΝΤΑΞΗΣ ΑΥΤΗΣ ΣΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΗΣ ΝΟΜΙΜΟΠΟΙΗΣΗΣ ΕΣΟΔΩΝ ΑΠΟ ΠΑΡΑΝΟΜΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ.....	94
7.1.1. Ορισμός της Τεχνητής Νοημοσύνης.....	94
7.1.2. Ο νέος Κανονισμός για την Τεχνητή Νοημοσύνη (AI Act) ως φορέας αλλαγών στο πεδίο της Τεχνητής Νοημοσύνης.	96
7.2. Η συμβολή της Τεχνητής Νοημοσύνης στην αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες	99
7.2.1. Η ενσωμάτωση της Τεχνητής Νοημοσύνης στον τομέα της νομιμοποίησης εσόδων.	99
7.2.2. Τα οφέλη της Τεχνητής Νοημοσύνης στην αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες.....	100
7.3. Οι επιρροές της Τεχνητής Νοημοσύνης για την αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες στο πεδίο των προσωπικών δεδομένων.....	103
7.3.1 Οι επιρροές της Τεχνητής Νοημοσύνης στο πεδίο των προσωπικών δεδομένων.....	103
7.3.2 Η περίπτωση της αυτοματοποιημένης κατάρτισης προφίλ στον Νέο Κανονισμό 2024/1624.....	105
ΑΝΤΙ ΕΠΙΛΟΓΟΥ.....	113
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	115

ΚΑΤΑΛΟΓΟΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

Ευρωπαϊκή Ένωση	Ε.Ε.
Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα	ΑΠΔΠΧ
Ηνωμένες Πολιτείες της Αμερικής	ΗΠΑ
Οργανισμός Ηνωμένων Εθνών	ΟΗΕ
Καταπολέμηση Της Νομιμοποίησης Εσόδων Από Εγκληματικές Δραστηριότητες Και Χρηματοδότησης Της Τρομοκρατίας	ΚΕΤ/ΧΤ
Μονάδες Χρηματικοοικονομικών Πληροφοριών	ΜΧΠ
Γενικός Κανονισμός για την Προστασία Δεδομένων	ΓΚΠΔ
Ευρωπαϊός Επόπτης προστασίας δεδομένων	ΕΕΠΔ
Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων	ΕΣΠΔ
Χάρτης Θεμελιωδών Δικαιωμάτων ΕΕ	ΧΘΔΑ
Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων	ΕΔΔΑ
Δικαστήριο Ευρωπαϊκής Ένωσης	ΔΕΕ
Συνθήκη για την Λειτουργία Ευρωπαϊκής Ένωσης	ΣΛΕΕ
Σύμπραξη Δημοσίου Ιδιωτικού Τομέα	ΣΔΙΤ
Ultimate Beneficial Owner	UBO
Anti-Money Laundering	AML
Financial Action Task Force	FATF

Περίληψη

Η παρούσα διπλωματική εργασία, εξετάζει την επίδραση των πολιτικών κατά του ξεπλύματος χρήματος, στην προστασία των προσωπικών δεδομένων. Το παρόν πόνημα, υπό το πρίσμα του πρόσφατου νομοθετικού πλαισίου για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες (AML Package), επιχειρεί να σκιαγραφήσει τις αλλαγές που το νομοθετικό πακέτο επιφέρει και τον αντίκτυπο που έχουν στα προσωπικά δεδομένα. Αρχικά, παρουσιάζεται μια συνοπτική ιστορική καταγραφή της νομοθετικής εξέλιξης γύρω από το ζήτημα της καταπολέμησης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Εν συνέχεια, καταγράφονται διαδικασίες που απαιτούν να ακολουθούν οι υπόχρεες οντότητες, ενώ καταδεικνύεται πώς η αυξημένη ρύθμιση και η υποχρέωση ανταλλαγής και επεξεργασίας δεδομένων που εφαρμόζονται για την καταπολέμηση της νομιμοποίησης παράνομων εσόδων, μπορεί να συγκρουστεί με τις αρχές προστασίας δεδομένων που προβλέπονται στον ΓΚΠΔ, διερευνώντας κατά πόσο επηρεάζει την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων. Σε αυτό το πλαίσιο, αναλύεται η περίφημη απόφαση αναφορικά με το Μητρώο Πραγματικών Δικαιούχων, που απασχόλησε το σύνολο του νομικού κόσμου, επιφέροντας σημαντικές νομοθετικές αλλαγές. Τέλος, η εργασία εξετάζει επίσης τον ρόλο της τεχνητής νοημοσύνης στην πρόληψη και καταστολή του ξεπλύματος χρήματος, αναδεικνύοντας ταυτόχρονα τις προκλήσεις που εγείρονται στην προστασία προσωπικών δεδομένων από την εφαρμογή της. Η έρευνα καταλήγει επισημαίνοντας την ανάγκη για ισορροπημένη προσέγγιση, όπου οι νέες τεχνολογίες και αυστηρότεροι κανονισμοί πρέπει να εφαρμόζονται με σεβασμό στα θεμελιώδη δικαιώματα και την ιδιωτικότητα των ατόμων.

Λέξεις Κλειδιά: AML, Ξέπλυμα χρήματος, καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, προσωπικά δεδομένα, Τεχνητή Νοημοσύνη, Πραγματικός Δικαιούχος, ΚΕΤ/ΧΤ

Abstract

This thesis examines the impact of anti-money laundering policies on the protection of personal data. This paper, under the framework of the recent legislative measures for combating the legalization for anti-money laundering (AML Package), attempts to outline the changes brought by the new legislative package and their impact on personal data. Initially, a concise historical record of the legislative evolution concerning the issue of anti-money laundering is presented. Subsequently, the processes that obligated entities must follow are recorded, while demonstrating how increased regulation and the obligation to exchange and process data applied for combating the legalization of illicit proceeds can conflict with the data protection principles stipulated by the GDPR, exploring how it affects the exercise of the rights of data subjects. In this context, the famous decision regarding the Register of Ultimate Beneficial Owners, which occupied the entire legal world and led to significant legislative changes, is analyzed. Finally, the paper also examines the role of artificial intelligence in the prevention and suppression of money laundering, highlighting the challenges that arise in the protection of personal data from its application. The research concludes by emphasizing the need for a balanced approach, where new technologies and stricter policies must be applied with respect for fundamental rights and the privacy of individuals.

Keywords: AML, anti- money laundering, personal data, Artificial Intelligence, Ultimate Beneficial Owner.

ΕΙΣΑΓΩΓΗ

Η καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας (στο εξής ΚΕΤ/ΧΤ και Anti-Money Laundering, εφεξής AML) αποτελεί κρίσιμο στοιχείο της διεθνούς στρατηγικής για την καταπολέμηση της οικονομικής εγκληματικότητας. Το νομοθετικό πλαίσιο AML απαιτεί την παρακολούθηση, τη συλλογή και την ανταλλαγή σημαντικών ποσοτήτων πληροφοριών, οι οποίες περιλαμβάνουν μεταξύ άλλων, και προσωπικά δεδομένα. Αυτή η ανταλλαγή πληροφοριών αποτελεί σημαντική συνιστώσα για την αναγνώριση, την ανίχνευση την πρόληψη και καταστολή ενεργειών και διαδικασιών που σχετίζονται με την νομιμοποίηση εσόδων από παράνομες δραστηριότητες. Ωστόσο, η ευρεία επεξεργασία προσωπικών δεδομένων που απαιτείται για την εφαρμογή των αντίστοιχων πολιτικών και μέτρων, δημιουργεί σημαντικές προκλήσεις σε ό,τι αφορά την προστασία της ιδιωτικότητας και των ατομικών δικαιωμάτων εν γένει.

Πιο συγκεκριμένα, η παρούσα εργασία έχοντας ως αφετηρία την υιοθέτηση του νέου νομοθετικού πλαισίου για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες από την ΕΕ, το λεγόμενο AML Package και συγκεκριμένα το γράμμα του νέου Κανονισμού 2024/1624 (εφεξής ο «Κανονισμός») και της Έκτης Οδηγίας, επιχειρεί να σκιαγραφήσει κατά πόσο η νέα αυτή ευρωπαϊκή νομοθετική πρωτοβουλία, συμπλέει με το ήδη υπάρχον κανονιστικό πλαίσιο για την προστασία των προσωπικών δεδομένα και ειδικά με τις επιταγές του περίφημου Γενικού Κανονισμού Προστασίας Δεδομένων (εφεξής ΓΚΠΔ).

Προκειμένου να επιτευχθεί η ως άνω σκιαγράφηση, το παρόν πόνημα, αναλύει τις διαδικασίες που οφείλουν να τηρούν οι υπόχρεες από τον νόμο οντότητες για την εφαρμογή ΚΕΤ/ΧΤ και τις αλλαγές που θα επέλθουν μετά την πλήρη υιοθέτηση του νέου νομοθετικού πακέτου.

Εν συνεχεία, υπό το πρίσμα των θεμελιωδών αρχών που προβλέπει ο ΓΚΠΔ για την προστασία των δεδομένων των υποκειμένων, επιχειρείται να αναδειχθεί

κατά πόσο οι συγκεκριμένες αρχές επηρεάζονται από τα μέτρα για την αντιμετώπιση του ξεπλύματος χρήματος αλλά και τι ρόλο διαδραματίζουν τα ως άνω μέτρα, στην άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων. Υπό αυτή τη βάση, η παρούσα διπλωματική εργασία, αναλύει την περίφημη υπόθεση του Πραγματικού Δικαιούχου (WM and Sovim SA v. Luxembourg Business Registers) που ανέδειξε εν πολλοίς τα ως άνω ζητήματα, διαμορφώνοντας καθοριστικά τα τελικά κείμενα του περίφημου AML Package.

Ενώ, το παρόν πόνημα καταλήγει στον καθοριστικό ρόλο της τεχνητής νοημοσύνης, εξετάζοντας κατά πόσο οι νέες τεχνολογίες που χρησιμοποιούνται ολοένα και περισσότερο για την πρόληψη και την καταστολή του φαινομένου ξεπλύματος χρήματος με τον εντοπισμό ύποπτων συναλλαγών, επηρεάζουν τα προσωπικά δεδομένα.

Η διπλωματική εργασία, μέσω της κριτικής ανάλυσης και της σύγκρισης μεταξύ των παλαιότερων πολιτικών AML, με την νέα νομοθετική ευρωπαϊκή πρωτοβουλία για την αντιμετώπιση του φαινομένου, αποσκοπεί να αναδείξει το ζήτημα της λεπτής ισορροπίας πρέπει να επιτευχθεί μεταξύ ασφάλειας, προστασίας του δημοσίου συμφέροντος και ιδιωτικότητας.

ΚΕΦΑΛΑΙΟ 1

ΕΠΙΣΚΟΠΗΣΗ ΤΟΥ ΚΑΝΟΝΙΣΤΙΚΟΥ ΠΛΑΙΣΙΟΥ ΤΗΣ ΕΕ

1.1. Ιστορική Αναδρομή

Η νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες, όρος ο οποίος είναι ευρέως γνωστός ως «ξέπλυμα χρήματος»,¹ (διεθνής ονομασία money laundering), αποτελεί μία μέθοδο απόκτησης χρημάτων που παράγονται από εγκληματική δραστηριότητα, σύμφωνα με την οποία η παράνομη απόκτηση περιουσιακών στοιχείων φαίνεται ως νόμιμη μέσω της συγκάλυψης των κερδών, τα οποία τελικώς αποτυπώνονται ως σαν να προέρχονται από νόμιμη πηγή εσόδων.

Η νομιμοποίηση εσόδων από παράνομες δραστηριότητες έχει εξελιχθεί σε μια σημαντική παγκόσμια ανησυχία. Αρχικά, συσχετιζόταν κυρίως με τη διακίνηση ναρκωτικών, αλλά το εύρος της έχει επεκταθεί ώστε να περιλαμβάνει διάφορες μορφές διασυνοριακών εγκληματικών δραστηριοτήτων. Η αυξανόμενη συνειδητοποίηση του επιζήμιου αντίκτυπου της νομιμοποίησης εσόδων από παράνομες δραστηριότητες στα χρηματοπιστωτικά συστήματα και στην κοινωνία γενικότερα, έχει οδηγήσει σε αυξημένη διεθνή συζήτηση στην καταπολέμηση αυτού του ζητήματος².

Στις Ηνωμένες Πολιτείες της Αμερικής (ΗΠΑ), η πρώτη μεγάλη νομοθετική προσπάθεια για την αντιμετώπιση του ζητήματος, ήταν ο Νόμος για τον Έλεγχο

¹ Οι απαρχές του φαινομένου του ξεπλύματος χρήματος ως έννοια υπάρχουν από τις αρχές του 20ού αιώνα. Κατά τη διάρκεια της περιόδου της Ποτοαπαγόρευσης στις Ηνωμένες Πολιτείες (1920-1933) πρωτοεμφανίστηκε ο όρος «ξέπλυμα βρώμικου χρήματος». Εγκληματίες προσπαθούσαν να νομιμοποιήσουν τα κέρδη τους από παράνομες πωλήσεις αλκοόλ, «ξεπλένοντάς» τα μέσω νόμιμων επιχειρήσεων, όπως πλυντήρια, από τα οποία προέκυψε και ο όρος «ξέπλυμα βρώμικου χρήματος». Καθοριστική έχει θεωρηθεί συνδρομή του περιβόητου εγκληματία ΆλΚαπόνε, ο οποίος ήταν ένας σημαντικός αρχηγός της μαφίας στο Σικάγο και θεωρείται ότι ο όρος «ξέπλυμα βρώμικου χρήματος» προήλθε από αυτόν, καθώς ίδρυσε πλυντήρια ρούχων σε όλη την πόλη για να αποκρύψει την προέλευση του χρήματος που κέρδιζε από τις πωλήσεις αλκοόλ.

² (A. Bakardjieva Engelbrekt et al. (eds.), 2024)

της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες του 1986,³ που τόνισε την ανάγκη περιορισμού της ροής παράνομου χρήματος και έδωσε τον εξής ορισμό: «Ως νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες περιγράφεται η διαδικασία μέσω της οποίας αποκρύπτεται η ύπαρξη, η παράνομη πηγή ή η παράνομη χρήση εσόδων, τα οποία στη συνέχεια μεταμφιέζονται με τέτοιο τρόπο ώστε η προέλευσή τους να εμφανίζεται νόμιμη». Σε διεθνές επίπεδο, το ζήτημα βρέθηκε στο επίκεντρο με τη Σύμβαση του ΟΗΕ του 1988⁴ κατά της Παράνομης Διακίνησης Ναρκωτικών και Ψυχοτρόπων Ουσιών (Σύμβαση του 1988), η οποία, αν και επικεντρώθηκε στη διακίνηση ναρκωτικών, έθεσε τις βάσεις για ευρύτερη διεθνή συνεργασία κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και είναι η πρώτη πολυμερής συνθήκη που ασχολείται γενικά με τα αδικήματα της.

Αντίστοιχα, η ανταπόκριση της Ευρωπαϊκής Ένωσης (ΕΕ) στο ζήτημα ήταν άμεση καθώς το ενδιαφέρον για την ΚΕΤ/ΧΤ δεν είναι ούτε νέο, ούτε απομονωμένο από τις παγκόσμιες πρωτοβουλίες. Η ανάγκη προστασίας του χρηματοοικονομικού συστήματος και ο φόβος ότι η εφαρμογή ριζικά διαφορετικών μέτρων στον συγκεκριμένο τομέα θα μπορούσε να υπονομεύσει την απρόσκοπτη λειτουργία της αγοράς αποτέλεσαν για την Ευρωπαϊκή Επιτροπή τη νομική βάση σύμφωνα με τη Σύμβαση του 1988, προκειμένου να προτείνει τη θέσπιση κοινοτικής νομοθεσίας.⁵

1.2.1 Η 1^η Οδηγία

Τα πρώτα ουσιαστικά βήματα που έγιναν στην Ευρώπη, για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες εντοπίζονται στην Οδηγία του Ευρωπαϊκού Συμβουλίου το 1991, αναφορικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη

³ (Doyle, 2017)

⁴ Στην ελληνική έννομη τάξη η σύμβαση κυρώθηκε με τον Ν.1990/1991, «Κύρωση Σύμβασης Ηνωμένων Εθνών κατά της παράνομης διακίνησης ναρκωτικών φαρμάκων και ψυχοτρόπων ουσιών», διαθέσιμο στο <https://www.kodiko.gr/nomothesia/document/230535/nomos-1990-1991>

⁵ Ανακοίνωση της Επιτροπής προς το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο σχετικά με την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος στον χρηματοοικονομικό τομέα (Επιτροπή, 2004)

νομιμοποίηση εσόδων από παράνομες δραστηριότητες (εφεξής «Πρώτη Οδηγία»)).⁶

Το περιεχόμενο της Πρώτης Οδηγίας στηρίχτηκε κυρίως στις «40 συστάσεις» της FATF⁷ και ήταν η πρώτη φορά που προβλέφθηκε το ξέπλυμα χρήματος σε κοινοτικό επίπεδο. Οι «40 συστάσεις της FATF» θεωρούνται ως ένα ντε φάκτο πρότυπο παγκόσμιας ισχύος ΚΕΤ/ΧΤ. Υπό αυτό το πρίσμα, η Οδηγία προχώρησε περισσότερο ένα βήμα πέρα από την FATF, καθώς οι αρχικές «40 συστάσεις» προέβλεπαν ότι η γνωστοποίηση περιπτώσεων ξεπλύματος χρήματος ήταν προαιρετική, ενώ η Οδηγία προέβλεπε ήδη ότι η γνωστοποίηση αυτή ήταν υποχρεωτική.⁸ Παράλληλα, η Πρώτη Οδηγία εστίαζε στο ρόλο των τραπεζών, ως τις κύριες υπόχρεες οντότητες για την αντιμετώπιση του ζητήματος και παρείχε το αρχικό πλαίσιο καθιερώνοντας βασικά προληπτικά μέτρα, όπως η ταυτοποίηση πελατών, η τήρηση αρχείων και οι αναφορές ύποπτων συναλλαγών. Η Πρώτη Οδηγία, ψηφίστηκε προκειμένου να διασφαλιστεί η υιοθέτηση μιας καθολικής προσέγγισης ΚΕΤ/ΧΤ από τα κράτη μέλη.

1.2.2. Η 2^η Οδηγία

Η Οδηγία 2001/97/ΕΚ (εφεξής «Δεύτερη Οδηγία») τροποποίησε την Πρώτη Οδηγία.⁹ Καταλυτικός παράγοντας για την έκδοση της, ήταν η τρομοκρατική επίθεση που είχαν δεχθεί οι ΗΠΑ μόλις πριν από περίπου τρεις μήνες. Παρόλα αυτά το περιεχόμενο της είχε ήδη αποφασιστεί και στόχευε στην κάλυψη των κενών της Πρώτης Οδηγίας.¹⁰ Ως καθοριστική αλλαγή εντοπίζεται η υποχρέωση σύστασης μιας

⁶ (Οδηγία 91/308/ΕΟΚ, 1991)

⁷ FATF: Η Ομάδα Χρηματοοικονομικής Δράσης (FATF) είναι ένας διακυβερνητικός οργανισμός που ιδρύθηκε το 1989 με πρωτοβουλία της G7, η γραμματεία της στεγάζεται στην έδρα του ΟΟΣΑ στο Παρίσι και έχει σκοπό την ανάπτυξη πολιτικών για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, της χρηματοδότησης της τρομοκρατίας και της διάδοσης όπλων μαζικής καταστροφής. Ως διεθνής φορέας που θέτει τα παγκόσμια πρότυπα συμμόρφωσης των χωρών ως προς την τεχνική τους επάρκεια και την αποτελεσματικότητά τους στην καταπολέμηση του ξεπλύματος χρήματος και της χρηματοδότησης της τρομοκρατίας (ΧΤ), παρακολουθεί την πρόοδο των χωρών μελών στην εφαρμογή των συστάσεών της μέσω διαδικασίας αμοιβαίας αξιολόγησης.

⁸ (Οδηγία 91/308/ΕΟΚ, 1991)

⁹ Η Οδηγία ενσωματώθηκε στην Ελλάδα με τον νόμο 3424/2005.

¹⁰ (Παντής, 2021)

ειδικής Αρχής σε κάθε κράτος-μέλος, στην οποία τα υπόχρεα πρόσωπα του κάθε κράτους θα υπέβαλαν τις ύποπτες συναλλαγές που εντόπιζαν. Η νέα Οδηγία επέκτεινε το πεδίο εφαρμογής της σχετικής νομοθεσίας, προσθέτοντας νέα βασικά αδικήματα και διεύρυνε το πεδίο των επαγγελματιών που θεωρούνται υπόχρεα πρόσωπα. Ιδιαίτερα αμφιλεγόμενη ήταν η επέκταση των υποχρεώσεων σε δικηγόρους, συμβολαιογράφους και άλλους νομικούς επαγγελματίες, για την οποία διατυπώθηκαν αντιρρήσεις περί παραβίασης του απορρήτου και του εξ ορισμού εμπιστευτικού χαρακτήρα της σχέσης δικηγόρου - πελάτη. Το γεγονός ότι, επιμέρους ζητήματα ρύθμισης των σχετικών υποχρεώσεων των δικηγόρων, αφέθηκαν στη διακριτική ευχέρεια των κρατών – μελών, πήρε το χαρακτήρα πολιτικού συμβιβασμού.¹¹

1.2.3. Η 3^η Οδηγία

Εξαιτίας της ανάγκης να δώσει η ΕΕ μια απάντηση στον «Πόλεμο κατά της Τρομοκρατίας» η οδηγία 2005/60/EK (εφεξής «Τρίτη Οδηγία»)¹² ήρθε μόλις τέσσερα χρόνια αργότερα καταργώντας την Οδηγία 91/308/ΕΟΚ.¹³ Ορισμένα κράτη βέβαια, όπως το Ηνωμένο Βασίλειο με την UK's Terrorism Act, είχαν ήδη θεσπίσει σχετική νομοθεσία στο εθνικό τους δίκαιο,¹⁴ πριν καν συμβεί η τρομοκρατική επίθεση στις 11 Σεπτεμβρίου 2001. Η υιοθέτηση της Τρίτης Οδηγίας AML, ευθυγράμμισε τους περιφερειακούς κανόνες της ΕΕ με τις αναθεωρημένες και διευρυμένες συστάσεις της FATF.¹⁵ Ως αποτέλεσμα, τα προληπτικά μέτρα της οδηγίας κάλυπταν πλέον όχι μόνο τη διαχείριση χρημάτων που προέρχονται από εγκλήματα, αλλά και τη συλλογή χρημάτων ή περιουσιακών στοιχείων για τρομοκρατικούς σκοπούς. Μια σημαντική

¹¹ (Mitsilegas V, 2007)

¹² (2005/60/EK) σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας.

¹³ Στην Ελλάδα ενσωματώθηκε με τον νόμο 3691/2008 «Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας και άλλες διατάξεις» διαθέσιμο στο <http://elib.aade.gr/elib/view?d=/gr/act/2008/3691/art/7%CE%91/para/1>

¹⁴ Βλέπε UK's Terrorism Act 2000

¹⁵ (A. Bakardjieva Engelbrekt et al. (eds.), 2024)

προσθήκη με την Τρίτη Οδηγία ήταν οι 9 «ειδικές συστάσεις» της FATF για την καταπολέμηση της χρηματοδότησης της τρομοκρατίας, τις οποίες εξέδωσε το 2003.

Η ενσωμάτωσή τους στο νομοθετικό πλαίσιο, οδήγησε στην επέκταση του νομικού και κανονιστικού οπλοστασίου που χρησιμοποιούνταν για το ξέπλυμα χρήματος και τη χρηματοδότηση της τρομοκρατίας. Επιπλέον, η Τρίτη Οδηγία, προέβλεψε ρητά την υποχρέωση σύστασης Μονάδων Χρηματοοικονομικών Πληροφοριών¹⁶ (ΜΧΠ) για την αναφορά ύποπτων συναλλαγών και την απαγόρευση γνωστοποίησης στον εμπλεκόμενο ότι θα διεξαχθεί ή διεξάγεται έρευνα εις βάρος του.

Εκτός από την επέκταση των διατάξεων σε όλες τις χρηματοοικονομικές συναλλαγές που μπορεί να συνδέονται με τρομοκρατικές δραστηριότητες, η μεγαλύτερη αλλαγή στην Τρίτη Οδηγία ήταν η καθιέρωση ενός προτύπου για την ανάλυση κινδύνου. Το σημείο εκκίνησης ήταν ότι οι κίνδυνοι διαφέρουν μεταξύ χωρών, πελατών και επιχειρηματικών τομέων, καθώς και με την πάροδο του χρόνου. Ως εκ τούτου, στην Τρίτη Οδηγία εισήχθησαν για πρώτη φορά τα περίφημα μέτρα δέουσας επιμέλειας προς τις υπόχρεες οντότητες¹⁷ έτσι ώστε να εξασφαλίζεται ότι δεν παρέχουν υπηρεσίες σε τρομοκράτες ή τρομοκρατικές οργανώσεις. Ενώ ταυτόχρονα, επεκτάθηκε η λίστα των υπόχρεων οντοτήτων συμπεριλαμβάνοντας τους λογιστές και τα καζίνο, φέρνοντας μια νέα οπτική στην εφαρμογή των πρακτικών για την καταπολέμηση του ξέπλυματος χρήματος, δυνάμει του εκάστοτε κινδύνου που παρουσιάζει ο συγκεκριμένος πελάτης.¹⁸¹⁹

¹⁶ Αιτιολογική Σκέψη 29 Οδηγίας 2005/60/ΕΚ: «Οι ύποπτες συναλλαγές θα πρέπει να γνωστοποιούνται στη Μονάδα Χρηματοοικονομικών Πληροφοριών (ΜΧΠ), η οποία αποτελεί το εθνικό κέντρο παραλαβής, ανάλυσης και διαβίβασης προς τις αρμόδιες αρχές των αναφορών για τις ύποπτες συναλλαγές καθώς και άλλων πληροφοριών σχετικά με την ενδεχόμενη νομιμοποίηση παράνομων εσόδων ή χρηματοδότηση της τρομοκρατίας.»

¹⁷ Συγκεκριμένα νομικά και φυσικά πρόσωπα που οφείλουν να εφαρμόζουν εσωτερικές πολιτικές, διαδικασίες και ελέγχους για τον μετριασμό και την αποτελεσματική διαχείριση των κινδύνων νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας

¹⁸ (Κασιμάτη, 2021)

¹⁹ (A. Bakardjieva Engelbrekt et al. (eds.), 2024)

Ενώ, προβλέφθηκε και αναγνώριση της ανάγκης επιβολής κυρώσεων στα υπόχρεα πρόσωπα που δεν τηρούν τις διατάξεις του νόμου. Ωστόσο, η Τρίτη Οδηγία απέφυγε να ορίσει συγκεκριμένες κυρώσεις, αφήνοντας αυτό το θέμα στη διακριτική ευχέρεια της εθνικής νομοθεσίας. Όπως αναφέρεται στην πρώτη παράγραφο του Άρθρου 39 «οι κυρώσεις πρέπει να είναι αποτελεσματικές, αναλογικές και αποτρεπτικές».

1.2.4 Η Τέταρτη Οδηγία

Μία ακόμα αναθεώρηση του καταλόγου των Συστάσεων της FATF, που έλαβε χώρα το έτος 2013, οδήγησε στην έκδοση της περίφημης Οδηγίας 2015/849 (εφεξής «Τέταρτη Οδηγία»), οποία τροποποίησε την προγενέστερη αναφερθείσα Τρίτη Οδηγία και την αντίστοιχη εκτελεστική Οδηγία 2006/70/EK της Επιτροπής και τέθηκε σε ισχύ στις 26 Ιουνίου 2015. Η προσέγγιση βάσει κινδύνου που εισήχθη από τις αναθεωρημένες συστάσεις της FATF και την Τρίτη Οδηγία αναπτύχθηκε περαιτέρω προς μια πιο στοχευμένη και επικεντρωμένη προσέγγιση βάσει κινδύνου με αποφάσεις που βασίζονται σε αποδεικτικά στοιχεία²⁰. Η πλειοψηφία των διατάξεων της Τέταρτης Οδηγίας, στόχευε στην πρόληψη του ξεπλύματος βρώμικου χρήματος, η οποία φαίνεται να προκρίνεται σε σχέση με τον ποινικό κολασμό του. Επιπλέον, η Τέταρτη Οδηγία περιέχει ένα σύνολο διατάξεων που διευρύνουν το κανονιστικό πλαίσιο σχετικά με τα υπόχρεα πρόσωπα, συμπεριλαμβάνοντας και μη χρηματοπιστωτικά ιδρύματα²¹.

²⁰ (A. Bakardjieva Engelbrekt et al. (eds.), 2024)

²¹ Αναφορικά με το πεδίο εφαρμογής της, αυτό περιλαμβάνει έναν διευρυμένο αριθμό επιχειρήσεων που χαρακτηρίζονται ως «υπόχρεες οντότητες» (*obliged entities*), οι οποίες, ανεξάρτητα από το μέγεθος και τον όγκο των δραστηριοτήτων τους, πραγματοποιούν χρηματοπιστωτικές συναλλαγές. Αυτές οι υπόχρεες οντότητες, σύμφωνα με το άρθρο 2, περιλαμβάνουν πέραν των πιστωτικών ιδρυμάτων & των χρηματοπιστωτικών επιχειρήσεων, και άλλες καθορισμένες μη-χρηματοπιστωτικές επιχειρήσεις και επαγγέλματα²⁷²(*Designated Non-Financial Businesses and Professions - DNFBP*). Τα DNFBP υπόκεινται στις Συστάσεις της FATF, και περιλαμβάνουν, μεταξύ άλλων: ελεγκτές, εξωτερικούς λογιστές και φορολογικούς συμβούλους, καζίνο και άλλους φορείς παροχής τυχερών παιχνιδιών, έμπορους πολύτιμων μετάλλων & λίθων, δικηγόρους, συμβολαιογράφους & άλλους ανεξάρτητους νομικούς επαγγελματίες, μεσιτικά γραφεία, όπως και δομές καταπιστευμάτων (*trusts*)

Ενώ, αρκετή έμφαση δόθηκε επίσης στην ενίσχυση της διαφάνειας στις εταιρικές δομές, για την αντιμετώπιση διαφθοράς και της φοροδιαφυγής. Στο πλαίσιο αυτό, ορίζεται η υποχρέωση καταγραφής των πραγματικών δικαιούχων των νομικών οντοτήτων²² εισάγοντας το περίφημο Κεντρικό Μητρώο Πραγματικών Δικαιούχων-εφεξής «UBO»²³. Η οδηγία έδωσε έμφαση στην έννοια του Πραγματικού Δικαιούχου (BO), υποχρεώνοντας τα νομικά πρόσωπα να τηρούν επικαιροποιημένα δεδομένα για τους πραγματικούς δικαιούχους τους, τα οποία να παρέχονται στις αρμόδιες αρχές.

Τέταρτον, ρυθμίστηκαν τα προϊόντα ηλεκτρονικού χρήματος (εφεξής «**e-money**») για πρώτη φορά, προκειμένου να αντιμετωπιστούν ζητήματα νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας που μπορεί να προκύψουν μέσω συστημάτων ηλεκτρονικών πληρωμών, όπως οι προπληρωμένες κάρτες και τα ηλεκτρονικά πορτοφόλια.

Τέλος, θεσπίστηκαν διοικητικές κυρώσεις καθώς προβλέφθηκε συνεργασία μεταξύ των εθνικών ΜΧΠ και των αρμόδιων εθνικών αρχών για την επιβολή διοικητικών κυρώσεων σε περιπτώσεις σοβαρών παραβιάσεων.

1.2.5 Η Πέμπτη Οδηγία

Η Οδηγία 2018/843 (εφεξής «Πέμπτη Οδηγία») για το ξέπλυμα βρώμικου χρήματος,²⁴ εκδόθηκε τον Ιούνιο του 2018.²⁵ Σύμφωνα με τις αιτιολογικές σκέψεις που περιλαμβάνονται στο προοίμιό της, σημαντικό ρόλο διαδραμάτισαν οι αυξανόμενες τρομοκρατικές επιθέσεις²⁶, για την οργάνωση και χρηματοδότηση των οποίων, χρησιμοποιήθηκαν νέες μέθοδοι και τεχνολογίες, ως εναλλακτικά χρηματοπιστωτικά συστήματα.

²² Άρθρο 20 της Οδηγίας ΕΕ 2015/849

²³ Στην Ελλάδα ενσωματώνεται με τον νόμο 4557/2018, αφού προηγουμένως η Ευρωπαϊκή Επιτροπή είχε παραπέμψει τη χώρα στο Δικαστήριο της ΕΕ επειδή δεν είχε ενσωματώσει εγκαίρως την εν λόγω Οδηγία (η προθεσμία ήταν η 26η Ιουνίου 2017).

²⁴ (2018/843)

²⁵ Ενσωματώθηκε στην ελληνική έννομη τάξη με τον νόμο 4734/2020, μαζί με το Άρθρο 3 της Οδηγίας 2019/2177 (τροποποιεί το Άρθρο 6 της 2015/849)

²⁶ Αιτιολογική Σκέψη 2, Οδηγίας 2018/843

Οι βασικότερες τροποποιήσεις σε σχέση με τις προγενέστερες Οδηγίες, αφορούσαν ρυθμίσεις για τα προπληρωμένα μέσα πληρωμής, που εκδίδονται εντός και εκτός Ε.Ε. Επίσης, αυστηροποιούνται οι διαδικασίες αναγνώρισης Πολιτικά Εκτεθειμένων Προσώπων (ΠΕΠ), τα οποία θεωρούνται υψηλού κινδύνου, και επεκτείνεται το πεδίο εφαρμογής της Οδηγίας σε νέους τομείς, όπως οι μεσίτες ακινήτων και οι έμποροι τέχνης. Επιπλέον, η μεγάλη προσθήκη που έφερε η Οδηγία είναι οι διατάξεις περί κρυπτονομισμάτων και ηλεκτρονικών πορτοφολιών, ορίζοντας τα «εικονικά νομίσματα» και τους «παρόχους υπηρεσιών θεματοφυλακής πορτοφολιών».

1.2.6 Η Οδηγία 2018/1673

Η Οδηγία για «την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες μέσω του ποινικού δικαίου» εκδόθηκε τον Οκτώβριο του έτους 2018.²⁷ Τα βασικά σημεία αυτής είναι: η θέσπιση ελάχιστων ποινικών κανόνων σχετικά με τα αδικήματα και τις κυρώσεις που επιφέρουν, η ευθύνη των νομικών οντοτήτων που τελούνται προς όφελός τους και τέλος, η άρση των εμποδίων στη διασυνοριακή συνεργασία με τη συμμετοχή της Eurojust. Στόχος της Οδηγίας είναι η επαναπροσέγγιση βασικών ζητημάτων, όπως το ποιες πράξεις αποτελούν εγκληματικές δραστηριότητες, ποια είναι τα υπόχρεα πρόσωπα και ποιες κυρώσεις πρέπει να τους επιβάλλονται.²⁸

1.2.7 AML PACKAGE

Σημείο τομής για την μάχη κατά του ξεπλύματος χρήματος, αποτελεί η υιοθέτηση του περίφημου AML PACKAGE. Η Επιτροπή δημοσίευσε ένα φιλόδοξο και πολύπλευρο σχέδιο δράσης, στοχεύοντας όπως χαρακτηριστικά δήλωσε

²⁷ Η οδηγία (2018/1673)

²⁸ Στις 30 Ιουνίου 2021, κατατέθηκε προς ψήφιση στη Βουλή των Ελλήνων το σχέδιο Νόμου «Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας - Τροποποίηση του ν. 4557/2018 - Ενσωμάτωση της Οδηγίας (ΕΕ) 2018/1673 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, σχετικά με την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες μέσω του ποινικού δικαίου και διατάξεις για την επιτάχυνση της απονομής της δικαιοσύνης»

ο Εκτελεστικός Αντιπρόεδρος Valdis Dombrovskis στο να «βάλουμε ένα τέλος στο βρώμικο χρήμα που διεισδύει στο χρηματοπιστωτικό μας σύστημα. Σήμερα, ενισχύουμε περαιτέρω τις άμυνές μας για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, με ένα ολοκληρωμένο και εκτεταμένο Σχέδιο Δράσης».²⁹

Πιο συγκεκριμένα, τον Μάιο του 2020, η Ευρωπαϊκή Επιτροπή δημοσίευσε ανακοίνωση σχετικά με ένα σχέδιο δράσης για μια ολοκληρωμένη πολιτική της Ένωσης για την πρόληψη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, στην οποία εξέφρασε την πρόθεσή της να υποβάλει νέες νομοθετικές προτάσεις σχετικά με την καταπολέμηση του ξεπλύματος χρήματος.³⁰ Το ως άνω σχέδιο δράσης περιείχε έξι βασικούς πυλώνες που στοχεύουν στη βελτίωση της συνολικής αποτελεσματικότητας των μέτρων της ΕΕ. Αυτοί οι πυλώνες περιλάμβαναν την ενίσχυση της εφαρμογής των υφιστάμενων κανόνων, τη δημιουργία ενός ενιαίου εγχειριδίου κανόνων για όλη την ΕΕ καθώς και τη σύσταση εποπτικής αρχής σε επίπεδο ΕΕ για την αποφυγή εποπτικών κενών. Επιπλέον, αναφορά γινόταν στην ενίσχυση του συντονισμού μεταξύ των ΜΧΠ, στην προώθηση της επιβολής ποινικών διατάξεων και της ανταλλαγής πληροφοριών σε επίπεδο ΕΕ, ειδικά σε συνεργασία με τρίτες χώρες και διεθνείς οργανισμούς όπως η FATF.

Συνολικά, το σχέδιο στοχεύει στη δημιουργία ενός πιο εναρμονισμένου και αποτελεσματικού πλαισίου για την ΚΕΤ/ΧΤ, ενισχύοντας τον ρόλο της ΕΕ σε παγκόσμιο επίπεδο.³¹

Εν συνεχεία, στις 20 Ιουλίου 2021, η Επιτροπή, ανακοίνωσε τη «*Νομοθετική δέσμη μέτρων για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες*

²⁹ (Euractiv, 2020)

³⁰ (Επιτροπή Ε., Ανακοίνωση σχετικά με σχέδιο δράσης για ολοκληρωμένη ενωσιακή πολιτική με σκοπό την πρόληψη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, 2020)

³¹ (Επιτροπή Ε., Η Επιτροπή εντείνει τα μέτρα για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, 2020)

δραστηριότητες και την καταπολέμηση της χρηματοδότησης της τρομοκρατίας», με σκοπό την δημιουργία ενός ισχυρού και ασφαλούς στο μέλλον συστήματος επιβολής, το οποίο θα βελτιώσει τον εντοπισμό της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας στην ΕΕ και θα κλείσει τα υπάρχοντα κενά που χρησιμοποιούνται από εγκληματίες για τη νομιμοποίηση παράνομων προϊόντων εγκλήματος.³² Το ως άνω Πακέτο περιλαμβάνει τα ακόλουθα:

- Κανονισμό για τη δημιουργία Αρχής της ΕΕ για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και την καταπολέμηση της χρηματοδότησης της τρομοκρατίας (« AMLA») εξοπλισμένη με την αρμοδιότητα να επιβάλλει κυρώσεις ³³
- Κανονισμό σχετικά με την πρόληψη της χρήσης του χρηματοπιστωτικού συστήματος για τους σκοπούς της νομιμοποίησης εσόδων από παράνομες δραστηριότητες (ΞΕ) και της χρηματοδότησης της τρομοκρατίας .³⁴
- Οδηγία για τους μηχανισμούς καταπολέμησης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες
- Κανονισμό για την αναδιτύπωση του κανονισμού (ΕΕ) 2015/847 για την επέκταση των απαιτήσεων ιχνηλασιμότητας στα κρυπτονομικά περιουσιακά στοιχεία.

Μετά από σειρά κύκλων συζητήσεων, στις 30 Μαΐου 2024, το Συμβούλιο ενέκρινε την ως άνω δέσμη νέων κανόνων ενάντια στο ξέπλυμα χρήματος ³⁵ και στις 19 Ιουνίου 2024, δημοσιεύθηκαν στην Επίσημη Εφημερίδα της ΕΕ.

³² (Wahl, AML Package II: Commission Proposes AML Regulation, 2020)

³³ Ευρωπαϊκή Επιτροπή, Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας, COM(2021)<https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52021PC0420>

³⁴ Εξαιτίας του ήδη εκτενούς αντικειμένου που πραγματεύεται η παρούσα διπλωματική εργασία, δεν θα εξεταστεί το πεδίο των κρυπτονομισμάτων, που χρήζει αναλυτικής και εξειδικευμένης παρουσίασης.

³⁵ Συμβούλιο ΕΕ, 2024

Ο Κανονισμός 2024/1624

Ο Κανονισμός 2024/1624³⁶ αντικαθιστά το προηγούμενο σύστημα οδηγιών, το οποίο είχε οδηγήσει σε αποκλίσεις κατά την ενσωμάτωσή του στις εθνικές νομοθεσίες των κρατών μελών, προκαλώντας ασυνέπειες στην εφαρμογή των κανόνων ΚΕΤ/ΧΤ.

Ο νέος Κανονισμός καθορίζει τα μέτρα που πρέπει να εφαρμόζουν οι υπόχρεες οντότητες για την πρόληψη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, τις απαιτήσεις διαφάνειας για τους πραγματικούς δικαιούχους νομικών οντοτήτων, εκπεφρασμένων καταπιστευμάτων και παρόμοιων νομικών ρυθμίσεων.

Μία από τις κύριες καινοτομίες του Κανονισμού, είναι η επέκταση του καταλόγου των υπόχρεων οντοτήτων, που οφείλουν να εφαρμόζουν εσωτερικές πολιτικές, διαδικασίες και ελέγχους για τον μετριασμό και την αποτελεσματική διαχείριση των κινδύνων νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας που έχουν εντοπιστεί. Εκτός από τον τρέχοντα κατάλογο, ο οποίος περιλαμβάνει σχεδόν όλα τα χρηματοπιστωτικά ιδρύματα και διάφορους τύπους μη χρηματοπιστωτικών οντοτήτων και χειριστών (π.χ. δικηγόρους, λογιστές, κτηματομεσίτες, καζίνο και ορισμένους τύπους παρόχων υπηρεσιών κρυπτογράφησης), ο νέος Κανονισμός έχει προσθέσει νέες υπόχρεες οντότητες. Επί παραδείγματι στον κατάλογο των υπόχρεων οντοτήτων έχουν προστεθεί διαμεσολαβητές στεγαστικών πιστώσεων, φορείς εκμετάλλευσης που εργάζονται για λογαριασμό υπηκόων τρίτων χωρών για τη λήψη άδειας διαμονής για να ζήσουν σε χώρα της ΕΕ, εμπόρους αγαθών υψηλής αξίας, όπως οι ιδιοκτήτες κοσμηματοπωλείων, ωρολόγοι και έμποροι πολυτελών αυτοκινήτων, αεροπλάνων

³⁶ Κανονισμός (ΕΕ) 2024/1624 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 31ης Μαΐου 2024, σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

και γιουτ καθως και εργων τεχνης,ε παγγελματικοι ποδοσφαιρικοι συλλογοι και πρακτορες εαν πραγματοποιουν ορισμενες συναλλαγες.³⁷

Επιπλέον, ο Κανονισμός εισάγει ενισχυμένα μέτρα δέουσας επιμέλειας για διασυνοριακές σχέσεις ανταπόκρισης για παρόχους υπηρεσιών κρυπτονομισμάτων. Όσον αφορά τους πραγματικούς δικαιούχους, ο Κανονισμός περιλαμβάνει πιο λεπτομερείς και εναρμονισμένους κανόνες. Διευκρινίζει ότι η πραγματική κυριότητα μπορεί να βασίζεται σε δύο συνιστώσες - το ιδιοκτησιακό συμφέρον και τον έλεγχο - οι οποίες πρέπει να αξιολογούνται ανεξάρτητα και παράλληλα. Η ταυτοποίηση ιδιοκτησιών σε πολυεπίπεδες ή πολύπλοκες δομές καθίσταται ευκολότερη. Νομικές οντότητες που έχουν συσταθεί εκτός της ΕΕ υποχρεούνται να καταχωρούν τους πραγματικούς δικαιούχους τους στα κεντρικά μητρώα όταν έχουν σημαντικές επιχειρηματικές σχέσεις ή αποκτούν ακίνητη περιουσία στην ΕΕ.

Αυτές οι αλλαγές στοχεύουν στην ενίσχυση της συνοχής και της αποτελεσματικότητας του πλαισίου για την αντιμετώπιση του ξεπλύματος χρήματος στην ΕΕ, διασφαλίζοντας ότι οι κανόνες εφαρμόζονται με συνέπεια σε όλα τα κράτη μέλη. Ο Κανονισμός θα ισχύει από τις 10 Ιουλίου 2027, εκτός από τις διατάξεις που περιλαμβάνουν ποδοσφαιρικούς συλλόγους και παράγοντες ως υπόχρεες οντότητες καθώς οι διατάξεις αυτές θα ισχύουν από τις 10 Ιουλίου 2029.³⁸

Η Έκτη Οδηγία

Η Οδηγία 2024/1640³⁹ (στο εξής «Έκτη Οδηγία») εισάγει ένα εκτενές πλαίσιο νέων κανόνων που πρέπει να ενσωματωθούν στο εθνικό δίκαιο των κρατών μελών της Ευρωπαϊκής Ένωσης. Η συγκεκριμένη οδηγία απαιτεί την εφαρμογή αυστηρών μέτρων σε τομείς που είναι ευάλωτοι στη νομιμοποίηση εσόδων από παράνομες

³⁷ [Wahl, 2024, The EU's New AML Single Rulebook Regulation](#)

³⁸ Συμβούλιο ΕΕ, 2024 <https://www.consilium.europa.eu/el/policies/fight-against-terrorist-financing/>

³⁹ Η Έκτη Οδηγία σχετικά με τους μηχανισμούς που πρέπει να συγκροτήσουν τα κράτη μέλη για την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τους σκοπούς της νομιμοποίησης εσόδων από παράνομες δραστηριότητες ή της χρηματοδότησης της τρομοκρατίας, για την τροποποίηση της οδηγίας (ΕΕ) 2019/1937 και για την τροποποίηση και την κατάργηση της οδηγίας (ΕΕ) 2015/849 https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=OJ:L_202401640

δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας. Ειδικότερα, τα κράτη μέλη οφείλουν να ενισχύσουν την εποπτεία των πραγματικών δικαιούχων των υπόχρεων οντοτήτων, διασφαλίζοντας ότι τα στοιχεία τους είναι διαφανή, ακριβή και ενημερωμένα. Οι αρμόδιες εθνικές αρχές καλούνται να επιβλέπουν την ορθή εφαρμογή αυτών των μέτρων για να αποτρέψουν εγκληματικές δραστηριότητες.⁴⁰Επιπλέον, μέσω της Έκτης Οδηγίας, οι ΜΧΠ θα έχουν αυξημένες δυνατότητες πρόσβασης σε ευρύ φάσμα διοικητικών, οικονομικών και νομικών πληροφοριών, συμπεριλαμβανομένων των φορολογικών δεδομένων.

Εκ παραλλήλου, η Οδηγία ενθαρρύνει την αυξημένη συνεργασία μεταξύ των εθνικών εποπτικών αρχών για να διασφαλιστεί η αποτελεσματική εποπτεία των υπόχρεων οντοτήτων που δραστηριοποιούνται σε πολλαπλά κράτη μέλη. Αυτό περιλαμβάνει τη δυνατότητα σύστασης εποπτικών σωμάτων τόσο στον χρηματοπιστωτικό όσο και στον μη χρηματοπιστωτικό τομέα για τη συντονισμένη παρακολούθηση και ρύθμιση των διασυνοριακών δραστηριοτήτων.

Η Έκτη Οδηγία απαιτεί επίσης από τα κράτη μέλη να διενεργούν αξιολογήσεις κινδύνου τόσο σε εθνικό επίπεδο όσο και σε επίπεδο ΕΕ, προκειμένου να εντοπίζουν και να μετριάζουν τους κινδύνους που σχετίζονται με τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας. Σε επίπεδο ΕΕ, η Επιτροπή θα αναλαμβάνει την αξιολόγηση των κινδύνων και θα παρέχει συστάσεις προς τα κράτη μέλη για τα απαραίτητα μέτρα, ενώ σε εθνικό επίπεδο, τα κράτη μέλη θα πρέπει να προσαρμόζουν τις πολιτικές τους βάσει των εντοπισμένων κινδύνων.

Τέλος, οι διατάξεις της Έκτης Οδηγίας πρέπει να μεταφερθούν στο εθνικό δίκαιο των κρατών μελών σε διαφορετικά χρονικά διαστήματα, ανάλογα με το θέμα. Η γενική προθεσμία για την πλήρη ενσωμάτωση των διατάξεων είναι η 10η Ιουλίου 2027, ενώ ορισμένες διατάξεις, όπως η πλήρης πρόσβαση σε πληροφορίες

⁴⁰ Αναλυτικά για το θέμα των Πραγματικών Δικαιούχων στο Κεφάλαιο 6

πραγματικού δικαιούχου πρέπει να εφαρμοστούν νωρίτερα, έως τις 10 Ιουλίου 2025. Άλλες προθεσμίες αφορούν την περαιτέρω ανάπτυξη των μητρώων πραγματικών κυριοτήτων έως τις 10 Ιουλίου 2026 και τη δημιουργία ενός ενιαίου σημείου πρόσβασης σε πληροφορίες ακίνητης περιουσίας έως τις 10 Ιουλίου 2029.⁴¹

Η ίδρυση της AMLA

Ο Mairead McGuinness, Επίτροπος για τις Χρηματοπιστωτικές Υπηρεσίες, τη Χρηματοπιστωτική Σταθερότητα και την Ένωση Κεφαλαιαγορών, δήλωσε ότι: « Η AMLA θα αλλάξει το παιχνίδι στη μάχη κατά του ξεπλύματος χρήματος. Θα είναι το κέντρο του νέου μας εποπτικού συστήματος, ως επόπτης σε ορισμένες περιπτώσεις και ως συντονιστής εποπτικών αρχών σε άλλες, θέτοντας υψηλά πρότυπα σε ολόκληρη την ΕΕ.»

Επιπροσθέτως, ο Κανονισμός (που θεσπίζει την Αρχή για την Καταπολέμηση της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες και της Χρηματοδότησης της Τρομοκρατίας (ΑΚΝΕΠΑΔ), δημοσιεύθηκε τον Ιούνιο του 2024 και η Φρανκφούρτη της Γερμανίας επιλέχθηκε ως έδρα της.⁴² Η ΑΚΝΕΠΑΔ θα έχει άμεση εποπτική εξουσία σε επιλεγμένες οντότητες υψηλού κινδύνου στον χρηματοπιστωτικό τομέα και θα διαδραματίζει συντονιστικό ρόλο.⁴³ διασφαλίζοντας τη συνοχή σε ολόκληρη την ΕΕ. Εκ παραλλήλου, προβλέπεται η συνεργασία της με άλλα όργανα της ΕΕ, όπως η OLAF, η Europol, η Eurojust και η EPPO, ειδικά σε διασυνοριακές υποθέσεις. Η ΑΚΝΕΠΑΔ θα ξεκινήσει τη λειτουργία της στα μέσα του 2025, με πλήρη στελέχωση έως το 2027, και άμεση εποπτεία επιλεγμένων οντοτήτων από το 2028.⁴⁴

⁴¹ (Wahl, *New Anti-Money Laundering Directive (AMLD 6)*, 2024)

⁴² (Συμβούλιο, *Στη Φρανκφούρτη η νέα αρχή της ΕΕ κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες*, 2024)

⁴³ Η AMLA θα απασχολεί πάνω από 430 υπαλλήλους έως το 2027, με περισσότερους από 200 αφιερωμένους στην άμεση εποπτεία

⁴⁴ (Wahl, *Tasks, Powers and Structures of the New EU Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA)*, 2024)

ΚΕΦΑΛΑΙΟ 2

ΕΡΓΑΛΕΙΑ ΣΥΜΜΟΡΦΩΣΗΣ ΓΙΑ ΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΗΣ ΝΟΜΙΜΟΠΟΙΗΣΗΣ ΕΣΟΔΩΝ ΑΠΟ ΠΑΡΑΝΟΜΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Στον σύγχρονο χρηματοπιστωτικό κόσμο, η ΚΕΤ/ΧΤ αποτελεί θεμελιώδη πυλώνα των στρατηγικών συμμόρφωσης. Κάποια συγκεκριμένα νομικά πρόσωπα (π.χ. τράπεζες, χρηματοπιστωτικά ιδρύματα, ασφαλιστικές εταιρείες) αλλά και φυσικά πρόσωπα (π.χ. δικηγόροι, λογιστές), επικαλούμενα στο εξής «υπόχρεες οντότητες» είναι επιφορτισμένα με την νομική υποχρέωση, εφαρμόζουν μέτρα για την πρόληψη και ανίχνευση οικονομικών εγκλημάτων, όπως το ξέπλυμα χρήματος και η χρηματοδότηση της τρομοκρατίας. Η Προσέγγιση Βάσει Κινδύνου (Risk-Based Approach - RBA) διαδραματίζει κρίσιμο ρόλο σε αυτό το πλαίσιο, καλώντας τις υπόχρεες οντότητες να εντοπίσουν και να κατανοήσουν τους κινδύνους που ενδέχεται να αντιμετωπίσουν και να προσαρμόσουν ανάλογα τα μέτρα τους.

Το κεφάλαιο αυτό εξετάζει τη σημασία της RBA για την πρόληψη του οικονομικού εγκλήματος και παρουσιάζει βασικά εργαλεία συμμόρφωσης, όπως η διαδικασία «Γνωρίσε τον πελάτη σου» (KYC) και η δέουσα επιμέλεια (**Due Diligence**). Τα εργαλεία αυτά είναι απαραίτητα για τον εντοπισμό και την αξιολόγηση πελατών και συναλλαγών, διασφαλίζοντας την ασφάλεια και τη νομιμότητα των χρηματοοικονομικών πράξεων. Η συμμόρφωση με τις συγκεκριμένες απαιτήσεις δεν είναι μόνο μια νομική υποχρέωση, αλλά και ένας μηχανισμός προστασίας των οργανισμών από οικονομικούς και νομικούς κινδύνους, διασφαλίζοντας τη διαφάνεια και την εμπιστοσύνη στις συναλλαγές.

2.1. Προσέγγιση Βάσει Κινδύνου- **Risk-Based Approach - RBA**)

Η ως άνω πρακτική, αποτελεί θεμελιώδη πυλώνα σύγχρονης στρατηγικής που διατρανώνεται σε όλο το πλαίσιο. Πιο συγκεκριμένα, σύμφωνα με το Συμβούλιο της Ευρώπης, η RBA σημαίνει ότι οι χώρες, οι κρατικές αρχές, καθώς και ο ιδιωτικός τομέας, πρέπει να έχουν πλήρη κατανόηση των κινδύνων νομιμοποίησης εσόδων από

παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας στους οποίους εκτίθενται.⁴⁵

Η ως άνω διαπίστωση είναι κρίσιμη και καθοριστική για την κατάλληλη και αποτελεσματική εφαρμογή των σωστών μέτρων κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και κατά της χρηματοδότησης της τρομοκρατίας αλλά και για την άμβλυση αυτών των κινδύνων. Η FATF ήδη από τις συστάσεις της το 2003 αλλά και με τις αναθεωρημένες το 2012⁴⁶τόνιζε την σημασία της Προσέγγισης Βάσει Κινδύνου. Ωστόσο, ενώ οι συστάσεις του 2003 ζητούσαν την εφαρμογή της μόνο σε συγκεκριμένες περιπτώσεις, οι αναθεωρημένες συστάσεις της, την επιβάλλουν ως θεμελιώδη απαίτηση, απαραίτητη για την αποτελεσματική εφαρμογή όλων των κατευθυντήριων γραμμών. Ως εκ τούτου, υποστηρίζεται ότι η υιοθέτηση μιας Προσέγγισης Βάσει Κινδύνου δεν είναι απλώς προαιρετική, αλλά απαραίτητη για τη συμμόρφωση με όλες τις άλλες απαιτήσεις της FATF.⁴⁷ Αυτή η Προσέγγιση περιλαμβάνει την ταυτοποίηση, αξιολόγηση και κατανόηση των κινδύνων και στη συνέχεια την εφαρμογή μέτρων που είναι ανάλογα με αυτούς τους κινδύνους, προκειμένου να εξασφαλιστεί η αποτελεσματική άμβλυση τους.⁴⁸

Η ανάγκη της RBA υπήρχε και στην Τέταρτη Οδηγία⁴⁹⁵⁰ αλλά αναλύεται εκτενώς και στον νέο Κανονισμό. Πιο συγκεκριμένα, ο Κανονισμός θέτει

⁴⁵ Council of Europe, "Risk-based approach," MONEYVAL

⁴⁶ Το 2012, η FATF επικαιροποίησε τις Συστάσεις της για την ενίσχυση της παγκόσμιας ασφάλειας και την περαιτέρω προστασία της ακεραιότητας του χρηματοπιστωτικού συστήματος, παρέχοντας στις κυβερνήσεις ισχυρότερα εργαλεία κατά του χρηματοοικονομικού εγκλήματος. Μία από τις σημαντικότερες αλλαγές ήταν η αυξημένη έμφαση στην RBA για τις εξεταζόμενες θεματικές περιοχές, ιδίως σε σχέση με τα προληπτικά μέτρα και την εποπτεία, όσο οι ίδιες Συστάσεις λαμβάνουν πλέον υπόψη, ότι η εν λόγω προσέγγιση αποτελεί ουσιαστικό θεμέλιο του πλαισίου πολιτικής AML/CFT μιας χώρας, όπως κι απαραίτητη προϋπόθεση για την συνεπή υλοποίηση των προτύπων της.

⁴⁷ (FATF, Risk-Based Approach for the Banking Sector)

⁴⁸ Council of Europe, "Risk-based approach," MONEYVAL

⁴⁹ Άρθρο 8, της Οδηγίας ΕΕ 2015/849

⁵⁰ Στις 26 Ιουνίου 2017, η Επιτροπή δημοσίευσε την πρώτη της Υπερεθνική Έκθεση Εκτίμησης Κινδύνου 282 (Supranational Risk Assessment Report - SRNA), κατ' απαίτηση της 4ης Οδηγίας AML. Η ανάλυση αυτή σχεδιάστηκε ως βασικό εργαλείο για τον εντοπισμό και την αντιμετώπιση των κινδύνων στις υπό εξέταση θεματικές περιοχές στην ΕΕ, προκειμένου να παρέχει ολοκληρωμένη χαρτογράφηση των κινδύνων σε όλους τους σχετικούς τομείς, καθώς και συστάσεις προς τα κράτη μέλη, τις Ευρωπαϊκές

συγκεκριμένες απαιτήσεις για την Προσέγγιση Βάσει Κινδύνου από τις υπόχρεες οντότητες με στόχο την αποτροπή νομιμοποίησης εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας. Ειδικότερα, οι υπόχρεες οντότητες πρέπει να θεσπίζουν και να εφαρμόζουν εσωτερικές πολιτικές, διαδικασίες και ελέγχους αναλογικά με τη φύση, τους κινδύνους, την πολυπλοκότητα και το μέγεθος των επιχειρηματικών τους δραστηριοτήτων. Οι πολιτικές αυτές περιλαμβάνουν την εκτίμηση και διαχείριση κινδύνου δέουσα επιμέλεια πελατών, αναφορά ύποπτων συναλλαγών⁵¹, και διατήρηση αρχείων.⁵²

Επιπρόσθετα, οι υπόχρεες οντότητες πρέπει να λαμβάνουν τα κατάλληλα μέτρα για να εντοπίζουν και να εκτιμούν τους κινδύνους νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας στους οποίους εκτίθενται, λαμβάνοντας υπόψη τις μεταβλητές κινδύνου⁵³ και τα πορίσματα των εθνικών και ενωσιακών εκτιμήσεων κινδύνου. Ενώ, πριν την εισαγωγή νέων προϊόντων ή υπηρεσιών, πρέπει να εντοπίζουν και να εκτιμούν τους σχετικούς κινδύνους και να λαμβάνουν τα κατάλληλα μέτρα για τη διαχείρισή τους.⁵⁴ Τονίζεται

Εποπτικές Αρχές και τις υπόχρεες οντότητες, για τον μετριασμό τους. Επισημαίνεται ότι, στις 24 Ιουλίου 2019, η Επιτροπή δημοσίευσε τη δεύτερη υπερεθνική έκθεση εκτίμησης κινδύνου(SRNA Report 2019).

⁵¹ Άρθρο 9 του Κανονισμού

⁵² Επίσης, απαιτούνται διαδικασίες παρακολούθησης της συμμόρφωσης, έλεγχος του προσωπικού, και κατάρτιση εργαζομένων.

⁵³ Πιο συγκεκριμένα, σύμφωνα με το Παράρτημα 1 του Κανονισμού προβλέπονται μεταβλητές κινδύνου οι οποίες μπορούν να διακριθούν σε τέσσερις βασικές κατηγορίες. Πρώτον, μεταξύ άλλων, ως προς τον πελάτη, λαμβάνεται υπόψη η επιχειρηματική ή επαγγελματική δραστηριότητα του πελάτη και του πραγματικού δικαιούχου του καθώς και η φήμη του αλλά και το είδος και η συμπεριφορά τους, οι περιοχές δικαιοδοσίας στις οποίες εδρεύουν, οι κύριοι τόποι επιχειρηματικής τους δραστηριότητας, καθώς και οι περιοχές δικαιοδοσίας όπου διατηρούν σημαντικούς προσωπικούς δεσμούς. Δεύτερον, ως προς τα προϊόντα, τις υπηρεσίες ή τις συναλλαγές, αξιολογούνται ο σκοπός ενός λογαριασμού ή μιας σχέσης, η κανονικότητα ή η διάρκεια της επιχειρηματικής σχέσης, το επίπεδο των περιουσιακών στοιχείων που θα κατατεθούν ή το μέγεθος των πραγματοποιούμενων συναλλαγών, το επίπεδο διαφάνειας ή αδιαφάνειας που παρέχει το προϊόν ή η υπηρεσία, η πολυπλοκότητα του προϊόντος ή της συναλλαγής, και η αξία ή το μέγεθος του προϊόντος ή της υπηρεσίας. Τρίτον, ως προς τους διαύλους παράδοσης, εξετάζεται ο βαθμός στον οποίο η επιχειρηματική σχέση αναπτύσσεται χωρίς φυσική παρουσία των μερών και η παρουσία εισηγητών ή διαμεσολαβητών που ενδέχεται να χρησιμοποιεί ο πελάτης, καθώς και η φύση της σχέσης τους με τον πελάτη.

⁵⁴ Έως τις 10 Ιουλίου 2026, η ΑΚΝΕΠΑΔ εκδίδει κατευθυντήριες γραμμές σχετικά με τις ελάχιστες απαιτήσεις για το περιεχόμενο της εκτίμησης κινδύνου σε επίπεδο επιχείρησης την οποία διενεργεί

πως η εκτίμηση κινδύνου πρέπει να τεκμηριώνεται, να επικαιροποιείται τακτικά, και να τίθεται στη διάθεση των εποπτικών φορέων κατόπιν αιτήματος.⁵⁵

Υπό αυτό το πρίσμα, προβλέπεται ότι οι υπόχρεες οντότητες πρέπει να διορίζουν υπεύθυνο συμμόρφωσης, ο οποίος θα φέρει την ευθύνη για την εφαρμογή των πολιτικών, των διαδικασιών και των ελέγχων της εταιρείας⁵⁶ και να διασφαλίζεται ότι το εκάστοτε προσωπικό είναι ενήμερο για τις απαιτήσεις του Κανονισμού και εκπαιδεύεται κατάλληλα για να εντοπίζει και να διαχειρίζεται τους σχετικούς κινδύνους.⁵⁷

Εκ παραλλήλου, τονίζεται η ανάγκη ώστε η μητρική επιχείρηση κάθε ομίλου, να φροντίζει ότι οι ως άνω απαιτήσεις για τις εσωτερικές διαδικασίες, την εκτίμηση κινδύνου και το προσωπικό, εφαρμόζονται σε όλα τα υποκαταστήματα και τις θυγατρικές του ομίλου, τόσο εντός της Ένωσης όσο και σε τρίτες χώρες.⁵⁸ Ενώ, προβλέπεται ότι σε περιπτώσεις που οι απαιτήσεις συμμόρφωσης σε τρίτες χώρες είναι λιγότερο αυστηρές από τον Κανονισμό, η μητρική επιχείρηση πρέπει να διασφαλίζει τη συμμόρφωση με τον Κανονισμό. Εάν η νομοθεσία τρίτης χώρας δεν επιτρέπει τη συμμόρφωση, πρέπει να λαμβάνονται επιπρόσθετα μέτρα για την αντιμετώπιση των σχετικών κινδύνων και να ενημερώνονται οι εποπτικές αρχές της χώρας καταγωγής.

Επομένως, η αξιολόγηση κινδύνου είναι το πρώτο και πιο σημαντικό βήμα για τη διαμόρφωση ενός αποτελεσματικού μηχανισμού για την αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Απαραίτητα εργαλεία για την επιβοήθησή του παραπάνω σκοπού, αποτελούν η διαδικασία Γνώρισε τον Πελάτη σου και η Δέουσα Επιμέλεια.

η υπόχρεη οντότητα σύμφωνα με την παράγραφο 1, καθώς και με τις πρόσθετες πηγές πληροφοριών που πρέπει να λαμβάνονται υπόψη κατά την εκπόνηση της εκτίμησης κινδύνου σε επίπεδο επιχείρησης.

⁵⁵ Άρθρο 10 Κανονισμού

⁵⁶ Άρθρο 11 Κανονισμού

⁵⁷ Άρθρο 12 Κανονισμού

⁵⁸ Άρθρο 16 Κανονισμού

2.2 Η διαδικασία Γνώρισε Τον Πελάτη Σου (KYC)

Η πρόληψη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας είναι υψίστης σημασίας στο σύγχρονο χρηματοοικονομικό τοπίο, όπως έχει ήδη πολλάκις αναφερθεί. Ως εκ τούτου, τα χρηματοπιστωτικά ιδρύματα υποχρεούνται να εφαρμόζουν διαδικασίες, επονομαζόμενες Know Your Customer (KYC) ήτοι Γνώρισε τον Πελάτη Σου, οι οποίες έχουν σχεδιαστεί για να επιτρέπουν την ταυτοποίηση και επαλήθευση της ταυτότητας των πελατών τους, καθώς και να αξιολογούν τους κινδύνους που συνδέονται με τις συναλλαγές με αυτούς και να διασφαλίζουν ότι η εξεταζόμενη επιχείρηση δεν εμπλέκεται με άτομα που σχετίζονται με παράνομες δραστηριότητες, όπως η τρομοκρατία, η διαφθορά ή η νομιμοποίηση εσόδων από παράνομες δραστηριότητες.⁵⁹

Αξίζει να σημειωθεί ότι οι υποχρεώσεις KYC των χρηματοπιστωτικών ιδρυμάτων δεν είναι στατικές, αλλά υπόκεινται σε συνεχή εξέλιξη ως απάντηση στις αλλαγές στο χρηματοοικονομικό τοπίο και στη συνεχώς αυξανόμενη εξειδίκευση των νομιμοποιητών εσόδων από παράνομες δραστηριότητες και άλλων οικονομικών εγκληματιών.

Μάλιστα έχει δημιουργηθεί στην Ελλάδα, η ηλεκτρονική εφαρμογή «Συστηθείτε» (Know Your Customer, εφεξής eGov - KYC) η οποία στοχεύει στην ψηφιοποίηση των διαδικασιών και των μέσων επαλήθευσης στοιχείων που εφαρμόζονται ως προς τον πελάτη από τα υπόχρεα πιστωτικά ιδρύματα για ΚΧΤ/ΕΤ

Για τον ως άνω σκοπό, οι κατηγορίες των δεδομένων του φυσικού προσώπου που δύνανται να αντλούνται από τα εκάστοτε Μητρώα⁶⁰ και να διαβιβάζονται είναι α) στοιχεία ταυτότητας β) στοιχεία επικοινωνίας γ) στοιχεία εισοδήματος δ) στοιχεία επαγγελματικής δραστηριότητας απασχολούμενου στο Δημόσιο ε) στοιχεία

⁵⁹ (Leventopoulou, 2023)

⁶⁰ π.χ. το Μητρώο Ταυτοτήτων της Ελληνικής Αστυνομίας, από το Μητρώο Ανθρώπινου Δυναμικού Δημοσίου Τομέα, από το ΠΣ ΕΡΓΑΝΗ, από το Μητρώο φορολογουμένων της Α.Α.Δ.Ε

επαγγελματικής δραστηριότητας απασχολούμενου με εξαρτημένη σχέση εργασίας ιδιωτικού δικαίου στ) στοιχεία επαγγελματικής δραστηριότητας επιτηδευματία.⁶¹

Σύμφωνα με την διάθεση των στοιχείων γίνεται αποκλειστικά κατόπιν της ρητής συγκατάθεσης του πολίτη, κάθε φορά που ζητείται πρόσβαση, με γνώμονα την προστασία των προσωπικών δεδομένων παράλληλα με την σύγχρονη και έγκυρη διάθεση στοιχείων που συλλέγονται από αξιόπιστες πηγές.

2.3. Δέουσα Επιμέλεια (Due Diligence)

Οι απαιτήσεις Δέουσας Επιμέλειας⁶² ως προς τον πελάτη αποτελούν κρίσιμο στοιχείο για την εξασφάλιση της ικανότητας των υπόχρεων οντοτήτων να προσδιορίζουν, να ελέγχουν και να παρακολουθούν τις επιχειρηματικές σχέσεις με τους πελάτες τους, αναφορικά με τους κινδύνους νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας⁶³. Μαζί με την ΚΥC, αποτελεί εξαιρετικά κοινή και επιβεβλημένη πρακτική, για την έναρξη οποιαδήποτε συνεργασίας, μεταξύ επιχειρήσεων, ειδικά χρηματοπιστωτικών οργανισμών

Πιο συγκεκριμένα, κατά την έναρξη δέουσας επιμέλειας, πραγματώνονται τα κάτωθι στάδια:⁶⁴ α) Ταυτοποίηση του πελάτη, και αν πρόκειται για νομικό πρόσωπο, του Πραγματικού Δικαιούχου της εταιρίας,⁶⁵ β) Επαλήθευση της ταυτότητας του

⁶¹ Άρθρο 2 της ΥΑ 9747/2-4-2021 με θέμα «Ηλεκτρονική διεκπεραίωση μέτρων δέουσας επιμέλειας μέσω της εφαρμογής eGov-ΚΥC».

⁶² Δεν θα πρέπει να ζητείται από τις υπόχρεες οντότητες να εφαρμόζουν μέτρα δέουσας επιμέλειας σε πελάτες που διενεργούν περιστασιακές συναλλαγές ή συνδεδεμένες συναλλαγές οι οποίες δεν υπερβαίνουν μια συγκεκριμένη αξία, εκτός αν υπάρχει υπόνοια νομιμοποίησης εσόδων από παράνομες δραστηριότητες ή χρηματοδότησης της τρομοκρατίας. Παρότι για τις περισσότερες περιστασιακές συναλλαγές ισχύει ανώτατο όριο 10 000 EUR, ή το ισόποσο σε εθνικό νόμισμα, οι υπόχρεες οντότητες οι οποίες δραστηριοποιούνται σε τομείς ή διενεργούν συναλλαγές που παρουσιάζουν υψηλότερο κίνδυνο νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας θα πρέπει να υποχρεούνται να εφαρμόζουν μέτρα δέουσας επιμέλειας ως προς τον πελάτη για συναλλαγές με χαμηλότερο όριο. Για τον προσδιορισμό των τομέων ή των συναλλαγών, καθώς και των ενδεδειγμένων ορίων για τους εν λόγω τομείς και συναλλαγές, η ΑΚΝΕΠΑΔ θα πρέπει να καταρτίσει ειδικά σχέδια ρυθμιστικών τεχνικών προτύπων.

⁶³ Άρθρο 20 Κανονισμού

⁶⁴ Guidance for a risk-based approach, FATF (2014): σελ. 19

⁶⁵ Αναλύεται διεξοδικά στο κεφάλαιο 6 της παρούσας εργασίας

προσώπου βάσει αξιόπιστων και ανεξάρτητων πληροφοριών, δεδομένων ή τεκμηρίωσης, καθώς και γ) του σκοπού και της φύσης της επιθυμητής επιχειρηματικής σχέσης, και σε περιπτώσεις υψηλότερου κινδύνου, την συλλογή περαιτέρω πληροφοριών.⁶⁶

Εντούτοις, παρά την ευρεία και διαδεδομένη χρήση των ως άνω διαδικασιών, έχει υποστηριχθεί ότι αν και η Τέταρτη Οδηγία, δεν καθόρισε λεπτομερείς κανόνες όσον αφορά τις διαδικασίες που πρέπει να ακολουθούν οι υπόχρεες οντότητες. Εξαιτίας της σημασίας που διαδραματίζει στην πρόληψη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, είναι απαραίτητο να οριστούν πιο εξειδικευμένες προϋποθέσεις αναφορικά με την ταυτοποίηση του πελάτη.^{67 68} Αυτό θα έχει ως αποτέλεσμα να περιοριστούν οι εθνικές αποκλίσεις και να εξασφαλιστούν ίσοι όροι ανταγωνισμού στην αγορά, ενώ προωθεί τη συνεπή εφαρμογή των διατάξεων σε ολόκληρη την Ένωση.⁶⁹ Ταυτόχρονα, οι υπόχρεες οντότητες πρέπει να εφαρμόζουν τα μέτρα δέουσας επιμέλειας βάσει του εκτιμώμενου κινδύνου, διασφαλίζοντας ότι οι αποφάσεις τους είναι τεκμηριωμένες και αποτελεσματικές στην αντιμετώπιση των σχετικών κινδύνων νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας.⁷⁰⁷¹

Ωστόσο, σε περιπτώσεις που δεν είναι δυνατή η συμμόρφωση με τα μέτρα Δέουσας Επιμέλειας, η διακοπή της επιχειρηματικής σχέσης αποτελεί ένα μέτρο για τη μείωση της έκθεσης της υπόχρεης οντότητας σε πιθανούς κινδύνους που μπορεί

⁶⁶ (Κασιμάτη, 2021)

⁶⁷ Αιτ. Σκέψη 65 Κανονισμού

⁶⁸ Αιτ. Σκέψη 37 Κανονισμού

⁶⁹ Αιτιολογική Σκέψη 37 Κανονισμού

⁷⁰ Αιτιολογική Σκέψη 38 και άρθρο 20 Κανονισμού

⁷¹ Στο γράμμα του νέο Κανονισμού προβλέπεται για τους τακτικούς πελάτες, η δυνατότητα επαλήθευσης της ακρίβειας των πληροφοριών μέσω της επιβεβαίωσης από τον πελάτη ότι τα στοιχεία που διατηρούνται στα αρχεία παραμένουν αμετάβλητα. ⁷¹ Αυτή η πρακτική διευκολύνει τη συμμόρφωση με τις υποχρεώσεις που απορρέουν από την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, υπό την προϋπόθεση ότι η υπόχρεη οντότητα είναι πεπεισμένη πως οι πληροφορίες του πελάτη δεν έχουν μεταβληθεί. Σε κάθε περίπτωση, η επιβεβαίωση από τον πελάτη καθώς και οποιεσδήποτε τυχόν αλλαγές στις πληροφορίες του πελάτη πρέπει να καταγράφονται λεπτομερώς.

να προκύψουν από αλλαγές στο προφίλ του πελάτη. Παρόλα αυτά, υπάρχουν εξαιρέσεις όπου η διακοπή της σχέσης δεν είναι σκόπιμη, κυρίως για λόγους δημοσίου συμφέροντος. Για παράδειγμα, σε συμβάσεις ασφάλειας ζωής, οι υπόχρεες οντότητες θα πρέπει, αντί της διακοπής της σχέσης, να εξετάζουν εναλλακτικά μέτρα, όπως το πάγωμα της επιχειρηματικής σχέσης, την απαγόρευση παροχής περαιτέρω υπηρεσιών, και την παρακράτηση πληρωμών προς τους δικαιούχους, μέχρις ότου καταστεί δυνατή η συμμόρφωση με τις απαιτήσεις δέουσας επιμέλειας ως προς τον πελάτη.⁷²

2.3.2 Οι Κατηγορίες Δέουσας Επιμέλειας

Όπως είδαμε και στην εισαγωγή, η κατηγοριοποίηση της δέουσας επιμέλειας, είχε επικρατήσει στον μηχανισμό για την αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και αποτελεί συνήθη διαδικασία για τις υπόχρεες οντότητες. Στο ίδιο πνεύμα, ο Κανονισμός για την Καταπολέμηση της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες και της Χρηματοδότησης της Τρομοκρατίας, θέτει ένα ολοκληρωμένο πλαίσιο για την εφαρμογή μέτρων δέουσας επιμέλειας από τις υπόχρεες οντότητες, με σκοπό την πρόληψη και τον εντοπισμό τέτοιων παράνομων δραστηριοτήτων διακρίνοντας τα σε τρεις κύριες κατηγορίες:

- Η βασική δέουσα επιμέλεια (Customer Due Diligence – CDD),⁷³ περιλαμβάνει τις διαδικασίες που πρέπει να ακολουθούν οι υπόχρεες οντότητες όταν πρόκειται να συνάψουν επιχειρηματικές σχέσεις ή διενεργούν συναλλαγές. Η βασική δέουσα επιμέλεια, αποτελείται από την ταυτοποίηση και επαλήθευση της ταυτότητας του πελάτη. Αυτό γίνεται μέσω εγγράφων, δεδομένων ή πληροφοριών, καθώς και τον προσδιορισμό και την επαλήθευση των πραγματικών δικαιούχων του πελάτη, ώστε να γίνει αντιληπτή το ιδιοκτησιακό καθεστώς της νομικής οντότητας.. Η συνεχής παρακολούθηση της επιχειρηματικής σχέσης είναι επίσης απαραίτητη, με την εξέταση των

⁷² Άρθρο 21(1) του Κανονισμού

⁷³ Άρθρο 20 του Κανονισμού

συναλλαγών για να διασφαλιστεί ότι συνάδουν με το προφίλ του πελάτη. Τέλος, πρέπει να ελέγχεται αν ο πελάτης ή οι πραγματικοί δικαιούχοι υπόκεινται σε στοχευμένες οικονομικές κυρώσεις.

- Η απλουστευμένη δέουσα επιμέλεια⁷⁴ (Simplified Due Diligence – SDD), όταν μια επιχειρηματική δραστηριότητα εμφανίζει χαμηλό βαθμό κινδύνου, οι υπόχρεες οντότητες μπορούν να εφαρμόσουν λιγότερο αυστηρή διαδικασία ελέγχου, όπως η επαλήθευση της ταυτότητας του πελάτη μετά τη σύναψη της επιχειρηματικής σχέσης, η μείωση της συχνότητας επικαιροποίησης των στοιχείων του πελάτη, η μείωση του όγκου των πληροφοριών που συλλέγονται για την κατανόηση του σκοπού της επιχειρηματικής σχέσης, και η μείωση του βαθμού ενδελεχούς εξέτασης των συναλλαγών. Η απλουστευμένη δέουσα επιμέλεια εφαρμόζεται πάντα με την προϋπόθεση ότι η οντότητα συνεχίζει να παρακολουθεί επαρκώς τις συναλλαγές, ώστε να εντοπίζει τυχόν ασυνήθιστες ή ύποπτες δραστηριότητες.
- Η αυξημένη δέουσα επιμέλεια, (Enhanced Due Diligence – EDD) στις περιπτώσεις που η επιχειρηματική σχέση ή η συναλλαγή παρουσιάζει υψηλότερο κίνδυνο προβλέπεται η εφαρμογή αυξημένων μέτρων δέουσας επιμέλειας. Τα μέτρα αυτά περιλαμβάνουν τη συλλογή πρόσθετων πληροφοριών για τον πελάτη, τους πραγματικούς δικαιούχους και τον σκοπό της επιχειρηματικής σχέσης, καθώς και την ενδελεχή παρακολούθηση των συναλλαγών και λεπτομέρεια στους ελέγχους για τον εντοπισμό ασυνήθιστων μοτίβων. Επιπλέον, απαιτείται η λήψη έγκρισης από ανώτερα διοικητικά στελέχη πριν από την έναρξη ή τη συνέχιση της επιχειρηματικής σχέσης, και η εξέταση της προέλευσης των χρηματικών ποσών που διακινούνται και του σκοπού της συναλλαγής.⁷⁵

⁷⁴ Άρθρο 33 Κανονισμού

⁷⁵ Άρθρο 34 Κανονισμού

Εκ παραλλήλου, ιδιαίτερη πρόβλεψη γίνεται για τις διασυννοριακές σχέσεις ανταπόκρισης ⁷⁶ καθώς σε αυτές τις περιπτώσεις, οι οντότητες υποχρεούνται να συλλέγουν εκτενείς πληροφορίες για το ίδρυμα-πελάτη και να αξιολογούν τους ελέγχους που διενεργεί, εξασφαλίζοντας την ποιότητα της εποπτείας και της συμμόρφωσης στις χώρες όπου δραστηριοποιείται το ίδρυμα.

Σημαντική πρόβλεψη αποτελεί το Τμήμα VI του Κανονισμού, το οποίο επικεντρώνεται στη στήριξη που μπορούν να παρέχουν οι υπόχρεες οντότητες μεταξύ τους κατά τη διαδικασία δέουσας επιμέλειας ως προς τον πελάτη.⁷⁷ Επιπλέον, καθορίζεται η διαδικασία μέσω της οποίας οι υπόχρεες οντότητες μπορούν να βασίζονται σε άλλες για τη λήψη των απαραίτητων πληροφοριών. Οι οντότητες που στηρίζονται σε άλλες, πρέπει να διασφαλίζουν ότι τα έγγραφα και τα δεδομένα που χρησιμοποιούνται για την ταυτοποίηση και την επαλήθευση των πελατών είναι διαθέσιμα σε περίπτωση ανάγκης..^{78 79}

Ο ΕΕΠΔ υπογραμμίζει τη σημασία της προσαρμογής της διαδικασίας δέουσας επιμέλειας βάσει της προσέγγισης κινδύνου. Συγκεκριμένα, η ποσότητα και οι κατηγορίες δεδομένων που συλλέγονται καθώς και οι τύποι πηγών δεδομένων που χρησιμοποιούνται, θα πρέπει να διαφέρουν ανάλογα με τον τύπο του πελάτη. Επί παραδείγματι, η δέουσα επιμέλεια που εφαρμόζεται στους συνήθεις πελάτες θα πρέπει να είναι πιο περιορισμένη σε σχέση με εκείνη που εφαρμόζεται σε πολιτικώς εκτεθειμένα πρόσωπα, τα οποία θεωρούνται υψηλότερου κινδύνου.

⁷⁶ Άρθρα 36, 37 Κανονισμού

⁷⁷ Αυτή η στήριξη προϋποθέτει ότι οι άλλες οντότητες τηρούν τις ίδιες ή ισοδύναμες απαιτήσεις και ότι η συμμόρφωσή τους εποπτεύεται επαρκώς, όπως ορίζει το κεφάλαιο IV της οδηγίας (ΕΕ) 2024/1640.

⁷⁸ Αυτές οι πληροφορίες πρέπει να διαβιβάζονται άμεσα, και η διαβίβαση πρέπει να διέπεται από γραπτή συμφωνία μεταξύ των εμπλεκόμενων οντοτήτων, εκτός αν πρόκειται για οντότητες εντός του ίδιου ομίλου, όπου μπορεί να εφαρμόζεται εσωτερική διαδικασία.

⁷⁹ Το Άρθρο 50 προβλέπει την έκδοση κατευθυντήριων γραμμών από την ΑΚΝΕΠΑΔ έως το 2027, οι οποίες θα διευκρινίζουν τις αποδεκτές συνθήκες υπό τις οποίες οι υπόχρεες οντότητες μπορούν να στηρίζονται σε άλλες για τη δέουσα επιμέλεια, τον ρόλο και τις ευθύνες των εμπλεκόμενων οντοτήτων, καθώς και τις εποπτικές προσεγγίσεις που πρέπει να υιοθετηθούν.

Τέλος, το ΕΣΠΑ τονίζει την ανάγκη για σαφή διάκριση μεταξύ της διαδικασίας δέουσας επιμέλειας και της KYC. Η ως άνω διαδικασία, επικεντρώνεται στην προσφορά χρηματοπιστωτικών προϊόντων και υπηρεσιών με βάση το προφίλ των πελατών, και ως εκ τούτου, απαιτεί τη συλλογή διαφορετικών πληροφοριών και την πρόσβαση σε διαφορετικές πηγές από αυτές που χρησιμοποιούνται για σκοπούς ΚΕΤ/ΧΤ.⁸⁰

Όπως είναι έκδηλο, η RBA είναι ζωτικής σημασίας για την ΚΕΤ/ΧΤ επιτρέποντας στα χρηματοπιστωτικά ιδρύματα και άλλες υπόχρεες οντότητες να προσαρμόζουν τα μέτρα τους σύμφωνα με το προφίλ κινδύνου κάθε πελάτη. Μέσω εργαλείων όπως το KYC και το Due Diligence, εντοπίζονται και αξιολογούνται οι κίνδυνοι, ενισχύοντας τη διαφάνεια και την ασφάλεια στις συναλλαγές.

Ταυτόχρονα, η συμμόρφωση με τις απαιτήσεις προστασίας προσωπικών δεδομένων, φέρνει στο προσκήνιο την ανάγκη εξισορρόπησης της πρόληψης του οικονομικού εγκλήματος με τον σεβασμό της ιδιωτικής ζωής. Αυτή η ισορροπία αποτελεί σημαντική πρόκληση για τις υπόχρεες οντότητες, οι οποίες πρέπει να επιτύχουν αμοιβαία συμμόρφωση και με τα δύο νομοθετήματα, συλλέγοντας τα απαραίτητα δεδομένα που απαιτούνται για την δέσμια υποχρέωσή τους στο πλαίσιο της αντιμετώπισης του ξεπλύματος χρήματος, διασφαλίζοντας όμως παράλληλα την προστασία των προσωπικών πληροφοριών των πελατών.

Η επιτυχής διαχείριση αυτών των υποχρεώσεων, αποτελεί ένα μεγάλο στοίχημα, που συμβάλλει στη διατήρηση ενός αξιόπιστου και ασφαλούς χρηματοοικονομικού συστήματος, ενισχύοντας την εμπιστοσύνη των πελατών και την αξιοπιστία των οργανισμών σε ένα συνεχώς εξελισσόμενο ρυθμιστικό περιβάλλον.

⁸⁰ Ο.π. ΕΣΠΑ, 2021

ΚΕΦΑΛΑΙΟ 3

Η ΣΥΣΧΕΤΙΣΗ ΜΕΤΑΞΥ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΜΕΤΡΩΝ ΓΙΑ ΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΗΣ ΝΟΜΙΜΟΠΟΙΗΣΗΣ ΕΣΟΔΩΝ ΑΠΟ ΠΑΡΑΝΟΜΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

3.1. Εισαγωγή

Είναι πασίδηλο ότι οι πολιτικές και τα μέτρα ΚΕΤ/ΧΤ είναι απαραίτητα για την αντιμετώπιση των οικονομικών εγκλημάτων. Ωστόσο, παρατηρείται ότι πολύ συχνά τα μέτρα για την αντιμετώπιση των παράνομων ενεργειών, διασταυρώνονται με την προστασία δεδομένων και τα δικαιώματα ιδιωτικότητας. Η αλληλεπίδραση μεταξύ των νομοθετημάτων κατά του ξεπλύματος χρήματος και εκείνων για τα προσωπικά δικαιώματα, δημιουργεί ένα περίπλοκο νομικό τοπίο, στο οποίο πρέπει να περιηγηθούν και αφενός να πλεύσουν οι υπόχρεες οντότητες, όπως τα χρηματοπιστωτικά ιδρύματα αλλά και οι αρμόδιοι φορείς. Σε αυτό το κεφάλαιο, αποπειράται να διερευνηθεί ο αντίκτυπος των μέτρων κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, στα προσωπικά δικαιώματα, επιχειρώντας μια σύγκριση του ήδη ισχύοντος ευρωπαϊκού νομοθετικού πλαισίου με το πρόσφατα ψηφισθέν AML PACKAGE, επιχειρώντας να δοθεί ένα πρώτο φως στην μεταξύ τους συσχέτιση.

3.2. Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ)

Ακρογωνιαίος λίθος του νομοθετικού πλαισίου για την προστασία των προσωπικών δεδομένων στον ευρωπαϊκό χώρο, αποτελεί ο ΓΚΠΔ⁸¹, ο οποίος τέθηκε σε ισχύ από τον Μάιο του 2018⁸² και αντικατέστησε την Οδηγία για την Προστασία Δεδομένων 95/46/ΕΚ.⁸³ Στόχος του ήταν η εναρμόνιση της νομοθεσίας για την προστασία δεδομένων σε ολόκληρη την ΕΕ, διασφαλίζοντας την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής των πολιτών της ΕΕ. Ο ΓΚΠΔ βασίζεται εν πολλοίς στο άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης,⁸⁴ και στο άρθρο 16 παρ. 1 της Συνθήκης για την Λειτουργία της Ευρωπαϊκής Ένωσης, αποτελώντας τις νομικές βάσεις για την προστασία των προσωπικών δεδομένων.⁸⁵ Όπως χαρακτηριστικά αναφέρεται στο κείμενο του Κανονισμού, “στοχεύει στη διεύρυνση της προστασίας δεδομένων στην εποχή των μεγάλων δεδομένων και της μεταφοράς των πληροφοριών, διασφαλίζοντας ότι η προστασία των δεδομένων αποτελεί θεμελιώδες δικαίωμα που θα ρυθμίζεται με συνέπεια σε όλη την Ευρώπη” ενώ δίνεται ιδιαίτερη έμφαση στην ανάγκη «κάθε

⁸¹ 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

⁸² Ο ΓΚΠΔ τέθηκε σε εφαρμογή από τις 25-5-2018, σύμφωνα με το άρθρο 99 παρ. 2 αυτού. Σύμφωνα με το άρθρο 288 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), ο ΓΚΠΔ έχει άμεση εφαρμογή σε όλα τα κράτη μέλη, τα οποία υποχρεούνται να λάβουν τα αναγκαία μέτρα για την προσαρμογή της εθνικής νομοθεσίας τους: Αρχή Προστασίας Δεδομένων https://www.dpa.gr/el/enimerwtiko/nomothesia/proswpikon_dedomenon

⁸³ Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:31995L0046>

⁸⁴ Άρθρο 8 ΧΘΔΑ - Προστασία των δεδομένων προσωπικού χαρακτήρα

«1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγμένα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους.

3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής.» διαθέσιμο στο https://www.europarl.europa.eu/charter/pdf/text_el.pdf

⁸⁵ Βλ. σκέψη 1 του ΓΚΠΔ

εταιρεία που εξυπηρετεί ευρωπαίους πελάτες και συλλέγει τα δεδομένα τους θα πρέπει να συμμορφώνεται με αυτήν την οδηγία, ακόμη και αν εδρεύει σε τρίτη χώρα”.

3.3. Οι αρχές του ΓΚΠΔ

Ο ΓΚΠΔ, στο άρθρο 5, βασίζεται σε επτά θεμελιώδεις αρχές, οι οποίες καθορίζουν το πλαίσιο για τη νόμιμη και υπεύθυνη επεξεργασία των προσωπικών δεδομένων. Αυτές οι αρχές δεν αποτελούν απλώς κατευθυντήριες γραμμές αλλά νομικές απαιτήσεις, τις οποίες οι υπόχρεες οντότητες και οι αρμόδιες αρχές οφείλουν να τηρούν προκειμένου να εξασφαλίζουν την απαιτούμενη συμμόρφωση με τις επιταγές του ΓΚΠΔ.

Εν συνεχεία θα αναλυθούν κάποιες από τις βασικές αρχές του ΓΚΠΔ ο τρόπος που αλληλοεπιδρούν με τις πολιτικές και τις διατάξεις που προβλέπονται για την αντιμετώπιση του ξεπλύματος χρήματος.

3.3.1 Επί της αρχής του περιορισμού του σκοπού

Η αρχή του περιορισμού σκοπού της επεξεργασίας προβλέπεται ρητώς στο άρθρο 5 παρ. 1 περ. β' του ΓΚΠΔ, σύμφωνα με την οποία τα δεδομένα προσωπικού χαρακτήρα πρέπει να «συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς »υτούς” («περιορισμός του σκοπού»)). Η ως άνω θεμελιώδης αρχή, που πηγάζει από τις διατάξεις του πρωτογενούς ενωσιακού δικαίου του άρθρου 8 παρ. 2 ΧΘΔΕΕ, στοχεύει στην προστασία των υποκειμένων των δεδομένων, θέτοντας τα όρια αναφορικά με τον τρόπο, με τον οποίο οι υπεύθυνοι επεξεργασίας μπορούν να χρησιμοποιούν τα δεδομένα.⁸⁶ Ο σκοπός επεξεργασίας πρέπει να είναι σαφής κατά τη συλλογή των δεδομένων και η τυχόν περαιτέρω επεξεργασία δεν πρέπει να παρεκκλίνει από τον αρχικό σκοπό.⁸⁷

⁸⁶ (Βενέρη, 2020)

⁸⁷ Brewczykńska, M., & Kosta, E. (2023)

Η διάταξη του άρθρου 5 παρ. 1 στοιχ. β' ΓΚΠΔ, αποτελείται από δύο καίριες συνιστώσες :

- i) τα δεδομένα προσωπικού χαρακτήρα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς (προσδιορισμός του σκοπού) ενώ πριν ή το αργότερο κατά την στιγμή της συλλογής των δεδομένων, ο σκοπός πρέπει να περιγράφεται επακριβώς, προκειμένου να μπορεί να προσδιοριστεί τι εμπίπτει και τι όχι στο πεδίο της σκοπούμενης επεξεργασίας
- ii) και επιπλέον να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους αρχικούς σκοπούς (ασύμβατη περαιτέρω χρήση). Ειδικότερα, ο σκοπός της επεξεργασίας πρέπει να είναι σαφής και ρητός διασφαλίζοντας και τις απαιτήσεις νομιμότητας.⁸⁸

Σύμφωνα με τον Κανονισμό, η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να επιτρέπεται μόνο για σκοπούς που προβλέπει ο ίδιος, όπως η δέουσα επιμέλεια πελάτη, η συνεχής εποπτεία, η αναφορά ύποπτων συναλλαγών και η αναγνώριση πολιτικώς εκτεθειμένων προσώπων. Η συλλογή και επεξεργασία πρέπει να περιορίζονται στα αναγκαία για τους σκοπούς συμμόρφωσης και απαγορεύεται αυστηρά η χρήση δεδομένων για εμπορικούς σκοπούς.⁸⁹

Ωστόσο, ο ΕΕΠΔ έχει εντοπίσει πιθανότητα κινδύνου που μπορεί να προκύψει σε σχέση με τις Συμπράξεις Δημοσίου και Ιδιωτικού δικαίου (εφεξής «ΣΔΙΤ») στο πλαίσιο της νομιμοποίησης εσόδων από παράνομες δραστηριότητες καθώς «*οι υπόχρεες οντότητες που συμμετέχουν σε ΣΔΙΤ μπορεί να μπουν στον πειρασμό να ενσωματώσουν τις πληροφορίες που μοιράζονται οι αρχές επιβολής του νόμου ώστε να την επαναχρησιμοποιήσουν αργότερα, ως μέρος του προφίλ πελατών τους*». Ως εκ τούτου «*αυτό θα μπορούσε να οδηγήσει σε διακρίσεις εις βάρος ορισμένων πελατών, για παράδειγμα, εκείνων που προσφέρουν χαμηλή κερδοφορία για την τράπεζα και παρουσιάζουν σημαντικό επίπεδο κινδύνου, που θα μπορούσε να προκύψει στον*

⁸⁸ Ο.π. Βενέρης, 2020

⁸⁹ Βλ. σκέψη 151 Κανονισμού

οικονομικό αποκλεισμό ενάλωτων ατόμων και κοινοτήτων (ο λεγόμενος αποκλεισμός των χρηματοπιστωτικών οντοτήτων)»⁹⁰.

Επιπλέον, σύμφωνα με το άρθρο 34 του Κανονισμού «τυχόν διάδοση.. πληροφοριών από την παραλήπτρια ΜΧΠ σε οποιαδήποτε άλλη αρχή, οργανισμό ή υπηρεσία, ή τυχόν χρήση των πληροφοριών αυτών για σκοπούς εκτός των αρχικώς εγκριθέντων ...υπόκειται σε εκ των προτέρων συγκατάθεση από τη ΜΧΠ που παρέχει τις πληροφορίες». Η εν λόγω διάταξη, υπήρχε στο άρθρο 55 της Τέταρτης Οδηγίας και επαναλαμβάνεται και στο κείμενο του νέου Κανονισμού. Ως εκ τούτου, είναι έκδηλο ότι η αρχή του περιορισμού του σκοπού κάμπτεται σημαντικά, παρά την επισήμανση του ΕΕΠΔ ότι: «πρέπει να αναφέρεται ρητά στις προτάσεις ότι ο αποκλειστικός σκοπός της επεξεργασίας των δεδομένων είναι η πρόληψη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, καθώς και ότι η περαιτέρω επεξεργασία για μη συναφείς σκοπούς απαγορεύεται».⁹¹

3.3.2. Η αρχή της ακρίβειας των δεδομένων

Η αρχή της ακρίβειας των δεδομένων, όπως προβλέπεται στο άρθρο 5 παρ. 1 περ. δ' του ΓΚΠΔ, απαιτεί τα δεδομένα να είναι ακριβή και επικαιροποιημένα και με δυνατότητα ενημέρωσης και επικαιροποίησης τους.

Ως εκ τούτου, το ΕΣΠΔ προτείνει ότι η νομοθεσία για την αντιμετώπιση τέτοιων φαινομένων, χρειάζεται να ορίζει ρητά ότι τα προσωπικά δεδομένα που επεξεργάζονται οι υπόχρεες οντότητες πρέπει να είναι ακριβή, αξιόπιστα και ενημερωμένα, ώστε να συμμορφώνονται με τις υποχρεώσεις για την αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες.⁹²

Επιπλέον, σύμφωνα με τον Κανονισμό, παρόλο που η Τέταρτη Οδηγία κατάφερε να εναρμονίσει, εν πολλοίς, τους κανόνες των κρατών μελών της

⁹⁰ ΕΣΠΔ, 2020 σκέψη 46

⁹¹ ΕΕΠΔ, 2014

⁹² (EDPS, 2020)

Ευρωπαϊκής Ένωσης αναφορικά με τις υποχρεώσεις για την εξακρίβωση της ταυτότητας των πελατών, δεν θέσπισε αναλυτικούς κανόνες για τις συγκεκριμένες διαδικασίες που πρέπει να ακολουθούν οι υπόχρεες οντότητες κατά τη διαδικασία ταυτοποίησης των πελατών τους. Λόγω της κρίσιμης σημασίας αυτής της διαδικασίας για την ΚΕΤ/ΧΤ, κρίνεται αναγκαίο, στο πλαίσιο μιας προσέγγισης που βασίζεται στον κίνδυνο, να καθοριστούν πιο συγκεκριμένες και λεπτομερείς διατάξεις για τον προσδιορισμό και την επαλήθευση της ταυτότητας των πελατών, όπως αναλυτικά είδαμε στο προηγούμενο κεφάλαιο. Κατά συνέπεια, είναι απαραίτητο να θεσπιστούν σαφείς κανόνες που να καθορίζουν τα μέτρα αυξημένης δέουσας επιμέλειας, τα οποία θα περιλαμβάνουν ειδικές διαδικασίες για τις διασυνοριακές σχέσεις ανταπόκρισης, όπου ο κίνδυνος είναι συχνά υψηλότερος.

Επιπροσθέτως, στον Κανονισμό φαίνεται πως έχει δοθεί έμφαση ειδικά στην εξασφάλιση της ακρίβειας των πληροφοριών, ορίζοντας μια δέσμη συγκεκριμένων μέτρων. Πιο συγκεκριμένα, το Άρθρο 63, υποχρεώνει τις νομικές οντότητες να διατηρούν επαρκείς, ακριβείς και ενημερωμένες πληροφορίες για τους πραγματικούς δικαιούχους τους. Οι πληροφορίες αυτές πρέπει να αναφέρονται στο εκάστοτε Μητρώο χωρίς καθυστέρηση και οποιαδήποτε αλλαγή στις πληροφορίες, πρέπει να ενημερώνεται εντός 28 ημερών, διασφαλίζοντας ότι τα δεδομένα που περιέχονται στα κεντρικά μητρώα είναι πάντα επίκαιρα, αποτρέποντας τη χρήση ψευδών ή ανακριβών πληροφοριών. Επιπλέον, το άρθρο 24⁹³ απαιτεί από τις υπόχρεες οντότητες να αναφέρουν οποιεσδήποτε αποκλίσεις που εντοπίζονται μεταξύ των διαθέσιμων πληροφοριών στα κεντρικά μητρώα και των πληροφοριών που συλλέγουν. Αυτό ενισχύει την ακρίβεια των δεδομένων, επιτρέποντας έτσι την έγκαιρη διόρθωση τυχόν ανακριβειών.⁹⁴

⁹³ Εάν υπόχρηη οντότητα καταλήξει στο συμπέρασμα ότι οι πληροφορίες σχετικά με τον πραγματικό δικαιούχο στο κεντρικό μητρώο είναι εσφαλμένες, προσκαλεί τον πελάτη να υποβάλλει τις ορθές πληροφορίες στο κεντρικό μητρώο σύμφωνα με τα άρθρα 63, 64 και 67 χωρίς αδικαιολόγητη καθυστέρηση και, σε κάθε περίπτωση, εντός 14 ημερολογιακών ημερών.

⁹⁴ Επίσης, στον Κανονισμό (ΕΕ) 2024/1620, η ακρίβεια των δεδομένων είναι επίσης καίριας σημασίας. Στο Άρθρο 17, αναφέρεται ότι η Αρχή μπορεί να απαιτεί από επιλεγμένες υπόχρεες οντότητες να παρέχουν

Τα ως άνω συναντώνται εν πολλοίς και στην Έκτη Οδηγία, με την επισήμανση ότι προβλέπεται η αναφορά αναντιστοιχιών μεταξύ των πληροφοριών για τους πραγματικούς δικαιούχους που τηρούνται στα κεντρικά μητρώα και των πληροφοριών για τους πραγματικούς δικαιούχους που διατίθενται στις υπόχρεες οντότητες και, κατά περίπτωση, στις αρμόδιες αρχές γεγονός που αποτελεί αποτελεσματικό μηχανισμό για την επαλήθευση της ακρίβειας των πληροφοριών. Τυχόν απόκλιση που εντοπίζεται θα πρέπει να αναφέρεται και να διορθώνεται τάχιστα, σύμφωνα με τις απαιτήσεις περί προστασίας των δεδομένων.

Εντούτοις, σύμφωνα με το νυν άρθρο 76 παρ. 2 στοιχείο β του Κανονισμού που εφαρμόζεται στον ιδιωτικό τομέα, οι υπόχρεες οντότητες μπορούν να επεξεργάζονται ειδικές κατηγορίες δεδομένων που καλύπτονται από το Άρθρο 9 του ΓΚΠΔ, "υπό την προϋπόθεση ότι τα δεδομένα που προέρχονται από αξιόπιστες πηγές, είναι ακριβή και επικαιροποιημένα". Το ΕΣΠΔ θεωρεί ότι η υποχρέωση χρήσης αξιόπιστων, ακριβών και επικαιροποιημένων πηγών πρέπει να επεκταθεί σε κάθε πληροφορία που επεξεργάζονται οι υπόχρεες οντότητες για σκοπούς ΚΕΤ/ΧΤ

Επιπλέον, δεδομένου ότι η επεξεργασία ανακριβών δεδομένων θα παραβίαζε τις αρχές του άρθρου 5 παράγραφος 1 στοιχείο γ) και του άρθρου 5 παράγραφος 1 στοιχείο δ) του ΓΚΠΔ, κρίνει ότι απαιτείται ρητή αναφορά στην υποχρέωση των υπόχρεων οντοτήτων να χρησιμοποιούν μόνο ακριβείς και αξιόπιστες πηγές και να τεκμηριώνουν την αξιολόγηση της αξιοπιστίας και της ακρίβειας κάθε πηγής πληροφοριών που χρησιμοποιείται.

Επιπρόσθετα, σύμφωνα με το ΕΣΠΔ, οι περισσότερες υπόχρεες οντότητες χρησιμοποιούν παρόχους υπηρεσιών επιτήρησης (watchlist) για να εκπληρώσουν τις

όλες τις αναγκαίες πληροφορίες, εξασφαλίζοντας ότι οι πληροφορίες αυτές είναι σαφείς, ακριβείς και πλήρεις. Αυτή η διάταξη εξασφαλίζει ότι τα δεδομένα που παρέχονται είναι αξιόπιστα και ενημερωμένα, επιτρέποντας την Αρχή να εκτελεί τα καθήκοντά της με ακρίβεια.

Η παράγραφος 2 του Άρθρου 17 ενισχύει περαιτέρω αυτήν την απαίτηση, επισημαίνοντας ότι οι πληροφορίες πρέπει να παρέχονται χωρίς αδικαιολόγητη καθυστέρηση και να είναι σαφείς και ακριβείς. Οι πληροφορίες αυτές μπορεί να παρέχονται από εξουσιοδοτημένους δικηγόρους για λογαριασμό των πελατών τους, αλλά η ευθύνη για την ακρίβεια των πληροφοριών παραμένει στους πελάτες έτσι ώστε να διασφαλίζεται η υπευθυνότητα και η αξιοπιστία των δεδομένων που παρέχονται.

υποχρεώσεις τους βάσει των απαιτήσεων της ΚΕΤ/ΧΤ. Το ΕΣΠΑ σε πρώτο στάδιο, αναγνωρίζει την ανάγκη αυτές οι οντότητες να βασίζονται σε τέτοιες υπηρεσίες για να εκπληρώνουν τις υποχρεώσεις τους, καθώς παρέχουν ευκολότερη και ταχύτερη πρόσβαση στις πληροφορίες, βοηθώντας στην αποτελεσματική εφαρμογή των υποχρεώσεων ΚΕΤ/ΧΤ. Ωστόσο, η επεξεργασία δεδομένων προσωπικού χαρακτήρα από αυτούς τους παρόχους εγείρει σημαντικά ζητήματα προστασίας δεδομένων, καθώς οι πάροχοι λειτουργούν ως υπεύθυνοι επεξεργασίας δεδομένων βάσει του ΓΚΠΔ.

Το ΕΣΠΑ κατά το στάδιο ακόμα πρότασης του AML Package είχε κρίνει ως απαραίτητο να θεσπιστούν ειδικοί κανόνες για την προστασία των δεδομένων, που περιλαμβάνουν και ειδικές κατηγορίες προσωπικών δεδομένων και δεδομένων σχετικά με ποινικές καταδίκες, ώστε να διασφαλιστεί η ακρίβεια και η αξιοπιστία των πληροφοριών. Σε διαφορετική περίπτωση, οι εθνικές εποπτικές αρχές πρέπει να επιβάλλουν τη νομοθεσία για την προστασία των δεδομένων. Επιπλέον, προτείνεται η εισαγωγή αναφοράς σε κώδικες δεοντολογίας και πιστοποιήσεις για τους παρόχους επιτήρησης (watchlist), σύμφωνα με τα άρθρα 40 και 42 του ΓΚΠΔ.⁹⁵

3.3.3. Η αρχή της ελαχιστοποίησης των δεδομένων και του περιορισμού της αποθήκευσης

Επιπλέον, η αρχή της ελαχιστοποίησης, των δεδομένων απαιτεί τα δεδομένα να είναι επαρκή, συναφή και περιορισμένα σε ό,τι είναι απαραίτητο σε σχέση με τους σκοπούς της επεξεργασίας. Ενώ, η αρχή της περιορισμένης αποθήκευσης ορίζει ότι τα δεδομένα δεν πρέπει να διατηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων για περισσότερο χρόνο από όσο είναι αναγκαίο για τους σκοπούς της συλλογής ή της περαιτέρω επεξεργασίας τους. Οι αρχές αυτές έχουν ιδιαίτερη σημασία και για τη συμμόρφωση με τους κανονισμούς κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες καθώς η ελαχιστοποίηση των δεδομένων και

⁹⁵ (EDPB, 2021)

η περιορισμένη αποθήκευση βοηθούν στη διαχείριση του όγκου των δεδομένων και στη μείωση του κινδύνου παραβιάσεων και διαρροής τους.

Πιο συγκεκριμένα, στο άρθρο 5 παρ.1 στοιχείο γ του ΓΚΠΔ, διατυπώνεται η αρχή της ελαχιστοποίησης των δεδομένων, κατά την οποία τα προσωπικά δεδομένα που υποβάλλονται σε επεξεργασία θα πρέπει να είναι «κατάλληλα, συναφή και να περιορίζονται σε ό,τι είναι αναγκαίο σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία».

Ως εκ τούτου, οι οντότητες που διαβιβάζουν τα δεδομένα πρέπει να είναι σε θέση να αιτιολογούν, σε κάθε περίπτωση ανταλλαγής δεδομένων τους λόγους για τους οποίους τα συγκεκριμένα δεδομένα ήταν αναγκαία για τον συγκεκριμένο σκοπό.⁹⁶ Η ελαχιστοποίηση δεδομένων έχει τη σημασία της συλλογής μόνο των προσωπικών δεδομένων που απαιτούνται αυστηρά για σκοπούς καταπολέμησης του ξεπλύματος χρήματος. Περιορίζοντας τη συλλογή δεδομένων στα απαραίτητα, οι οργανισμοί μπορούν να μειώσουν τον κίνδυνο παραβίασης δεδομένων και να προστατεύσουν ευαίσθητες πληροφορίες. Η εφαρμογή πρακτικών ελαχιστοποίησης δεδομένων όχι μόνο ενισχύει τη συμμόρφωση με την ΚΕΤ/ΧΤ, αλλά προωθεί επίσης ένα πιο αποτελεσματικό σύστημα διαχείρισης δεδομένων που διατηρεί το απόρρητο.⁹⁷

Μία προσπάθεια εισαγωγής της αρχής της ελαχιστοποίησης, εντοπίζεται στο νομικό πλαίσιο για την πρόσβαση σε χρηματοοικονομικές πληροφορίες⁹⁸, η οποία διευκρινίζει ότι «λόγω του ευαίσθητου χαρακτήρα των χρηματοοικονομικών δεδομένων που θα πρέπει να αναλύουν οι ΜΧΠ και των απαραίτητων εγγυήσεων για την προστασία των δεδομένων, η παρούσα οδηγία θα πρέπει να ορίζει ρητά το είδος και το εύρος των πληροφοριών που μπορούν να ανταλλάσσονται μεταξύ των ΜΧΠ

⁹⁶ Ο.π. Kosta (2023)

⁹⁷ FCA, 2024

⁹⁸ Ο.π. Kosta

και μεταξύ αυτών και των αρμόδιων αρχών και μεταξύ των αρμοδίων αρχών των διαφόρων κρατών μελών.»⁹⁹

Ο πρόσφατος Κανονισμός περιλαμβάνει συγκεκριμένες διατάξεις για την επεξεργασία ευαίσθητων και ποινικών δεδομένων, καθορίζοντας ότι αυτή πρέπει να είναι “αυστηρά απαραίτητη” για την ΚΕΤ/ΧΤ. Ωστόσο, η έλλειψη σαφούς καθορισμού του τι σημαίνει “αυστηρά απαραίτητο” εγείρει ανησυχίες σχετικά με την παραβίαση της αρχής της ελαχιστοποίησης. Ο ΕΕΠΔ, κρίνει ότι θα πρέπει να προσδιορίζονται οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που πρέπει να υποβάλλονται σε επεξεργασία από τις υπόχρεες οντότητες. Ενώ, λαμβανομένης υπόψη και της αρχής της αναγκαιότητας και της αναλογικότητας ο ΕΕΠΔ θεωρεί ότι δεν θα πρέπει να επιτρέπεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που σχετίζονται με τον γενετήσιο προσανατολισμό ή την εθνική καταγωγή.¹⁰⁰ Επί παραδείγματι, η FATF απαιτεί από τις υπόχρεες οντότητες να αναγνωρίζουν μέλη της οικογένειας (π.χ., συζύγους) και στενούς συνεργάτες Πολιτικά Εκτεθειμένων Προσώπων (PEPs),¹⁰¹ περιλαμβάνοντας γνωστούς, σεξουαλικούς συντρόφους εκτός οικογενειακής μονάδας (π.χ., φίλες, φίλους, ερωμένες)” καθώς αυτές οι σχέσεις και οι λογαριασμοί τους είναι τυπικοί δρόμοι για τη νομιμοποίηση χρημάτων. Ωστόσο, ο σεξουαλικός προσανατολισμός θα μπορούσε εύκολα να προκύψει από αυτές τις πληροφορίες. Παρομοίως, η εθνική καταγωγή μπορεί επίσης να αποκαλυφθεί¹⁰² στα έγγραφα ταυτοποίησης από τον τόπο γέννησης ή την υπηκοότητα.

⁹⁹ ΟΔΗΓΙΑ (ΕΕ) 2019/1153 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 20ής Ιουνίου 2019 για τη θέσπιση κανόνων με σκοπό τη διευκόλυνση της χρήσης χρηματοοικονομικών και άλλων πληροφοριών για την πρόληψη, την ανίχνευση, τη διερεύνηση ή τη δίωξη ορισμένων ποινικών αδικημάτων και την κατάργηση της απόφασης 2000/642/ΔΕΥ του Συμβουλίου, αιτιολογική σκέψη 19

¹⁰⁰ (EDPB, 2021)

¹⁰¹ Ένα πολιτικώς εκτεθειμένο πρόσωπο (PEP) είναι ένα άτομο που κατέχει ή κατείχε σημαντική δημόσια θέση. Πολλοί PEPs κατέχουν θέσεις που μπορεί να καταχραστούν για σκοπούς όπως η νομιμοποίηση παράνομων εσόδων ή άλλες συναφείς εγκληματικές πράξεις, όπως η διαφθορά ή η δωροδοκία. Λόγω των κινδύνων που συνδέονται με τα PEPs, οι Συντάσεις της FATF απαιτούν την εφαρμογή πρόσθετων μέτρων για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας στις επιχειρηματικές σχέσεις με PEPs.

¹⁰² (Frasher, 2021)

Όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα, ο ΕΕΠΔ θεωρεί ότι αποτελεί ασάφεια που χρήζει περαιτέρω διευκρίνισης, η αναφορά σε «ισχυρισμούς» επιπλέον των «ερευνών», «διαδικασιών» και «καταδικαστικών αποφάσεων» στο νυν άρθρο 76 παράγραφος 3 στοιχείο β) του Κανονισμού.

Ως εκ τούτου, καταλήγουμε στο συμπέρασμα ότι το νέο νομοθετικό πλαίσιο δεν συμμορφώνεται πλήρως με την αρχή της ελαχιστοποίησης δεδομένων, καθώς δεν παρέχονται οι απαιτούμενες εγγυήσεις προκειμένου να διασφαλιστεί ότι τα δεδομένα που συλλέγονται προς επεξεργασία, περιορίζονται αποκλειστικά στα κατάλληλα, σχετικά και περιορισμένα στις απαραίτητες πληροφορίες σε σχέση με τους σκοπούς της πρόληψης, ανίχνευσης ΚΕΤ/ΧΤ

3.3.4. Ο περιορισμός της αποθήκευσης

Στενά συνδεδεμένη με την αρχή της ελαχιστοποίησης των δεδομένων είναι η αρχή του περιορισμού της αποθήκευσης. Σύμφωνα με το άρθρο 5 παρ 1 εδ του ΓΚΠΔ *“τα προσωπικά διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα”* ¹⁰³.

Η αρχή του περιορισμού της αποθήκευσης επιβάλλει κάθε σχετική νομοθεσία να αναφέρει σαφώς και επακριβώς τις περιόδους διατήρησης των δεδομένων. Κατά τον καθορισμό της περιόδου διατήρησης, πρέπει να τηρείται η αρχή της αναλογικότητας. Αναφορικά με την νομοθεσία για την αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες το ΕΣΠΔ είχε διατυπώσει ήδη από την Τέταρτη Οδηγία, τον ενδιασμό του αναφορικά με το γεγονός ότι οι

¹⁰³ ΓΚΠΔ άρθρο 5 παρ

περίοδοι διατήρησης των προσωπικών που προτείνονται στην ως άνω οδηγία, ήταν υπερβολικά μεγάλες¹⁰⁴.

Πιο συγκεκριμένα, στην ευρωπαϊκή νομοθεσία για την ΚΕΤ/ΧΤ, το άρθρο 40¹⁰⁵(1)(β) της Πέμπτης Οδηγίας, προέβλεπε στις υπόχρεες οντότητες να διατηρούν αρχεία συναλλαγών, αποτελούμενα από τα πρωτότυπα έγγραφα ή αντίγραφα αποδεκτά σε δικαστικές διαδικασίες βάσει του εφαρμοστέου εθνικού δικαίου, τα οποία είναι απαραίτητα για την ταυτοποίηση των συναλλαγών, για περίοδο πέντε ετών μετά τη λήξη της επιχειρηματικής τους σχέσης με τον πελάτη ή μετά την ημερομηνία μιας περιστασιακής συναλλαγής .

Στον πρόσφατο Κανονισμό κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες δεν εντοπίζονται ουσιαστικές αλλαγές σε αυτές τις υποχρεώσεις. Το άρθρο 72 παρ.1 του Κανονισμού διαβάζεται σχεδόν ταυτόσημα με το άρθρο 40 παρ. 1 της Πέμπτης Οδηγίας. Όπως και η προκάτοχός του, διακρίνει μεταξύ των πληροφοριών που είναι απαραίτητες για την εκτέλεση των μέτρων δέουσας επιμέλειας στην παράγραφο 1(α) και των αρχείων συναλλαγών στην παράγραφο 1(β) επαναλαμβάνοντας την υποχρέωση διατήρησης αρχείων οποιασδήποτε συναλλαγής, ανεξάρτητα από το εύρος των εφαρμοζόμενων μέτρων δέουσας επιμέλειας.¹⁰⁶

Ο όρος «μετά το τέλος της επιχειρηματικής σχέσης» είναι ένα ενδιαφέρον σημείο¹⁰⁷ καθώς, η περίοδος διατήρησης υπολογίζεται τελικά, ως το άθροισμα της διάρκειας της επιχειρηματικής σχέσης και της πενταετούς περιόδου διατήρησης μετά τη λήξη της επιχειρηματικής σχέσης που ορίζεται στο άρθρο 40 της παλιάς οδηγίας

¹⁰⁴ (ΕΣΠΑ, Δήλωση σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία στο πλαίσιο της πρόληψης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότηση της τρομοκρατίας, 2020)

¹⁰⁵ Οδηγία (ΕΕ) 2018/843 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ης Μαΐου 2018, για την τροποποίηση της οδηγίας (ΕΕ) 2015/849 για την πρόληψη της χρήσης του χρηματοπιστωτικού συστήματος για σκοπούς νομιμοποίησης εσόδων από παράνομες δραστηριότητες ή χρηματοδότησης της τρομοκρατίας και για την τροποποίηση των οδηγιών 2009/138/ΕΚ και 2013/36/ΕΕ, ΕΕ L

¹⁰⁶ (Landerer, 2022)

¹⁰⁷ (Milaj, 2017)

και στο 56 του νέου Κανονισμού. Επί παραδείγματι, όταν υπάρχει μακροπρόθεσμη επιχειρηματική σχέση, όπως αυτή που έχει μια τράπεζα με τους πελάτες της, η περίοδος διατήρησης συχνά εκτείνεται σε αρκετές δεκαετίες. Ενώ, οι περίοδοι διατήρησης μπορούν να παραταθούν από τα κράτη μέλη με πέντε επιπλέον έτη.¹⁰⁸

Ως εκ τούτου, σύμφωνα με τον Κανονισμό, οι περίοδοι διατήρησης δεν έχουν αλλάξει από το 2011 και εξακολουθούν να ανέρχονται σε πέντε χρόνια¹⁰⁹ συντηρώντας τον μεγάλο προβληματισμό των νομικών αναλυτών για την χρησιμότητα της ως άνω νομοθετικής αγκύλωσης.

Ωστόσο, τα προσωπικά δεδομένα πρέπει να διατηρούνται στην ΕΕ μόνο για το διάστημα που είναι απαραίτητο για την επεξεργασία τους. Ειδικές νομοθεσίες για τη διατήρηση δεδομένων έχουν θεσπιστεί, όπως η Οδηγία για τη Διατήρηση Δεδομένων (DRD¹¹⁰), που υιοθετήθηκε το 2006. Σκοπός της ήταν η υποστήριξη των αρχών επιβολής του νόμου στην έρευνα, ανίχνευση και δίωξη σοβαρών εγκλημάτων μέσω της διατήρησης δεδομένων από τις εταιρείες τηλεπικοινωνιών και παρόχους υπηρεσιών διαδικτύου. Σύμφωνα με την συγκεκριμένη οδηγία, οι πάροχοι ήταν υποχρεωμένοι να διατηρούν μεταδεδομένα για διάστημα από 6 έως 24 μήνες, ανάλογα με τον εθνικό νόμο.

Ωστόσο, το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) εξέδωσε στις 8.4.2014 την απόφασή του στις συνεκδικαζόμενες υποθέσεις C-293/12 και C-594/12 (Digital Rights Ireland), με την οποία έκρινε ότι η οδηγία 2006/24/EK είναι αντίσχυρη. Στην απόφασή του, το Δικαστήριο έκρινε ότι η DRD παραβίαζε τα άρθρα 7 και 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ και υπερέβαινε την αρχή της αναλογικότητας. Ενώ αναγνώρισε ότι η διατήρηση δεδομένων μπορεί μεν να εξυπηρετεί έναν στόχο

¹⁰⁸ Ο.π. (ΕΣΠΔ, Δήλωση σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία στο πλαίσιο της πρόληψης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότηση της τρομοκρατίας, 2020)

¹⁰⁹ Ο.π (Landerer, 2022)

¹¹⁰ Οδηγία 2006/24/EK “για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/EK” <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32006L0024>

γενικού ενδιαφέροντος, όπως η καταπολέμηση σοβαρών εγκλημάτων, εντούτοις διαπίστωσε ότι οι κανόνες για την πρόσβαση και τη χρήση των δεδομένων δεν ήταν επαρκώς σαφείς και οριοθετημένοι και ότι αυτή η πρακτική ήταν υπερβολικά επεμβατική και δεν συνοδευόταν από αντίστοιχες διασφαλίσεις για την προστασία των δικαιωμάτων των παρακολουθούμενων, σχετικά με τη συλλογή και χρήση των προσωπικών τους δεδομένων. Η ως άνω παρακολούθηση, δεν περιοριζόταν σε άτομα που είχαν συγκεντρώσει συγκεκριμένες υποψίες ή υπόνοιες για εγκληματικές συμπεριφορές και δεν παρείχε στοιχεία για την αποτελεσματικότητά της.¹¹¹

Έχει υποστηριχθεί από την βιβλιογραφία, ότι αυτή η περίπτωση αναδεικνύει τις προκλήσεις και τις ενδεχόμενες ανησυχίες σχετικά με την εφαρμογή παρόμοιων τεχνολογιών για την ΚΕΤ/ΧΤ. Οι προσεγγίσεις που εφαρμόζονται στο πλαίσιο των ως άνω πολιτικών, περιλαμβάνουν την αδιάκριτη συλλογή και διατήρηση των δεδομένων όλων των τραπεζικών πελατών, κάτι που αντιμετωπίζεται ως σοβαρή παραβίαση των προσωπικών δικαιωμάτων. Οι διαδικασίες που υιοθετούνται συχνά δεν προσφέρουν την ενημέρωση των ατόμων για την παρακολούθηση ή τη δυνατότητα αντίρρησης στην επεξεργασία των δεδομένων τους.¹¹²

3.3.5 Η αρχή της ακεραιότητας και εμπιστευτικότητας

Η αρχή της ακεραιότητας και της εμπιστευτικότητας αποτελεί θεμελιώδες στοιχείο του ΓΚΠΔ, ο οποίος ορίζει ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να διασφαλίζει την ασφάλειά τους, έναντι μη εξουσιοδοτημένης πρόσβασης, παράνομης χρήσης και τυχαίας απώλειας ή καταστροφής. Αυτό επιτυγχάνεται με την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων προστασίας.

¹¹¹ *Iγγλεζάκης, 2014*

¹¹² *Kosta, E. (2021)*

Η αρχή της ακεραιότητας επικεντρώνεται στη διατήρηση της ακρίβειας και της πληρότητας των δεδομένων, απαιτώντας να διατηρούνται ενημερωμένα και ακριβή κατά τη διάρκεια της επεξεργασίας. Τα δεδομένα πρέπει να προστατεύονται από ανεπιθύμητες ή μη εξουσιοδοτημένες τροποποιήσεις που θα μπορούσαν να οδηγήσουν σε εσφαλμένα αποτελέσματα. Από την άλλη πλευρά, η εμπιστευτικότητα αφορά τον έλεγχο της πρόσβασης, διασφαλίζοντας ότι μόνο εξουσιοδοτημένα πρόσωπα έχουν πρόσβαση σε προσωπικά δεδομένα. Η προστασία αυτή επιτυγχάνεται μέσω κρυπτογράφησης και πολιτικών που περιορίζουν την πρόσβαση σε ευαίσθητα δεδομένα, ώστε να αποτρέπεται κάθε μη εξουσιοδοτημένος χειρισμός.

Ενώ η ίδια λογική υποχρέωσης διασφάλισης της εμπιστευτικότητας και της προστασίας των δεδομένων, συναντάται και για τις υπόχρεες οντότητες και τις αρμόδιες αρχές όταν θα χρειάζεται να ανταλλάσσουν πληροφορίες στο πλαίσιο σύμπραξης για τον διαμοιρασμό πληροφοριών για τη συμμόρφωση με τις υποχρεώσεις και τα καθήκοντά τους στον τομέα της αντιμετώπισης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες.¹¹³ Ως εκ τούτου, οι υπόχρεες οντότητες καλούνται να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, ώστε να κατοχυρώνεται ένα επίπεδο ασφάλειας και εμπιστευτικότητας ανάλογο προς τη φύση και την έκταση των πληροφοριών που ανταλλάσσονται.

Παράλληλα, διατυπώνεται ότι επειδή οι συμπράξεις για τον διαμοιρασμό πληροφοριών περιλαμβάνουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, γεγονός που συνεπάγεται υψηλό κίνδυνο για δικαιώματα των φυσικών προσώπων, θα πρέπει να διενεργηθεί εκτίμηση επιπτώσεων σχετικά με την προστασία των δεδομένων δυνάμει του ΓΚΠΔ, πριν από την έναρξη των δραστηριοτήτων της σύμπραξης. Ενώ, προβλέπεται ότι τα κράτη μέλη θα πρέπει να έχουν τη δυνατότητα να διατηρούν ή να θεσπίζουν ειδικότερες διατάξεις ώστε να προβλέπονται πιο συγκεκριμένες απαιτήσεις σε σχέση με την επεξεργασία δεδομένων προσωπικού

¹¹³ Αιτιολογική σκέψη 147 Κανονισμού

χαρακτήρα που ανταλλάσσονται στο πλαίσιο σύμπραξης για τον διαμοιρασμό πληροφοριών.¹¹⁴

Επιπλέον, γίνεται ρητή αναφορά περί υποχρέωσης τήρησης των απαιτήσεων που προβλέπονται στο άρθρο 32 του ΓΚΠΔ, κατά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα¹¹⁵. Πιο συγκεκριμένα, το άρθρο 32 καθιστά σαφές ότι ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία θα πρέπει να θεσπίζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζουν κατάλληλο επίπεδο ασφάλειας των δεδομένων προσωπικού χαρακτήρα με την ικανότητα έγκαιρου εντοπισμού, αντιμετώπισης και αναφοράς μιας παραβίασης να θεωρούνται βασικά στοιχεία αυτών των μέτρων.¹¹⁶

Με την αλματώδη αύξηση των περιστατικών κυβερνοεπιθέσεων και διαρροής δεδομένων, ειδικά σε χρηματοπιστωτικά ιδρύματα και οργανισμούς, η λήψη των κατάλληλων τεχνικών και οργανικών μέτρων, όπως προβλέπεται στο άρθρο 32 του ΓΚΠΔ, κρίνεται επιβεβλημένη, καθώς διαδραματίζει καθοριστικό ρόλο στην προστασία των προσωπικών δεδομένων, στην πρόληψη και την αντιμετώπιση διαρροών. Η συμμόρφωση με τις διατάξεις του άρθρου αυτού, συμβάλλει στην ελαχιστοποίηση των κινδύνων και στην προστασία των δικαιωμάτων των υποκειμένων των δεδομένων, εξασφαλίζοντας παράλληλα την ακεραιότητα και την εμπιστευτικότητα των δεδομένων που επεξεργάζονται οι οργανισμοί.

¹¹⁴ Αιτιολογική σκέψη 148 Κανονισμού

¹¹⁵ Άρθρο 76 παρ. 2 Κανονισμού: 2. « Οι υπόχρεες οντότητες είναι σε θέση να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα που καλύπτονται από το άρθρο 9 του κανονισμού (ΕΕ) 2016/679, υπό την προϋπόθεση ότι:

α) ενημερώνουν τους πελάτες τους ή τους δυνητικούς πελάτες τους ότι οι εν λόγω κατηγορίες δεδομένων μπορεί να υποβληθούν σε επεξεργασία για τους σκοπούς της συμμόρφωσης με τις απαιτήσεις του παρόντος κανονισμού·

β) τα δεδομένα προέρχονται από αξιόπιστες πηγές, είναι ακριβή και επικαιροποιημένα

γ) δεν λαμβάνουν αποφάσεις που θα οδηγούσαν σε μεροληπτικά αποτελέσματα βάσει των εν λόγω δεδομένων·

δ) λαμβάνουν μέτρα υψηλού βαθμού ασφαλείας σύμφωνα με το άρθρο 32 του κανονισμού (ΕΕ) 2016/679, ιδίως όσον αφορά την εμπιστευτικότητα.»

¹¹⁶ Ομάδα Εργασίας 29,2018

3.4. Νομική Βάση Επεξεργασίας

Η αρχή της νομιμότητας είναι η πρώτη αρχή που αναφέρεται τόσο στον ΓΚΠΔ όσο και στην Οδηγία LED και απαιτεί η επεξεργασία των προσωπικών δεδομένων να βασίζεται σε τουλάχιστον μία από τις κατάλληλες νομικές βάσεις. Ο ΓΚΠΔ προσφέρει έναν κατάλογο έξι νομικών βάσεων για την επεξεργασία δεδομένων. Πιο συγκεκριμένα, στο άρθρο 6 του Κανονισμού η επεξεργασία είναι σύμφωνη μόνον εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις: α) το υποκείμενο έχει δώσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων για έναν ή περισσότερους σκοπούς β) η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για τη λήψη μέτρων πριν τη σύναψη της σύμβασης κατόπιν αιτήσεως του υποκειμένου των δεδομένων, γ) η επεξεργασία είναι αναγκαία για την εκπλήρωση εκ του νόμου υποχρέωσης του υπευθύνου επεξεργασίας, δ) η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, ε) η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημοσίου συμφέροντος ή άσκησης δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, και ζ) η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση εννόμου συμφέροντος του υπεύθυνου της επεξεργασίας ή τρίτου, στον οποίο ανακοινώνονται τα δεδομένα, το οποίο (συμφέρον) υπερέχει προφανώς των δικαιωμάτων και συμφερόντων του υποκειμένου, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.¹¹⁷

Στον αντίποδα, η Οδηγία για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων (γνωστή και ως Law Enforcement Directive – LED) συμπληρώνει τον ΓΚΠΔ. Σύμφωνα με την ως άνω οδηγία, η επεξεργασία στην οποία

¹¹⁷ Προϋποθέσεις νόμιμης επεξεργασίας προσωπικών δεδομένων («απλών»)
https://www.dpa.gr/index.php/el/foreis/arxes_nomimotitas/proipotheseis_nomimis_epexergasias

εφαρμόζεται η Οδηγία LED είναι νόμιμη «μόνο εάν και στον βαθμό που η επεξεργασία είναι αναγκαία για την εκτέλεση ενός καθήκοντος που εκτελείται από αρμόδια αρχή για σκοπούς επιβολής του νόμου (...) και ότι αυτή βασίζεται στο δίκαιο της Ένωσης ή των κρατών μελών».¹¹⁸

Ο προσδιορισμός του εφαρμοστέου νομικού πλαισίου και της νομικής βάσης για την ανταλλαγή δεδομένων είναι περίπλοκος στον τομέα της ΚΕΤ/ΧΤ, όπου εμπλέκονται διάφοροι παράγοντες.¹¹⁹

Στο κείμενο της Έκτης Οδηγίας, ορίζεται ότι αναφορικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφαρμόζεται ο ΓΚΠΔ¹²⁰. Πιο συγκεκριμένα, επισημαίνεται ότι η ΚΕΤ/ΧΤ, αναγνωρίζεται όπως έχουμε ήδη δει, από τα κράτη μέλη ως ζήτημα σημαντικού δημοσίου συμφέροντος. Επιπλέον, προβλέπεται ότι ο κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα θεσμικά όργανα και τους οργανισμούς της Ένωσης για τους σκοπούς της παρούσας οδηγίας. Ωστόσο, τονίζεται ότι οι αρμόδιες αρχές που είναι υπεύθυνες σχετικά με την διερεύνηση ή τη δίωξη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, των βασικών αδικημάτων της ή της χρηματοδότησης της τρομοκρατίας ή εκείνες που έχουν το καθήκον του εντοπισμού, της κατάσχεσης ή της δέσμευσης και της δήμευσης περιουσιακών στοιχείων προερχόμενων από εγκληματικές δραστηριότητες θα πρέπει να τηρούν τους κανόνες που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις,

¹¹⁸ Άρθρο 8 παρ.1 της Οδηγίας 680/2016

¹¹⁹ Kosta,2023

συμπεριλαμβανομένης της οδηγίας (ΕΕ) 2016/680¹²¹ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.¹²²

Ως εκ τούτου, αυτό συμβαίνει διότι ο ΓΚΠΔ εφαρμόζεται σε οποιαδήποτε επεξεργασία προσωπικών δεδομένων, εκτός αν ισχύουν συγκεκριμένες εξαιρέσεις που προβλέπονται στα άρθρα 2(2) και 2(3) του ΓΚΠΔ. Δεδομένου ότι τα υπόχρεα πρόσωπα δεν είναι αρμόδιες αρχές κατά την έννοια της Οδηγίας LED και δεν επεξεργάζονται προσωπικά δεδομένα άμεσα για σκοπούς επιβολής του νόμου, ο ΓΚΠΔ θεωρείται το κατάλληλο πλαίσιο.¹²³ Παρόλα αυτά, η επιλογή της κατάλληλης νομικής βάσης για την επεξεργασία προσωπικών δεδομένων από τα υπόχρεα πρόσωπα παραμένει πρόκληση, καθώς μπορεί να αφορά νομική υποχρέωση, έννομο συμφέρον, ή την εκτέλεση ενός καθήκοντος προς το δημόσιο συμφέρον. Ειδικά για τα δεδομένα που επεξεργάζονται τα υπόχρεα πρόσωπα για την τήρηση των υποχρεώσεων δέουσας επιμέλειας, μπορεί να υποστηριχθεί ότι αυτά βασίζονται στη συμμόρφωση με μια νομική υποχρέωση, αν και οι ασαφείς διατυπώσεις ενδέχεται να μην πληρούν πλήρως τις αρχές του κράτους δικαίου. Συνεπώς, παραμένει αμφίβολο αν αυτή η βάση είναι η πιο κατάλληλη για την επεξεργασία.¹²⁴

Συμπερασματικά, η διατήρηση της ισορροπίας μεταξύ της αποτελεσματικής ΚΕΤ/ΧΤ και της προστασίας των δεδομένων προσωπικού χαρακτήρα εξακολουθεί να αποτελεί πρόκληση τόσο για τον Ευρωπαϊκό νομοθέτη, τις αρμόδιες αρχές αλλά και τις υπόχρεες οντότητες. Η ανάλυση αυτή επιχειρεί να αναδείξει ότι, παρά τις προσπάθειες εναρμόνισης, με τις διατάξεις του ΓΚΠΔ, εξακολουθούν να υπάρχουν ασάφειες και συγκρούσεις που απαιτούν προσεκτικό χειρισμό. Η ενίσχυση των εγγυήσεων για την προστασία των δεδομένων, ο σαφής καθορισμός των σκοπών

¹²¹ Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου

¹²² Αιτιολογική σκέψη 122 της Οδηγίας 2024/1640

¹²³ Γιαννακίδου, 2023

¹²⁴ Brewczyńska, M., & Kosta, E. (2023)

επεξεργασίας και η τήρηση των αρχών της αναγκαιότητας και της αναλογικότητας είναι ζωτικής σημασίας για τη διασφάλιση των δικαιωμάτων των πολιτών. Στο συνεχώς εξελισσόμενο νομικό τοπίο, η συνεργασία μεταξύ των αρχών προστασίας δεδομένων και των οντοτήτων ΚΕΤ/ΧΤ είναι απαραίτητη για τη δημιουργία ενός πλαισίου που προστατεύει τόσο την ασφάλεια όσο και την ιδιωτική ζωή. Συνεπώς, απομένει να διαπιστωθεί εν τοις πράγματι, κατά πόσο το νέο AML PACKAGE, θα καταφέρει κατά την εφαρμογή του να πετύχει την αναγκαία αυτή ισορροπία

ΚΕΦΑΛΑΙΟ 4

ΟΙ ΠΕΡΙΟΡΙΣΜΟΙ ΣΤΑ ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ

Το κεφάλαιο αυτό επιχειρεί να διερευνήσει τον τρόπο με τον οποίο οι πολιτικές για την ΚΕΤ/ΧΤ επηρεάζουν εν γένει την προστασία των προσωπικών δεδομένων, σε σημαντικές πτυχές εφαρμογής τους. Στόχος του κεφαλαίου είναι να αναδείξει τις περιστάσεις υπό τις οποίες οι πρακτικές ΚΕΤ/ΧΤ επιτρέπουν περιορισμούς στα δικαιώματα των ατόμων, εστιάζοντας στα δικαιώματα της ενημέρωσης και πρόσβασης.

4.1. Περιορισμοί στο πλαίσιο της Καταπολέμησης της Νομιμοποίησης εσόδων από παράνομες δραστηριότητες

Σύμφωνα με το κείμενο του νέου Κανονισμού, όπως επαναλαμβάνεται εν πολλοίς και στο κείμενο της Έκτης Οδηγίας «Τα δικαιώματα πρόσβασης στα δεδομένα του υποκειμένου των δεδομένων ισχύουν για τα προσωπικά δεδομένα που τυγχάνουν επεξεργασίας για τους σκοπούς του παρόντος κανονισμού. Ωστόσο, η πρόσβαση του υποκειμένου των δεδομένων σε οποιεσδήποτε πληροφορίες σχετίζονται με αναφορά ύποπτης συναλλαγής θα υπονόμευε σοβαρά την αποτελεσματικότητα της ΚΕΤ/ΧΤ. Επομένως, ενδέχεται να δικαιολογηθούν εξαιρέσεις και περιορισμοί του δικαιώματος αυτού σύμφωνα με το άρθρο 23 του κανονισμού (ΕΕ) 2016/679.»¹²⁵ ενώ σε πολλά σημεία του Κανονισμού διατρανώνεται επαναλαμβανόμενα ότι «είναι πάγια νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης ότι η ΚΕΤ/ΧΤ αποτελεί σκοπό γενικού δημόσιου συμφέροντος, το ίδιο δε ισχύει και για τους εν λόγω συνδεδεμένους με αυτόν σκοπούς δημόσιας ασφάλειας.»¹²⁶

Ως εκ τούτου, συμπεραίνουμε ότι παρά τις επαναλαμβανόμενες στο νέο νομοθετικό πλαίσιο, εξαγγελίες περί διαφύλαξης της προστασίας των προσωπικών δεδομένων των υποκειμένων που ελέγχονται, προβλέπονται περιορισμοί στο όνομα του δημοσίου συμφέροντος, όπως ίσχυαν και στα κείμενα των Οδηγιών 4 και 5 .

¹²⁵ Σκεψη 157 Κανονισμού

¹²⁶ Σκέψη 43 της 6^{ης} Οδηγίας

Ωστόσο, οι περιορισμοί πρέπει να πληρούν τις απαιτήσεις του άρθρου 23 ΓΚΠΔ. Πιο συγκεκριμένα, η ως άνω διάταξη, παρέχει την δυνατότητα περιορισμού των δικαιωμάτων που αποδίδονται στα υποκείμενα των δεδομένων «στα άρθρα 12 έως 22 και στο άρθρο 34 και της εφαρμογής όλων των βασικών αρχών της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που προβλέπονται στο άρθρο 5, εφόσον οι διατάξεις του αντιστοιχούν στα δικαιώματα και τις υποχρεώσεις που προβλέπονται στα άρθρα 12 έως 23». Όταν ανταλλάσσονται δεδομένα προσωπικού χαρακτήρα στο πλαίσιο ΚΕΤ/ΧΤ τα δικαιώματα των δεδομένων ενδέχεται να περιορίζονται σε τρεις κύριες περιπτώσεις, σύμφωνα με το άρθρο 23¹²⁷ του ΓΚΠΔ, ήτοι στο α) στο όνομα της πρόληψης, διερεύνησης και δίωξης εγκλημάτων β) στο όνομα της εθνικής ασφάλειας ή γ) στο όνομα άλλων σημαντικών στόχων δημοσίου συμφέροντος. Η διάταξη αυτή έχει τον τίτλο «περιορισμοί». Οι περιορισμοί θα πρέπει να θεωρούνται εξαιρέσεις στον γενικό κανόνα που επιτρέπει την άσκηση των δικαιωμάτων και επιβάλλει τις υποχρεώσεις που κατοχυρώνονται στον ΓΚΠΔ.¹²⁸

Το άρθρο 23 απλώς επαναλαμβάνει και διευκρινίζει τις προϋποθέσεις που υπάρχουν ήδη στο άρθρο 52 παράγραφος 1 του Χάρτη¹²⁹ και στη νομολογία του ΔΕΕ. Η νομολογία του ΔΕΕ έχει κρίνει ότι οι πρακτικές παρακολούθησης για τον εντοπισμό δυνητικής εγκληματικής δραστηριότητας δημιουργούν σοβαρές παρεμβάσεις στην ιδιωτική ζωή, αλλά οι παρεμβάσεις αυτές μπορούν να

¹²⁷ Σε όλες τις περιπτώσεις, όταν το δίκαιο της Ένωσης ή του κράτους μέλους επιτρέπει περιορισμούς στα δικαιώματα των υποκειμένων των δεδομένων ή στις υποχρεώσεις των υπευθύνων επεξεργασίας (συμπεριλαμβανομένων των από κοινού υπευθύνων επεξεργασίας 3) και των εκτελούντων την επεξεργασία, θα πρέπει να σημειωθεί ότι εξακολουθεί να ισχύει η αρχή της λογοδοσίας, όπως ορίζεται στο άρθρο 5 παράγραφος 2 του ΓΚΠΔ. Αυτό σημαίνει ότι ο υπεύθυνος επεξεργασίας είναι υπόλογος και είναι σε θέση να αποδείξει στα υποκείμενα των δεδομένων τη συμμόρφωσή του με το πλαίσιο προστασίας δεδομένων της ΕΕ, συμπεριλαμβανομένων των αρχών που αφορούν την επεξεργασία των δεδομένων τους.

¹²⁸ (ΕΣΠΔ, Κατευθυντήριες γραμμές 10/2020 σχετικά με τους περιορισμούς βάσει του άρθρου 23 του ΓΚΠΔ, 2021)

¹²⁹ Άρθρο 52, παρ. 1 Χάρτη «Κάθε περιορισμός στην άσκηση των δικαιωμάτων και ελευθεριών που αναγνωρίζονται στον παρόντα Χάρτη πρέπει να προβλέπεται από το νόμο και να σέβεται το βασικό περιεχόμενο των εν λόγω δικαιωμάτων και ελευθεριών.»

δικαιολογηθούν εάν πληρούνται οι προϋποθέσεις του άρθρου 52 παράγραφος 1 του Χάρτη.¹³⁰

Στο σημείο αυτό, πρέπει να τονιστεί ότι μέχρι στιγμής δεν υπάρχει σχετική απόφαση που να έχει απασχολήσει το ΔΕΕ και να σχετίζεται αποκλειστικά με την αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Εντούτοις, πολύ συχνά στην νομολογία και στην θεωρία παραλληλίζεται η εξετασθείσα περίπτωση με εκείνη των τηλεπικοινωνιακών δεδομένων. Ως εκ τούτου, για λόγους που θα αναλυθούν παρακάτω, στο παρόν κεφάλαιο θα επιχειρηθεί ο συσχετισμός του τιθέμενου ζητήματος και εν γένει του ερευνητικού ερωτήματος που απασχολεί την παρούσα εργασία, με πολύ σημαντικές αποφάσεις που διαδραμάτισαν καθοριστικό ρόλο στην διαμόρφωση του υπάρχοντος πλαισίου για τα προσωπικά δεδομένα.^{131 132}

Το ΕΣΠΔ, έχει αναγνωρίσει ότι στην περίπτωση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, η παροχή πληροφοριών στα υποκείμενα των δεδομένων που αποτελούν αντικείμενο έρευνας, ενδέχεται να θέσει σε κίνδυνο την επιτυχία της εν λόγω έρευνας, κρίνοντας ότι ο περιορισμός του δικαιώματος πληροφόρησης ή άλλων δικαιωμάτων των υποκειμένων των δεδομένων μπορεί να θεωρηθεί αναγκαίος, σύμφωνα με όσα ορίζονται στο άρθρο 23 παράγραφος 1 στοιχείο δ) του ΓΚΠΔ, αιτιολόγηση που συναντάται και στο κείμενο του νέου Κανονισμού, όπως διατυπώθηκε παραπάνω.

Εντούτοις, το ΕΣΠΔ, κρίνει ότι η ενημέρωση που έχει παραλειφθεί, πρέπει να πραγματοποιηθεί από τη στιγμή που δεν δύναται να θέσει σε κίνδυνο πια τις έρευνες που διεξάγονται, ούτως ώστε το υποκείμενο των δεδομένων να λάβει την εξατομικευμένη γνωστοποίηση για την προστασία των δεδομένων.¹³³ Η ενημέρωση των ενδιαφερομένων, αποτελεί σημαντικό δικαίωμα το οποίο συγκρούεται συχνά με

¹³⁰ (Maxwell, 2021)

¹³¹ Kosta, 2023

¹³² Ο.π. Maxwell (2021)

¹³³ Ο.π. ΕΣΠΔ

τις πολιτικές για το AML, καθώς δεν υπάρχει σχετική πρόβλεψη. Ωστόσο, το εν λόγω δικαίωμα, μπορεί να περιοριστεί μόνο υπό συγκεκριμένες προϋποθέσεις.

4.2 Περιορισμοί στο όνομα της εθνικής ασφάλειας

Έχει διατυπωθεί ότι ο περιορισμός των δικαιωμάτων των υποκειμένων των δεδομένων μπορεί να έχει στόχο τη διασφάλιση της ασφάλειας του κράτους, της δημόσιας ασφάλειας και/ή της εθνικής άμυνας των κρατών μελών, όπως αναφέρεται στο άρθρο 23 παράγραφος 1 στοιχεία α), β) και γ) του ΓΚΠΔ.¹³⁴

Πιο συγκεκριμένα, στην υπόθεση *Privacy International*¹³⁵, το (ΔΕΕ) εξέτασε την εθνική νομοθεσία που επιτρέπει σε κρατική αρχή να απαιτεί από παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών να διαβιβάζουν δεδομένα κίνησης και δεδομένα θέσης στις υπηρεσίες ασφάλειας και πληροφοριών με σκοπό τη διαφύλαξη της εθνικής ασφάλειας.¹³⁶ Το ΔΕΕ κατέληξε στο συμπέρασμα ότι, παρόλο που εναπόκειται στα κράτη μέλη να καθορίζουν τα ουσιώδη συμφέροντα ασφαλείας τους και να λαμβάνουν κατάλληλα μέτρα για τη διασφάλιση της εσωτερικής και εξωτερικής τους ασφάλειας, το γεγονός ότι έχει ληφθεί εθνικό μέτρο με σκοπό την προστασία της εθνικής ασφάλειας δεν μπορεί να καταστήσει ανεφάρμοστο το δίκαιο της ΕΕ και να απαλλάξει τα κράτη μέλη από την υποχρέωσή τους να συμμορφωθούν με αυτό.

Το ίδιο συμπέρασμα συναντάται και στην υπόθεση *La Quadrature du Net (LQDN)*¹³⁷, σύμφωνα με το οποίο, η εθνική νομοθεσία που υποχρεώνει τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών να διατηρούν δεδομένα κίνησης και δεδομένα θέσης για τους σκοπούς της προστασίας της εθνικής ασφάλειας και της καταπολέμησης του εγκλήματος εμπίπτει στο πεδίο εφαρμογής της οδηγίας 2002/58/ΕΚ¹³⁸.

¹³⁴ Οπ. ΕΣΠΑ σκέψη 22

¹³⁵ *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*

¹³⁶ Ο.π. *Kosta*, 2021

¹³⁷ *La Quadrature du Net and Others v Premier ministre and Others*

¹³⁸ Οδηγία 2002/58/ΕΚ, 2002

Ως εκ τούτου, σύμφωνα με το σκεπτικό του ΔΕΕ, οι ιδιωτικοί φορείς που συμμετέχουν στην ανταλλαγή δεδομένων προσωπικού χαρακτήρα για την ΚΕΤ/ΧΤ εξακολουθούν να εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ, ακόμη και όταν η ανταλλαγή έχει ζητηθεί από αρμόδια αρχή. Αυτό σημαίνει ότι πρέπει να εξετάζεται προσεκτικά το καθεστώς υπό το οποίο πραγματοποιείται η ανταλλαγή δεδομένων, ιδιαίτερα όταν εμπλέκονται ιδιωτικοί φορείς, προκειμένου να διασφαλιστεί ότι οι περιορισμοί στα δικαιώματα των υποκειμένων των δεδομένων είναι αναγκαίοι και αναλογικοί.¹³⁹

4.2. Το δικαίωμα ενημέρωσης

Το δικαίωμα ενημέρωσης των υποκειμένων για τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων προβλέπεται στα άρθρα 12-14 του ΓΚΠΔ. Το δικαίωμα αυτό, επιτρέπει στα υποκείμενα των δεδομένων να ενημερώνονται με σαφήνεια και ακρίβεια σχετικά με τον σκοπό της επεξεργασίας, τη νομική βάση, τις πηγές των δεδομένων και τους τυχόν αποδέκτες τους. Η διαφάνεια αυτή ενισχύει την εμπιστοσύνη των πολιτών και τους παρέχει τη δυνατότητα να ασκούν τα δικαιώματά τους στον τομέα της προστασίας των προσωπικών δεδομένων. Το δικαίωμα αυτό μπορεί να περιοριστεί, μόνο υπό συγκεκριμένες συνθήκες και παρέχοντας συγκεκριμένες εγγυήσεις στα υποκείμενα των δεδομένων.

Πιο συγκεκριμένα, σύμφωνα με πάγια νομολογία του ΕΔΔΑ και του ΔΕΕ, η κοινοποίηση των καταγγελιών συνδέεται άρρηκτα με την αποτελεσματικότητα των ενδίκων βοηθημάτων ενώπιον των δικαστηρίων και οι ενδιαφερόμενοι¹⁴⁰ θα πρέπει να ενημερώνονται μόλις καταστεί δυνατή η κοινοποίηση χωρίς να τίθεται σε κίνδυνο σκοπός του περιορισμού μετά τη λήξη του μέτρου παρακολούθησης.¹⁴¹

¹³⁹ Ο.π. *Bregczynska* (2023)

¹⁴⁰ Ο.π. *Brewczynska* (2023)

¹⁴¹ Ο.π. ΕΣΠΔ σκέψη 24

Το ζήτημα της ενημέρωσης των θιγόμενων προσώπων απασχόλησε την νομολογία στις απόφαση Tele2/Watchon¹⁴²¹⁴³, στην οποία το ΔΕΕ έκρινε ότι τα θιγόμενα πρόσωπα πρέπει να ενημερώνονται για τη διαβίβαση των δεδομένων τους και για τη χρήση αυτών, από τη στιγμή που η ενημέρωση αυτή δεν μπορεί να θέσει σε κίνδυνο τις έρευνες τις οποίες διεξάγουν οι δημόσιες αρχές. Συγκεκριμένα, η ενημέρωση αυτή είναι, στην πράξη, αναγκαία, προκειμένου τα θιγόμενα πρόσωπα να μπορούν να ασκήσουν τα δικαιώματά τους περί παροχής πρόσβασης στα δεδομένα τα οποία τους αφορούν και, ενδεχομένως, άσκησης, σύμφωνα με το άρθρο 47¹⁴⁴, πρώτο εδάφιο, του ΧΘΔΑ, αποτελεσματικής προσφυγής ενώπιον δικαστηρίου. Πάντως, η ενημέρωση αυτή επιβάλλεται μόνον από τη στιγμή που δεν μπορεί να θέσει σε κίνδυνο τις έρευνες τις οποίες διεξάγουν οι διαλαμβανόμενες στη σχεδιαζόμενη συμφωνία δημόσιες αρχές.

Ωστόσο, στο πλαίσιο της ΚΕΤ/ΧΤ, το δικαίωμα ενημέρωσης περιορίζεται σημαντικά. Σύμφωνα με τον νέο Κανονισμό, όπως ορίζεται στο άρθρο 73, οι υπόχρεες οντότητες, οι διευθυντές και οι υπάλληλοί τους απαγορεύεται να ενημερώνουν τα υποκείμενα των δεδομένων για το γεγονός ότι οι πληροφορίες τους έχουν διαβιβαστεί ή πρόκειται να διαβιβαστούν στις αρμόδιες αρχές ή ότι διεξάγεται έρευνα για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή τη χρηματοδότηση της τρομοκρατίας. Αυτή η απαγόρευση έχει ως στόχο την προστασία της έρευνας, καθώς η γνωστοποίηση προς το ερευνώμενο πρόσωπο θα μπορούσε να το οδηγήσει σε απόκρυψη κρίσιμων αποδεικτικών στοιχείων.

Η ανάγκη για μυστικότητα κατά τη διάρκεια της έρευνας δικαιολογείται, *mutatis mutandis*, από τις διατάξεις του ποινικού δικαίου, όπως αυτές προβλέπονται

¹⁴² ΔΕΕ,2016, C-203/15, *Tele2 Sverige AB κατά Post- och telestyrelsen και Secretary of State for the Home Department κατά Tom Watson και άλλων*

¹⁴³ Βλ. και ΔΕΕ,2017, Γνωμοδότηση 1/15 σχετικά με τη συμφωνία PNR μεταξύ ΕΕ και Καναδά

¹⁴⁴ Άρθρο 47 ΧΘΔΑ - Δικαίωμα πραγματικής προσφυγής και αμερόληπτου δικαστηρίου
Κάθε πρόσωπο του οποίου παραβιάστηκαν τα δικαιώματα και οι ελευθερίες που διασφαλίζονται από το δίκαιο της Ένωσης, έχει δικαίωμα πραγματικής προσφυγής ενώπιον δικαστηρίου, τηρουμένων των προϋποθέσεων που προβλέπονται στο παρόν άρθρο.

κατά το στάδιο της προανακριτικής και ανακριτικής διαδικασίας¹⁴⁵. Ωστόσο, ο ΕΕΠΔ έχει εκφράσει ανησυχίες σχετικά με την απειριορίστη απαγόρευση παροχής πληροφοριών στα υποκείμενα των δεδομένων. Στη γνωμοδότησή του, της 4ης Ιουλίου 2013, ο ΕΕΠΔ προτείνει την προσθήκη ειδικής διάταξης που θα κατοχυρώνει την αρχή της παροχής πληροφοριών στα υποκείμενα σχετικά με την επεξεργασία των δεδομένων τους, σύμφωνα με τα άρθρα 10 και 11 της τότε ισχύουσας Οδηγίας 95/46/ΕΚ.¹⁴⁶ Παράλληλα, τονίζει ότι η γενική απαγόρευση χωρίς χρονικό όριο είναι δυσανάλογη, ειδικά σε περιπτώσεις που οι συνέπειες των ερευνών μπορεί να επηρεάσουν σημαντικά τα υποκείμενα των δεδομένων, όπως η αδυναμία σύναψης εμπορικής σχέσης ή το άνοιγμα τραπεζικού λογαριασμού. Ως εκ τούτου, προτείνεται η θέσπιση ενός χρονικού ορίου για τη σχετική απαγόρευση, ώστε να εξισορροπηθεί η ανάγκη προστασίας της έρευνας με τα δικαιώματα των υποκειμένων των δεδομένων.¹⁴⁷

Ωστόσο, με την εισαγωγή του άρθρου 73 στον νέο Κανονισμό, καθίστανται λεπτομερείς εξαιρέσεις στην απαγόρευση της γνωστοποίησης. Συγκεκριμένα, το άρθρο 73 επιτρέπει τη γνωστοποίηση πληροφοριών σε αρμόδιες αρχές και αυτορρυθμιζόμενους φορείς όταν αυτό είναι απαραίτητο για την άσκηση εποπτικών αρμοδιοτήτων ή για τη δίωξη εγκλημάτων που σχετίζονται με τη νομιμοποίηση εσόδων και τη χρηματοδότηση της τρομοκρατίας. Επιπλέον, επιτρέπεται η γνωστοποίηση μεταξύ υπόχρεων οντοτήτων που ανήκουν στον ίδιο όμιλο ή μεταξύ υποκαταστημάτων και θυγατρικών σε τρίτες χώρες, εφόσον πληρούνται συγκεκριμένες προϋποθέσεις, όπως η συμμόρφωση με τις πολιτικές και διαδικασίες του ομίλου. Εκ παραλλήλου, ακολουθώντας το πνεύμα της οδηγίας 2015/849, προβλέπεται ότι η αναφορά ύποπτων συναλλαγών στην ΜΧΠ), συμπεριλαμβανομένων των περιπτώσεων απόπειρας συναλλαγών, δεν παραβιάζει

¹⁴⁵ Γιαννακίδου Χ, 2023

¹⁴⁶ Γνωμοδότηση ΕΕΠΔ της 04.07.2013 C 32 σελ.9

¹⁴⁷ ΕΕ C 32

καμία απαγόρευση γνωστοποίησης και δεν συνεπάγεται νομική ευθύνη για την υπόχρη οντότητα ή τους υπαλλήλους της.¹⁴⁸

4.3. Το δικαίωμα πρόσβασης

Σημαντική πτυχή του οπλοστασίου των υποκειμένων των δεδομένων, αποτελεί το δικαίωμα πρόσβασης το οποίο επιτρέπει στα υποκείμενα των δεδομένων να ενημερώνονται σχετικά με το αν τα προσωπικά τους δεδομένα υπόκεινται σε επεξεργασία καθώς και να λαμβάνουν αντίγραφο αυτών των δεδομένων αλλά και πληροφορίες σχετικά με τον επιδιωκόμενο σκοπό της επεξεργασίας τους¹⁴⁹. Εντούτοις, αυτό το δικαίωμα μπορεί να δεχθεί σημαντικούς περιορισμούς στο πλαίσιο των προσπαθειών ΚΕΤ/ΧΤ.

Πιο συγκεκριμένα, στην Τέταρτη Οδηγία, υπήρχε ήδη αναφορά για περιορισμό του δικαιώματος πρόσβασης των υποκειμένων στα δεδομένα τους, σε περιπτώσεις κατά την οποία η γνωστοποίηση των πληροφοριών θα καθιστούσε δυνατή την υπονόμηση των ερευνών για την αντιμετώπιση του ξεπλύματος χρήματος. Μάλιστα, το άρθρο 39 της ως άνω Οδηγίας προέβλεπε ότι τα κράτη μέλη είχαν την δυνατότητα να θεσπίσουν νομοθετικά μέτρα για τον περιορισμό ή και τον αποκλεισμό του δικαιώματος πρόσβασης στα δεδομένα προσωπικού χαρακτήρα,

¹⁴⁸ Άρθρο 73 Κανονισμού

¹⁴⁹ Τα φυσικά πρόσωπα, ως υποκείμενα των δεδομένων, έχουν το δικαίωμα να ζητούν και να λαμβάνουν επιβεβαίωση σχετικά με το αν τα δεδομένα τους υπόκεινται σε επεξεργασία, αντίγραφο των δεδομένων τους, καθώς και πληροφορίες για την επεξεργασία τους, όπως προβλέπεται από τα άρθρα 12 και 15 του ΓΚΠΔ. Το δικαίωμα πρόσβασης επιτρέπει στο υποκείμενο των δεδομένων να ενημερώνεται για τα προσωπικά του δεδομένα και για τις σχετικές πληροφορίες επεξεργασίας, προκειμένου να μπορεί να ελέγχει τη νομιμότητα της διαδικασίας, χωρίς να χρειάζεται να αιτιολογήσει το αίτημά του. Στο πλαίσιο άσκησης του δικαιώματος πρόσβασης, ο υπεύθυνος επεξεργασίας οφείλει να παρέχει στο υποκείμενο των δεδομένων πληροφορίες που περιλαμβάνουν: τους σκοπούς της επεξεργασίας, τις κατηγορίες των δεδομένων που επεξεργάζονται, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων, εφόσον είναι δυνατόν τη χρονική διάρκεια διατήρησης των δεδομένων ή, αν αυτό δεν είναι εφικτό, τα κριτήρια που καθορίζουν τη διάρκεια αυτή. Επιπλέον, περιλαμβάνονται πληροφορίες για τα δικαιώματα του υποκειμένου των δεδομένων, την προέλευση των δεδομένων, όταν δεν έχουν συλλεχθεί απευθείας από αυτό, καθώς και για την ύπαρξη αυτοματοποιημένων αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, με σημαντικές πληροφορίες για τη λογική, τη σημασία και τις πιθανές συνέπειες της επεξεργασίας αυτής. Πηγή: ΑΠΔΠΧ <https://www.dpa.gr/el/polites/gkpd/dikaiwma-prosvasis-upokeimenou>

προκειμένου να διασφαλιστεί η αποτελεσματικότητα των ερευνών και να περιοριστεί ο κίνδυνος επηρεασμού τους.

Υπό αυτό το πρίσμα, το ΕΣΠΑ είχε αιτηθεί την επανεξέταση της σχέσης μεταξύ των μέτρων για την ΚΕΤ/ΧΤ και των δικαιωμάτων στην ιδιωτική ζωή και την προστασία των δεδομένων. Έκρινε ότι τα μέτρα αυτά πρέπει να συμμορφώνονται με τα θεμελιώδη δικαιώματα που διασφαλίζονται στα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, καθώς και με τις αρχές της αναγκαιότητας και της αναλογικότητας σε μια δημοκρατική κοινωνία, όπως αυτές έχουν ερμηνευτεί από τη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης. Σε αυτό το πλαίσιο, τόνιζε ότι είναι κρίσιμο να διασφαλιστεί ότι τα δεδομένα που συλλέγονται είναι ακριβή και σχετίζονται άμεσα με τους σκοπούς της επεξεργασίας.

Με την εισαγωγή του νέου Κανονισμού, η απαγόρευση πρόσβασης των υποκειμένων στα δεδομένα τους, παραμένει σε ισχύ και φαίνεται πως ενισχύεται περαιτέρω. Ο Κανονισμός, διατηρεί την απαγόρευση πρόσβασης σε πληροφορίες που σχετίζονται με ύποπτες συναλλαγές, προκειμένου να προστατευθεί η αποτελεσματικότητα των μέτρων κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας. Η σκέψη 157 του Κανονισμού επιβεβαιώνει ότι, παρόλο που το δικαίωμα πρόσβασης στα προσωπικά δεδομένα είναι θεμελιώδες, μπορεί να περιοριστεί ή να αποκλειστεί σε περιπτώσεις που η πρόσβαση των υποκειμένων, θα έθετε σε κίνδυνο τις έρευνες.

Πιο συγκεκριμένα, υποστηρίζεται ότι η πρόσβαση του υποκειμένου των δεδομένων σε οποιεσδήποτε πληροφορίες σχετίζονται με αναφορά ύποπτης συναλλαγής θα υπονόμειυε σοβαρά την αποτελεσματικότητα της ΚΕΤ/ΧΤ. Επομένως μπορούν να δικαιολογηθούν εξαιρέσεις και περιορισμοί του δικαιώματος αυτού σύμφωνα με το άρθρο 23 του κανονισμού ΓΚΠΔ, κατά περίπτωση, το άρθρο 25 του κανονισμού (ΕΕ) 2018/1725.¹⁵⁰ Το υποκείμενο των δεδομένων έχει το δικαίωμα να

¹⁵⁰ Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού

ζητήσει τον έλεγχο της νομιμότητας της επεξεργασίας από εποπτική αρχή όπως αναφέρεται στο άρθρο 51 του ΓΚΠΔ ή, κατά περίπτωση, από τον Ευρωπαϊκό Επόπτη Προστασίας Δεδομένων, καθώς και το δικαίωμα να προσφύγει ενώπιον δικαστηρίου όπως αναφέρεται στο άρθρο 79. Η εποπτική αρχή που αναφέρεται στο άρθρο 51 του κανονισμού ΓΚΠΔ, μπορεί επίσης να ενεργήσει αυτεπάγγελτα. Με την επιφύλαξη των περιορισμών στο δικαίωμα πρόσβασης, η εποπτική αρχή θα πρέπει να έχει τη δυνατότητα να ενημερώσει το υποκείμενο των δεδομένων ότι έχει διεξαγάγει όλες τις απαραίτητες επαληθεύσεις, καθώς και για το αποτέλεσμα ως προς τη νομιμότητα της σχετικής επεξεργασίας¹⁵¹

Τουτέστιν, σε αντίθεση με όσα ρητά προβλέπονται και κατοχυρώνονται στον ΓΚΠΔ, τα υποκείμενα των δεδομένων, δεν μπορούν να ασκήσουν το δικαίωμα πρόσβασης σε δεδομένα που τους αφορούν και σχετίζονται με αναφορές ύποπτων συναλλαγών, διότι αυτή η πρόσβαση θα μπορούσε να αποκαλύψει κρίσιμες πληροφορίες, να υπονομεύσει την προσπάθεια αντιμετώπισης οικονομικών εγκλημάτων και της τρομοκρατίας και να επηρεάσει τον συντονισμό των ενεργειών για την καταπολέμηση τους. Ο νέος Κανονισμός διατηρεί τη δυνατότητα για τις αρμόδιες αρχές να περιορίζουν ή να αποκλείουν πλήρως το δικαίωμα πρόσβασης, προσδοκώντας στην ακεραιότητα και την αποτελεσματικότητα των ερευνών.

Εντούτοις, ο Κανονισμός προβλέπει διαδικασίες για την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων, όπως η δυνατότητα να ζητήσουν τον έλεγχο της νομιμότητας της επεξεργασίας από εποπτική αρχή ή να προσφύγουν ενώπιον δικαστηρίου. Ωστόσο, ακόμη και αυτές οι διαδικασίες υπόκεινται στους ίδιους περιορισμούς, με την εποπτική αρχή να έχει το δικαίωμα να περιορίσει τις πληροφορίες που παρέχονται στα υποκείμενα, εφόσον αυτό είναι απαραίτητο για την προστασία των ερευνών.

χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ

¹⁵¹ Αιτιολογική Σκέψη 157 Κανονισμού

Στο πνεύμα αυτό, ο ΕΕΠΔ το 2021 τόνισε τις ελλείψεις της προταθείσας τότε διάταξης, τονίζοντας ότι το υποκειμένο των δεδομένων πρέπει να αναγράφεται ρητά ότι έχει δικαίωμα πραγματικής δικαστικής προσφυγής σύμφωνα με το άρθρο 78 του ΓΚΠΔ, καθώς και το δικαίωμα να ασκήσει να δικαστική προσφυγή κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία σύμφωνα με Άρθρο 79 του ΓΚΠΔ

Η απαγόρευση πρόσβασης των υποκειμένων στα δεδομένα τους, σε συνδυασμό με την απαγόρευση ενημέρωσης και τις ευρείες εξουσίες που έχουν οι ελεγκτικές αρχές για την πρόσβαση και ανταλλαγή δεδομένων, είχε προκαλέσει σοβαρούς προβληματισμούς στην Ομάδα Εργασίας του άρθρου 29.¹⁵² Η Ομάδα αυτή εξέφρασε ανησυχίες σχετικά με την πιθανότητα παράνομης επεξεργασίας προσωπικών δεδομένων, επισημαίνοντας ότι η κατάσταση αυτή μπορεί να οδηγήσει σε εκτεταμένη και μαζική επεξεργασία δεδομένων προσωπικού χαρακτήρα. Μάλιστα, τόνισε ότι αυτές οι πρακτικές δεν περιορίζονται σε τυπικές αστυνομικές έρευνες, όπου η επεξεργασία δεδομένων πραγματοποιείται στο πλαίσιο ειδικών και στοχευμένων ερευνών. Αντίθετα, φαίνεται ότι σημειώνεται ένα σημαντικό άλμα στην έκταση και την ένταση της επεξεργασίας προσωπικών δεδομένων, αυξάνοντας τον κίνδυνο παραβιάσεων. Αυτός ο κίνδυνος επιτείνεται από την έλλειψη κατάλληλων ελέγχων που θα μπορούσαν να περιορίσουν αυτές τις απειλές σε αποδεκτά επίπεδα, όπως προβλέπεται από τον ΓΚΠΔ.¹⁵³

Για να αντιμετωπιστούν αυτοί οι κίνδυνοι, η Ομάδα Εργασίας υπογράμμισε την ανάγκη για ενισχυμένους ελέγχους που να καλύπτουν τόσο την προληπτική όσο και την επακόλουθη φάση της επεξεργασίας δεδομένων. Αυτοί οι έλεγχοι περιλαμβάνουν έναν προληπτικό έλεγχο (εκ των προτέρων) που καθορίζει τη νομική βάση, τους στόχους και τη στρατηγική της επεξεργασίας, καθώς και τις απαραίτητες διασφαλίσεις για να διασφαλιστεί ότι τα δεδομένα δεν θα χρησιμοποιηθούν για άλλους σκοπούς. ¹⁵⁴Επιπλέον, οι προληπτικοί έλεγχοι πρέπει να συμπληρώνονται

¹⁵² Γιαννακίδου,2023

¹⁵³ WP29,Falque-Pierrotin,2016

¹⁵⁴ Ο,π. Γιαννακίδου 2023

από συνεχείς ελέγχους ασφαλείας, αυτοαξιολόγηση και εποπτικούς ελέγχους από τις αρμόδιες εποπτικές αρχές.¹⁵⁵

¹⁵⁵ Σχετικά με τα δικαιώματα των υποκειμένων για διόρθωση, διαγραφή και φορητότητα των προσωπικών τους δεδομένων, στο ισχύον νομοθετικό πλαίσιο δεν προκύπτει σχετική πρόβλεψη. Οι περιορισμοί αυτοί εφαρμόζονται κατ' εφαρμογήν του άρθρου 23 του ΓΚΠΔ, όπου η ενημέρωση του υποκειμένου για την επεξεργασία των δεδομένων του μπορεί να απαγορευτεί στο πλαίσιο της πρόληψης της νομιμοποίησης εσόδων και της χρηματοδότησης τρομοκρατικών ενεργειών. Ελλείψει ενημέρωσης, το υποκείμενο δεν έχει τη δυνατότητα να γνωρίζει, ώστε να ασκήσει δικαιώματα διόρθωσης ή διαγραφής. Γιαννακίδου, 2023

ΚΕΦΑΛΑΙΟ 5:

ΔΙΑΣΥΝΟΡΙΑΚΕΣ ΜΕΤΑΦΟΡΕΣ ΔΕΔΟΜΕΝΩΝ

Η διασφάλιση της προστασίας προσωπικών δεδομένων κατά τη διαβίβαση σε τρίτες χώρες αποτελεί θεμελιώδες ζήτημα στο πλαίσιο της Ευρωπαϊκής Ένωσης, ιδίως όταν πρόκειται για διακρατικές ανταλλαγές δεδομένων για φορολογικούς σκοπούς και για την ΚΕΤ/ΧΤ. Οι αυστηροί κανονισμοί και οι διατάξεις που έχουν θεσπιστεί σε επίπεδο ΕΕ, διασφαλίζουν ότι τα προσωπικά δεδομένα των υποκειμένων προστατεύονται ανεξάρτητα από το που μεταφέρονται. Ωστόσο, η αποτελεσματικότητα αυτών των διατάξεων εξαρτάται από την ικανότητα εφαρμογής τους σε τρίτες χώρες, όπου οι νόμοι περί προστασίας δεδομένων μπορεί να είναι λιγότερο αυστηροί ή ανύπαρκτοι.¹⁵⁶

5.1. Το Νομικό Πλαίσιο για τις Διαβιβάσεις Δεδομένων

Αναφορικά με την προστασία των δεδομένων των υποκειμένων, σημαντικό ζήτημα που έχει απασχολήσει πολλάκις τον νομικό κόσμο, αποτελεί η περίπτωση της διαβίβασης των δεδομένων. Ο ΓΚΠΔ ορίζει ότι οι διαβιβάσεις δεδομένων σε τρίτες χώρες επιτρέπονται μόνο όταν υπάρχει απόφαση επάρκειας της Ευρωπαϊκής Επιτροπής¹⁵⁷. Εάν δεν υπάρχει τέτοια απόφαση, οι διαβιβάσεις επιτρέπονται μόνο εάν έχουν ληφθεί κατάλληλες εγγυήσεις, όπως τυποποιημένες συμβατικές ρήτρες ή δεσμευτικοί εταιρικοί κανόνες¹⁵⁸. Σε ορισμένες περιπτώσεις, η διαβίβαση μπορεί να πραγματοποιηθεί χωρίς απόφαση επάρκειας ή κατάλληλες εγγυήσεις, όπως όταν υπάρχει ρητή συγκατάθεση του υποκειμένου των δεδομένων ή όταν η διαβίβαση είναι απαραίτητη για σημαντικούς λόγους δημόσιου συμφέροντος^{159, 160}.

¹⁵⁶ (Βλαχόπουλος, 2018), σελ. 27

¹⁵⁷ Άρθρο 45 του ΓΚΠΔ

¹⁵⁸ Άρθρο 46 του ΓΚΠΔ

¹⁵⁹ Άρθρο 49 του ΓΚΠΔ

¹⁶⁰ Η εκσυγχρονισμένη Σύμβαση 108 του Συμβουλίου της Ευρώπης αποτελεί το θεμέλιο για τις διασυνοριακές μεταφορές δεδομένων. Προβλέπει ότι τα κράτη μέλη που είναι συμβαλλόμενα μέρη της Σύμβασης δεν πρέπει να απαγορεύουν ή να υποβάλλουν σε ειδική άδεια τη μεταφορά προσωπικών

Στην υπόθεση Schrems I¹⁶¹, το ΔΕΕ ακύρωσε τις αρχές του Safe Harbour, που ρύθμιζαν τις μεταφορές δεδομένων από την ΕΕ προς τις ΗΠΑ, λόγω ανεπάρκειας των προστατευτικών μηχανισμών που παρείχε η συμφωνία αυτή. Το ΔΕΕ θεώρησε απαραίτητο τα άτομα, των οποίων τα προσωπικά δεδομένα έχουν μεταφερθεί ή μπορεί να μεταφερθούν σε τρίτη χώρα, να έχουν το δικαίωμα να προσφύγουν στις εθνικές αρχές προστασίας δεδομένων. Αυτό είναι κρίσιμο, ειδικά όταν οι νόμοι και οι πρακτικές της τρίτης χώρας δεν εξασφαλίζουν επαρκές επίπεδο προστασίας. Το ΔΕΕ τόνισε ότι η πρόσβαση σε δεδομένα από δημόσιες αρχές πρέπει να είναι αυστηρά απαραίτητη και αναλογική για την προστασία της εθνικής ασφάλειας, ενώ η γενικευμένη πρόσβαση υπονομεύει το θεμελιώδες δικαίωμα στην ιδιωτική ζωή.

Μετά την υπόθεση Schrems I, η ΕΕ και οι ΗΠΑ συμφώνησαν σε μια νέα συμφωνία για τη μεταφορά δεδομένων, γνωστή ως Privacy Shield. Ωστόσο, το ΔΕΕ ακύρωσε και αυτή τη συμφωνία στην υπόθεση Schrems II¹⁶², επισημαίνοντας την προτεραιότητα που δίνει η νομοθεσία των ΗΠΑ στις απαιτήσεις εθνικής ασφάλειας έναντι της προστασίας προσωπικών δεδομένων, την έλλειψη επαρκών περιορισμών και διασφαλίσεων και την απουσία αποτελεσματικής νομικής προστασίας για τους πολίτες της ΕΕ.¹⁶³

Οι αποφάσεις Schrems I και II έχουν σημαντικές επιπτώσεις για τη μεταφορά προσωπικών δεδομένων από την ΕΕ σε τρίτες χώρες, θέτοντας ερωτήματα για τη συμμόρφωση των διακρατικών ανταλλαγών δεδομένων με τα πρότυπα προστασίας της ΕΕ. Οι διασφαλίσεις που καθιέρωσε το ΔΕΕ αναδεικνύουν την ανάγκη για

δεδομένων σε έναν παραλήπτη που βρίσκεται υπό τη δικαιοδοσία άλλου συμβαλλόμενου μέρους. Ωστόσο, αν υπάρχει πραγματικός και σοβαρός κίνδυνος ότι η περαιτέρω μεταφορά θα οδηγήσει σε παράκαμψη των διατάξεων της Σύμβασης, μπορεί να δικαιολογηθεί εξαίρεση. Όσον αφορά τις διασυνοριακές μεταφορές δεδομένων σε παραλήπτες εκτός των χωρών που είναι μέρη της Σύμβασης 108+, η μεταφορά επιτρέπεται μόνο όταν διασφαλίζεται κατάλληλο επίπεδο προστασίας. Αυτό μπορεί να εξασφαλιστεί μέσω της νομοθεσίας της χώρας παραλήπτη ή μέσω *ad hoc* ή εγκεκριμένων τυποποιημένων εγγυήσεων.

¹⁶¹ Δ.Ε.Ε., C-362/14 (Grand Chamber), *Maximillian Schrems v. Data Protection Commissioner*, 6.10.2015, διαθέσιμη σε: <https://curia.europa.eu/juris/liste.jsf?num=C-362/14>.

¹⁶² Δ.Ε.Ε., C-311/18 (Grand Chamber), *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, 16.7.2020, διαθέσιμη σε: <https://curia.europa.eu/juris/liste.jsf?num=C-311/18>.

¹⁶³ Παναγοπούλου, Παπακωνσταντίνου

πρόσθετες εγγυήσεις όταν πραγματοποιούνται διακρατικές ανταλλαγές δεδομένων, ειδικά στον τομέα της φορολογίας και της ΚΕΤ/ΧΤ.

Μετά την απόφαση Schrems II, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων εξέδωσε τις συστάσεις 1/2020 και 2/2020. Οι συστάσεις αυτές παρέχουν κατευθυντήριες γραμμές για τη συμπλήρωση των εργαλείων μεταφοράς δεδομένων, εξασφαλίζοντας ότι οι μεταφορές αυτές συμμορφώνονται με τα επίπεδα προστασίας που απαιτεί η ΕΕ. Περιλαμβάνουν τεχνικά, συμβατικά και οργανωτικά μέτρα που πρέπει να ληφθούν υπόψη όταν οι ξένες προστασίες κρίνονται ανεπαρκείς σε σύγκριση με τα ευρωπαϊκά πρότυπα. Το ΕΣΠΔ τόνισε τη σημασία των "Ευρωπαϊκών Βασικών Εγγυήσεων"¹⁶⁴, επισημαίνοντας ότι η επεξεργασία θα πρέπει να βασίζεται σε σαφείς, ακριβείς και προσβάσιμους κανόνες, ενώ θα πρέπει να αποδεικνύεται η αναγκαιότητα και η αναλογικότητα ως προς τους θεμιτούς επιδιωκόμενους στόχους, σε συνδυασμό με έναν ανεξάρτητο μηχανισμό εποπτείας, διασφαλίζοντας ότι τα μέσα προσφυγής είναι διαθέσιμα και αποτελεσματικά.¹⁶⁵

5.2 Το ισχύον νομοθετικό πλαίσιο

Σύμφωνα με το μέχρι ισχύον νομοθετικό πλαίσιο, η Τέταρτη Οδηγία 2015/849, περιλάμβανε σημαντικές διατάξεις που ρύθμιζαν τη διαβίβαση δεδομένων και πληροφοριών, όπως των ΜΧΠ σε τρίτες χώρες.¹⁶⁶

Σύμφωνα με το Άρθρο 45 της εν λόγω Οδηγίας, η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες επιτρεπόταν μόνο εφόσον η τρίτη χώρα παρείχε ένα επαρκές επίπεδο προστασίας των δεδομένων, όπως αυτό εκτιμάτο από την Ευρωπαϊκή Επιτροπή. Εάν δεν υπήρχε απόφαση επάρκειας, η διαβίβαση

¹⁶⁴ Kosta, 2021

¹⁶⁵ ΕΣΠΔ, 2020

¹⁶⁶ Στις 7 Μαΐου 2020, η Ευρωπαϊκή Επιτροπή ενέκρινε τον νέο κατ'εξουσιοδότηση Κανονισμό αριθ. 2020/855284 (όπως τροποποίησε τον κατ'εξουσιοδότηση Κανονισμό (ΕΕ) αριθ. 2016/1675) σε σχέση με τρίτες χώρες που έχουν στρατηγικές ελλείψεις στα καθεστώτα τους για την καταπολέμηση των ML/FT, και που αποτελούν σημαντικές απειλές για το χρηματοπιστωτικό σύστημα της Ένωσης. Ο προσδιορισμός τρίτων χωρών υψηλού κινδύνου αποτελεί νομική απαίτηση που απορρέει από το άρθρο 9 της 4^{ης} Οδηγίας, και αποσκοπεί στην προστασία του χρηματοπιστωτικού συστήματος της Ένωσης και την ορθή λειτουργία της εσωτερικής αγοράς

μπορούσε να γίνει κατόπιν παροχής κατάλληλων εγγυήσεων , όπως δεσμευτικοί εταιρικοί κανόνες ή τυποποιημένες συμβατικές ρήτρες που είχαν εγκριθεί από την Επιτροπή. Εξαιρέσεις προβλέπονταν για συγκεκριμένες περιπτώσεις, όπως όταν το υποκείμενο των δεδομένων είχε δώσει τη ρητή συγκατάθεσή του ή όταν η διαβίβαση ήταν απαραίτητη για την εκτέλεση ενός συμβολαίου.

Επιπλέον, το Άρθρο 53 προέβλεπε ότι τα κράτη μέλη και οι αρμόδιες αρχές τους μπορούσαν να συνεργάζονται με τις αρχές τρίτων χωρών για την ανταλλαγή πληροφοριών που ήταν απαραίτητες για την ΚΕΤ/ΧΤ συμπεριλαμβανομένων των ΜΧΠ. Αυτή η συνεργασία ,έπρεπε να βασίζεται σε συμφωνίες που διασφάλιζαν την προστασία των δεδομένων και την εμπιστευτικότητα και η διαβίβαση επιτρεπόταν μόνο εφόσον η τρίτη χώρα παρείχε επαρκές επίπεδο προστασίας των δεδομένων.

Το άρθρο 56 ενίσχυε τη σημασία της εμπιστευτικότητας κατά την ανταλλαγή πληροφοριών, αναφέροντας ότι οι πληροφορίες που διαβιβάζονταν έπρεπε να χρησιμοποιούνται μόνο για τους σκοπούς για τους οποίους διαβιβάστηκαν και ότι οποιαδήποτε περαιτέρω χρήση τους απαιτούσε τη συγκατάθεση της αρχής που παρείχε τις πληροφορίες. Ενώ, σύμφωνα με το Άρθρο 47, τα κράτη μέλη ήταν υποχρεωμένα να διασφαλίζουν ότι οι αρμόδιες αρχές τους είχαν την εξουσία να επιβλέπουν τη συμμόρφωση με τις διατάξεις για τη διαβίβαση δεδομένων σε τρίτες χώρες και να επιβάλλουν κυρώσεις σε περίπτωση παραβίασης αυτών των κανόνων.

Σύμφωνα με την Τέταρτη Οδηγία, η Ευρωπαϊκή Επιτροπή, καθίστατο υπεύθυνη για τον εντοπισμό τρίτων χωρών υψηλού κινδύνου με στρατηγικές ελλείψεις στα καθεστώτα ΚΕΤ/ΧΤ.Επιπλέον, όπως ορίζεται στο άρθρο 18^α της Οδηγίας (ΕΕ) 2018/843 απαιτείται από τις τράπεζες και άλλα χρηματοπιστωτικά ιδρύματα να επιδεικνύουν αυξημένη επαγρύπνηση όταν συναλλάσσονται με τρίτες χώρες υψηλού κινδύνου.¹⁶⁷

¹⁶⁷ (Commission) *Anti-money laundering and countering the financing of terrorism at international level*

Η τελευταία έκδοση της λίστας τρίτων χωρών υψηλού κινδύνου δημοσιεύτηκε στις 12 Δεκεμβρίου 2023, η Ευρωπαϊκή Επιτροπή εξέδωσε νέο κατ' εξουσιοδότηση κανονισμό¹⁶⁸ σε σχέση με τρίτες χώρες που έχουν στρατηγικές ελλείψεις στα καθεστώτα καταπολέμησης του ΚΕΧ/ΧΤ. Ο κατ' εξουσιοδότηση κανονισμός τροποποιεί τον κατ' εξουσιοδότηση κανονισμό (ΕΕ) 2016/1675.

5.3 Το νέο Νομοθετικό Πλαίσιο

Η Ευρωπαϊκή Ένωση, προχωράει σε αναθεώρηση της προσέγγισής της για την αντιμετώπιση των απειλών που προέρχονται από τρίτες χώρες στον τομέα της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας. Ο νέος Κανονισμός 2024/1624 και οι συνοδευτικές πολιτικές του AML Package, έχουν ως στόχο να εξασφαλίσουν μια εναρμονισμένη και αναλογική αντιμετώπιση των κινδύνων αυτών, λαμβάνοντας υπόψη τόσο τους καταλόγους της FATF όσο και αυτόνομες αξιολογήσεις από την ίδια την Επιτροπή.¹⁶⁹

Σύμφωνα με τον νέο Κανονισμό ο όρος «τρίτη χώρα» αναφέρεται σε κάθε δικαιοδοσία, ανεξάρτητο κράτος ή αυτόνομο έδαφος που δεν αποτελεί μέρος της Ευρωπαϊκής Ένωσης και διαθέτει δική του νομοθεσία ή δικό του σύστημα επιβολής για την ΚΕΤ/ΧΤ.

Η Ευρωπαϊκή Επιτροπή προτείνει μια αναθεωρημένη πολιτική που βασίζεται στη διαμόρφωση δύο κατηγοριών χωρών, στενά ευθυγραμμισμένων με τις κατηγορίες της FATF, αλλά και εμπλουτισμένη με αυτόνομες αξιολογήσεις της ΕΕ. Οι χώρες αυτές θα υπόκεινται σε διαφορετικά επίπεδα ελέγχου και αντίμετρων, ανάλογα με τον κίνδυνο που ενέχουν για το χρηματοπιστωτικό σύστημα της Ένωσης.

¹⁶⁸ Κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2024/163 της Επιτροπής, της 12ης Δεκεμβρίου 2023, για την τροποποίηση του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2016/1675 όσον αφορά τη διαγραφή των Νήσων Κέιμαν και της Ιορδανίας από τον πίνακα του σημείου I του παραρτήματος C/2023/8595 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R0163>

¹⁶⁹ (Επιτροπή Ε., 2021)

1. Μαύρη Λίστα: Περιλαμβάνει τρίτες χώρες που παρουσιάζουν σοβαρές στρατηγικές ελλείψεις στο πλαίσιο της αντιμετώπισης του ξεπλύματος χρήματος και έχουν χαρακτηριστεί ως «υπόκεινται σε πρόσκληση για ανάληψη δράσης» από την FATF. Για αυτές τις χώρες, εφαρμόζονται όλα τα ενισχυμένα μέτρα δέουσας επιμέλειας και επιβάλλονται ειδικά ανά χώρα αντίμετρα για τη μείωση των σχετικών κινδύνων .
2. Γκριζα Λίστα: Αυτή η λίστα περιλαμβάνει χώρες με αδυναμίες συμμόρφωσης στο πλαίσιο της αντιμετώπισης του ξεπλύματος χρήματος οι οποίες έχουν χαρακτηριστεί ως «υποκείμενες σε αυξημένη παρακολούθηση» από την FATF. Οι χώρες αυτές υπόκεινται σε ειδικά ανά χώρα ενισχυμένα μέτρα δέουσας επιμέλειας, προσαρμοσμένα στον βαθμό κινδύνου .¹⁷⁰

Η Ευρωπαϊκή Επιτροπή έχει τη δυνατότητα να προσθέτει τρίτες χώρες στις παραπάνω λίστες, ακόμα και αν δεν περιλαμβάνονται στους καταλόγους της FATF, εφόσον αυτές συνιστούν ειδική απειλή για το χρηματοπιστωτικό σύστημα της ΕΕ και οι οποίες, βάσει της απειλής αυτής, θα υπόκεινται είτε σε ειδικά ανά χώρα ενισχυμένα μέτρα δέουσας επιμέλειας είτε, κατά περίπτωση, σε όλα τα ενισχυμένα μέτρα δέουσας επιμέλειας και σε αντίμετρα. Κατά την εκτίμηση του επιπέδου της απειλής που προέρχεται από τις εν λόγω τρίτες χώρες, η Επιτροπή μπορεί να βασίζεται στην τεχνική εμπειρογνωσία της ΑΚΝΕΔΑΠ.¹⁷¹

Πιο συγκεκριμένα, σύμφωνα με την αιτιολογική σκέψη 46 του Κανονισμού, οι υπόχρεες οντότητες υποχρεούνται να εφαρμόζουν τα ως άνω πρότυπα ή να ενημερώνουν τις αρμόδιες αρχές εάν δεν είναι δυνατή η συμμόρφωση. Ιδιαίτερα, όταν υποκαταστήματα ή θυγατρικές των υπόχρεων οντοτήτων δραστηροποιούνται σε τρίτες χώρες με λιγότερο αυστηρές απαιτήσεις από τα ευρωπαϊκά πρότυπα.

¹⁷⁰ (Επιτροπή Ε. , 2021)

¹⁷¹ AML Package II: Commission Proposes AML Regulation

<https://eucrim.eu/news/aml-package-ii-commission-proposes-aml-regulation/>

Αξίζει να τονιστεί ότι η αιτιολογική σκέψη 167 του Κανονισμού δίνει στην Ευρωπαϊκή Επιτροπή την εξουσία έκδοσης πράξεων σύμφωνα με το άρθρο 290 της ΣΛΕΕ προκειμένου να προσδιορίζει τρίτες χώρες υψηλού κινδύνου, τρίτες χώρες με ανεπάρκειες ως προς την συμμόρφωση και τρίτες χώρες που συνιστούν συγκεκριμένη και σοβαρή απειλή για το χρηματοπιστωτικό σύστημα της Ένωσης και να επιβάλλει κατάλληλα αντίμετρα για τη διασφάλιση της προστασίας των δεδομένων. Ενώ η αμέσως επόμενη αιτιολογική σκέψη επιτρέπει στην Ευρωπαϊκή Επιτροπή να εγκρίνει ρυθμιστικά τεχνικά πρότυπα που καταρτίζονται από την ΑΚΝΕΔΑΠ. Αυτά τα πρότυπα καθορίζουν τις ελάχιστες απαιτήσεις όσον αφορά τις πολιτικές, τις διαδικασίες και τους ελέγχους σε επίπεδο ομίλου, καθώς και τα μέτρα που πρέπει να λαμβάνονται όταν η νομοθεσία τρίτων χωρών δεν επιτρέπει την εφαρμογή αυτών των πολιτικών.¹⁷²

Ακόμη, ο Κανονισμός αναφέρεται στις τρίτες χώρες που έχουν αναγνωριστεί από διεθνείς οργανισμούς, όπως η FATF, ως χώρες με σημαντικές στρατηγικές ανεπάρκειες στα πλαίσια της αντιμετώπισης του ξεπλύματος χρήματος. Οι χώρες αυτές, ενέχουν υψηλό κίνδυνο για το χρηματοπιστωτικό σύστημα της ΕΕ, καθώς οι ανεπαρκείς πολιτικές τους, μπορούν να αποτελέσουν γόνιμο πεδίο δράσης για επίδοξους εγκληματίες. Σε αυτές τις περιπτώσεις, οι υπόχρεες οντότητες στην ΕΕ πρέπει να εφαρμόζουν αυξημένα μέτρα δέουσας επιμέλειας και, όπου απαιτείται, πρόσθετα ειδικά αντίμετρα, ώστε να μετριάσουν τους σχετικούς κινδύνους.¹⁷³

Εκ παραλλήλου, στην αιτιολογική σκέψη 85, τονίζεται η ανάγκη για προσαρμοσμένα μέτρα στις τρίτες χώρες που υπόκεινται σε αυξημένη παρακολούθηση από τη FATF. Ενώ οι χώρες αυτές έχουν δεσμευτεί να βελτιώσουν τα συστήματά τους, οι υφιστάμενες αδυναμίες τους εξακολουθούν να αποτελούν κίνδυνο για το χρηματοπιστωτικό σύστημα της ΕΕ. Ως εκ τούτου, τα μέτρα δέουσας επιμέλειας που εφαρμόζουν οι υπόχρεες οντότητες θα πρέπει να είναι αναλογικά και

¹⁷² Αιτιολογική σκέψη 167 του Κανονισμού

¹⁷³ Αιτιολογική σκέψη 83 Κανονισμού

προσαρμοσμένα στις συγκεκριμένες αδυναμίες της κάθε χώρας. Ενώ, στις περιπτώσεις όπου τρίτες χώρες, που δεν έχουν δημόσια αναγνωριστεί ως αποδέκτες πρόσκλησης για ανάληψη δράσης ή αυξημένης παρακολούθησης, μπορεί να αποτελούν συγκεκριμένη και σοβαρή απειλή για το χρηματοπιστωτικό σύστημα της ΕΕ. Σε αυτές τις περιπτώσεις, η Ευρωπαϊκή Επιτροπή πρέπει να έχει τη δυνατότητα να αναλαμβάνει δράση σε εξαιρετικές περιστάσεις, προσδιορίζοντας αυτές τις χώρες και λαμβάνοντας τα αναγκαία μέτρα. Ενώ, επισημαίνεται η σημασία της συνεχούς αναθεώρησης των μέτρων αυξημένης δέουσας επιμέλειας που εφαρμόζονται στις τρίτες χώρες. Καθώς οι συνθήκες σε αυτές τις χώρες ενδέχεται να αλλάξουν, η Επιτροπή πρέπει να προσαρμόζει τα μέτρα για να διασφαλίζει ότι παραμένουν αναλογικά και αποτελεσματικά. Η τακτική επανεξέταση και προσαρμογή αυτών των μέτρων είναι απαραίτητη για να αντιμετωπίζονται οι μεταβαλλόμενοι κίνδυνοι που προκύπτουν από τις εξελίξεις στα πλαίσια της αντιμετώπισης του ξεπλύματος χρήματος των τρίτων χωρών.¹⁷⁴

Επιπροσθέτως, σύμφωνα με την Έκτη Οδηγία τα κράτη-μέλη υποχρεούνται να διασφαλίζουν ότι οι ΜΧΠ μπορούν να ανταλλάσσουν πληροφορίες με αντίστοιχες ΜΧΠ τρίτων χωρών, υπό συγκεκριμένες προϋποθέσεις και εγγυήσεις για την προστασία των προσωπικών δεδομένων. Η αιτιολογική σκέψη 75 της Οδηγίας τονίζει την ανάγκη ταχείας, εποικοδομητικής και αποτελεσματικής συνεργασίας, η οποία πρέπει να είναι σύμφωνη με τους κανόνες προστασίας δεδομένων και τις διεθνείς συστάσεις της Ομάδας Χρηματοοικονομικής Δράσης (FATF) και τις αρχές της ομάδας Egmont¹⁷⁵.

Επιπλέον, η αιτιολογική σκέψη 77 της Έκτης Οδηγίας καθορίζει τη χρήση ασφαλών διαύλων επικοινωνίας και την πλήρη κρυπτογράφηση των δεδομένων κατά την ανταλλαγή πληροφοριών μέσω του συστήματος FIU.net, που διαχειρίζεται

¹⁷⁴ Αιτιολογική σκέψη 88 του Κανονισμού

¹⁷⁵ Η Επιτροπή είναι παρατηρητής στον Όμιλο Egmont, έναν διεθνή οργανισμό που παρέχει στις μονάδες χρηματοοικονομικών πληροφοριών μια πλατφόρμα για την ασφαλή ανταλλαγή εμπειρογνωμοσύνης και χρηματοοικονομικών πληροφοριών για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, της χρηματοδότησης της τρομοκρατίας και των συναφών βασικών αδικημάτων.

ΑΚΝΕΠΑΔ. Αυτό το σύστημα επιτρέπει στις ΜΧΠ να συγκρίνουν δεδομένα με ψευδώνυμο τρόπο για τον εντοπισμό ύποπτων δραστηριοτήτων σε άλλα κράτη μέλη ή τρίτες χώρες, εξασφαλίζοντας ταυτόχρονα την προστασία των προσωπικών δεδομένων. Επιπλέον, η Οδηγία τονίζει τη σημασία της συνεργασίας μεταξύ των εποπτικών φορέων, ειδικά όταν εμπλέκονται τρίτες χώρες καθώς προβλέπει ότι οι εποπτικοί φορείς της Ένωσης πρέπει να αλληλοενημερώνονται και να συνεργάζονται για να εξασφαλίσουν την εφαρμογή των πολιτικών ΚΕΤ/ΧΤ. Οι διαβιβάσεις δεδομένων σε τρίτες χώρες πρέπει να συμμορφώνονται με τα ενωσιακά πρότυπα προστασίας δεδομένων, και οι χώρες που λαμβάνουν τα δεδομένα πρέπει να παρέχουν ισοδύναμες εγγυήσεις προστασίας.¹⁷⁶

Τέλος, σύμφωνα με την αιτιολογική σκέψη 76 της Οδηγίας, οι ΜΧΠ μπορούν να επιβάλουν περιορισμούς και όρους σχετικά με τη χρήση των πληροφοριών που διαβιβάζονται σε άλλες ΜΧΠ ή αρχές τρίτων χωρών. Η Οδηγία απαιτεί οι πληροφορίες να χρησιμοποιούνται μόνο για τους σκοπούς για τους οποίους ζητήθηκαν και παρέχονται, ενώ οποιαδήποτε περαιτέρω διάθεση των δεδομένων απαιτεί προηγούμενη συγκατάθεση από την αρχική ΜΧΠ.

Ως εκ τούτου, συμπεραίνουμε ότι με το νέο Νομοθετικό Πακέτο (AML Package) έχουν διανυθεί κάποια βήματα για την ενίσχυση της προστασίας των προσωπικών δεδομένων κατά τη διαβίβαση σε τρίτες χώρες, στον τομέα της ΚΕΤ/ΧΤ. Ωστόσο, η αποτελεσματικότητά του εξαρτάται από τη δυνατότητα επιβολής των διατάξεών του σε χώρες εκτός της ΕΕ, όπου τα νομικά πλαίσια ενδέχεται να είναι λιγότερο αυστηρά ή ανεπαρκή.

Μια σημαντική πρόκληση που ανακύπτει είναι η επιβολή των κανόνων αυτών σε διεθνές επίπεδο, ιδιαίτερα όταν τρίτες χώρες δεν διαθέτουν το ίδιο υψηλό επίπεδο προστασίας δεδομένων με την ΕΕ. Παρά την εφαρμογή πρόσθετων εγγυήσεων, όπως οι δεσμευτικοί εταιρικοί κανόνες και οι τυποποιημένες συμβατικές ρήτρες, η επιβολή

¹⁷⁶ Αιτιολογική σκέψη 123

αυτών των μέτρων εξαρτάται από την ικανότητα των χωρών αυτών να συμμορφωθούν με τα ευρωπαϊκά πρότυπα. Η ανησυχία αυτή γίνεται ακόμα πιο έντονη στις περιπτώσεις όπου τα κράτη με λιγότερο αυστηρούς νόμους επιτρέπουν ευρεία πρόσβαση στις προσωπικές πληροφορίες από τις αρχές τους, χωρίς επαρκείς μηχανισμούς εποπτείας ή δυνατότητα έννομης προστασίας για τους πολίτες της ΕΕ.

ΚΕΦΑΛΑΙΟ 6

Η ΥΠΟΘΕΣΗ ΤΟΥ ΠΡΑΓΜΑΤΙΚΟΥ ΔΙΚΑΙΟΥΧΟΥ

6.1. Εννοιολογική Προσέγγιση

Έχει υποστηριχθεί ότι οι εταιρικές οντότητες, μέσω του ιδιαίτερου νομικού καθεστώτος τους, είναι ευάλωτες σε παράνομες πρακτικές όπως η νομιμοποίηση εσόδων από παράνομες δραστηριότητες, η διαφθορά, η φορολογική απάτη και η χρηματοδότηση της τρομοκρατίας, λόγω της απόκρυψης των πραγματικών δικαιούχων τους¹⁷⁷. Η έλλειψη επαρκών, ακριβών και ενημερωμένων πληροφοριών για τους πραγματικούς δικαιούχους διευκολύνει τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας, αποκρύπτοντας την ταυτότητα γνωστών ή ύποπτων συναλλαγών, τον πραγματικό σκοπό ενός λογαριασμού ή περιουσιακού στοιχείου που κατέχεται από μια εταιρική οντότητα και την πηγή ή τη χρήση των κεφαλαίων ή των περιουσιακών στοιχείων που σχετίζονται με αυτή. Συχνά, οι επίδοξοι εγκληματίες χρησιμοποιούν αυτές τις οντότητες, για να αποκρύψουν την ταυτότητά τους και την προέλευση ή τον προορισμό των κεφαλαίων τους¹⁷⁸.

Η έννοια του πραγματικού δικαιούχου εισήχθη προκειμένου να αυξηθεί η διαφάνεια στο πλαίσιο πολύπλοκων εταιρικών δομών. Η ανάγκη για πρόσβαση σε ακριβείς, επικαιροποιημένες και επαρκείς πληροφορίες σχετικά με τον πραγματικό δικαιούχο αποτελεί καθοριστικό παράγοντα για τον εντοπισμό των εγκληματιών, οι οποίοι διαφορετικά θα μπορούσαν να αποκρύπτουν την ταυτότητά τους πίσω από ανάλογες αδιαφανείς δομές. Για τις ανάγκες της παρούσης θα περιοριστούμε στην γενική διατύπωση, ότι η κατοχή ιδιοκτησιακού δικαιώματος ίσου με το 25 % ή άνω

¹⁷⁷ Ειδικότερα, οι εταιρείες, τα καταπιστεύματα, τα ιδρύματα, οι περιορισμένες εταιρικές σχέσεις και οι υβριδικές επιχειρηματικές μορφές, όπως οι εταιρείες περιορισμένης ευθύνης (LLP) και οι εταιρείες περιορισμένης ευθύνης (LLC), είναι τα εταιρικά οχήματα που συνδέονται συχνότερα με τέτοιες ενέργειες

¹⁷⁸ FATF (2023)

των μετοχών ή των δικαιωμάτων ψήφου ή άλλου ιδιοκτησιακού δικαιώματος γενικά προσδιορίζει τον πραγματικό δικαιούχο μίας εταιρικής οντότητας.¹⁷⁹

Προκειμένου να αντιμετωπιστεί το παραπάνω, η FATF, προχώρησε στην διατύπωση των συστάσεων 24 και 25, καθιερώνοντας το πρώτο διεθνές πρότυπο του πραγματικού δικαιούχου το 2003, ορίζοντας τη διαφάνεια και την επαλήθευση των πληροφοριών για τους πραγματικούς δικαιούχους των νομικών οντοτήτων και επιβάλλοντας στις χώρες να διασφαλίζουν ότι οι αρμόδιες αρχές έχουν πρόσβαση σε ακριβείς και ενημερωμένες πληροφορίες σχετικά με τους πραγματικούς δικαιούχους.¹⁸⁰

Τον δρόμο αυτό ακολούθησε και Ευρωπαϊκή Ένωση, και ο όρος «πραγματικός δικαιούχος» εισήχθη με την οδηγία 2005/60/EK.¹⁸¹ Ωστόσο, πλήρη εφαρμογή άρχισε να αποκτά με την Τέταρτη Οδηγία με την οποία ο προσδιορισμός του πραγματικού δικαιούχου έχει καταστεί ένα από τα υποχρεωτικά μέτρα δέουσας επιμέλειας που εφαρμόζονται από τις υπόχρεες οντότητες, κυρίως τα χρηματοπιστωτικά ιδρύματα και συνιστά σημαντικό στοιχείο των χρηματοοικονομικών ερευνών που διενεργούνται από τις αρμόδιες δημόσιες αρχές, συμπεριλαμβανομένων των ΜΧΠ

Κυρίως όμως, προέταξε στα Κράτη Μέλη την υποχρέωση να αποκτούν και να διατηρούν ενημερωμένες και ακριβείς πληροφορίες σχετικά με τον πραγματικό δικαιούχο των νομικών οντοτήτων σε ένα κεντρικό μητρώο το επονομαζόμενο «Μητρώο Πραγματικών Δικαιούχων» το οποίο θα ήταν προσβάσιμο πέρα από συγκεκριμένες κατηγορίες και από οποιοδήποτε άτομο ή οργανισμό μπορεί να

¹⁷⁹ Έχουν διατυπωθεί και νομοθετικά και στην βιβλιογραφία πολλές κατηγοριοποιήσεις σχετικά με την εξεύρεση της έννοιας του πραγματικού δικαιούχου, ωστόσο η εξαντλητική αναφορά τους θα απομάκρυνε από τον στόχο της παρούσας εργασίας, συνεπώς καθαρά και μονό για τις ανάγκες τις εργασίες υιοθετείται ο ως άνω ορισμός.

¹⁸⁰ Cindori, S. (2023).

¹⁸¹ Οδηγία (ΕΕ) 2005/60/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Οκτωβρίου 2005 σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και χρηματοδότηση της τρομοκρατίας (ΕΕ L 309 της 25ης Νοεμβρίου 2005).

αποδείξει το απαιτούμενο έννομο συμφέρον.¹⁸² Ωστόσο, εν συνεχεία, το άρθρο 1 παράγραφος 15 στοιχείο γ) της Πέμπτης Οδηγίας εισήγαγε μια ουσιώδη τροποποίηση, η οποία απαιτούσε την επέκταση της εν λόγω πρόσβασης σε «οποιοδήποτε μέλος του ευρέος κοινού»¹⁸³ εξαλείφοντας την απαίτηση για απόδειξη νόμιμου συμφέροντος για να αποκτηθούν οι πληροφορίες τους.¹⁸⁴

Εντούτοις, ένα μέρος του επαγγελματικού και επιχειρηματικού τομέα έχει για καιρό εντοπίσει τη σύγκρουση μεταξύ του δικαιώματος στην ιδιωτικότητα και της προστασίας των προσωπικών δεδομένων, έναντι της δημοσιότητας των δεδομένων στα μητρώα παρόλο που η θέσπιση αυτών των μητρώων αποτελεί έναν από τους πυλώνες των πολιτικών ΚΕΤ/ΧΤ.¹⁸⁵

6.2. Η Περίφημη Απόφαση WM και Sovim SA κατά Εμπορικού Μητρώου του Λουξεμβούργου

Τρανή απόδειξη για το βάσιμο του ως άνω προβληματισμού, αποτελεί η περίφημη απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ), στις συνεκδικαζόμενες υποθέσεις C-37/20 και C-601/20 “WM και Sovim SA κατά Εμπορικού Μητρώου του Λουξεμβούργου”. Η οποία αναλύεται εκτενώς ακολούθως:

6.2.1. Το Ιστορικό των συνεκδικαζόμενων υποθέσεων

Οι δύο συνεκδικαζόμενες υποθέσεις που συζητήθηκαν εν προκειμένω, αφορούσαν το Μητρώο επιχειρήσεων του Λουξεμβούργου και υποβλήθηκαν αμφότερες στο Πρωτοδικείο του Λουξεμβούργου (tribunal d'arrondissement de Luxembourg).

¹⁸² Zigo, D. (2023)

¹⁸³ Ο.π. Brewczykńska, Μ. Σύμφωνα με την τροποποιημένη διάταξη, οι επίμαχες πληροφορίες θα έπρεπε «τουλάχιστον» να περιλαμβάνουν το όνομα, τον μήνα και το έτος γέννησης, τη χώρα διαμονής και την ιθαγένεια του UBO, καθώς και τη φύση και την έκταση των δικαιωμάτων που κατέχει ο πραγματικός δικαιούχος

¹⁸⁴ Ο.π. Zigo (2023)

¹⁸⁵ Milaj, J. and Kaiser, C. (2017)

Σύμφωνα με την Τέταρτη Οδηγία, όπως τροποποιήθηκε από την Πέμπτη Οδηγία καθώς και ο σχετικός νόμος του Λουξεμβούργου που μετέφερε αυτές τις Οδηγίες, προέβλεπε μια εξαίρεση από την υποχρεωτική αποκάλυψη δεδομένων για τους πραγματικούς δικαιούχους. Αυτή η εξαίρεση, επιτρέπει τη χορήγηση εξαιρέσεων ανά περίπτωση σε εξειδικευμένες περιστάσεις, όπου η δημόσια πρόσβαση σε τέτοιες πληροφορίες θα έθετε τον πραγματικό δικαιούχο σε κίνδυνο απάτης, απαγωγής, εκβιασμού, βίας, απειλής ή όπου ο πραγματικός δικαιούχος είναι ανήλικος ή αλλιώς νομικά ανίκανος.¹⁸⁶Και οι δύο εταιρείες υπέβαλαν αίτηση στο Εμπορικό Μητρώο του Λουξεμβούργου για εξαίρεση, κάθε μία για διαφορετικό λόγο. Ωστόσο, και οι δύο αιτήσεις απορρίφθηκαν. Ως εκ τούτου, οι εταιρείες κατέθεσαν προσφυγές στο Περιφερειακό Δικαστήριο του Λουξεμβούργου

Η πρώτη υπόθεση, η WM, αφορούσε φυσικό πρόσωπο το οποίο αποκαλύφθηκε ως πραγματικός δικαιούχος εταιρείας ακινήτων Στο Μητρώο Πραγματικών Δικαιούχων του Λουξεμβούργου. Αντιτάχθηκε σε αυτό, επικαλούμενος τον κίνδυνο απαγωγής, εκβιασμού, παρενόχλησης του ίδιου και της οικογένειάς του κ.λπ.¹⁶ Αυτή η ανάγκη προέκυπτε επειδή η θέση του ως εκτελεστικού διευθυντή, απαιτούσε συχνά ταξίδια σε χώρες με ασταθές πολιτικό καθεστώς και υψηλά επίπεδα εγκληματικότητας, δημιουργώντας έτσι σημαντικούς κινδύνους.

Στη δεύτερη περίπτωση, η εταιρία Sovim αντιτάχθηκε στο Μητρώο Επιχειρήσεων του Λουξεμβούργου σχετικά με τη δημοσιοποίηση των μετόχων της στο ευρύ κοινό. Για το σκοπό αυτό, βασίστηκε στα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων αναφορικά με το σεβασμό της ιδιωτικής και οικογενειακής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα¹⁸⁷.Επιπλέον, η Sovim ισχυρίστηκε ότι αυτή η υποχρέωση, επηρέαζε κυρίως τις αρχές που σχετίζονται με την επεξεργασία προσωπικών δεδομένων που

¹⁸⁶ Η 4η Οδηγία AML όπως τροποποιήθηκε, Άρθρο 30(9)¹⁸⁶

¹⁸⁷ *Siems, Mathias, Privacy vs. Shareholder Transparency (2023)*

περιλαμβάνονται στο άρθρο 5 του ΓΚΠΔ και, μεταξύ άλλων, στο άρθρο 25 του ίδιου Κανονισμού, το οποίο ορίζει ότι πρέπει να επεξεργάζονται μόνο τα προσωπικά δεδομένα που είναι απαραίτητα για κάθε συγκεκριμένο σκοπό της επεξεργασίας.¹⁸⁸

Το Περιφερειακό Δικαστήριο του Λουξεμβούργου αποφάσισε να αναστείλει τις διαδικασίες και στις δύο υποθέσεις και να υποβάλει ερωτήματα στο Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) για προδικαστική απόφαση. Το Δικαστήριο, υπέβαλε διάφορα ερωτήματα σχετικά με την ερμηνεία που πρέπει να δοθεί. Στην υπόθεση C-37/20 WM, τα κύρια θέματα αφορούσαν τις έννοιες των εξαιρετικών περιστάσεων, του κινδύνου και του δυσανάλογου κινδύνου κατά την έννοια του άρθρου 30(9) της τροποποιημένης Τέταρτης Οδηγίας. Στην υπόθεση C-601/20 Sovim, το Περιφερειακό Δικαστήριο του Λουξεμβούργου βασίστηκε, κυρίως στο ερώτημα, εάν η πρόσβαση του γενικού κοινού στα δεδομένα του μητρώου πραγματικών δικαιούχων είναι συμβατή με τον Χάρτη και τον ΓΚΠΔ.

6.2.2. Η πρόταση του Εισαγγελέα

Ο Γενικός Εισαγγελέας του ΔΕΕ G. Pitruzzella, εξέδωσε τις προτάσεις του για το αίτημα προδικαστικής απόφασης από το Περιφερειακό Δικαστήριο του Λουξεμβούργου στις 20 Ιανουαρίου 2022. Ο Γενικός Εισαγγελέας προχώρησε στον καταμερισμό των προκαταρκτικών ερωτήσεων που υπέβαλε το δικαστήριο του Λουξεμβούργου, σε τρεις κύριες κατηγορίες.

Πρώτον, εξέτασε την εγκυρότητα της δημόσιας πρόσβασης στις πληροφορίες πραγματικής ιδιοκτησίας υπό το πρίσμα των δικαιωμάτων για σεβασμό της ιδιωτικής ζωής και προστασία των προσωπικών δεδομένων, όπως κατοχυρώνονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.¹⁸⁹ Δεύτερον, εξέτασε τη συμβατότητα της δημόσιας πρόσβασης στις πληροφορίες πραγματικής ιδιοκτησίας με τις διατάξεις του ΓΚΠΔ. Τρίτον, εξέτασε την ερμηνεία της τροποποιημένης

¹⁸⁸ Ο.π. Ζίγο

¹⁸⁹ Προτάσεις του Γεν. Εισαγγελέα G. Pitruzzella, 2022, παρ. 34

Τέταρτης Οδηγίας όσον αφορά τις εξαιρέσεις από τη ρύθμιση της δημόσιας πρόσβασης στις πληροφορίες πραγματικής ιδιοκτησίας.¹⁹⁰

Ο Γενικός Εισαγγελέας εκκίνησε τονίζοντας ότι, σύμφωνα με τις παραδόσεις των κρατών μελών, η κρατική δραστηριότητα πρέπει να καθορίζεται από τη διαφάνεια, η οποία μπορεί να περιορίζεται μόνο σε εξαιρετικές περιπτώσεις. Αυτό το γεγονός έρχεται σε αντίθεση με την εμπιστευτικότητα της ιδιωτικής σφαίρας, που προστατεύεται από την αναγνώριση του θεμελιώδους δικαιώματος στην ιδιωτική ζωή. Ωστόσο, μπορεί να υπάρχει γενικό ενδιαφέρον για τη γνώση ορισμένων πτυχών της ιδιωτικής σφαίρας ενός ατόμου, επεκτείνοντας έτσι το πεδίο εφαρμογής της αρχής της διαφάνειας, για παράδειγμα, στη ρύθμιση των χρηματοπιστωτικών αγορών, όπου αυτή η αρχή συμβάλλει στην καταπολέμηση φαινομένων όπως η διαφθορά ή η τρομοκρατία.¹⁹¹

Προχωρώντας στην ανάλυση των προδικαστικών ερωτημάτων, ο Γεν. Εισαγγελέας εντόπισε ότι η αποκάλυψη των δεδομένων των πραγματικών ιδιοκτητών, αποτελεί παρέμβαση στα δικαιώματα που προβλέπονται από τον ΧΘΔΑ, ωστόσο έκρινε ότι η παρέμβαση αυτή είναι αποδεκτή εφόσον είναι νόμιμη, σέβεται την ουσία των δικαιωμάτων, εξυπηρετεί τους στόχους του γενικού συμφέροντος και είναι αναλογική.¹⁹² Αφού συζήτησε αυτές τις προϋποθέσεις, ο Γενικός Εισαγγελέας κατέληξε στο ότι οι συνέπειες για τα πρόσωπα που επηρεάζονται από τη δημοσιοποίηση των μητρών στο ευρύ κοινό, μπορούν να θεωρηθούν μέτριες, λόγω του περιορισμένου εύρους και της όχι ιδιαίτερα ευαίσθητης φύσης των προσωπικών δεδομένων που περιλαμβάνονται στην παρέμβαση. Έτσι, έκρινε την παρέμβαση στα θεμελιώδη δικαιώματα που διασφαλίζονται από τα άρθρα 7 και 8 του Χάρτη ως όχι ιδιαίτερα σοβαρή, καθώς τα δεδομένα αυτά δεν επιτρέπουν από μόνα τους, την

¹⁹⁰ Προτάσεις του Γεν. Εισαγγελέα G. Pitruzzella, 2022, παρ. 36

¹⁹¹ Προτάσεις του Γεν. Εισαγγελέα G. Pitruzzella, 2022, παρ. 48

¹⁹² Προτάσεις του Γεν. Εισαγγελέα G. Pitruzzella, 2022, παρ. 80

απόκτηση ακριβών πληροφοριών για τα ενδιαφερόμενα πρόσωπα και συνεπώς δεν επηρεάζουν άμεσα και έντονα την ιδιωτική τους ζωή.¹⁹³

Παρά αυτό το συμπέρασμα για το πιο θεμελιώδες ζήτημα της διαδικασίας, ο Γενικός Εισαγγελέας πρότεινε την ακύρωση μέρους της Πέμπτης Οδηγίας¹⁹⁴. Ενώ, υποστήριξε ότι για να διασφαλιστεί ότι οι πραγματικοί ιδιοκτήτες έχουν επαρκείς εγγυήσεις για την προστασία των δεδομένων τους από τον κίνδυνο κατάχρησης, είναι απαραίτητο τα κράτη μέλη να γνωρίζουν την ταυτότητα των ατόμων που έχουν πρόσβαση σε αυτά τα μητρώα και να παρέχουν στους πραγματικούς ιδιοκτήτες πληροφορίες για αυτά τα άτομα αν αυτό είναι απαραίτητο για να διασφαλιστεί ο σεβασμός των θεμελιωδών δικαιωμάτων¹⁹⁵.

6.2.3. Η Απόφαση του Δικαστηρίου

Το ΔΕΕ επικεντρώθηκε κυρίως στο πρώτο προδικαστικό ερώτημα της υπόθεσης *Sovim* (Υπόθεση C-601/20), το οποίο αφορούσε τη συμμόρφωση του σημείου (γ) της πρώτης παραγράφου του άρθρου 30(5) της Τέταρτης Οδηγίας ΚΕΤ/ΧΤ όπως τροποποιήθηκε, με τα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

Το Δικαστήριο εξέτασε αν η πρόσβαση του κοινού σε δεδομένα πραγματικών δικαιούχων παραβιάζει τα δικαιώματα του σεβασμού της ιδιωτικής ζωής και της προστασίας των προσωπικών δεδομένων. Κατέληξε ότι η δημοσίευση τέτοιων δεδομένων επηρεάζει το θεμελιώδες δικαίωμα στον σεβασμό της ιδιωτικής ζωής, ανεξάρτητα από το αν τα δεδομένα αφορούν επαγγελματικές δραστηριότητες¹⁹⁶. Επίσης, η διαθεσιμότητα προσωπικών δεδομένων σε τρίτους θεωρείται παραβίαση των θεμελιωδών δικαιωμάτων, ανεξάρτητα από την ευαισθησία των δεδομένων ή την ενόχληση των ατόμων που αφορούν.¹⁹⁷

¹⁹³ Προτάσεις του Γεν. Εισαγγελέα G. Pitruzzella, 2022, παρ. 104

¹⁹⁴ T. Ο νομοθέτης της ΕΕ τροποποίησε την παράγραφο 2 και 3 του άρθρου 30(5) της 4ης οδηγίας AML, ώστε τα μεμονωμένα κράτη μέλη να μπορούν να επεκτείνουν το εύρος των προσωπικών δεδομένων που είναι διαθέσιμα στο κοινό τα πρόσωπα ή οι οργανισμοί που αναφέρονται στο στ έχουν πρόσβαση τουλάχιστον στο όνομα, τον μήνα και το έτος γέννησης, την εθνικότητα και τη χώρα διαμονής του πραγματικού δικαιούχου, καθώς και τη φύση και την έκταση των ωφελούμενων συμφερόντων.

¹⁹⁵ Προτάσεις του Γεν. Εισαγγελέα G. Pitruzzella, 2022, παρ. 208

¹⁹⁶ WM και *Sovim SA* κατά *Luxembourg Business Registers*, 2022, παρ. 38

¹⁹⁷ WM και *Sovim SA* κατά *Luxembourg Business Registers*, 2022, παρ. 39.

Το ΔΕΕ εκτίμησε ότι η δημοσίευση επιτρέπει τη δημιουργία προφίλ ορισμένων προσωπικών δεδομένων ταυτοποίησης, μεγαλύτερης ή μικρότερης έκτασης, αναλόγως των ρυθμίσεων του εθνικού δικαίου, την οικονομική κατάσταση του ενδιαφερομένου καθώς και με τους συγκεκριμένους οικονομικούς τομείς, χώρες και επιχειρήσεις όπου αυτός έχει επενδύσει.¹⁹⁸Επιπλέον, η ελεύθερη πρόσβαση σε τέτοιες πληροφορίες μπορεί να οδηγήσει σε κατάχρηση, καθιστώντας αδύνατη την αποτελεσματική άμυνα των επηρεαζόμενων ατόμων.

Πιο συγκεκριμένα, σύμφωνα με το ΔΕΕ, αυτές οι πληροφορίες μπορούν να γίνουν γνωστές σε δυνητικά απεριόριστο αριθμό ατόμων, τα οποία, για λόγους άσχετους με τον σκοπό του μέτρου, προσπαθούν να ενημερωθούν ειδικά για την περιουσιακή και οικονομική κατάσταση ενός πραγματικού δικαιούχου, το οποίο μπορεί να διευκολυνθεί μέσω της διαδικτυακής πρόσβασης σε αυτές τις πληροφορίες.

Επιπλέον, έκρινε ότι υπάρχει κίνδυνος τα προσωπικά δεδομένα να χρησιμοποιηθούν καταχρηστικά, καθώς μπορούν να αποθηκευτούν και να διαδοθούν ελεύθερα. Σε τέτοιες περιπτώσεις, εντόπισε ότι γίνεται ακόμα πιο δύσκολο, αν όχι αδύνατο, για τα υποκείμενα των δεδομένων να προστατευθούν αποτελεσματικά από τέτοιες καταχρήσεις. Για αυτούς τους λόγους, το ΔΕΕ θεώρησε ότι η πρόσβαση του κοινού σε πληροφορίες πραγματικών δικαιούχων αποτελεί σοβαρή παραβίαση των θεμελιωδών δικαιωμάτων των άρθρων 7 και 8 του Χάρτη.¹⁹⁹

¹⁹⁸ WM και Sovim SA κατά Luxembourg Business Registers, 2022, παρ.41.

¹⁹⁹ WM και Sovim SA κατά Luxembourg Business Registers, 2022, παρ. 44

Κατά την εξέταση του ζητήματος αν το επίμαχο μέτρο ανταποκρίνεται στον σκοπό γενικού συμφέροντος που αναγνωρίζει η Ένωση, το Δικαστήριο διέκρινε δύο ζητήματα, ήτοι μεταξύ της δημιουργίας εχθρικού περιβάλλοντος για τους εγκληματίες μέσω της ενισχυμένης διαφάνειας και της αρχής της διαφάνειας αυτής καθαυτής, η οποία νοείται ως παράγοντας διευκόλυνσης της συμμετοχής των πολιτών στις δημοκρατικές διαδικασίες²⁰⁰. Στον ως άνω προβληματισμό το ΔΕΕ κατέληξε ότι η αρχή της διαφάνειας, όπως απορρέει από τα άρθρα 1 και 10 ΣΕΕ καθώς και από το άρθρο 15 ΣΛΕΕ, δεν μπορεί να θεωρηθεί, αυτή κάθε αυτήν, ως σκοπός γενικού συμφέροντος ικανός να δικαιολογήσει την επέμβαση στα κατοχυρωμένα στα άρθρα 7 και 8 του ΧΘΔΑ η οποία απορρέει από την πρόσβαση του ευρύτερου κοινού στις πληροφορίες σχετικά με τους πραγματικούς δικαιούχους.²⁰¹

Για την αξιολόγηση της αναλογικότητας της παρέμβασης, το ΔΕΕ ακολούθησε έλεγχο τριών σταδίων, το οποίο απαιτεί αξιολόγηση της συμμόρφωσης του μέτρου με τις απαιτήσεις καταλληλότητας, αναγκαιότητας και αναλογικότητας σε σχέση με τον επιδιωκόμενο στόχο γενικού συμφέροντος.

Πρώτον, το Δικαστήριο υποστήριξε ότι ο δημόσιος χαρακτήρας της πρόσβασης και η συνακόλουθη αυξημένη διαφάνεια (UBO), όπς καθιερώνεται από την Πέμπτη Οδηγία, είναι κατάλληλες για την επίτευξη του στόχου του γενικού συμφέροντος καθώς τα συγκεκριμένα συμβάλλουν στη δημιουργία ενός περιβάλλοντος λιγότερο επιρρεπούς στη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας.²⁰²

Δεύτερον, το Δικαστήριο διευκρίνισε ότι το «απολύτως αναγκαίο» σημαίνει ότι «όταν υπάρχει δυνατότητα επιλογής μεταξύ περισσότερων κατάλληλων μέτρων για την επίτευξη των επιδιωκόμενων θεμιτών σκοπών, πρέπει να επιλέγεται το λιγότερο

²⁰⁰ Ο.π. *Brewczyńska* (2023)

²⁰¹ *WM και Sovim SA κατά Luxembourg Business Registers*, 2022, παρ. 61-62.

²⁰² *WM και Sovim SA κατά Luxembourg Business Registers*, 2022, παρ. 66-67

επαχθές».²⁰³ Πιο συγκεκριμένα, εξετάζοντας το σκεπτικό της τροποποίησης που εισήγαγε η Πέμπτη Οδηγία, η οποία διευρύνει τη δυνατότητα πρόσβασης σε πληροφορίες του μητρώου πέραν από χωρίς να απαιτείται η απόδειξη από τον ενδιαφερόμενο του εννόμου συμφέροντος», το Δικαστήριο απέρριψε το επιχείρημα της Επιτροπής ότι η αλλαγή αυτή δικαιολογείται από τη δυσκολία καθορισμού του κριτηρίου του «έννομου συμφέροντος».²⁰⁴ Το ΔΕΕ τόνισε ότι, όταν η πρόσβαση σε πληροφορίες σχετικά με το Μητρώο Πραγματικών Δικαιούχων, εξυπηρετεί τους στόχους που αναφέρονται στην αιτιολογική σκέψη 30 της Πέμπτης Οδηγίας, υπάρχει ήδη έννομο συμφέρον, καθιστώντας την επέκταση της προσβασιμότητας στο ευρύ κοινό περιττή.²⁰⁵

Τρίτον, το Δικαστήριο εξέτασε την απαίτηση αναλογικότητας, εξετάζοντας εάν τα νομοθετικά μέτρα που εμπλέκονται σε παρεμβάσεις στα δικαιώματα που προβλέπονται στα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ προβλέπουν "σαφείς και ακριβείς κανόνες που διέπουν το πεδίο εφαρμογής και την εφαρμογή των μέτρων (...) και επιβάλλουν ελάχιστες εγγυήσεις, ώστε τα υποκείμενα των δεδομένων να έχουν επαρκείς εγγυήσεις για την αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν από τον κίνδυνο κατάχρησης".²⁰⁶

Το Δικαστήριο κατέληξε στο συμπέρασμα, ότι οι κανόνες που επιτρέπουν πρόσβαση στο ευρύ κοινό σε πληροφορίες σχετικά με τον Πραγματικό Δικαιούχο (UBO) ιδίως το άρθρο 30 παράγραφος 5 της Τέταρτης Οδηγίας, το οποίο επιτρέπει την πρόσβαση σε "πρόσθετες πληροφορίες" που επιτρέπουν την ταυτοποίηση UBO, δεν πληρούν τα πρότυπα σαφήνειας και ακρίβειας.²⁰⁷

²⁰³ WM και Sovim SA κατά Luxembourg Business Registers, 2022, παρ. 64

²⁰⁴ WM και Sovim SA κατά Luxembourg Business Registers, 2022, παρ. 68-73

²⁰⁵ WM και Sovim SA κατά Luxembourg Business Registers, 2022, παρ. 74-76

²⁰⁶ WM και Sovim SA κατά Luxembourg Business Registers, 2022, παρ. 64

²⁰⁷ WM και Sovim SA κατά Luxembourg Business Registers, 2022, παρ. 78-82

Τέλος, αντιπαραβάλλοντας τη σοβαρότητα της διαπιστωθείσας παρέμβασης με τη σημασία του επιδιωκόμενου στόχου γενικού συμφέροντος, το Δικαστήριο σημείωσε ότι η υλοποίηση της πολιτικής για την αντιμετώπιση ξεπλύματος χρήματος, αποτελεί πρωτίστως καθήκον των αρμόδιων δημόσιων αρχών και των υπόχρεων οντοτήτων, οι οποίες είχαν πρόσβαση σε πληροφορίες σχετικά με τον πραγματικό δικαιούχο ανεξάρτητα από την τροποποίηση που εισήγαγε η Πέμπτη Οδηγία.²⁰⁸

Υπό το πρίσμα αυτό, το Δικαστήριο δεν αναγνώρισε την προστιθέμενη αξία της παροχής πρόσβασης στις πληροφορίες UBO στο ευρύ κοινό, η οποία, σε σύγκριση με τον προηγούμενο κανόνα, αποτελεί μέτρο που "συνιστά πολύ σοβαρότερη παρέμβαση" στα δικαιώματα που κατοχυρώνονται στα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

Τέλος, σύμφωνα με το Δικαστήριο, η εξαιρετική δυνατότητα περιορισμού της πρόσβασης στις πληροφορίες που είναι αποθηκευμένες στα μητρώα UBO δεν είναι ικανή να αποδείξει την κατάλληλη ισορροπία μεταξύ του επιδιωκόμενου σκοπού γενικού συμφέροντος και των αντίστοιχων δικαιωμάτων, ούτε συνιστά επαρκείς εγγυήσεις που επιτρέπουν στα υποκείμενα των δεδομένων να προστατεύουν αποτελεσματικά τα δεδομένα προσωπικού χαρακτήρα που τα αφορούν από τους κινδύνους κατάχρησης.²⁰⁹ Λαμβανομένων υπόψη των ανωτέρω, το άρθρο 1 παράγραφος 15 στοιχείο γ) της Πέμπτης Οδηγίας κρίθηκε άκυρο στον βαθμό που τροποποίησε το άρθρο 30 παράγραφος 5 πρώτο εδάφιο στοιχείο γ) Τέταρτης Οδηγίας και απαίτησε από τα κράτη μέλη να διασφαλίσουν την μη εφαρμογή του.

6.3. Μετά την Απόφαση

Η απόφαση του ΔΕΕ στις υποθέσεις C-37/20 και C-601/20, WM και Sovim SA κατά Luxembourg Business Registers, προκάλεσε αμφίσημες αντιδράσεις. Από μερίδα του επιχειρηματικού και νομικού κόσμου κατακρίθηκε ότι αγνοεί όλα τα διδάγματα

²⁰⁸ WM και Sovim SA κατά Luxembourg Business Registers, 2022, παρ. 84

²⁰⁹ WM και Sovim SA κατά Luxembourg Business Registers, 2022, παρ. 86

που αντλήθηκαν την τελευταία δεκαετία από διαρροές όπως τα Pandora Papers και τα Panama Papers²¹⁰ που αποκαλύφθηκε πληθώρα περιπτώσεων κρυφής φοροδιαφυγής και νομιμοποίησης κεφαλαίων που δεν εντοπίστηκαν αρχικά από δημόσιες αρχές, αλλά από δημοσιογραφικές έρευνες και ακτιβιστικά κινήματα. Το Πρόγραμμα Αναφοράς Οργανωμένου Εγκλήματος και Διαφθοράς (OCCRP), με την δημοσίευση της απόφασης, εξέφρασε τις ανησυχίες του για τις επιπτώσεις αυτής της απόφασης στην Ευρώπη και πέραν αυτής, κυρίως στην ικανότητα των αρχών να προλαμβάνουν και να καταπολεμούν το οργανωμένο έγκλημα και τη νομιμοποίηση κεφαλαίων.²¹¹

Για πολλούς θεωρήθηκε ως μια νίκη για τα θεμελιώδη δικαιώματα και την προστασία δεδομένων έναντι της δημόσιας διαφάνειας των μητρών UBO και καλά νέα για όλους τους επιχειρηματίες που δεν είναι πρόθυμοι να μοιραστούν δημόσια πληροφορίες για τον εαυτό τους και τα ωφέλιμα συμφέροντά τους.²¹² Εκτός από το σοκ και τη δυσπιστία ορισμένων παρατηρητών, η πρώτη άμεση αντίδραση των ευρωπαϊκών χωρών ήταν η τήρηση της απόφασης καθώς χωρίς καθυστέρηση η πρόσβαση στα Μητρώα σχετικά με τους πραγματικούς δικαιούχους των κρατών μελών ανεστάλη ή περιορίστηκε.²¹³

Στην Ελλάδα συγκεκριμένα, ο Νόμος 4557/2018 «Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας» ο οποίος τέθηκε σε ισχύ στις 30.07.2018 ενσωμάτωσε την Ευρωπαϊκή Οδηγία 2015/849 στην Ελληνική έννομη τάξη και παρέχει τη βασική δομή για την εισαγωγή Μητρών, όπου οι Πραγματικοί Δικαιούχοι θα πρέπει να γνωστοποιηθούν.

²¹⁰ Γιαννακίδου Χ.(2023) «Η σύγκρουση μεταξύ της προστασίας δεδομένων και της ανάγκης πρόληψης της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας», Επιθεώρηση Δικαίου Πληροφορικής @ *Information Law Journal*, διαθέσιμο στο <https://ejournals.lib.auth.gr/infolawj/>

²¹¹ Ο.π. Siems (2023)

²¹² Οπ. Brewczykńska (2023)

²¹³ Ο.π. Siems (2023)

Ακολούθως, αναφορικά με την υλοποίηση και εφαρμογή του Μητρώου Πραγματικών Δικαιούχων δημοσιεύτηκε η υπ. αριθμ. 125209 ΕΞ 2022 απόφαση του Υπουργού Οικονομικών με τίτλο «Ρύθμιση ειδικών θεμάτων σχετικά με την πρόσβαση στο Κεντρικό Μητρώο Πραγματικών Δικαιούχων των άρθρων 20 και 21 του ν. 4557/2018» η οποία ορίζει τις διαδικασίες και τους τρόπους πρόσβασης στο Μητρώο. Πιο συγκεκριμένα, τα μέλη του ευρύτερου κοινού έχουν πρόσβαση στα στοιχεία του πραγματικού δικαιούχου που αφορούν στο επώνυμο, όνομα, πατρώνυμο, μήνα και έτος γέννησης, χώρα υπηκοότητας και στα στοιχεία των νομικών προσώπων που αφορούν στο είδος, αριθμό ΓΕΜΗ, επωνυμία, διακριτικό τίτλο, έδρα και στοιχεία επικοινωνίας. Για την περίπτωση νομικών προσώπων που κατέχουν ποσοστό μετοχών ή ιδιοκτησιακό δικαίωμα άλλων νομικών προσώπων, κατά τα οριζόμενα στην παρ. 17 του άρθρου 3 του ν. 4557/2018, το ευρύτερο κοινό έχει πρόσβαση μόνο στα στοιχεία των τελικών πραγματικών δικαιούχων. Μέλος του ευρύτερου κοινού μπορεί να έχει πρόσβαση σε επιπρόσθετες πληροφορίες που επιτρέπουν την ταυτοποίηση του πραγματικού δικαιούχου, συμπεριλαμβανομένου του αριθμού φορολογικού Μητρώου (Α.Φ.Μ.) ή Tax Identification Number (ΤΙΝ), ύστερα από απόδειξη ειδικού εννόμου συμφέροντος που διαπιστώνεται κατόπιν εισαγγελικής παραγγελίας σύμφωνα με το άρθρο 34 του Κώδικα Ποινικής Δικονομίας. Στην περίπτωση αυτή, το μέλος του ευρύτερου κοινού υποβάλει νέο αίτημα για τις επαυξημένες αυτές πληροφορίες επισυνάπτοντας τη σχετική εισαγγελική παραγγελία, ώστε να του χορηγηθεί ο ρόλος με τα επαυξημένα δικαιώματα. Η παρούσα παράγραφος εφαρμόζεται με την επιφύλαξη της παρ. 7β του άρθρου 20 του ν. 4557/2018.

Σύμφωνα με την ως άνω απόφαση η πρόσβαση για το κοινό θα διενεργείται με χρήση των κωδικών διαπιστευτηρίων (taxisnet) της Γενικής Γραμματείας Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης του Υπουργείου Ψηφιακής Διακυβέρνησης (Γ.Γ.Π.Σ.Δ.Δ.) για την είσοδο στο σύστημα και καταχώριση σε σχετική φόρμα του λόγου αναζήτησης, υπό τους όρους και προϋποθέσεις που αναφέρθηκαν

παραπάνω. Αξίζει να τονιστεί ότι σύμφωνα με το άρθρο 10 της ως άνω απόφασης, οι υπόχρεοι καταχώρισης ενημερώνονται για τις αναζητήσεις που έγιναν για αυτούς από μέλη του κοινού και οι χρήστες του συστήματος αποδέχονται την ενημέρωση των υπόχρεων καταχώρισης για τις αναζητήσεις που έγιναν από αυτούς.²¹⁴

6.4. Η Νομοθετική Μεταρρύθμιση

Η απόλυτη προσπάθεια εναρμόνισης και συμμόρφωσης με την απόφαση του ΔΕΕ, αποτυπώνεται στα τελικά κείμενα του λεγόμενου AML Package. Πιο συγκεκριμένα, παρόλο που τα κείμενα που είχαν προταθεί το 2021, ακολουθούσαν εν πολλοίς την λογική της Πέμπτης Οδηγίας, ο Ευρωπαίος νομοθέτης, φαίνεται ότι προσαρμόστηκε με τις επιταγές του ΔΕΕ όπως ρητά αποτυπώνεται στην σκέψη 134 της Έκτης Οδηγίας ²¹⁵τονίζοντας ότι «η απόφαση του Δικαστηρίου ακύρωσε την τροποποίηση που επέφερε η οδηγία (ΕΕ) 2018/843 στο άρθρο 30 παράγραφος 5 της οδηγίας (ΕΕ) 2015/849 στο βαθμό που απαιτούσε από τα κράτη μέλη να διασφαλίζουν ότι οι πληροφορίες για τον πραγματικό δικαιούχο εταιρειών ή άλλων νομικών οντοτήτων που έχουν συσταθεί στο έδαφός τους είναι προσβάσιμες από οποιοδήποτε μέλος του ευρέος κοινού.» Συνεπώς, έκρινε ότι η νομοθετική γραμμή και αντιμετώπιση του ζητήματος επρέπει να προσαρμοστεί.

Ως εκ τούτου, προβλέφθηκε στην σκέψη 40 ότι είναι αναγκαίο να διαμορφωθεί ένα πλαίσιο για την αναγνώριση και τη διαπίστωση ύπαρξης έννομου συμφέροντος

²¹⁴ Παρά τις εξαγγελίες περί έναρξης της παραγωγικής λειτουργίας πρόσβασης στο Κεντρικό Μητρώο Πραγματικών Δικαιούχων στις αρχές του 2023, δημοσιεύθηκε στο ΦΕΚ η απόφαση 20931 ΕΞ 2023 με την οποία τροποποιείται το άρθρο 12 της ΚΥΑ 125209 ΕΞ 2022/06.09.2022, σύμφωνα με την οποία για τα υπόχρεα πρόσωπα ορίστηκε η 01.11.2022 και για το ευρύτερο κοινό η 01.07.2023, η οποία τροποποιήθηκε με τη νέα απόφαση 184655 ΕΞ 2023, ορίζοντας ότι η έναρξη παραγωγικής λειτουργίας της πρόσβασης στο Κεντρικό Μητρώο Πραγματικών Δικαιούχων για τα υπόχρεα πρόσωπα παραμένει η 01.11.2022 ενώ για το ευρύτερο κοινό η 31.12.2024. Στο περιβάλλον της ίδιας της εφαρμογής του gov.gr αναγράφεται επακριβώς η ένδειξη ότι «ΠΡΟΣΟΧΗ !! Για τα φυσικά πρόσωπα έχει ανασταλεί η πρόσβαση στις αναζητήσεις πραγματικών δικαιούχων λόγω απόφασης του Ευρωπαϊκού Δικαστηρίου».

σε επίπεδο Ένωσης, με πλήρη σεβασμό του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, ορίζοντας ότι όταν υφίσταται έννομο συμφέρον, θα πρέπει να επιτρέπεται στο κοινό η πρόσβαση σε πληροφορίες σχετικά με τους πραγματικούς δικαιούχους νομικών οντοτήτων και νομικών μορφωμάτων.²¹⁶

Πιο συγκεκριμένα, στο άρθρο 12 της Έκτης Οδηγίας προβλέφθηκε ότι τα κράτη μέλη διασφαλίζουν ότι κάθε φυσικό ή νομικό πρόσωπο που μπορεί να αποδείξει έννομο συμφέρον για την πρόληψη και την αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, των βασικών αδικημάτων της και της χρηματοδότησης της τρομοκρατίας έχει πρόσβαση για τους πραγματικούς δικαιούχους νομικών οντοτήτων και νομικών μορφωμάτων, χωρίς ωστόσο να ειδοποιείται η σχετική νομική οντότητα, στις ακόλουθες πληροφορίες, ήτοι α) στο όνομα του πραγματικού δικαιούχου, β) στο μήνα και έτος γέννησής του, γ) στην χώρα διαμονής και την ιθαγένεια του δ) στο είδος και έκταση δικαιωμάτων που κατέχουν.

Εντούτοις, προβλέπεται αναλυτική διαδικασία απόδειξης του έννομου συμφέροντος σχετικά με την πρόσβαση σε πληροφορίες για τους πραγματικούς δικαιούχους, η οποία διαπιστώνεται εν πολλοίς, λαμβανομένων υπόψη των καθηκόντων ή του επαγγέλματος του αιτούντος.²¹⁷ Ωστόσο, η Έκτη Οδηγία ορίζει ρητά στο άρθρο 15 ότι τα κράτη μέλη θα πρέπει να προβλέπουν εξαιρέσεις από τη γνωστοποίηση των προσωπικών πληροφοριών του πραγματικού δικαιούχου όταν οι πληροφορίες αυτές θα τον εξέθεταν σε δυσανάλογο κίνδυνο εξαπάτησης, απαγωγής, εκβιασμού, εκβίασης, παρενόχλησης, βίας ή εκφοβισμού.²¹⁸

Παράλληλα, εντοπίζονται και επιπρόσθετες ασφαλιστικές δικλείδες για την προστασία των προσωπικών δεδομένων των φυσικών προσώπων που είναι πραγματικοί δικαιούχοι νομικών οντοτήτων. Πιο συγκεκριμένα, στα κράτη μέλη θα πρέπει να παρέχεται η δυνατότητα να απαιτούν επιγραμμική εγγραφή, προκειμένου να ταυτοποιούν κάθε πρόσωπο που ζητεί πληροφορίες από το κεντρικό μητρώο,

²¹⁶ 6^η Οδηγία, σκέψη 40

²¹⁷ 6^η Οδηγία, άρθρο 12, παρ. 2

²¹⁸ 6^η Οδηγία άρθρο 15

καθώς και την καταβολή τέλους για την πρόσβαση στις πληροφορίες του.²¹⁹ Καθώς, έχει προβλεφθεί ότι τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι τα κεντρικά μητρώα τηρούν αρχεία των προσώπων που έχουν πρόσβαση στις πληροφορίες αυτές και είναι σε θέση να τα γνωστοποιούν στους πραγματικούς δικαιούχους, όταν υποβάλλουν αίτημα σύμφωνα με το άρθρο 15 παράγραφος 1 στοιχείο γ) του κανονισμού (ΕΕ) 2016/679.²²⁰

Ωστόσο, όταν οι αρχές ζητούν πρόσβαση σε πληροφορίες για τους πραγματικούς δικαιούχους, πρέπει να προσδιορίσουν την περίοδο για την οποία ζητούν να μην αποκαλυφθεί το αίτημα αυτό στους πραγματικούς δικαιούχους. Αυτή η περίοδος δεν μπορεί να υπερβαίνει τα πέντε χρόνια, αιτιολογώντας γιατί ζητούν αυτόν τον περιορισμό, δηλαδή πώς η αποκάλυψη του αιτήματος θα μπορούσε να θέσει σε κίνδυνο τους στόχους των ερευνών ή των αναλύσεών τους.²²¹

Επιπλέον, σύμφωνα με την παράγραφο 20 του άρθρου 10 της πρόσφατης Έκτης Οδηγίας, οι πληροφορίες που αναφέρονται στον πραγματικό δικαιούχο καθίστανται διαθέσιμες μέσω των κεντρικών μητρώων και μέσω του συστήματος διασύνδεσης των κεντρικών μητρώων επί 5 έτη, αφότου η νομική οντότητα έχει λυθεί ή το νομικό μόρφωμα έχει παύσει να υφίσταται.

Ενώ, με την επιφύλαξη της εκάστοτε ποινικής νομοθεσίας κάθε κράτους-μέλους περί αποδεικτικών στοιχείων, η οποία ισχύει για εν εξελίξει ποινικές έρευνες και νομικές διαδικασίες, τα κράτη-μέλη μπορούν, σε συγκεκριμένες υποθέσεις, να επιτρέπουν οι πληροφορίες αυτές να διατηρούνται, ή να ζητούν τη διατήρηση των πληροφοριών αυτών για επιπλέον μέγιστο διάστημα 5 ετών όταν τα κράτη μέλη έχουν διαπιστώσει ότι η διατήρηση αυτή είναι αναγκαία και αναλογική για τον σκοπό της πρόληψης, του εντοπισμού, της έρευνας ή της άσκησης δίωξης όταν υπάρχουν

²¹⁹ 6^η Οδηγία σκέψη 52

²²⁰ γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινολογήθηκαν ή πρόκειται να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς

²²¹ 6^η Οδηγία άρθρο 12 παρ.4

υπόνοιες για νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή χρηματοδότηση της τρομοκρατίας. Ωστόσο, μετά τη λήξη της περιόδου διατήρησης που αναφέρεται, τα κράτη μέλη διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα διαγράφονται από τα κεντρικά μητρώα.²²²

Με την σειρά του, ο Κανονισμός, τονίζει ότι το αποτελεσματικό πλαίσιο διαφάνειας για τον πραγματικό δικαιούχο απαιτεί οι νομικές οντότητες στην ΕΕ να συλλέγουν και να διατηρούν επαρκείς, ακριβείς και ενημερωμένες πληροφορίες για τους πραγματικούς δικαιούχους. Αυτές οι πληροφορίες όπως είδαμε και παραπάνω, πρέπει να διατηρούνται για πέντε χρόνια. Η εν λόγω περίοδος διατήρησης είναι ισόχρονη με την περίοδο διατήρησης των πληροφοριών που αποκτώνται μέσω της εφαρμογής των απα, όπως τα μέτρα δέουσας επιμέλειας ως προς τον πελάτη. Οι νομικές οντότητες πρέπει να επικαιροποιούν άμεσα αυτές τις πληροφορίες μετά από κάθε αλλαγή και να τις επαληθεύουν περιοδικά, π.χ. κατά την υποβολή οικονομικών καταστάσεων.

Μια σημαντική καινοτομία του Κανονισμού αποτελεί η υποχρέωση αναφοράς αναντιστοιχιών. Πιο συγκεκριμένα τονίζεται ότι οι υπόχρεες οντότητες θα πρέπει να λαμβάνουν εύλογα μέτρα για την επαλήθευση της ταυτότητας του πραγματικού δικαιούχου χρησιμοποιώντας αξιόπιστα έγγραφα και πηγές πληροφοριών, ωστόσο όταν οι υπόχρεες οντότητες εντοπίζουν αναντιστοιχίες μεταξύ των πληροφοριών που τηρούνται στα κεντρικά μητρώα και των πληροφοριών που λαμβάνουν από τον πελάτη ή άλλες αξιόπιστες πηγές στο πλαίσιο της δέουσας επιμέλειας ως προς τον πελάτη, θα πρέπει να αναφέρουν τις εν λόγω αναντιστοιχίες στην οντότητα που είναι αρμόδια για το σχετικό κεντρικό μητρώο, ώστε να μπορούν να ληφθούν μέτρα για τη διόρθωση των ανακολουθιών.²²³

Συμπερασματικά, είναι έκδηλη η επιρροή της απόφασης του Δικαστηρίου στα τελικά νομοθετικά κείμενα τόσο της Έκτης Οδηγίας όσο και του Κανονισμού,

²²² 6^η Οδηγία, άρθρο 10, παρ. 20

²²³ Σκέψη 54 Κανονισμού και άρθρο 24

ωστόσο, η επιρροή εντοπίζεται όχι μόνο στην αναδιαμόρφωση του προηγούμενου καθεστώτος της ελεύθερης πρόσβασης του κοινού στα στοιχεία των πραγματικών δικαιούχων, αλλά και σε μία γενικότερη προσέγγιση διασφάλισης και προστασίας των προσωπικών δεδομένων τους, συγκριτικά με τα τις αρχικές διατυπωθείσες προτάσεις που είχαν υποστηριχτεί το 2021. Εντούτοις, η δημοσίευση των ως άνω νομοθετικών κειμένων είναι εξαιρετικά πρόσφατη και χρειάζεται αρκετός καιρός ώστε να αφομοιωθούν από τον νομικό κόσμο και να διαπιστωθεί κατά πόσο οι νέες απαιτήσεις θα υιοθετηθούν από τις υπόχρεες οντότητες αλλά και το πως θα λειτουργήσουν εν τοις πράγμασι αποτελεσματικά τα Μητρώα Πρακτικών Δικαιούχων των Κρατών- Μελών.

ΚΕΦΑΛΑΙΟ 7

Η ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΟΙ ΣΥΝΕΠΕΙΕΣ ΤΗΣ ΕΝΤΑΞΗΣ ΑΥΤΗΣ ΣΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΗΣ ΝΟΜΙΜΟΠΟΙΗΣΗΣ ΕΣΟΔΩΝ ΑΠΟ ΠΑΡΑΝΟΜΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Η τεχνητή νοημοσύνη (AI) έχει αναδειχθεί ως ένα από τα πλέον σημαντικά εργαλεία στην προσπάθεια για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Μέσω της ικανότητάς της να επεξεργάζεται τεράστιους όγκους δεδομένων και να αναγνωρίζει σύνθετα μοτίβα η Τεχνητή Νοημοσύνη μπορεί να ενισχύσει σημαντικά τις διαδικασίες εντοπισμού και αναφοράς ύποπτων συναλλαγών, βοηθώντας στην πρόληψη αλλά και στην καταστολή του φαινομένου. Εντούτοις, παρά τα πλεονεκτήματα αυτά, η χρήση της Τεχνητής Νοημοσύνης, θέτει σοβαρά ζητήματα αναφορικά με την προστασία των προσωπικών δεδομένων. Η φύση των δεδομένων που εμπλέκονται στις διαδικασίες αυτές, καθιστά επιτακτική την ανάγκη για αυστηρές ρυθμίσεις και μηχανισμούς προστασίας της ιδιωτικότητας. Το κεφάλαιο αυτό εξετάζει συνοπτικά την χρήση της Τεχνητής Νοημοσύνης στον τομέα της αντιμετώπισης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, υπό το πρίσμα της προστασίας των δεδομένων προσωπικού χαρακτήρα.

7.1.1. Ορισμός της Τεχνητής Νοημοσύνης

Με τον όρο «Τεχνητή Νοημοσύνη» (Artificial Intelligence), εννοούνται τα συστήματα, τα οποία χαρακτηρίζονται από ευφυή συμπεριφορά, αναλύουν το περιβάλλον τους και ενεργούν, με κάποιο βαθμό αυτονομίας, προκειμένου να επιτευχθούν συγκεκριμένοι στόχοι²²⁴. Ειδικότερα, Τεχνητή Νοημοσύνη είναι η ικανότητα μίας μηχανής -ήτοι ενός μη έμβιου όντος²²⁵- να αναπαράγει αυτόνομα τις ανώτερες γνώσεις και λειτουργίες του ανθρώπου (λ.χ. δημιουργικότητα, αντίληψη

²²⁴ Ευρωπαϊκή Επιτροπή, 2019

²²⁵ Χριστοδούλου Κ., 2019, σελ. 239

περιβάλλοντος κ.λπ.)²²⁶. Στόχος της Τεχνητής Νοημοσύνης είναι η δημιουργία αλγορίθμων διά των οποίων οι υπολογιστές θα επιτυγχάνουν να αποφασίζουν για τον τρόπο εκτέλεσης μίας διεργασίας μαθαίνοντας από τα δεδομένα που τους παρέχονται, σε αντίθεση με την κλασική προσέγγιση κατά την οποία ο υπολογιστής έπρεπε να προγραμματιστεί επακριβώς προκειμένου να ολοκληρώσει μία διεργασία²²⁷

Σήμερα, η παρουσία της Τεχνητής Νοημοσύνης παρατηρείται σε όλους σχεδόν τους επιχειρηματικούς κλάδους και λειτουργεί μέσω της μηχανικής εκμάθησης²²⁸, δηλαδή του πεδίου μελέτης που περιλαμβάνει τη χρήση αλγορίθμων και μεθοδολογιών παρμένων από τη στατική, ώστε να επιτρέψει σε έναν αλγόριθμο να βελτιώσει την απόδοσή του σε συγκεκριμένη εργασία έτσι ώστε να μαθαίνει από τα δεδομένα που του παρέχονται, δίχως να έχει προγραμματιστεί γι' αυτό και να προβαίνει σε σχετικές προβλέψεις σύμφωνα με αυτά. Η σχέση της Τεχνητής Νοημοσύνης με τα προσωπικά δεδομένα χαρακτηρίζεται ως μία σχέση «διπλής κατεύθυνσης», καθώς τα προσωπικά δεδομένα τροφοδοτούν την Τεχνητή Νοημοσύνη, η οποία παράγει περισσότερα δεδομένα και πληροφορίες²²⁹.

Το 2019, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Organisation for Economic and Development, εφεξής «ο OECD) ανέπτυξε ένα σύνολο κατευθυντήριων Αρχών για την προώθηση της Τεχνητής Νοημοσύνης ως καινοτόμου και αξιόπιστης τεχνολογίας, η οποία σέβεται τα ανθρώπινα δικαιώματα και τις δημοκρατικές αξίες²³⁰. Η πρώτη Αρχή του OECD (OECD Principle 1) πρεσβεύει την αναγκαιότητα να προωθήσει η Τεχνητή Νοημοσύνη την βιώσιμη ανάπτυξη και την ευημερία, η δεύτερη Αρχή (OECD Principle 2) αναφέρει ότι τα συστήματα Τεχνητής Νοημοσύνης πρέπει να είναι συμβατά με το κράτος δικαίου, τις ανθρώπινες αξίες και την ποικιλομορφία, η τρίτη Αρχή (OECD Principle 3) προτρέπει την Τεχνητή

²²⁶ Παναγόπουλος, 2021

²²⁷ Σερβετάς, 2024

²²⁸ Ο.π. Σερβετάς, σελ. 16

²²⁹ Mitrou L., 2019, σελ. 19.

²³⁰ [Pavlidis, G.](#) (2023)

Νοημοσύνη για περισσότερη διαφάνεια και υπεύθυνη αποκάλυψη σχετικά με τα συστήματα Τεχνητής Νοημοσύνης, γεγονός που απαιτεί τη δημιουργία μίας μεθοδολογίας με στόχο την ορθή επεξήγηση και εποπτεία των συστημάτων, η τέταρτη Αρχή (OECD Principle 4) υποστηρίζει την αδιάλειπτη αξιολόγηση και διαχείριση των πιθανών κινδύνων, ενώ τέλος η πέμπτη Αρχή (OECD Principle 5) αναφέρει ότι τα άτομα που χειρίζονται τα συστήματα της Τεχνητής Νοημοσύνης, θα πρέπει να λογοδοτούν για την ορθή λειτουργία τους²³¹.

Αξίζει να επισημανθεί στο σημείο αυτό, ότι η Ευρωπαϊκή Επιτροπή προέβη την 19.02.2020 στη δημοσίευση της «Λευκής Βίβλου»²³² για την Τεχνητή Νοημοσύνη, σύμφωνα με την οποία οι σκοποί της επικείμενης νομοθετικής πρωτοβουλίας είναι η τεχνολογία να λειτουργεί στο πλαίσιο εμπιστοσύνης με τους πολίτες, μέσα σε μία ανταγωνιστική οικονομία, που στόχο έχει την επίρρωση της δημοκρατικής, δίκαιης και ανοικτής κοινωνίας. Η Τεχνητή Νοημοσύνη δηλαδή, πρέπει να ληφθεί ως μέσο για την προαγωγή της ανθρώπινης ανάπτυξης και η ορθή λειτουργία της μπορεί να διασφαλιστεί μόνον διά της θέσπισης νομικών κανόνων που θα μεριμνούν για την διαφάνεια των συστημάτων Τεχνητής Νοημοσύνης²³³.

7.1.2. Ο νέος Κανονισμός για την Τεχνητή Νοημοσύνη (AI Act) ως φορέας αλλαγών στο πεδίο της Τεχνητής Νοημοσύνης.

Η αυξανόμενη ανάπτυξη και χρήση των συστημάτων και εφαρμογών της Τεχνητής Νοημοσύνης κατέστησε αναγκαία τη δημιουργία ενός ρυθμιστικού και νομικού πλαισίου, το οποίο θα καθορίζει τον τρόπο ανάπτυξης, λειτουργίας και αλληλεπίδρασης της με τον άνθρωπο²³⁴. Η Ευρωπαϊκή Ένωση επιδιώκει την αντιμετώπιση των κινδύνων που προκύπτουν από συγκεκριμένες χρήσεις της Τεχνητής Νοημοσύνης, δεδομένου μάλιστα του διασυνοριακού χαρακτήρα αυτής, ο

²³¹ OECD, 2023.

²³² European Commission, (2020)

²³³ Ο.π. Παναγόπουλος

²³⁴ Γ. Ζέκος, 2024, σελ. 38 επ.

οποίος δημιουργεί συνέπειες στο ενωσιακό δίκαιο²³⁵. Στο ανωτέρω πλαίσιο, η Ευρωπαϊκή Ένωση, προέβη στην άρθρωση μίας ανθρωποκεντρικής προσέγγισης της Τεχνητής Νοημοσύνης, επιζητώντας τη διασφάλιση ότι οι ανθρώπινες αξίες έχουν κεντρικό ρόλο στον τρόπο με τον οποίο αναπτύσσονται, εγκαθίστανται, χρησιμοποιούνται και παρακολουθούνται από τα συστήματα της Τεχνητής Νοημοσύνης²³⁶, προτείνοντας διά του Ευρωπαϊκού Κοινοβουλίου την ψήφιση Κανονισμού περί Τεχνητής Νοημοσύνης (εφεξής «ο AI Act»).

Ήδη από την πρόταση του AI Act, είχε καταστεί σαφές ότι σκοπός του ήταν η αξιοποίηση της Τεχνητής Νοημοσύνης με την παράλληλη εξασφάλιση και τον πλήρη σεβασμό των θεμελιωδών δικαιωμάτων²³⁷. Στις 13.03.2024, το Κοινοβούλιο ενέκρινε τον AI Act, όπως αυτός είχε συμφωνηθεί από τα κράτη – μέλη τον Δεκέμβριο του 2023 και ο οποίος κατοχυρώνει την ασφάλεια των χρηστών και την τήρηση των θεμελιωδών δικαιωμάτων τους, ενισχύοντας παράλληλα την καινοτομία στην Ευρωπαϊκή Ένωση. Στόχος δηλαδή του AI Act είναι η προστασία των θεμελιωδών δικαιωμάτων, της δημοκρατίας, του κράτους δικαίου και της περιβαλλοντικής βιωσιμότητας από τα συστήματα τεχνητής νοημοσύνης υψηλού κινδύνου^{238 239}.

Η ratio της θέσπισης του AI Act είναι η πανθομολογούμενη επικινδυνότητα της Τεχνητής Νοημοσύνης²⁴⁰ και για τον λόγο αυτόν, η σχεδιαζόμενη υπερπεριπτωσιολογική και εκτενής ρύθμιση των διατάξεών του είναι κινδυνοκεντρική²⁴¹.

²³⁵ *European Commission*. (2018).

²³⁶ Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών «Τεχνητή νοημοσύνη για την Ευρώπη» COM(2018) 237 final. Έγγραφο με τίτλο «Ορισμός της τεχνητής νοημοσύνης: κύριες δυνατότητες και επιστημονικά πεδία» από την Ομάδα εμπειρογνομώνων υψηλού επιπέδου για την τεχνητή νοημοσύνη που εκδόθηκε στις 8 Απριλίου 2019.

²³⁷ *Council of the European Union*. (2022)

²³⁸ *Lawspot*. 2023.

²³⁹ Βλ. υποκεφ. 1.2.3. κατωτέρω.

²⁴⁰ *Μήτρου κ.α.* (2023), σελ.294

²⁴¹ *Hacker/ Berz*, «ZRP», 2023, σελ. 226.

Με τους κανόνες που θέτει ο AI Act, από τις εφαρμογές της Τεχνητής Νοημοσύνης, απαγορεύονται εκείνες που απειλούν τα δικαιώματα των πολιτών, η κοινωνική βαθμολόγηση, η προληπτική αστυνόμευση, όταν βασίζεται στην κατάρτιση προφίλ ενός ατόμου ή στην αξιολόγηση των χαρακτηριστικών του και η Τεχνητή Νοημοσύνη που δύναται να χειραγωγήσει την ανθρώπινη συμπεριφορά ή να εκμεταλλευτεί την ανθρώπινη συμπεριφορά²⁴².

Περαιτέρω, σε περίπτωση που τα συστήματα Τεχνητής Νοημοσύνης δεν τηρούν αρχεία καταγραφής της χρήσης τους και δεν εποπτεύονται από ανθρώπους, ώστε να τηρείται η διαφάνεια και η ακρίβεια, παρέχεται στους πολίτες το δικαίωμα για υποβολή καταγγελιών²⁴³, οι οποίοι μάλιστα θα λαμβάνουν εξηγήσεις για τυχόν αποφάσεις που βασίστηκαν σε συστήματα υψηλού κινδύνου και επηρεάζουν τα δικαιώματά τους.

Καταληκτικά, τα συστήματα Τεχνητής Νοημοσύνης πρέπει να τηρούν ορισμένες απαιτήσεις διαφάνειας, ενώ για τα ισχυρότερα μοντέλα Τεχνητής Νοημοσύνης που μπορούν να δημιουργήσουν συστημικούς κινδύνους, θα ισχύουν επιπλέον απαιτήσεις, όπως η αξιολόγησή τους και η εκτίμηση και ο περιορισμός των συστημικών κινδύνων²⁴⁴.

²⁴² «Τεχνητή Νοημοσύνη: Οι αλλαγές στη νομοθεσία - Έξι ειδικοί εξηγούν», διαθέσιμο στην ιστοσελίδα https://www.sofokleousin.gr/texniti-noimosyni-oi-allages-sti-nomothesia-eksi-eidikoi-eksigoun#goog_rewarded.

²⁴³ Κ. Χριστοδούλου, 2024

²⁴⁴ Lawspot, 2023

7.2. Η συμβολή της Τεχνητής Νοημοσύνης στην αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες

7.2.1. Η ενσωμάτωση της Τεχνητής Νοημοσύνης στον τομέα της νομιμοποίησης εσόδων.

Η διαρκής αύξηση του φαινομένου ξεπλύματος χρήματος²⁴⁵ οδήγησε τις εταιρείες και τα χρηματοπιστωτικά ιδρύματα στην εξεύρεση εναλλακτικών λύσεων για την εποπτεία και τον έλεγχο του φαινομένου, με σκοπό την μείωση των κινδύνων που προκαλεί, χρόνου επεξεργασίας καθώς και των οικονομικών πόρων²⁴⁶, που έπρεπε να διαθέσουν για την πρόληψη των οικονομικών εγκλημάτων. Συνεπεία του ανωτέρω, ήταν η ανάπτυξη νέων τεχνολογιών για την κΚΕΤ/ΧΤ η οποία έχει μάλιστα χαρακτηριστεί ως «ανερχόμενη επανάσταση»²⁴⁷. Τα πιο δημοφιλή μοντέλα ανίχνευσης της συγκεκριμένης απάτης είναι το μοντέλο m-score (Beneish²⁴⁸) και το μοντέλο F-score (Dechow²⁴⁹), τα οποία υπολογίζοντας πλειάδα χρηματοοικονομικών δεικτών, ανιχνεύουν, βάσει της υπέρβασης ή μη ενός ορισμένου ορίου τιμής, εάν υφίσταται κίνδυνος παραποίησης της οικονομικής κατάστασης του νομικού προσώπου. Έκτοτε, έχουν δημιουργηθεί πολλά μοντέλα ανίχνευσης, τα οποία βασίζονται στα μοντέλα Beneish και Dechow και επικεντρώνονται στην ανάλυση των οικονομικών καταστάσεων αναζητώντας τις μεθόδους που χρησιμοποιούνται για την σκόπιμη παραποίηση αυτών. Σύμφωνα μάλιστα με διεξαχθείσα έρευνα²⁵⁰, η μηχανική εκμάθηση και οι αλγόριθμοι της Τεχνητής Νοημοσύνης δύνανται να ανιχνεύσουν κατά ποσοστό 95% τις μεθόδους που χρησιμοποιούνται για την τέλεση

²⁴⁵ Στις ΗΠΑ κατά το έτος 2022, ο αριθμός των θυμάτων από παράνομα οικονομικά κέρδη ανήλθε σε 15 εκατομμύρια, ενώ το ύψος των κερδών ανήλθε σε 24 δισ. δολάρια ΗΠΑ, βλ. σχετικά *Javelin Strategy and Research*, “Identity fraud study: the virtual battleground”, *Javelin Report*, 2022, διαθέσιμο στην ιστοσελίδα: <https://javelinstrategy.com/2022-Identity-fraud-scams-report>.

²⁴⁶ *Walshe, J. and Cropper, T.*, 2018

²⁴⁷ *McKinsey and Company*, 2022.

²⁴⁸ *Beneish, Messod D.*, 1999, σελ. 24–36.

²⁴⁹ *Dechow, Patricia M.*, 2011, .17–42.

²⁵⁰ *Wyrobek J.*, 2020, σελ. 3037–3046.

του εγκλήματος της απάτης βάσει των ετήσιων χρηματοοικονομικών καταστάσεων της εταιρείας, από τις οποίες αποδεικνύεται η διάπραξη του ξεπλύματος χρήματος.

7.2.2. Τα οφέλη της Τεχνητής Νοημοσύνης στην αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες.

Ειδικά στον τραπεζικό τομέα, οι εθνικές νομοθεσίες και τα διεθνή πρότυπα²⁵¹ επιβάλλουν στα χρηματοπιστωτικά ιδρύματα και σε έτερες νομικές οντότητες εισηγμένες σε ρυθμιζόμενη αγορά την υποχρέωση να εντοπίζουν και να αναφέρουν ύποπτες συναλλαγές στις εθνικές με διοικητικές και ποινικές ποινές σε περίπτωση παράλειψης. Οι ΜΧΠ συλλέγουν και αναλύουν ύποπτες χρηματοοικονομικές συναλλαγές (SARs) που λαμβάνονται από ιδιωτικούς φορείς και μεταδίδουν τα αποτελέσματα στους αρμόδιους εκ του νόμου διαχειριστές για την μετέπειτα αναγκαία παρακολούθηση της συναλλαγής²⁵².

Τα εργαλεία της Τεχνητής Νοημοσύνης μπορούν να συμβάλλουν αποτελεσματικά στην εκπλήρωση της ανωτέρω υποχρέωσης των χρηματοπιστωτικών ιδρυμάτων, δεδομένου ότι βασιζόμενα στη μηχανική εκμάθηση, μπορούν να επιτρέψουν την άμεση επεξεργασία μεγάλου όγκου δεδομένων, να αναλύσουν μοτίβα συμπεριφοράς των πελατών και να εντοπίσουν τυχόν ύποπτες συναλλαγές άμεσα και με ακρίβεια²⁵³. Ως εκ τούτου, συνιστούν αρωγό στην πρόληψη και στην αντιμετώπιση της νομιμοποίησης εσόδων από ΚΕΤ/ΧΤ.²⁵⁴

Ήδη οι υπόχρεες οντότητες²⁵⁵ έχουν ξεκινήσει να εντάσσουν την Τεχνητή Νοημοσύνη στον τρόπο εντοπισμού και καταπολέμησης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και την πρόληψη της απάτης, καθώς μέσω της Τεχνητής Νοημοσύνης τους παρέχονται εργαλεία τα οποία δύνανται να

²⁵¹ Όπως η FATF Recommendation no. 20.

²⁵² Silvia Allegranza, "The proposed Anti-Money Laundering Authority, FIU cooperation, powers and exchanges of information", Study requested by the ECON Committee, 2022, σελ. 35.

²⁵³ Excell, D., 2019.

²⁵⁴ Astrid Bertrand, Winston Maxwell and Xavier Vamparys 2020,

²⁵⁵ Fernandez Ana, 2019.

χρησιμοποιήσουν δεδομένα από διάφορες πηγές και σε διαφορετικές γλώσσες (λ.χ. αριθμητικά δεδομένα, έγγραφα, προφορικές επικοινωνίες, βιομετρική αναγνώριση προσώπου, μητρώα εταιρειών και δικαιούχων κ.λπ.), προκειμένου να ανιχνεύσουν με μεγαλύτερη ακρίβεια τα άτομα/πρόσωπα που εμπλέκονται σε υποθέσεις απάτης²⁵⁶. Αξιοσημείωτο είναι επίσης ότι τα εργαλεία που βασίζονται στην Τεχνητή Νοημοσύνη μπορούν να ανιχνεύσουν τις μητρικές γλώσσες των πελατών βάσει ανάλυσης γραπτών επικοινωνιών των ύποπτων μερών, να εντοπίσουν παραποιημένες ψηφιακές εικόνες ή πηγές βίντεο, καθώς και δεδομένα GPS κινητών τηλεφώνων των πελατών για την αξιολόγηση των κινδύνων νομιμοποίησης εσόδων από παράνομες δραστηριότητες²⁵⁷.

Περαιτέρω, η Τεχνητή Νοημοσύνη προωθεί την αυτοματοποίηση των διαδικασιών της παρακολούθησης ύποπτων συναλλαγών και της συνακόλουθης αναφοράς αυτών, με αποτέλεσμα τον περιορισμό των σφαλμάτων που μπορούν να συμβούν κατά τον εντοπισμό των φαινομένων²⁵⁸. Ως σφάλματα κατά τον εντοπισμό, νοούνται εκείνα που συμβαίνουν από ανθρώπινο παράγοντα, λόγω της υποκειμενικής αντίληψης των χειριστών των συστημάτων ή λόγω έλλειψης εμπειρίας αυτών²⁵⁹. Με τη βοήθεια της μηχανικής εκμάθησης, τα χρηματοπιστωτικά ιδρύματα μπορούν να ανιχνεύσουν τυχόν σφάλματα στα δεδομένα και να αξιοποιήσουν τις πηγές που λαμβάνουν σε τόσο υψηλό βαθμό ακρίβειας, που θα ήταν εξαιρετικά δυσχερές να επιτευχθεί με έναν μη αυτόματο τρόπο (ήτοι αποκλειστικά με ανθρώπινο παράγοντα^{260 261}). Χαρακτηριστική είναι η υπόθεση της Danske Bank, η οποία κατόπιν των συνεπειών ενός τεράστιου σκανδάλου ξεπλύματος μαύρου χρήματος,²⁶² υιοθέτησε λύσεις βασισμένες στην τεχνητή νοημοσύνη για τη

²⁵⁶ FATF, "Opportunities and Challenges of New Technologies for AML/CFT", FATF Report, 2021a, Paris.

²⁵⁷ European Banking Authority (EBA), (2017)

²⁵⁸ Ο.π. Pavlidis, 2023, σελ. 158

²⁵⁹ Institute of International Finance, 2018.

²⁶⁰ Bertrand, Astrid, Maxwell, Winston, and Vamparys, Xavier. (2020), σελ. 15.

²⁶¹ Köbis, Nils, Starke, Christopher, & Rahwan, Iyad. (2021), σελ. 5.

²⁶² Το σκάνδαλο της Danske Bank με το ξέπλυμα βρώμικου χρήματος προέκυψε το 2017-2018, όταν έγινε γνωστό ότι περίπου 800 δισεκατομμύρια ευρώ ύποπτων συναλλαγών είχαν εισρεύσει από εσθονικές, ρωσικές, λετονικές και άλλες πηγές μέσω του υποκαταστήματος τράπεζας της Danske Bank με έδρα στην

βελτίωση της διαδικασίας παρακολούθησης των ροών εντός του δικτύου της τράπεζας. Η τράπεζα ενσωμάτωσε αλγόριθμους μηχανικής μάθησης για να εντοπίσει κόκκινες σημαίες και ασυνήθιστες δραστηριότητες επισημαίνοντας εκείνες που θα μπορούσαν να είναι δυνητικά ύποπτες ώστε να επιταχύνει τη διαδικασία λήψης αποφάσεων και να παρέχει έγκαιρη αναφορά στους ρυθμιστικούς οργανισμούς.²⁶³

Εξασφαλίζοντας έτσι, η εφαρμογή της διαφάνειας στον τομέα της συλλογής μεγάλου όγκου δεδομένων, της ανάλυσης τους, της ανίχνευσης και πρόβλεψης πιθανών κινδύνων για ύποπτες συμπεριφορές²⁶⁴.Επιπλέον, η Τεχνητή Νοημοσύνη μπορεί να βελτιστοποιήσει την βαθμολόγηση του κινδύνου που φέρει έκαστος αντισυμβαλλόμενος των χρηματοπιστωτικών ιδρυμάτων, εστιάζοντας σε επικίνδυνα προφίλ πελατών διά της χρήσης αλγορίθμων, οι οποίοι εξοικονομούν σημαντικό χρόνο και φόρτο εργασίας από τους υπεύθυνους στην (κανονιστική) συμμόρφωση των τραπεζών²⁶⁵.Επιπλέον έτερος τρόπος, συνιστά ο εντοπισμός μοτίβων συμπεριφορών (ακόμη και μέσω των κοινωνικών δικτύων) εκάστου πελάτη, οι οποίες αποκλίνουν από τις συνήθειες κι ως εκ τούτου κρίνονται ως επικίνδυνες για την τέλεση οικονομικών εγκλημάτων. Ιδιαίτερα σημαντικό κρίνεται το γεγονός ότι οι αλγόριθμοι μπορούν να εντοπίσουν όχι μόνον τα υφιστάμενα μοτίβα ύποπτων συμπεριφορών, αλλά και να ανακαλύψουν νέα, ακόμη και ιδιαίτερα περίπλοκα, τα οποία θα ήταν δυσπρόσιτα και μη αντιληπτά από τον άνθρωπο²⁶⁶.

Εσθονία από το 2007 έως το 2015 και θεωρείται πιθανώς το μεγαλύτερο σκάνδαλο ξεπλύματος βρώμικου χρήματος στην Ευρώπη. Πηγή: https://www-cbsnews-com.translate.google.com/news/how-the-danske-bank-money-laundering-scheme-involving-230-billion-unraveled-60-minutes-2019-05-19/?x_tr_sl=auto&x_tr_tl=el&x_tr_hl=el&x_tr_pto=wapp

²⁶³ Aml Watcher, 2024 **7 Use Cases Of Artificial Intelligence In Anti-Money Laundering**

²⁶⁴ Metz, Cade, & Satariano, Adam. (2020)

²⁶⁵ Wang, Su-Nan, & Yang, Jian-Gang. (2007).

²⁶⁶ Drausin Wulsin and others, (2012)

7.3. Οι επιρροές της Τεχνητής Νοημοσύνης για την αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες στο πεδίο των προσωπικών δεδομένων

7.3.1 Οι επιρροές της Τεχνητής Νοημοσύνης στο πεδίο των προσωπικών δεδομένων.

Αποτελεί κοινό τόπο ότι με την αδιάλειπτα αυξανόμενη χρήση της Τεχνητής Νοημοσύνης, προκύπτουν ζητήματα ως προς την προστασία της ιδιωτικότητας του ατόμου και ιδίως ως προς την πιθανότητα παραβίασης του ΓΚΠΔ, κατά τη λειτουργία των συστημάτων της Τεχνητής Νοημοσύνης²⁶⁷, γεγονός που υπονομεύει τη νομιμότητα της χρήσης τέτοιου είδους συστημάτων²⁶⁸. Η Τεχνητή Νοημοσύνη είναι ικανή να κατασκευάσει λεπτομερώς το προφίλ της ζωής κάποιου ατόμου, όπως προαναφέρθηκε, προκειμένου να χρησιμοποιηθεί από ιδιώτες, επιχειρήσεις, καθώς και από τις αρμόδιες αρχές ελέγχου συμμόρφωσης για τη νομιμοποίηση εσόδων, γεγονός που εγείρει σοβαρές υπόνοιες παράνομης επεξεργασίας των δεδομένων των προσώπων²⁶⁹.

Ειδικότερα, σε περίπτωση που η επεξεργασία των δεδομένων πραγματοποιείται αυτόματα μέσω των συστημάτων της Τεχνητής Νοημοσύνης, εγκυμονεί ο κίνδυνος να μεταβληθεί ο σκοπός της επεξεργασίας, δίχως να γίνει αντιληπτή η εν λόγω αλλαγή από το υποκείμενο της επεξεργασίας²⁷⁰. Μολονότι υποστηρίζεται ότι η Τεχνητή Νοημοσύνη προσφέρει διαφάνεια στην αντιμετώπιση των παράνομων δραστηριοτήτων, από μία έτερη οπτική, μπορεί να υποστηριχθεί επαρκώς και η άποψη ότι οι διαδικασίες της Τεχνητής Νοημοσύνης είναι αδιαφανείς για το υποκείμενο της επεξεργασίας με αποτέλεσμα να περιέρχεται σε αδυναμία να ενημερωθεί, ως οφείλει και ως δικαιούται²⁷¹. Πολλοί αλγόριθμοι μάλιστα, έχουν χαρακτηριστεί ως “black boxes”, δηλαδή «μαύρα κουτιά», διότι ο τρόπος λειτουργίας τους είναι δύσκολα κατανοητός και η πρόσβαση στον τρόπο λειτουργίας τους είναι

²⁶⁷ Τσινόρεμα, Αλεξάνδρα, 2020

²⁶⁸ Ο.π. Nils Köbis, Christopher Starke & Iyad Rahwa, 2021

²⁶⁹ Politou κ.α, 2019.

²⁷⁰ ό.π. Χριστοδούλου

²⁷¹ Αρθ. 13 παρ. 1 και 14 παρ. 1 ΓΚΠΔ.

αδύνατη, ενώ συχνά λαμβάνουν αποφάσεις που είναι μη κατανοητές ή μη αναμενόμενες. Το εν λόγω πρόβλημα ωστόσο, κατά μία άποψη²⁷², θα μπορούσε να επιλυθεί με την ειδικότερη ενημέρωση του υποκειμένου για το μεταβαλλόμενο σκοπό της επεξεργασίας. Για την κατ' εξαίρεσιν επεξεργασία των ευαίσθητων προσωπικών δεδομένων θα πρέπει να τηρούνται αυστηρά οι επιταγές της αρχής της αναλογικότητας, ήτοι το επίμαχο σύστημα της Τεχνητής Νοημοσύνης να είναι αναγκαίο για την κάλυψη της προσδιορισθείσας ανάγκης, να είναι αποτελεσματικό όσον αφορά την κάλυψη της εν λόγω ανάγκης, με βάση τα συγκεκριμένα χαρακτηριστικά της τεχνολογίας και τέλος, ο προκύπτων περιορισμός της ιδιωτικότητας να είναι ανάλογος με το αναμενόμενο όφελος και τέλος^{273 274}. Σε κάθε περίπτωση, θα πρέπει να εξεταστεί εάν ένα μέσο το οποίο θα είχε μειωμένες επιπτώσεις στην ιδιωτικότητα του ατόμου θα μπορούσε να επιτύχει τον αυτό επιδιωκόμενο σκοπό²⁷⁵.

Σε κάθε περίπτωση, καθοριστικό ρόλο στο πλαίσιο της νομιμότητας της επεξεργασίας των δεδομένων από τα συστήματα της Τεχνητής Νοημοσύνης καταλαμβάνει η συγκατάθεση του υποκειμένου των δεδομένων, όπως αυτή ορίζεται στο άρθρο 4 παρ. 11 του ΓΚΠΔ²⁷⁶. Συγκεκριμένα, στο ανωτέρω άρθρο προβλέπεται ότι η συγκατάθεση πρέπει να είναι συγκεκριμένη, ρητή, ελεύθερη και εν γνώσει του υποκειμένου, η οποία πραγματοποιείται είτε με δήλωση του υποκειμένου, είτε με άλλη συγκεκριμένη και αναμφίβολη ενέργειά του, εκ της οποίας προκύπτει ότι συναινεί στην επεξεργασία των προσωπικών του δεδομένων²⁷⁷. Η λήψη βέβαια εξ αρχής της συγκατάθεσης του υποκειμένου στην επεξεργασία των δεδομένων μπορεί

²⁷² Βορράς/Μήτρον, ΔΙΤΕ, (π. ΔΙΜΕΕ), 2018, σελ. 464.

²⁷³ Ανδρουλάκη, 2021

²⁷⁴ Για την αρχή της αναλογικότητας βλ. κατωτέρω κεφ. 1.3.2.

²⁷⁵ Παναγοπούλου-Κουτνατζή Φ., 2019

²⁷⁶ Άρθ. 4 παρ. 11 ΓΚΠΔ: «συγκατάθεση» του υποκειμένου των δεδομένων: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν».

²⁷⁷ Ζ Παναγόπουλος, 2021 ό.π., σελ. 43 επ., διαθέσιμο στην ιστοσελίδα <https://ikee.lib.auth.gr/record/330313/files/GRI-2021-30390.pdf>.

να αποτελέσει πρόβλημα, καθώς κατά τη λήψη μίας απόφασης από έναν αλγόριθμο ή κατά την ανάλυση δεδομένων, μπορεί να εμπλακούν επεξεργασίες, οι οποίες συχνά δεν δύνανται να οριοθετηθούν εκ των προτέρων. Ως εκ τούτου, ανακύπτει εύλογα προβληματισμός σχετικά με τη δυνατότητα προηγούμενης πλήρης ενημέρωσης του υποκειμένου για τους σκοπούς της επεξεργασίας των δεδομένων του, λαμβανομένων υπόψιν της αυτονομίας των συστημάτων της Τεχνητής Νοημοσύνης, της δημιουργίας συσχετίσεων μεταξύ των δεδομένων και της αλλαγής των σκοπών της επεξεργασίας²⁷⁸.

7.3.2 Η περίπτωση της αυτοματοποιημένης κατάρτισης προφίλ στον Νέο Κανονισμό 2024/1624

Αξιοσημείωτο είναι ότι οι διαδικασίες που χρησιμοποιούνται για την πρόληψη και αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες είναι ιδιαίτερα παρεμβατικές στις ζωές των υπό εξέταση υποκειμένων, διότι αναλύουν όλα ανεξαιρέτως τα δεδομένα των συναλλαγών και δημιουργούν προφίλ κινδύνου (Risk Profiles)²⁷⁹. Ως δημιουργία προφίλ (Profiling) ορίζεται η καταγραφή και ανάλυση των συμπεριφορικών και ψυχολογικών χαρακτηριστικών ενός ατόμου, με σκοπό την πρόβλεψη των τάσεων και της συμπεριφοράς του σε συγκεκριμένο πλαίσιο συνθηκών²⁸⁰. Η δημιουργία προφίλ διακρίνεται σε κατηγορίες και συγκεκριμένα σε ομαδική και ατομική ή εξατομικευμένη δημιουργία προφίλ. Στην πρώτη περίπτωση (ομαδική κατάρτιση προφίλ²⁸¹) η κατηγοριοποίηση των ατόμων γίνεται ανά ομάδες με βάση συγκεκριμένα χαρακτηριστικά της προσωπικότητάς τους ή την συναισθηματική τους κατάσταση, ενώ στη δεύτερη περίπτωση (ατομική ή εξατομικευμένη κατάρτιση προφίλ²⁸²) τα δεδομένα εξάγονται αποκλειστικά από ένα εξατομικευμένο υποκείμενο. Στόχος της ανωτέρω διαδικασίας είναι η αναφορά της

²⁷⁸ Κωστή Η..

²⁷⁹ ό.π Bertrand κ.α. σελ. 17

²⁸⁰ ό.π Politou,2019 κ.α.

²⁸¹ Politou, Eugenia, Alepis, Efthimios, & Patsakis, Constantinos,2017.

²⁸²Hildebrandt, M,2008

εγκληματικής δραστηριότητας, η οποία ωστόσο απαιτεί ειδικές διασφαλίσεις, σύμφωνα με το άρθρο 10 του ΓΚΠΔ^{283 284}.

Υπό αυτό το πρίσμα, στο νέο Κανονισμό, παρατηρείται ότι έχει εισαχθεί σε αντίθεση με την αρχική πρότασή του 2021, ειδική πρόβλεψη αναφορικά με την χρήση Τεχνητής Νοημοσύνης και της αυτοματοποιημένης κατάρτισης προφίλ. Πιο συγκεκριμένα, ορίζεται ότι οι υπόχρεες οντότητες μπορούν να εκδίδουν αποφάσεις που προκύπτουν από αυτοματοποιημένες διαδικασίες, συμπεριλαμβανομένης της κατάρτισης προφίλ²⁸⁵ όπως ορίζεται στο άρθρο 4 σημείο 4) ΓΚΠΔ ή από διαδικασίες που περιλαμβάνουν συστήματα Τεχνητής Νοημοσύνης²⁸⁶ υπό την προϋπόθεση ότι:

α) τα δεδομένα που υπόκεινται σε επεξεργασία από τα εν λόγω συστήματα περιορίζονται στα δεδομένα που αποκτώνται δυνάμει των όσων προβλέπονται κατά την διαδικασία της δέουσας επιμέλειας

β) κάθε απόφαση σύναψης ή άρνησης σύναψης ή διατήρησης επιχειρηματικής σχέσης με πελάτη ή εκτέλεσης ή άρνησης εκτέλεσης περιστασιακής συναλλαγής για πελάτη, ή αύξησης ή μείωσης της έκτασης των μέτρων δέουσας επιμέλειας ως προς

²⁸³ Άρθρο 10 ΓΚΠΔ: «Επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας που βασίζονται στο άρθρο 6 παράγραφος 1 διενεργείται μόνο υπό τον έλεγχο επίσημης αρχής ή εάν η επεξεργασία επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους το οποίο προβλέπει επαρκείς εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Πλήρες ποινικό μητρώο τηρείται μόνο υπό τον έλεγχο επίσημης αρχής».

²⁸⁴ Άρθρο 9 παρ. 1 ΓΚΠΔ: «Απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό».

²⁸⁵ Άρθρο 4 σημ. 4 ΓΚΠΔ: 4«κατάρτιση προφίλ»: οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου,

²⁸⁶ όπως ορίζονται στο άρθρο 3 σημείο 1) του κανονισμού (ΕΕ) 2024/... του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

τον πελάτη²⁸⁷, υπόκειται σε ουσιαστική ανθρώπινη παρέμβαση για τη διασφάλιση της ακρίβειας και της καταλληλότητας μιας τέτοιας απόφασης, και

γ)ο πελάτης μπορεί να λάβει εξηγήσεις σχετικά με την απόφαση στην οποία κατέληξε η υπόχρεη οντότητα και μπορεί να προσβάλει την εν λόγω απόφαση, εκτός αν σχετίζεται με αναφορά κατά τα οριζόμενα στο άρθρο 69 του Κανονισμού, *περι αναφοράς υπονοιών*.²⁸⁸

Ως εκ τούτου, δυνάμει των παραπάνω, προβλέπεται ότι προκειμένου οι υπόχρεες οντότητες να συμμορφωθούν με τους σκοπούς του Κανονισμού, θα έχουν τη δυνατότητα να θεσπίζουν διαδικασίες που επιτρέπουν την αυτοματοποιημένη ατομική λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, αλλά σύμφωνα με όσα ορίζεται στο άρθρο 22 ΓΚΠΔ.²⁸⁹

Πιο συγκεκριμένα, η παράγραφος 1 του ως άνω άρθρου του ΓΚΠΔ παρέχει στο υποκείμενο το δικαίωμα να μην υπόκειται σε αυτοματοποιημένη επεξεργασία που οδηγεί σε απόφαση η οποία το επηρεάζει σημαντικά ή παράγει έννομα αποτελέσματα που το αφορούν. Το άρθρο 22, όμως ορίζει πως δεν επιτρέπεται γενικά η επεξεργασία που αφορά την αυτοματοποιημένη επεξεργασία, συμπεριλαμβανόμενης της κατάρτισης προφίλ, εκτός αν υπάρχουν συγκεκριμένες προϋποθέσεις, που αποτελούν τις εξαιρέσεις στον κανόνα. Επιγραμματικά αυτές είναι: η ανάγκη σύναψη σύμβασης, νομοθεσία του κράτους μέλους ή της ΕΕ που επιτρέπει την επεξεργασία και η συγκατάθεση του ατόμου.²⁹⁰

²⁸⁷ εφαρμόζονται σύμφωνα με το άρθρο 20 Κανονισμού

²⁸⁸ Άρθρο 76 Κανονισμού

²⁸⁹ Στο πλαίσιο αυτό, οι απαιτήσεις του παρόντος κανονισμού για τη διασφάλιση των δικαιωμάτων των προσώπων που υπόκεινται σε τέτοιες διαδικασίες θα πρέπει να εφαρμόζονται επιπλέον κάθε άλλης σχετικής απαίτησης που ορίζεται στο δίκαιο της Ένωσης σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα.

²⁹⁰ Άρθρο 22 παρ. 2 ΓΚΠΣ: 2. Η παράγραφος 1 δεν εφαρμόζεται όταν η απόφαση:

α) είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας των δεδομένων,

β) επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας και το οποίο προβλέπει επίσης κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων ή

Εν προκειμένω, ισχύει η δεύτερη περίπτωση, κατά την οποία αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, μπορεί δυναμικά να πραγματοποιείται βάσει του άρθρου 22 παράγραφος 2 στοιχείο β) εφόσον η χρήση της προβλέπεται από το δίκαιο της Ένωσης ή κράτους μέλους. Η σχετική νομοθεσία πρέπει επίσης να θεσπίζει κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων. Στην αιτιολογική σκέψη 71 του ΓΚΠΔ αναφέρεται ότι η σχετική νομοθεσία μπορεί να περιλαμβάνει μεταξύ άλλων τη χρήση της αυτοματοποιημένης λήψης αποφάσεων που ορίζεται στο άρθρο 22 παράγραφος 2 για σκοπούς παρακολούθησης και πρόληψης της απάτης και της φοροδιαφυγής, ή προκειμένου να διασφαλιστεί η ασφάλεια και η αξιοπιστία της υπηρεσίας που παρέχει ο υπεύθυνος επεξεργασίας.²⁹¹ Απαραίτητη ωστόσο προϋπόθεση, σύμφωνα με τις επιταγές του ΓΚΠΔ είναι η πρόβλεψη κατάλληλων μέτρων για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων. Πράγματι αυτό φαίνεται να ρυθμίζεται στον Κανονισμό, καθώς υπάρχει ρητή διάταξη σύμφωνα με την οποία «κάθε απόφαση σύναψης ή άρνησης σύναψης ή διατήρησης επιχειρηματικής σχέσης με πελάτη ή εκτέλεσης ή άρνησης εκτέλεσης περιστασιακής συναλλαγής για πελάτη, ή αύξησης ή μείωσης της έκτασης των μέτρων δέουσας επιμέλειας ως προς τον πελάτη²⁹², υπόκειται σε ουσιαστική ανθρώπινη παρέμβαση για τη διασφάλιση της ακρίβειας και της καταλληλότητας μιας τέτοιας απόφασης».

Η σημασία της ως άνω πρόβλεψης είναι καθοριστική καθώς ο ΓΚΠΔ αναγνωρίζει ότι η αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, μπορεί να έχει σοβαρές συνέπειες για τα φυσικά πρόσωπα. Ο ΓΚΠΔ δεν προσδιορίζει τους όρους «έννομα» ή «σημαντικά αποτελέσματα με παρόμοιο τρόπο», ωστόσο, η διατύπωση καθιστά σαφές ότι το άρθρο 22 καλύπτει

γ) βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

²⁹¹ ΑΠΔΠΧ, 2020 σελ. 29

²⁹² εφαρμόζονται σύμφωνα με το άρθρο 20 Κανονισμού

μόνο τις σοβαρές συνέπειες.²⁹³ Συναφώς, εφιστάται εκ προοιμίου, η προσοχή στο γεγονός ότι στην αιτιολογική σκέψη 71 του ΓΚΠΔ γίνεται ρητώς μνεία σε «αυτόματη άρνηση επιγραμμικής αίτησης πίστωσης» ως χαρακτηριστικό παράδειγμα απόφασης που επηρεάζει «σημαντικά» το υποκείμενο των δεδομένων.²⁹⁴

Εν προκειμένω, είναι τουλάχιστον πρόδηλο, ότι η λήψη μιας απόφασης η οποία καθορίζει την σύναψη ή άρνηση σύναψη μίας σύμβασης ή διατήρηση ή λήξη μιας ήδη επιχειρηματικής σχέσης με πελάτη, αποτελεί κάτι παραπάνω από σοβαρή συνέπεια, καθώς επηρεάζει αφενός την οικονομική ελευθερία και τα συμφέροντα του πελάτη, αλλά μπορεί να επηρεάσει ανεπανόρθωτα την φήμη και την αξιοπιστία του στις συναλλαγές, μόνο με την υπόνοια ότι σχετίζεται με το ποινικό αδίκημα της νομιμοποίησης εσόδων από παράνομες δραστηριότητες.

Ως εκ τούτου, η ανθρώπινη παρέμβαση η οποία πρέπει να προβλέπεται στο συγκεκριμένο είδος αυτοματοποιημένης επεξεργασίας δεδομένων, διασφαλίζει ότι το υποκείμενο των δεδομένων θα έχει τη δυνατότητα να διατυπώσει την άποψή του, να λάβει αιτιολόγηση της απόφασης που ελήφθη στο πλαίσιο της εν λόγω αξιολόγησης και σε περίπτωση διαφωνίας με την εν λόγω απόφαση, να την αμφισβητήσει.²⁹⁵

Πέραν του περιορισμού της ιδιωτικότητας του ατόμου που παρατηρείται στη χρήση των συστημάτων της Τεχνητής Νοημοσύνης, ενδέχεται να επηρεάζεται η ανθρώπινη αξιοπρέπεια και ο σεβασμός της ιδιωτικής ζωής του ατόμου, δικαιώματα που προστατεύονται βάσει των άρθρων 7 και 8 του Χάρτη Θεμελιωδών Δικαιωμάτων²⁹⁶. Οι αλγόριθμοι είναι σχεδιασμένοι για να ανιχνεύουν τη συμπεριφορά των ανθρώπων και να δημιουργούν εξατομικευμένα προφίλ υπόπτων

²⁹³ Ο.π. ΑΠΔΠΧ, 2020 σελ. 25

²⁹⁴ Βλ. απόφαση ΔΕΕ C-204/21, ΟQ κατά Land Hessen, παρισταμένης της SCHUFA Holding AG, παρ. 21

²⁹⁵ Βλ. απόφαση ΔΕΕ C-204/21, ΟQ κατά Land Hessen, παρισταμένης της SCHUFA Holding AG, παρ. 19

²⁹⁶ Ανδρουλάκη Ε., ό.π., σελ. 14

με υψηλή ακρίβεια,²⁹⁷. Το γεγονός αυτό βάλει πρωτίστως την πληροφοριακή ιδιωτικότητα του ατόμου, ήτοι το δικαίωμά του να διαχειρίζεται αυτοτελώς τις πληροφορίες που τον αφορούν σε σχέση με τις προτιμήσεις, τις πεποιθήσεις και τις αξίες του, καθώς και άλλες ευαίσθητες πληροφορίες που δύνανται να διαμορφώσουν την ταυτότητά του²⁹⁸. Η πληροφοριακή αυτή ιδιωτικότητα αποτελεί στην πραγματικότητα μια αντανάκλαση της ανθρώπινης αξιοπρέπειας²⁹⁹.

Περαιτέρω, προκειμένου να τηρούνται οι επιταγές της αρχής του σεβασμού της ανθρώπινης αυτονομίας προϋποτίθεται ότι τα συστήματα Τεχνητής Νοημοσύνης πρέπει να υποστηρίζουν την ανθρώπινη δράση και λήψη αποφάσεων. Μολαταύτα, στα συστήματα αυτοματοποιημένης λήψης αποφάσεων, χρησιμοποιείται η εξόρυξη δεδομένων (data mining) και η προγνωστική ανάλυση (predictive analytics)³⁰⁰, μέθοδοι που περιορίζουν τον ανθρώπινο έλεγχο μόνον στις αποφάσεις σχεδιασμού και σε διαδικασίες επανεξέτασης, που τυχόν απαιτηθούν μετά τη λήψη της απόφασης. Η προγνωστική ανάλυση συνιστά μία τεχνική ευρέως διαδεδομένη ιδίως στον τραπεζικό κλάδο, η οποία χρησιμοποιείται με σκοπό την πρόβλεψη πιστωτικών κινδύνων, προβλέποντας τάσεις και πρότυπα συμπεριφοράς μέσω των δεδομένων και των πληροφοριών που εξάγει. Η προαναφερθείσα πρόβλεψη όμως σε συνδυασμό με την εφαρμογή προληπτικών στρατηγικών, κατά τις οποίες τα άτομα οδηγούνται σε συγκεκριμένη συμπεριφορά μέσω της απόρριψης ανεπιθύμητων επιλογών, προσβάλλει την αυτονομία και τον πληροφοριακό αυτοκαθορισμό των ατόμων³⁰¹.

Πέραν των ανωτέρω, τα συστήματα Τεχνητής Νοημοσύνης ενδέχεται να παρεμβαίνουν στο δικαίωμα έκφρασης³⁰² ³⁰³. Εάν υποκείμενα των δεδομένων,

²⁹⁷Blazquez, Desamparados, & Domenech, Josep, 2018.

²⁹⁸ Παναγιωτίδου, Μαρίνα-Ευθυμία, 2020

²⁹⁹ Glancy, Dorothy J. (2012).

³⁰⁰ Sloan, H. R., & Warner, R. (2018),σελ. 1-4.

³⁰¹Bayamlıoğlu, Emre,2018, σελ. 18.

³⁰² Αρθ. 11 παρ. 1 του Χάρτη Θεμελιωδών Δικαιωμάτων: «Κάθε πρόσωπο έχει δικαίωμα στην ελευθερία έκφρασης. Το δικαίωμα αυτό περιλαμβάνει την ελευθερία γνώμης και την ελευθερία λήψης ή μετάδοσης πληροφοριών ή ιδεών, χωρίς την ανάμειξη δημοσίων αρχών και αδιακρίτως συνόρων».

³⁰³ Bertrand, Astrid, Maxwell, Winston, and Vamparys, Xavier,2020

ενδεικτικά πελάτες τραπεζών θεωρούν ότι τα δεδομένα που χρησιμοποιούνται στις συναλλαγές τους παρακολουθούνται, το γεγονός αυτό τους αποτρέπει από το να προβούν σε ορισμένου είδους συναλλαγές, τη μυστικότητα και την ιδιωτικότητα των οποίων θέλουν κρατήσουν, όπως λ.χ. εμβάσματα προς φιλανθρωπικές οργανώσεις³⁰⁴. Συνεπώς, τα συστήματα Τεχνητής Νοημοσύνης που χρησιμοποιούνται για την αντιμετώπιση του ξεπλύματος χρήματος, μπορούν να επηρεάσουν αρνητικώς την αποτελεσματική προστασία για την οποία αρχικώς ρυθμίστηκαν, λόγω της ελλιπούς πληροφόρησης των ατόμων και της αδυναμίας τους να αμφισβητήσουν τη διαδικασία της επεξεργασίας των προσωπικών τους δεδομένων, λαμβανομένου υπόψιν ειδικά της αδιαφάνειας που ενδέχεται να τα χαρακτηρίζει, ως αναφέρθηκε ανωτέρω³⁰⁵. Το αποτέλεσμα φυσικά, είναι η προφανής παρέμβαση των συστημάτων Τεχνητής Νοημοσύνης που τηρούνται για την πρόληψη του ξεπλύματος χρήματος, στα θεμελιώδη δικαιώματα των πελατών των τραπεζών, ανεξαρτήτως του αν οι προαναφερθέντες υπέστησαν τελικώς δυσμενείς συνέπειες λόγω της παρέμβασης αυτής^{306 307}.

Συμπερασματικά, η ενσωμάτωση της τεχνητής νοημοσύνης στο οπλοστάσιο της ΚΕΤ/ΧΤ δημιουργεί έναν ισχυρό μηχανισμό ανίχνευσης οικονομικών εγκλημάτων ικανό να διαδραματίσει καθοριστικό ρόλο μελλοντικά στην πρόληψη και καταστολή του ξεπλύματος χρήματος. Η Τεχνητή Νοημοσύνη παρέχει τη δυνατότητα ανάλυσης και αξιολόγησης δεδομένων με τρόπο που δεν ήταν δυνατός με τις παραδοσιακές μεθόδους, καθιστώντας την ένα πολύτιμο εργαλείο για τις αρμόδιες αρχές και τις υπόχρεες οντότητες η εφαρμογή της Τεχνητής Νοημοσύνης δεν είναι χωρίς προκλήσεις καθώς η ανάγκη για συμμόρφωση με τον ΓΚΠΔ είναι καθοριστική δεδομένου ότι η επεξεργασία και διατήρηση μεγάλου όγκου

³⁰⁴ Βλ. απόφαση ΔΕΕ «*La Quadrature du Net (C-511/18)*», παρ. 113

³⁰⁵ Βλ. κεφ. 1.3.1 ανωτέρω.

³⁰⁶ Βλ. απόφαση ΔΕΕ «*La Quadrature du Net (C-511/18)*», ό.π., παρ. 115.

³⁰⁷ Βλ απόφαση ΕΔΔΑ, «*Breyer κατά Γερμανίας (C-582/14)*», 30.01.2020, παρ. 81, διαθέσιμο στην ιστοσελίδα <https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EL>.

προσωπικών δεδομένων από την Τεχνητή Νοημοσύνη μπορεί να παραβιάζει τα δικαιώματα των υποκειμένων δεδομένων εάν δεν γίνεται με τον κατάλληλο τρόπο.

Συνολικά, η επιτυχία της Τεχνητής Νοημοσύνης στην καταπολέμηση της νομιμοποίησης εσόδων εξαρτάται από την ικανότητα των οργανισμών να διαχειριστούν αποτελεσματικά αυτές τις προκλήσεις, υιοθετώντας πρακτικές που θα προστατεύουν τα προσωπικά δεδομένα χωρίς να υπονομεύουν την αποτελεσματικότητα της τεχνητής νοημοσύνης. Οι ρυθμιστικές αρχές θα πρέπει να είναι σε επαγρύπνηση, ώστε να εξασφαλίζουν μια βιώσιμη και ηθικά ορθή χρήση της ΑΙ στον χρηματοοικονομικό τομέα.

ANTI ΕΠΙΛΟΓΟΥ

Ολοκληρώνοντας, η σύνδεση μεταξύ της ΚΕΤ/ΧΤ από παράνομες δραστηριότητες και της προστασίας προσωπικών δεδομένων αναδεικνύει για τη λεπτή ισορροπία που πρέπει να επιτευχθεί μεταξύ ασφάλειας, προστασίας του δημοσίου συμφέροντος και ιδιωτικότητας. Ενώ η εφαρμογή των πολιτικών ΚΕΤ/ΧΤ πρέπει να γίνεται με σεβασμό στα ατομικά δικαιώματα και στις αρχές προστασίας των προσωπικών δεδομένων, εξασφαλίζοντας ότι η επεξεργασία προσωπικών δεδομένων γίνεται με νόμιμο, διαφανή και αναλογικό τρόπο, περιορίζοντας τις πιθανότητες κατάχρησης της εξουσίας.

Επιπλέον, η ενσωμάτωση της Τεχνητής Νοημοσύνης στο πλαίσιο της ΚΕΤ/ΧΤ φέρνει νέες προκλήσεις και ευκαιρίες. Η Τεχνητή Νοημοσύνη μπορεί να βελτιώσει σημαντικά την ανίχνευση ύποπτων συναλλαγών και να ενισχύσει την αποτελεσματικότητα των μηχανισμών συμμόρφωσης, αλλά ταυτόχρονα εγείρει ζητήματα σχετικά με την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων και τις πιθανές επιπτώσεις στα θεμελιώδη δικαιώματα. Είναι σημαντικό η χρήση της Τεχνητής Νοημοσύνης να συμμορφώνεται με τις απαιτήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα και του AML Package.

Το μεγάλο στοίχημα εντοπίζεται στο νέο Νομοθετικό Πλαίσιο για την αντιμετώπιση του ξεπλύματος χρήματος που φαίνεται να έρχεται προσπαθώντας να ενισχύσει το πλαίσιο προστασίας, επιβάλλοντας αυστηρότερες υποχρεώσεις για τις υπόχρεες οντότητες και διευκολύνοντας την εποπτεία των διαδικασιών από τις αρμόδιες αρχές. Παράλληλα, επιδιώκει να ενισχύσει τη συνεργασία μεταξύ των εθνικών και ευρωπαϊκών οργάνων για τη διασφάλιση της συμμόρφωσης και την προστασία των δικαιωμάτων των ατόμων. Εντούτοις, αποτελεί κρίσιμη συνιστώσα κατά πόσο θα καταστεί εφικτή η αποτελεσματική εφαρμογή του από το σύνολο των κρατών μελών σε ένα συνεχώς εξελισσόμενο τεχνολογικό και νομικό τοπίο. Σε κάθε περίπτωση, αναμένουμε.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Αρθρα

1. Ανδρουλάκη, Ε. (2021). Τεχνητή νοημοσύνη και προσωπικά δεδομένα: Η περίπτωση της εξ αποστάσεως βιομετρικής ταυτοποίησης. Επιθεώρηση Δικαίου Πληροφορικής, <https://ejournals.lib.auth.gr/infolawj/article/view/8236/7994>. Τελευταία Πρόσβαση 08.08.2024.
2. Βενέρης, Α. Π. (2020). Η διασφάλιση του δικαιώματος ενημέρωσης στην αλλαγή του σκοπού και την «περαιτέρω» επεξεργασία των δεδομένων. Επιθεώρηση Δικαίου Πληροφορικής, Διαθέσιμο στον σύνδεσμο: <http://ejournals.lib.auth.gr/infolawj/> Τελευταία Πρόσβαση 08.08.2024.
3. Βόρρας, Α., & Μήτρου, Λ. (2018). Τεχνητή νοημοσύνη και προσωπικά δεδομένα: Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679. ΔιΜΕΕ, 4.
4. Γιαννακίδου, Χ. (2023). Η σύγκρουση μεταξύ της προστασίας δεδομένων και της ανάγκης πρόληψης της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας. Επιθεώρηση Δικαίου Πληροφορικής @ Information Law Journal. Διαθέσιμο στο <https://ejournals.lib.auth.gr/infolawj/> Τελευταία Πρόσβαση 08.08.2024.
5. Ιγγλεζάκη, Ι. (2014). Υποχρεωτική διατήρηση δεδομένων: Ακύρωση της οδηγίας 2006/24 από το ΔΕΕ. Διαθέσιμο στο: <https://iglezakis.gr/2014/11/22/%CF%85%CF%80%CE%BF%CF%87%CF%81%CE%B5%CF%89%CF%84%CE%B9%CE%BA%CE%AE-%CE%B4%CE%B9%CE%B1%CF%84%CE%AE%CF%81%CE%B7%CF%83%CE%B7%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD-%CE%B1%CE%BA%CF%8D/> . Τελευταία Πρόσβαση 08.08.2024.
6. Κωστής, Η. (n.d.). Η Τεχνητή Νοημοσύνη και ΓΚΠΔ: Πόσο εφικτή είναι η συγκατάθεση; Rhetor. Διαθέσιμο στην ιστοσελίδα: <https://www.rhetor.gr/techniti->

[noimosyni-kai-ΓΚΠΔ-poso-efikti-einai-i-sygkatathesi-482](#) , Τελευταία Πρόσβαση 08.08.2024.

7. Lawspot. (2023). AI Act: Εγκρίθηκε ο Κανονισμός για την Τεχνητή Νοημοσύνη - Τι προβλέπει. Διαθέσιμο στο: <https://www.lawspot.gr/nomika-nea/ai-act-egkrithike-o-kanonismos-gia-tin-tehniti-noimosyni-ti-provlepei> Τελευταία Πρόσβαση 08.08.2024.
8. Παναγοπούλου, Φ., & Παπακωνσταντίνου, Σ. Διατλαντικές διαβιβάσεις δεδομένων προσωπικού χαρακτήρα: Η συμφωνία Ε.Ε. και Η.Π.Α. για το νέο Trans-Atlantic Data Privacy Framework. https://www.syntagmawatch.gr/trending-issues/diatlantikes-diavivaseis-dedomenwn-proswpikou-xarakthra-h-symfwnia-ee-kai-hpa-gia-to-neo-trans-atlantic-data-privacy-framework/#_ftn4, Τελευταία Πρόσβαση 08.08.2024.
9. Χριστοδούλου Κ,: «Εξελίξεις αιχμής στον ψηφιακό τομέα – IP, IT», προδημοσίευση από: ΕΛΛΔνη 2/2024, διαθέσιμο στην ιστοσελίδα sakkoulas-online.gr . Τελευταία Πρόσβαση 08.08.2024.
10. Χριστοδούλου Κ, 2019«Νομικά ζητήματα από την τεχνητή νοημοσύνη», Χρονικά Ιδιωτικού Δικαίου, Μηνιαίο Επιστημονικό Περιοδικό, ΙΘ/2019, Εκδόσεις Π. Ν. Σάκκουλας, σελ. 329.
11. Euractiv. (2020). Μέτρα ΕΕ κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Διαθέσιμο: <https://www.euractiv.gr/section/koinoniki-eyropi/news/eyropaiko-schedio-kata-tis-nomimopoiisis-esodon-aro-paranomes-drastiriotites/> Τελευταία Πρόσβαση 08.08.2024.

Βιβλία

12. Βλαχόπουλος, Σ. (2018). Διασυνοριακή μεταβίβαση δεδομένων προσωπικού χαρακτήρα από την Ευρωπαϊκή Ένωση προς τρίτες χώρες: Οι τελευταίες εξελίξεις, σε: Β. Τζώρτζη (επιμ.), Προστασία των δεδομένων προσωπικού χαρακτήρα. Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη.
13. Ζέκος, Γ. (2024). Τεχνητή Νοημοσύνη και Ανταγωνισμός. Εκδόσεις Σάκκουλα.
14. Ιγγλεζάκης, Ι. (2018). Δίκαιο Πληροφορικής. Εκδόσεις Σάκκουλα

15. Μήτρου κ.α. (2023). Μπορεί ο αλγόριθμος να είναι ηθικός, να είναι δίκαιος, να είναι διαφανής, να δικάζει και να διοικεί; Πανεπιστημιακές Εκδόσεις Κρήτης.
16. Μπετενιώτης, Α.Ι. (2022). Νομιμοποίηση εσόδων από παράνομες δραστηριότητες. Θεσμικό Πλαίσιο, διεθνή πρότυπα και πρακτική εφαρμογή. Αθήνα: Νομική Βιβλιοθήκη.

Ακαδημαϊκές Μελέτες

17. Παναγόπουλος Ζ.. (2021). Η Τεχνητή Νοημοσύνη και ο νέος ΓΚΠΔ στο πλαίσιο των ηλεκτρονικών συναλλαγών και των εφαρμογών τους. Διπλωματική Εργασία, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.
<https://ikee.lib.auth.gr/record/330313/files/GRI-2021-30390.pdf>, τελευταία Πρόσβαση 08.08.2024.
18. Κασιμάτη, Μ. (2021). Το ρυθμιστικό πλαίσιο σε σχέση με τον τραπεζικό τομέα για την καταστολή της νομιμοποίησης εσόδων από παράνομες δραστηριότητες στην Ευρωπαϊκή Ένωση και τις ΗΠΑ. Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών. <https://pergamos.lib.uoa.gr/uoa/dl/object/2973685/file.pdf> , Τελευταία Πρόσβαση 08.08.2024.
19. Παναγιωτίδου, Μ.-Ε. (2020). Τεχνητή Νοημοσύνη και Δίκαιο: Τεχνολογικά, Νομικά και Ηθικά Ζητήματα. Διπλωματική Εργασία, Πανεπιστήμιο Μακεδονίας.
<https://dspace.lib.uom.gr/bitstream/2159/23990/4/PanagiotidouMarina-EuthymiaMsc2020.pdf> , Τελευταία Πρόσβαση 08.08.2024.
20. Παντής. (2021). Καταπολέμηση Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες. Διπλωματική Εργασία, Οικονομικό Πανεπιστήμιο Αθηνών.
Ανακτήθηκε στις 10 Ιανουαρίου 2023 από
https://www.dept.aueb.gr/sites/default/files/%CE%A0%CE%91%CE%9D%CE%A4%CE%97%CE%A3_%CE%94%CE%99%CE%A0%CE%9B%CE%A9%CE%9C%CE%91%CE%A4%CE%99%CE%9A%CE%97.pdf , Τελευταία Πρόσβαση 08.08.2024.
21. Σερβετάς, Γ. (2023). Μηχανική Μάθηση στην Πρόβλεψη της τιμής ενοικίασης Airbnb στο Άμστερνταμ. Διπλωματική Εργασία, Πανεπιστήμιο Πειραιώς.

Διαθέσιμο:

https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/15959/Servetas_mpp119049.pdf?sequence=3&isAllowed=y , Τελευταία Πρόσβαση 08.08.2024.

22. Τσινόρεμα, Α. (2020). Η επεξεργασία Προσωπικών Δεδομένων από συστήματα Τεχνητής Νοημοσύνης. Διπλωματική Εργασία, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών. Διαθέσιμο στο:
<https://pergamos.lib.uoa.gr/uoa/dl/object/2939161/file.pdf> ,Τελευταία Πρόσβαση 08.08.2024.

Νομοθετικά Κείμενα

23. Οδηγία 91/308/ΕΟΚ του Συμβουλίου της 10ης Ιουνίου 1991 για την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες. Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, 166.
24. Οδηγία 2001/97/ΕΚ της 4ης Δεκεμβρίου 2001 που τροποποιεί την Οδηγία 91/308/ΕΟΚ του Συμβουλίου για την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες. Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, L344.
25. Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. "Σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).
26. Οδηγία 2005/60/ΕΚ της 26ης Οκτωβρίου 2005 σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για νομιμοποίηση εσόδων από παράνομες δραστηριότητες και χρηματοδότηση της τρομοκρατίας. Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, L309.
27. Οδηγία (ΕΕ) 2015/849 της 20ής Μαΐου 2015 για την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για σκοπούς νομιμοποίησης εσόδων από παράνομες δραστηριότητες ή χρηματοδότησης της τρομοκρατίας και την τροποποίηση του Κανονισμού (ΕΕ) αριθ. 648/2012 και την κατάργηση της

Οδηγίας 2005/60/EK και της Οδηγίας 2006/70/EK. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L141.

28. Οδηγία (ΕΕ) 2018/843 της 30ής Μαΐου 2018 που τροποποιεί την Οδηγία (ΕΕ) 2015/849 για την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή χρηματοδότηση της τρομοκρατίας και την τροποποίηση των Οδηγιών 2009/138/EK και 2013/36/ΕΕ. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L156.
29. Κανονισμός (ΕΕ) 2015/847 της 20ής Μαΐου 2015 σχετικά με τις πληροφορίες που συνοδεύουν τις μεταφορές χρηματικών ποσών και την κατάργηση του Κανονισμού (ΕΚ) αριθ. 1781/2006. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L141.
30. Κανονισμός (ΕΕ) 2018/1108 της 7ης Μαΐου 2018 για τη συμπλήρωση της Οδηγίας (ΕΕ) 2015/849 με ρυθμιστικά τεχνικά πρότυπα που προσδιορίζουν τα κριτήρια για τον ορισμό κεντρικών σημείων επαφής από εκδότες ηλεκτρονικού χρήματος και παρόχους υπηρεσιών πληρωμών. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L203.
31. Κανονισμός (ΕΕ) 2019/758 της 31ης Ιανουαρίου 2019 για τη συμπλήρωση της Οδηγίας (ΕΕ) 2015/849 σχετικά με ρυθμιστικά τεχνικά πρότυπα για τη μείωση του κινδύνου νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας σε ορισμένες τρίτες χώρες. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L125.
32. Κανονισμός (ΕΕ) 2024/163 που τροποποιεί τον Κανονισμό (ΕΕ) 2016/1675 σχετικά με την προσθήκη τρίτων χωρών υψηλού κινδύνου. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L44.
33. Οδηγία 2006/24/EK της 15ης Μαρτίου 2006 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε σχέση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/EK. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L105.

34. Ευρωπαϊκό Κοινοβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης, & Ευρωπαϊκή Επιτροπή. (2000). Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, C364.
35. Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο. (2016). Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας 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). Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L119.
36. Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο. (2016). Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για σκοπούς πρόληψης, έρευνας, διαπίστωσης ή δίωξης ποινικών αδικημάτων ή εκτέλεσης ποινών και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, και την κατάργηση της Απόφασης-Πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L119.
37. Κανονισμός (ΕΕ) 2024/1624 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 31ης Μαΐου 2024, σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας
38. ΗΟδηγία (ΕΕ) 2024/1640, σχετικά με τους μηχανισμούς που πρέπει να συγκροτήσουν τα κράτη μέλη για την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τους σκοπούς της νομιμοποίησης εσόδων από παράνομες δραστηριότητες ή της χρηματοδότησης της τρομοκρατίας, για την τροποποίηση της Οδηγίας (ΕΕ) 2019/1937 και για την τροποποίηση και την κατάργηση της Οδηγίας (ΕΕ) 2015/849 (AMLD).
39. Κανονισμός 2024/1620 σχετικά με τη σύσταση της Αρχής για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της

χρηματοδότησης της τρομοκρατίας και την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010 (AMLA).

40. Νόμος 4557/2018. Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας και άλλες διατάξεις. ΦΕΚ Α' 139/30.07.2018.
41. Νόμος 4734/2020. Τροποποιήσεις στον Ν. 4557/2018 για την ενσωμάτωση της Οδηγίας (ΕΕ) 2018/843 και άλλες διατάξεις. ΦΕΚ Α' 196/08.10.2020.
42. Νόμος 4816/2021. Ενσωμάτωση της Οδηγίας (ΕΕ) 2018/1673 σχετικά με την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες μέσω του ποινικού δικαίου. ΦΕΚ Α' 118/09.07.2021.
43. Νόμος 4624/2019. Αρχές, δικαιώματα και υποχρεώσεις για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. ΦΕΚ Α' 137/29.08.2019.
44. Υπουργική Απόφαση 9747/2-4-2021. "Ηλεκτρονική διεκπεραίωση μέτρων δέουσας επιμέλειας μέσω της εφαρμογής eGov-ΚΥC." ΦΕΚ Β' 1357/07.04.2021.

Ξενόγλωσσα Ευρωπαϊκά Κείμενα

45. Council of Europe. (n.d.). Risk-based approach. MONEYVAL. Διαθέσιμο σε: <https://www.coe.int/en/web/moneyval/implementation/risk-based-approach>, Τελευταία πρόσβαση: 21 Οκτωβρίου 2024.
46. ERPS. (2017). Fighting tax crimes – Cooperation between Financial Intelligence Units. Ex-Post Impact Assessment. Διαθέσιμο σε: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/598603/EPRS_STU%282017%29598603_EN.pdf, Τελευταία πρόσβαση: 29 Ιουλίου 2024.
47. European Commission. (2018). Preventing money laundering and terrorist financing across the EU - How does it work in practice? Διαθέσιμο σε: https://ec.europa.eu/info/sites/info/files/diagram_aml_2018.07_ok.pdf, Τελευταία πρόσβαση: 12 Δεκεμβρίου 2023.

48. European Parliament and Council Directive. (2002). Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications). Διαθέσιμο σε: <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32002L0058>, Τελευταία πρόσβαση: 12 Δεκεμβρίου 2023.
49. European Commission. (2020). White Paper on Artificial Intelligence (COM (2020) 65 final). Διαθέσιμο σε: <https://op.europa.eu/el/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1>, Τελευταία πρόσβαση: 12 Δεκεμβρίου 2023.
50. European Commission. (2018). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – Artificial Intelligence for Europe (COM (2018) 237 final). Διαθέσιμο σε: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1580907128927&uri=CELEX:52018DC0237>, Τελευταία πρόσβαση: 12 Δεκεμβρίου 2023.
51. European Data Protection Board (EDPB). (2021). EDPB letter to the European Commission on the protection of personal data in the AML-CFT legislative proposals. Διαθέσιμο σε: https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-protection-personal-data-processed-relation_en, Τελευταία πρόσβαση: 8 Αυγούστου 2024.
52. European Data Protection Supervisor (EDPS). (2020). Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing. Διαθέσιμο σε: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_2020121, Τελευταία πρόσβαση: 8 Αυγούστου 2024.
53. Council of the European Union. (2022). Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights. Διαθέσιμο σε: <https://www.consilium.europa.eu/el/press/press-releases/2022/12/06/artificial->

[intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/](#), Τελευταία πρόσβαση: 10 Αυγούστου 2024.

Ελληνόγλωσσα Ευρωπαϊκά Κείμενα

54. Επιτροπή. (2004). Ανακοίνωση της Επιτροπής προς το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο σχετικά με την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος στον χρηματοοικονομικό τομέα. Διαθέσιμο σε: <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX%3A52004DC0262>, τελευταία πρόσβαση: 08.08.2024.
55. Ευρωπαϊός Επόπτης Προστασίας Δεδομένων (ΕΕΠΔ). (2014). Περίληψη της γνωμοδότησης του Ευρωπαϊού Επόπτη Προστασίας Δεδομένων επί της πρότασης οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας και επί της πρότασης κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις πληροφορίες σχετικά με τον πληρωτή που συνοδεύουν τις μεταφορές χρηματικών ποσών. Διαθέσιμο σε: <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX%3A52004DC0262>, τελευταία πρόσβαση: 08.08.2024.
56. ΑΠΔΠΧ. (2020). Κατευθυντήριες Οδηγίες για τη Συγκατάθεση σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ). Διαθέσιμο σε: https://www.dpa.gr/sites/default/files/2020-05/wp251rev01_el.pdf, τελευταία πρόσβαση: 08.08.2024.
57. Επιτροπή, Ε. (2020). Ανακοίνωση σχετικά με σχέδιο δράσης για ολοκληρωμένη ενωσιακή πολιτική με σκοπό την πρόληψη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Διαθέσιμο σε: [123](https://eur-</p></div><div data-bbox=)

lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52020XC0513, τελευταία πρόσβαση: 08.08.2024.

58. Επιτροπή, Ε. (2021). Ερωτήσεις και απαντήσεις: Καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας (ΚΕΧ/ΧΤ). Διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/el/qanda_21_3689, τελευταία πρόσβαση: 08.08.2024.
59. Συμβούλιο Ευρωπαϊκής Ένωσης. τ. (2024). Ξέπλυμα χρήματος: Το Συμβούλιο εγκρίνει δέσμη κανόνων. Διαθέσιμο σε: <https://www.consilium.europa.eu/el/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/>, τελευταία πρόσβαση: 08.08.2024.
60. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2022). Κατευθυντήριες γραμμές 01/2021 σχετικά με την κοινοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα (εγκεκριμένη έκδοση). Διαθέσιμο σε: https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_el.pdf, τελευταία πρόσβαση: 10.08.2024.
61. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). Αρχές νομιμότητας. Διαθέσιμο σε: https://www.dpa.gr/el/foreis/arxes_nomimotitas, τελευταία πρόσβαση: 08.08.2024.

Ξενόγλωσση Βιβλιογραφία

62. Silvia Allegranza, “The proposed Anti-Money Laundering Authority, FIU cooperation, powers and exchanges of information”, Study requested by the ECON Committee, 2022, σελ. 35.

63. Bakardjieva Engelbrekt, A., et al. (Eds.). (2024). The borders of the European Union in a conflictual world. Διαθέσιμο σε: https://doi.org/10.1007/978-3-031-54200-8_1, Τελευταία πρόσβαση: 10.08.2024
64. Bayamlioglu, E. (2018). Transparency of automated decisions in the GDPR: An attempt for systemisation. Διαθέσιμο σε: <https://ssrn.com/abstract=3097653>, Τελευταία πρόσβαση: 10.08.2024
65. Bertrand, A., Maxwell, W., & Vamparys, X. (2020). Are AI-based anti-money laundering systems compatible with fundamental rights? Διαθέσιμο σε: <https://ssrn.com/abstract=3647420>, Τελευταία πρόσβαση: 10.08.2024
66. Blazquez, D., & Domenech, J. (2018). Big data sources and methods for social and economic analyses. *Technological Forecasting and Social Change*, 130, 99-113. Διαθέσιμο σε: <https://www.sciencedirect.com/science/article/pii/S0040162517310946>, Τελευταία πρόσβαση: 10.08.2024
67. Beneish, Messod D., 1999 "The Detection of Earnings Manipulation", 1999, *Financial Analysis Journal* 55, σελ. 24–36.
68. Brewczyńska, M. (2022). Privacy and data protection vs public access to entrepreneurs' personal data. *European Law Blog*. Διαθέσιμο σε: <https://europeanlawblog.eu/2022/12/15/privacy-and-data-protection-vs-public-access-to-entrepreneurs-personal-data-score-20/>, Τελευταία πρόσβαση: 10.08.2024
69. Brewczyńska, M. (2021). Financial intelligence units: Reflections on the applicable data protection legal framework. *Computer Law & Security Review*. Διαθέσιμο σε: <https://www.sciencedirect.com/science/article/pii/S0267364921000856#sec0002>, Τελευταία πρόσβαση: 10.08.2024
70. Brewczyńska, M., & Kosta, E. (2023). From the fight against money laundering and financing of terrorism towards the fight for fundamental rights: The role of data protection. In H. Matsumi, D. Hallinan, D. Dimitrova, E. Kosta, & P. De Hert (Eds.), *Data protection and privacy: In transitional times* (pp. 157-183). Bloomsbury Publishing.

71. Cindori, S. (2023). Beneficial ownership – Demand for transparency, threat to privacy. *Review of European and Comparative Law*, 55(4), 113–131. Διαθέσιμο σε: <https://doi.org/10.31743/recl.16352>, Τελευταία πρόσβαση: 10.08.2024
72. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Inter-state exchanges of data for tax purposes and CML. Διαθέσιμο σε: <https://rm.coe.int/t-pd-2021-4rev-inter-state-exchanges-of-data-for-tax-purposes-and-cml-/1680a3ed30>, Τελευταία πρόσβαση: 10.08.2024
73. Doyle, C. (2017). Money laundering: An overview of 18 U.S.C. § 1956 and related federal criminal law. Congressional Research Service. Διαθέσιμο σε: <https://sgp.fas.org/crs/misc/RL33315.pdf>, Τελευταία πρόσβαση: 10.08.2024
74. Dechow, Patricia M., Weili Ge, Chad R. Larson, and Richard G. Sloan, “*Predicting Material Accounting Misstatements.*”, 2011, *Contemporary Accounting Research* 28, σελ. 17–82.
75. ECOLEF Project. (2013). Economic and legal effectiveness of anti-money laundering and combating terrorist financing policy – Final report. Διαθέσιμο σε: [http://www2.econ.uu.nl/users/unger/ecolef_files/Final%20ECOLEF%20report%20\(digital%20version\).pdf](http://www2.econ.uu.nl/users/unger/ecolef_files/Final%20ECOLEF%20report%20(digital%20version).pdf), Τελευταία πρόσβαση: 10.08.2024
76. Euractiv. (2020). Μέτρα ΕΕ κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Διαθέσιμο σε: <https://www.euractiv.gr/section/koinoniki-eyropi/news/eyropaiko-schedio-kata-tis-nomimopoiisis-esodon-apo-paranomes-drastiriotites/>, Τελευταία πρόσβαση: 10.08.2024
77. European Banking Authority (EBA). (2017). Opinion of the European Banking Authority on the transition from the existing Payment Services Directive (PSD1) to the Revised Directive (PSD2). Διαθέσιμο σε: <https://www.cssf.lu/wp-content/uploads/EBA-Op-2017-81.pdf>, Τελευταία πρόσβαση: 10.08.2024
78. Excell, D., “Using adaptive behavioral analytics to detect fraud”, *Risk Management Monitor*, 2019, διαθέσιμο στην ιστοσελίδα:

- www.riskmanagementmonitor.com/usingadaptive-behavioral-analytics-to-detect-fraud. Τελευταία πρόσβαση: 10.08.2024
79. FATF. (n.d.). Guidance on beneficial ownership for legal persons (p. 4). Διαθέσιμο σε: <http://www.fatf-gafi.org/publications/FATFrecommendations/guidance-beneficial-ownership-legalpersons.html>, Τελευταία πρόσβαση: 10.08.2024
80. FATF. (n.d.). What is money laundering? Διαθέσιμο σε: <https://www.fatf-gafi.org/faq/moneylaundering/>, Τελευταία πρόσβαση: 10.08.2024
81. Fernandez Ana, "Artificial Intelligence in Financial Services", 2019, Banco de Espana, άρθρο 3/19, διαθέσιμο στην ιστοσελίδα https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3366846. Τελευταία πρόσβαση: 10.08.2024
82. Financial Action Task Force (FATF). (n.d.). Risk-Based Approach for the Banking Sector. Διαθέσιμο σε: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Risk-based-approach-banking-sector.html>, Τελευταία Πρόσβαση: 08.08.2024.
83. Frasher, M. (2021). Data protection and the EU's anti-money laundering regulation. Διαθέσιμο σε: <https://iapp.org/news/a/data-protection-and-the-eus-anti-money-laundering-regulation>, Τελευταία Πρόσβαση: 08.08.2024.
84. Financial Crime Academy (FCA). (2024). Privacy matters: Unraveling data privacy regulations in AML compliance. Διαθέσιμο σε: <https://financialcrimeacademy.org/data-privacy-regulations-in-aml/>, Τελευταία πρόσβαση: 10.08.2024
85. Glancy, D. J. (2012). Privacy in autonomous vehicles. *Santa Clara Law Review*, 52, 1171.
86. Hildebrandt, M. (2008). Defining, «Profiling: a new type of knowledge?». Διαθέσιμο σε: https://link.springer.com/chapter/10.1007/978-1-4020-6914-7_2, Τελευταία πρόσβαση: 10.08.2024
87. Institute of International Finance. (2018). Machine learning in anti-money laundering (AML).

94. Maxwell, W. (2021). The GDPR and Private Sector Measures to Detect Criminal Activity. *Revue des Affaires Européennes - Law and European Affairs*. Διαθέσιμο σε: <https://ssrn.com/abstract=3964066>, Τελευταία Πρόσβαση: 08.08.2024.
95. Mitsilegas, V., & Gilmore, B. (2007). The EU legislative framework against money laundering and terrorist finance: A critical analysis in the light of evolving global standards. *International and Comparative Law Quarterly*. Διαθέσιμο σε: <https://doi.org/10.1093/iclq/lei152>, Τελευταία Πρόσβαση: 08.08.2024.
96. Mathias. (2023,). Privacy vs. shareholder transparency: Did the ECJ decision in WM and Sovim SA impair the global fight against money laundering? Διαθέσιμο σε: <https://ssrn.com/abstract=4540817>, Τελευταία πρόσβαση: 10.08.2024
97. Metz, C., & Satariano, A. (2020, February 6). An algorithm that grants freedom, or takes it away. *The New York Times*.
98. Milaj, J., & Kaiser, C. (2017). Retention of data in the new anti-money laundering directive—‘Need to know’ versus ‘Nice to know’. *International Data Privacy Law*, 7(2), p. 117. Διαθέσιμο σε: <https://doi.org/10.1093/idpl/ix002>, Τελευταία πρόσβαση: 10.08.2024
99. Mitrou, L. (2019). Artificial intelligence and cognitive services / Is the General Data Protection Regulation (GDPR) “Artificial Intelligence proof”. *University of the Aegean Data Protection*, 19.
100. Morais, H. V. (2005). Fighting international crime and its financing: The importance of following a coherent global strategy based on the rule of law. *Villanova Law Review*, 50, 583, 599.
101. Mouzakiti, F. (2020). Cooperation between financial intelligence units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive. *New Journal of European Criminal Law*, 11(3), 351.
102. McKinsey and Company, 2022 “*The fight against money laundering: machine learning is a game changer*”, Insights, διαθέσιμο στην ιστοσελίδα:

- www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-moneylaundering-machine-learning-is-a-game-changer, Τελευταία πρόσβαση: 10.08.2024
103. OECD. (2023). The state of implementation of the OECD AI principles four years on. Διαθέσιμο σε: <https://www.oecd-ilibrary.org/docserver/835641c9en.pdf?expires=1713095995&id=id&accname=guest&checksum=3FF7629A354AA464FDD94B4DC3FE4E68>, Τελευταία πρόσβαση: 10.08.2024
104. Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: The dawn of a new era. *Journal of Money Laundering Control*, 26(7), 155-166. Διαθέσιμο σε: <https://doi.org/10.1108/JMLC-03-2023-0050>, Τελευταία πρόσβαση: 10.08.2024
105. Politou, E., Alepis, E., & Patsakis, C. (2017). A survey on mobile affective computing *Computer Science Review* 25(11) Διαθέσιμο σε :DOI:10.1016/j.cosrev.2017.07.002 Τελευταία πρόσβαση: 10.08.2024
106. Politou, E., Alepis, E., & Patsakis, C. (2019). Profiling tax and financial behaviour with big data under the GDPR. Διαθέσιμο σε: www.sciencedirect.com, Τελευταία πρόσβαση: 10.08.2024
107. Quintel, T. (2022). Data protection rules applicable to financial intelligence units: Still no clarity in sight. *ERA Forum*, 23, 53–74. Διαθέσιμο σε: <https://doi.org/10.1007/s12027-021-00697-z>, Τελευταία πρόσβαση: 10.08.2024
108. Sloan, H. R., & Warner, R. (2018). When is an algorithm transparent?: Predictive analytics, privacy, and policy.
109. Wahl, T. (2020). AML Package II: Commission proposes AML regulation. *Eucrim*. Διαθέσιμο σε: <https://eucrim.eu/news/aml-package-ii-commission-proposes-aml-regulation/>, Τελευταία πρόσβαση: 10.08.2024
110. Wahl, T. (2024). New Anti-Money Laundering Directive (AMLD 6). *Eucrim*. Διαθέσιμο σε: <https://eucrim.eu/news/new-anti-money-laundering-directive-amld-6/>, Τελευταία Πρόσβαση: 08.08.2024.

111. Wahl, T. (2024). Tasks, powers and structures of the new EU authority for anti-money laundering and countering the financing of terrorism (AMLA). Euclid. Διαθέσιμο σε: <https://euclid.eu/news/tasks-powers-and-structures-of-aml/>, Τελευταία Πρόσβαση: 08.08.2024.
112. Wahl, T. (2024). The EU's New AML Single Rulebook Regulation, <https://euclid.eu/news/the-eu-new-aml-single-rulebook-regulation/>, Euclid. Διαθέσιμο σε: Τελευταία Πρόσβαση: 08.08.2024.
113. Wang, S.-N., & Yang, J.-G. (2007). A money laundering risk evaluation method based on decision tree. International Conference on Machine Learning and Cybernetics.
114. Walshe, J. and Cropper, T., 2018 "Should you be banking on RegTech?", 2018, Journal of Securities Operations and Custody, Vol. 10 No. 2, σελ. 167-175.
115. Wulsin, D., et al. (2012). Semi-supervised anomaly detection for EEG waveforms using deep belief nets. Διαθέσιμο σε: <https://www.researchgate.net/publication/224217204>, Τελευταία πρόσβαση: 10.08.2024
116. Joanna Wyrobek, "Application of machine learning models and artificial intelligence to analyze annual financial statements to identify companies with unfair corporate culture", Procedia Computer Science 176, 2020, σελ. 3037–3046, διαθέσιμο στην ιστοσελίδα www.sciencedirect.com. Τελευταία πρόσβαση: 10.08.2024
117. Zigo, D. (2023). CJEU: WM and Sovim SA v. Luxembourg Business Registers (Joined Cases C-37/20 and C-601/20): Rethinking transparency of ultimate beneficial owners registers. Bratislava Law Review, 7(2), 227–240. Διαθέσιμο σε: <https://doi.org/10.46282/blr.2023.7.2.725>, Τελευταία πρόσβαση: 10.08.2024

Δικαστικές Αποφάσεις

118. Δικαστήριο της Ευρωπαϊκής Ένωσης (Δ.Ε.Ε.). Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources και άλλοι, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, απόφαση της 8ης Απριλίου

2014. Διαθέσιμο στο: <https://eur-lex.europa.eu/legalcontent/EL/TXT/PDF/?uri=CELEX:62012CJ0293>.
119. Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ). Ireland κατά Ηνωμένου Βασιλείου, απόφαση του 2018. Διαθέσιμο στο: [https://hudoc.echr.coe.int/eng/#{%22itemid%22:\[%22001-181585%22\]}](https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-181585%22]}).
120. Δικαστήριο της Ευρωπαϊκής Ένωσης (Δ.Ε.Ε.). Maximilian Schrems κατά Data Protection Commissioner, υπόθεση C-362/14 (Grand Chamber), απόφαση της 6ης Οκτωβρίου 2015. Διαθέσιμο στο: <https://curia.europa.eu/juris/liste.jsf?num=C-362/14>.
121. Δικαστήριο της Ευρωπαϊκής Ένωσης (Δ.Ε.Ε.). Data Protection Commissioner κατά Facebook Ireland Limited και Maximilian Schrems, υπόθεση C-311/18 (Grand Chamber), απόφαση της 16ης Ιουλίου 2020. Διαθέσιμο στο: <https://curia.europa.eu/juris/liste.jsf?num=C-311/18>.
122. Δικαστήριο της Ευρωπαϊκής Ένωσης (Δ.Ε.Ε.). La Quadrature du Net και άλλοι κατά Πρωθυπουργού και άλλοι, υπόθεση C-511/18 (Grand Chamber), απόφαση της 6ης Οκτωβρίου 2020. Διαθέσιμο στο: <https://curia.europa.eu/juris/liste.jsf?language=en&num=c-511/18&td=ALL>.
123. Δικαστήριο της Ευρωπαϊκής Ένωσης (Δ.Ε.Ε.). Privacy International κατά Secretary of State for Foreign and Commonwealth Affairs και άλλοι, υπόθεση C-623/17 (Grand Chamber), απόφαση της 6ης Οκτωβρίου 2020. Διαθέσιμο στο: <https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-623/17>.
124. Δικαστήριο της Ευρωπαϊκής Ένωσης (Δ.Ε.Ε.). OQ κατά Land Hessen, παρισταμένης της SCHUFA Holding AG, υπόθεση C-204/21, απόφαση του 2023. Διαθέσιμο στο: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=271343&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=1683584>.
125. Δικαστήριο της Ευρωπαϊκής Ένωσης (Δ.Ε.Ε.). Breyer κατά Γερμανίας, υπόθεση C-582/14, απόφαση της 30ης Ιανουαρίου 2020, παρ. 81. Διαθέσιμο στο: <https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EL>.

126. Δικαστήριο της Ευρωπαϊκής Ένωσης (Δ.Ε.Ε.). Tele2 Sverige AB κατά Post- och telestyrelsen και Secretary of State for the Home Department κατά Tom Watson και άλλων, υπόθεση C-203/15, απόφαση του 2016. Διαθέσιμο στο: <https://eur-lex.europa.eu/legal-content/EN/TXT/?>.
127. Δικαστήριο της Ευρωπαϊκής Ένωσης (Δ.Ε.Ε.). Γνωμοδότηση 1/15 σχετικά με τη συμφωνία PNR μεταξύ ΕΕ και Καναδά, απόφαση του 2017. Διαθέσιμο στο: <https://curia.europa.eu/juris/document/document.jsf?docid=160882&doclang=EL>.
128. Pitruzzella, G. Γνώμη του Γενικού Εισαγγελέα Giovanni Pitruzzella στις συνενωμένες υποθέσεις C-37/20 και C-601/20, WM και Sovim SA κατά Luxembourg Business Registers, 2022. EUR-Lex. Διαθέσιμο στο: <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62020CC0037> (Τελευταία πρόσβαση 10.08.2024).
129. Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ). WM και Sovim SA κατά Luxembourg Business Registers, συνεκδικασθείσες υποθέσεις C-37/20 και C-601/20, απόφαση του 2022. EUR-Lex. Διαθέσιμο στο: <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=ecli:ECLI:EU:C:2022:912> (Τελευταία πρόσβαση 10.08.2024)

