



ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

# ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΑΣΦΑΛΕΙΑ ΤΡΑΠΕΖΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΒΑΣΙΣΜΕΝΩΝ ΣΕ ΥΠΟΔΟΜΗ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

Διπλωματική Εργασία

του

Δημητριάδη Κωνσταντίνου

Θεσσαλονίκη, Ιούλιος 2020

# ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΑΣΦΑΛΕΙΑ ΤΡΑΠΕΖΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΒΑΣΙΣΜΕΝΩΝ ΣΕ ΥΠΟΔΟΜΗ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

Δημητριάδης Κωνσταντίνος

Πτυχίο Εφαρμοσμένης Πληροφορικής, ΠΑΜΑΚ, 2016

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπουσα Καθηγήτρια
κα. Ευγενία Αλεξανδροπούλου - Αιγυπτιάδου

Συν-επιβλέπουσα Δρ. Εφαρμοσμένης Πληροφορικής
κα. Μυλώση Μαρία

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 20/7/2020

| | | |
|---|---|---|
| Αλεξανδροπούλου – Αιγυπτιάδου Ευγενία | Μυλώση Μαρία | Ψάννης Κωνσταντίνος |

Δημητριάδης Κωνσταντίνος

# Περίληψη

Η ενσωμάτωση του υπολογιστικού νέφους στις τραπεζικές υπηρεσίες έφερε την επανάσταση στον τρόπο με τον οποίο πραγματοποιείται η επεξεργασία δεδομένων των φυσικών προσώπων. Η εξέλιξη των τεχνολογιών στα πληροφοριακά συστήματα (στο εξής ΠΣ) σε συνδυασμό με τη χρήση του υπολογιστικού νέφους, αύξησε τις απαιτήσεις ασφαλείας των ΠΣ που χρησιμοποιούσαν τα χρηματοπιστωτικά ιδρύματα, έχοντας ως στόχο την προστασία των προσωπικών δεδομένων των πελατών τους.

Η παρούσα διπλωματική εργασία εστιάζει στον τρόπο με τον οποίον τα τραπεζικά πληροφοριακά συστήματα διαμοιράζονται δεδομένα οικονομικής συμπεριφοράς για τη διεκπεραίωση σημαντικών επιχειρηματικών λειτουργιών μεταξύ τμημάτων ή χρηματοπιστωτικών ιδρυμάτων. Με την εξέλιξη της τεχνολογίας και την αύξηση του όγκου των δεδομένων προς επεξεργασία, δημιουργήθηκε η ανάγκη για αποτελεσματικότερα μοντέλα αποθήκευσης και διαχείρισης των δεδομένων στον τραπεζικό τομέα. Τα τραπεζικά ιδρύματα, με την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (στο εξής ΓΚΠΔ), προσπάθησαν να διαμορφώσουν έναν κώδικα δεοντολογίας, ώστε να μπορέσουν να προσαρμόσουν αποτελεσματικά τις υπηρεσίες του υπολογιστικού νέφους με τις τραπεζικές διεργασίες, εξασφαλίζοντας την προστασία των δεδομένων από μη εγκεκριμένες μεθόδους διαχείρισής τους.

**Λέξεις Κλειδιά:** Τραπεζικά Πληροφοριακά Συστήματα, Προστασία Δεδομένων, Απόρρητο Δεδομένων, Υπολογιστικό Νέφος, Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ)

# Abstract

Cloud computing in banking systems revolutionized the way of data processing. The evolution of information systems technology, along with cloud computing, increases the need of facing security issues in the information systems of financial institutions, while the main aim is the data protection of their customers.

In this thesis, we focus on how the banking information systems share their economic data to perform significant business functions between departments or financial institutions. The evolution of technology and the increase in the volume of data to be processed, arise the need for more efficient models of data storage and management in the banking sector. By implementing the General Data Protection Regulation (GDPR), banking institutions have tried to formulate a code of ethics so that they can effectively adapt computer cloud services to banking processes, ensuring that data is protected from unauthorized methods.



**Keywords:** Banking Information Systems, Data Protection Data Privacy, Cloud Computing, General Data Protection Regulation (GDPR)

# Ευχαριστίες

*Θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτριά μου Αλεξανδροπούλου Ευγένεια και την συν-επιβλέπουσα Δρ. Εφαρμοσμένης Πληροφορικής κα. Μυλώση Μαρία για την καθοδήγηση και τις πολύτιμες συμβουλές που μου παρείχαν καθώς επίσης και για την άρτια συνεργασία καθ' όλη τη διάρκεια της εργασίας.*

*Επίσης θα ήθελα να ευχαριστήσω τους γονείς μου, που μου έδειξαν τον δρόμο της γνώσης και με την πολύτιμη βοήθειά τους κατάφερα να φτάσω σε αυτό το σημείο των σπουδών μου.*

*Τέλος θα ήθελα να ευχαριστήσω ξεχωριστά τον αδερφό μου Δημήτρη Δημητριάδη ο οποίος αποτέλεσε πρότυπο στη ζωή μου, δείχνοντας μου τον σωστό δρόμο.*

# Περιεχόμενα

**1 ΕΙΣΑΓΩΓΗ ..... 1**

1.1 Περιγραφη Ερευνητικου Πεδιου ..... 1

1.2 Κινητρα και Στοχοι Έρευνας ..... 6

1.3 Ερωτηματα – Προβληματισμοι ..... 8

1.4 Συνεισφορα και περιορισμοι της ερευνας ..... 9

1.5 Βασικη Ορολογια ..... 11

1.6 Διαρθρωση της μελετης ..... 13

**2 ΤΡΑΠΕΖΙΚΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ..... 16**

2.1 Εισαγωγη ..... 16

2.2 Η εννοια των Τραπεζικων Πληροφοριακων Συστηματων ..... 18

2.3 Τα ειδη των Τραπεζικων Πληροφοριακων Συστηματων ..... 21

*2.3.1 Συστήματα Διαχείρισης Επιχειρηματικών Πόρων (ERP) ..... 22*

*2.3.2 Συστήματα Διαχείρισης Πελατειακών Σχέσεων (CRM) ..... 23*

*2.3.3 Πληροφοριακά Συστήματα Διοίκησης (MIS) ..... 25*

*2.3.4 Συστήματα Διαχείρισης Ανθρώπινου Δυναμικού (HRM) ..... 27*

2.4 Ο ρολος των Πληροφοριακων Συστηματων στις τραπεζες ..... 30

*2.4.1 Οφέλη από τη χρήση των Πληροφοριακών Συστημάτων ..... 31*

2.5 Θεματα ασφαλειας των τραπεζικων πληροφορικων συστηματων ..... 33

*2.5.1 Συλλογή προσωπικών δεδομένων ..... 34*

*2.5.2 Βάσεις δεδομένων των ΠΣ ..... 35*

2.6 Προστασια προσωπικων δεδομενων ..... 37

2.7 Συνοψη ..... 38

**3 ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ..... 40**

3.1 Εισαγωγη ..... 40

3.2 Η εννοια του Υπολογιστικου Νεφους ..... 41

*3.2.1 Αρχιτεκτονική Υπολογιστικού Νέφους ..... 41*

3.3 Μοντελα Αναπτυξης Υπολογιστικου Νεφους ..... 43

*3.3.1 Χαρακτηριστικά Υπολογιστικού Νέφους ..... 44*

*3.3.2 Μοντέλα Υπηρεσιών ..... 44*

3.4 Προστασια προσωπικων δεδομενων στο νεφος ..... 47

*3.4.1 Προβλήματα ασφαλείας στο σύννεφο ..... 48*

3.5 Συνοψη ..... 50

**4 ΤΡΑΠΕΖΙΚΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΜΕ ΥΠΟΔΟΜΗ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ ..... 51**

4.1 Εισαγωγη ..... 51
4.2 Η εξελιξη των Τραπεζικων υπηρεσιων με την εισαγωγη υποδομης Υπολογιστικου Νεφους ..... 51
4.3 Χρηση του Υπολογιστικου Νεφους στα Τραπεζικα Πληροφοριακα Συστηματα ..... 52
*4.3.1 Πλεονεκτήματα χρήσης υπηρεσιών Υπολογιστικού Νέφους στην Τράπεζα ..... 54*
4.4 Η αρχιτεκτονικη των Τραπεζικων ΠΣ με υποδομη Υπολογιστικου Νεφους ..... 55
4.5 Η συνδεση των Τραπεζικων ΠΣ με το Υπολογιστικο Νεφος ..... 57
*4.5.1 Διαπραγματεύσεις παρόχου υπολογιστικού νέφους με την τράπεζα ..... 58*
4.6 Συνοψη ..... 59

**5 ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΙ ΑΣΦΑΛΕΙΑ ΣΤΑ ΤΡΑΠΕΖΙΚΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΜΕ ΥΠΟΔΟΜΗ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ ..... 60**

5.1 Εισαγωγη ..... 60
5.2 Το αμφιλεγομενο ζητημα ασφαλειας του Υπολογιστικου Νεφους ..... 61
*5.2.1 Κίνδυνοι για προσωπικά δεδομένα σε περιβάλλον υπολογιστικού νέφους ..... 62*
5.3 Οι κυριοτερες απειλες για την ασφαλεια των προσωπικων δεδομενων στο συννεφο ..... 64
*5.3.1 Ανησυχίες και προβληματισμοί ..... 66*
5.4 Αντιμετωπιση απειλων απο την τραπεζα ..... 67
5.5 Προσωπικα δεδομενα και ιδιωτικοτητα στο συννεφο ..... 68
*5.5.1 Ο κύκλος ζωής των δεδομένων οικονομικού χαρακτήρα ..... 69*
5.6 Συνοψη ..... 71

**6 ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ ..... 73**

6.1 Εισαγωγη ..... 73
6.2 Η σημασια της νομοθετικης ρυθμισης των υπηρεσιων Υπολογιστικου Νεφους ..... 74
6.3 Υπολογιστικο Νεφος και ο Γενικος Κανονισμος Προστασιας Δεδομενων (ΓΚΠΔ) 679/2016 ..... 77
*6.3.1 Υπεύθυνοι επεξεργασίας κι εκτελούντες την επεξεργασία ..... 78*
6.3.1.1 Υποχρεώσεις τράπεζας ως υπεύθυνου επεξεργασίας δεδομένων στο σύννεφο ..... 79
6.3.1.2 Υποχρεώσεις παρόχου υπολογιστικού νέφους ως εκτελών την επεξεργασία ..... 81
6.3.1.3 Κοινές υποχρεώσεις παρόχου υπολογιστικού νέφους και τράπεζας ..... 82
*6.3.2 Επεξεργασία προσωπικών δεδομένων ..... 83*
*6.3.3 Διασυνοριακή ροή δεδομένων ..... 86*
*6.3.4 Δικαιώματα Υποκειμένου Επεξεργασίας Δεδομένων ..... 87*
6.4 Ο Ν. 4624/19: Προστασια προσωπικων δεδομενων και μετρα εφαρμογης του ΓΚΠΔ ..... 89
6.5 Ασφαλεια και προστασια προσωπικων δεδομενων ..... 90
6.6 Βιωσιμοτητα Υπολογιστικου Νεφους και ρυθμιση ..... 91
6.7 Αρχη Προστασιας των Προσωπικων Δεδομενων ..... 92
*6.7.1 Αποφάσεις Αρχής ..... 93*
6.8 Συνοψη ..... 98

**7 ΕΠΙΛΟΓΟΣ ..... 100**

7.1 Συμπερασματα ..... 100

7.2 Μελλοντικες Επεκτασεις ..... 101

**ΠΑΡΑΡΤΗΜΑ Ι – ΑΠΟΦΑΣΕΙΣ ΔΕΕ ΓΙΑ ΤΗ ΧΡΗΣΗ ΝΕΦΟΥΣ ..... 108**

# Κατάλογος Εικόνων

Εικόνα 1: Αρχιτεκτονική ενός πληροφοριακού συστήματος ..... 20
Εικόνα 2: Αρχιτεκτονική δομή ενός συστήματος ERP ..... 23
Εικόνα 3: Αρχιτεκτονική δομή ενός συστήματος CRM ..... 24
Εικόνα 4: Αρχιτεκτονική δομή ενός συστήματος MIS ..... 27
Εικόνα 5: Αρχιτεκτονική δομή ενός συστήματος HRM ..... 28
Εικόνα 6: Ανάλυση δεδομένων για πρόσληψη προσωπικού ..... 29
Εικόνα 7: Η χρησιμότητα των τραπεζικών βάσεων δεδομένων ..... 37
Εικόνα 8: Αρχιτεκτονική σχεδίαση Υπολογιστικού Νέφους ..... 42
Εικόνα 9: Αρχιτεκτονική του Υπολογιστικού Νέφους ..... 46
Εικόνα 10: Αρχιτεκτονική υποδομή υπολογιστικού νέφους στις τράπεζες ..... 56
Εικόνα 11: Κύκλος ζωής δεδομένων ..... 69

# 1 Εισαγωγή

## 1.1 Περιγραφή Ερευνητικού Πεδίου

Με την εξέλιξη της τεχνολογίας και την ανάδειξη νέων μορφών επεξεργασίας δεδομένων, κρίθηκε απαραίτητη η νομική προστασία των υποκειμένων των δεδομένων[1]. Η διαχείριση και η ασφάλεια των προσωπικών δεδομένων αποτελεί πλέον μία από τις βασικότερες αρχές για την αποτελεσματικότερη εκτέλεση των επιχειρηματικών διαδικασιών σ' έναν οργανισμό. Τα κράτη μέλη της Ευρωπαϊκής Ένωσης έδωσαν μεγάλη βαρύτητα στον τρόπο με τον οποίο ένας κρατικός ή μη φορέας, θα διαχειρίζεται τα δεδομένα των υποκειμένων για την διεκπεραίωση των υπηρεσιών του. Για την θέσπιση μίας κοινής στρατηγικής για την επεξεργασία των δεδομένων του υποκειμένου, η ΕΕ ενεργοποίησε νομικούς μηχανισμούς έχοντας ως κύριο στόχο την ασφάλεια των προσωπικών δεδομένων, από μη εγκεκριμένες μεθόδους διαχείρισής τους και την προάσπιση των συμφερόντων των ατόμων, των οποίων τα δεδομένα τους υπόκεινται σε επεξεργασία.

Η διαδικασία ενεργοποίησης των νομικών διατάξεων για την προστασία των δεδομένων, απαιτούσε την πλήρη συνεργασία των φορέων επεξεργασίας δεδομένων με την εποπτική αρχή που ήταν υπεύθυνη για την τήρηση των απαιτούμενων μέτρων που έπρεπε να λάβουν οι οργανισμοί που διαχειρίζονταν τα δεδομένα των υποκειμένων. Το μεγάλο πλήθος των μη συμμορφούμενων οργανισμών σχετικά με τις νομικές διατάξεις περί προστασίας προσωπικών δεδομένων, οδήγησε την ΕΕ στη θέσπιση ενός συνόλου κανόνων που θα έχει σα στόχο την αυστηρή συμμόρφωση των φορέων επεξεργασίας δεδομένων. Το σύνολο αυτών των κανόνων ονομάζεται Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ), ενώ στην αγγλική βιβλιογραφία ο όρος μεταφράζεται ως General Data Protection Regulation (GDPR).

Ο Γενικός Κανονισμός Προστασίας Δεδομένων της ΕΕ (GDPR), ο οποίος εφαρμόστηκε σε όλα τα κράτη μέλη της από τις 25 Μαΐου 2018[2], αποτελεί ορόσημο στην εξέλιξη του ευρωπαϊκού πλαισίου προστασίας της ιδιωτικής ζωής. Καθοδηγούμενη από μια φιλοσοφική προσέγγιση στην προστασία των δεδομένων, βασισμένη στην

[1] Ως υποκείμενο των δεδομένων νοείται, το άτομο ή ομάδα ατόμων των οποίων τα προσωπικά τους δεδομένα υπόκεινται σε επεξεργασία από κάποιον φορέα υπηρεσιών, όπως για παράδειγμα κρατικές αρχές, οργανισμοί κι επιχειρήσεις.

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

έννοια της ιδιωτικής ζωής ως θεμελιώδους ανθρώπινου δικαιώματος (όπως κατοχυρώνεται στον Χάρτη των Δικαιωμάτων της ΕΕ), ο Κανονισμός έχει ευρύ παγκόσμιο αντίκτυπο (Albrecht, 2016).

Ο νέος νόμος καλύπτει τα προσωπικά δεδομένα όλων των κατοίκων της ΕΕ, ανεξάρτητα από τον τόπο επεξεργασίας τους. Τα δεδομένα προσωπικού χαρακτήρα, σύμφωνα με τον ορισμό που δίνει ο ΓΚΠΔ, είναι «*κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (υποκείμενο των δεδομένων)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου*»[3]. Επίσης προσωπικά δεδομένα μπορούν να θεωρηθούν και πληροφορίες που, άμεσα ή έμμεσα, μπορούν να προσδιορίσουν ένα άτομο και συγκεκριμένα μπορεί να περιλαμβάνει διαδικτυακά αναγνωριστικά όπως διευθύνσεις IP, cookies και δεδομένα τοποθεσίας που θα μπορούσαν να προσδιορίσουν το προφίλ των υποκειμένων των δεδομένων. Αυτό είναι πολύ ευρύτερο από την έννοια των προσωπικών δεδομένων αναγνώρισης βάσει της νομοθεσίας περί απορρήτου των ΗΠΑ (Goddard, 2017).

Το ευρύ εδαφικό πεδίο και ο λεπτομερής ορισμός των προσωπικών δεδομένων διασφαλίζουν ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων θα έχει σημαντικό αντίκτυπο σε πολλούς φορείς οι οποίοι μπορούν να διαχειρίζονται έναν μεγάλο όγκο δεδομένων. Μέσα σε αυτούς τους φορείς ανήκουν και οι τράπεζες. Για την αποτελεσματική λειτουργία των τραπεζικών υπηρεσιών, το τραπεζικό σύστημα είναι υποχρεωμένο να συλλέγει τις απαραίτητες πληροφορίες των πελατών τους και να τις καταχωρεί στα πληροφοριακά συστήματα που διαθέτει. Οι πληροφορίες που συλλέγονται από τους πελάτες της τράπεζας, αφορούν δεδομένα προσωπικού χαρακτήρα ή δεδομένα οικονομικής συμπεριφοράς[4], τα οποία διασφαλίζουν την ταυτότητα του υποκειμένου, ώστε ν' απολαμβάνει τις υπηρεσίες που του προσφέρονται. Αυτά τα

[3] ΓΚΠΔ αρ. 4 (Ορισμοί) παρ. 1

[4] Ειδικότερα για τα δεδομένα οικονομικής συμπεριφοράς βλ. Μυλώση Μ. : Η έννομη προστασία των δεδομένων οικονομική συμπεριφοράς από την αθέμιτη ηλεκτρονική επεξεργασία τους: συγκριτική μελέτη της νομικής ρύθμισης, σε Ελλάδα και Γαλλία, (διδακτορική διατριβή, 2015).

δεδομένα μπορεί να είναι το ονοματεπώνυμο του πελάτη, τα στοιχεία της ταυτότητάς του, ο αριθμός του τηλεφώνου του, η διεύθυνση της κατοικίας του, κινήσεις λογαριασμών, χρηματικές μεταφορές, οφειλές δανείων και οτιδήποτε άλλο μπορεί να εξυπηρετήσει στη δημιουργία προφίλ του πελάτη της τράπεζας.

Η τεχνολογία σήμερα δίνει την ευκαιρία να ικανοποιήσει την ανάγκη ταχύτερης και αποτελεσματικής τραπεζικής συναλλαγής. Το σύστημα πληροφοριών που χρησιμοποιείται σε μια τράπεζα δεν είναι μόνο μεταξύ επιχειρήσεων (B2B), αλλά είναι και μεταξύ επιχειρήσεων με πελάτη (B2C). Η διαδικτυακή εισβολή είναι μια ενέργεια πρόσβασης από μη εξουσιοδοτημένο πρόσωπο σε ένα πληροφοριακό σύστημα χωρίς την άδεια του κατόχου. Εάν ένα σύστημα έχει παραβιαστεί, αυτό σημαίνει ότι έχει κενά ασφαλείας. Η εισβολή μπορεί να γίνει από οποιονδήποτε έχει γνώση της ασφάλειας των τραπεζικών πληροφοριακών συστημάτων και θα μπορούσε να συμβεί για διάφορους σκοπούς, είτε να αλλάξει εμπιστευτικά δεδομένα είτε να υποκλέψει χρηματικά ποσά από το χρηματοπιστωτικό ίδρυμα. Το σφάλμα και η αποτυχία που μπορεί να προκληθούν από αυτήν την εισβολή όχι μόνο μειώνουν την απόδοση του συστήματος, αλλά και την εμπιστοσύνη των πελατών προς το χρηματοπιστωτικό ίδρυμα, λόγω του κινδύνου απώλειας των χρημάτων και των περιουσιακών τους στοιχείων που βρίσκονται στην τράπεζα (Ahmad et al., 2010).

Το τραπεζικό σύστημα, διαθέτει τις υπηρεσίες του μόνο σε άτομα που προσφέρουν τα ζητούμενα προσωπικά δεδομένα σε αντάλλαγμα[5]. Μέσα στο όριο των νόμιμων αδειών που χορηγούνται, οι τράπεζες πραγματοποιούν δραστηριότητες που συνεπάγονται τη συλλογή και την επεξεργασία δεδομένων προσωπικού χαρακτήρα προκειμένου να επιτευχθούν οι καθορισμένοι στόχοι. Ωστόσο, για την επίτευξη των σκοπών που έχουν καθοριστεί, οι τράπεζες πολλές φορές παραμελούν τα δικαιώματα των υποκειμένων των δεδομένων, συμπεριλαμβανομένων των δικαιωμάτων που απορρέουν από την προστασία των προσωπικών δεδομένων (Pirvu & Boghirnea, 2014).

[5] Για τη λειτουργία του διατραπεζικού συστήματος στην Ελλάδα και τη Γαλλία, βλ. σε Milossi, M.-Alexandropoulou, E: Personal Financial Data: Regulatory Framework of their E-Processing Focusing on the Function of the Interbank Information Systems in Greece and France. An Information Law for the 21stCentury: Proceedings of the Third International Seminar on Information Law, Corfu, 25-26 June 2010. Editor Maria Bottis, NOMIKI BIBLIOTHIKI, Athens, 2011, pp. 237-52 και Μυλώση, Μ.-Αλεξανδροπούλου, Ε.: Προσωπικά δεδομένα οικονομικής συμπεριφοράς και ηλεκτρονική επεξεργασία τους από την ΤΕΙΡΕΣΙΑΣ ΑΕ, ΔΙΜΕΕ 2015/1, 25-37

Ο σημαντικότερος παράγοντας για τη εξασφάλιση της προστασίας προσωπικών δεδομένων στο τραπεζικό σύστημα είναι η ασφάλεια που διαθέτουν τα τραπεζικά πληροφοριακά συστήματα κατά την εκτέλεση βασικών λειτουργιών τους, όπως είναι η συλλογή και η επεξεργασία δεδομένων προσωπικού χαρακτήρα. Έτσι τίθεται το ζήτημα της ασφάλειας των τραπεζικών πληροφοριακών συστημάτων βάσει των οποίων αποθηκεύονται σημαντικές πληροφορίες των Τραπεζών. Σημαντικό ρόλο στην ασφάλεια των πληροφοριακών συστημάτων είναι η αρχιτεκτονική σχεδίαση των βάσεων δεδομένων. Όπως θα δούμε και παρακάτω, οι βάσεις δεδομένων αποτελούν το μέσο άντλησης προσωπικών δεδομένων, έχοντας ως στόχο την εξυπηρέτηση των τραπεζικών πληροφοριακών συστημάτων στη συλλογή και στην επεξεργασία των δεδομένων προσωπικού ή οικονομικού χαρακτήρα.

Ο κώδικας δεοντολογίας σε συνδυασμό με τη συμμόρφωση του τραπεζικού συστήματος, στον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ), έθεσαν σε εφαρμογή τους μηχανισμούς προστασίας δεδομένων εφαρμόζοντας προηγμένα συστήματα ασφαλείας. Τα συστήματα ασφαλείας, όπως αναφέρουμε σ' επόμενο κεφάλαιο, στηρίζονται περισσότερο σε μεθόδους κρυπτογράφησης κατά τους οποίους τα δεδομένα μεταξύ των τραπεζικών πληροφοριακών συστημάτων μεταφέρονται σε μη αναγνώσιμη μορφή ώστε να μην γίνονται αντιληπτά από τρίτο μη εξουσιοδοτημένο πρόσωπο. Καθώς ο αριθμός των πελατών που χρησιμοποιούν διαδικτυακές τραπεζικές συναλλαγές αυξάνεται, τα διαδικτυακά τραπεζικά συστήματα γίνονται πιο επιθυμητοί στόχοι για να επιτεθούν οι επιτήδειοι. Για να διατηρήσουν την εμπιστοσύνη των πελατών τους στην ασφάλεια των διαδικτυακών τραπεζικών λογαριασμών τους, τα χρηματοπιστωτικά ιδρύματα πρέπει να προσδιορίσουν τον τρόπο με τον οποίο οι κακόβουλοι χρήστες εισβάλουν στους λογαριασμούς και να αναπτύξουν μεθόδους για την προστασία τους (Edge et al., 2007).

Ο βασικός σκοπός της ασφάλειας των πληροφοριακών συστημάτων είναι η προστασία του υπολογιστικού συστήματος και οποιουδήποτε άλλου στοιχείου που σχετίζεται με αυτό όπως για παράδειγμα το λογισμικό και τα μέσα αποθήκευσης. Η ενδεχόμενη παραβίαση των πληροφοριακών συστημάτων, συνήθως έχει ως στόχο τη διαρροή των δεδομένων που είναι αποθηκευμένα στο υπολογιστικό σύστημα. Αυτό έχει δημιουργήσει την ανάγκη για μία τεχνολογία πληροφορικής που να είναι ικανή να παρέχει σ' ένα άτομο αναμφισβήτητες αποδείξεις της αθωότητάς του (Πάγκαλος & Μαυρίδης, 2002).

Οι απειλές στην ασφάλεια των τραπεζικών πληροφοριακών συστημάτων χωρίζονται σε δύο κατηγορίες ανάλογα με τρόπο δράσης των κακόβουλων ατόμων. Η πρώτη κατηγορία είναι η εσωτερική απειλή ή αλλιώς τα κακόβουλα εμπιστευτικά πρόσωπα, τα οποία δημιουργούν τεράστιες απώλειες σε οργανισμούς, καθώς έχουν αρκετές γνώσεις για να επιτεθούν σε πολύ ευαίσθητες πληροφορίες. Επιπλέον, η πρόληψη και η ανίχνευση επιθέσεων εσωτερικών προσώπων είναι δύσκολη δουλειά, επειδή οι κακόβουλοι εμπιστευτικοί ακολουθούν νόμιμους δρόμους για την έναρξη επιθέσεων. Αυτή η απειλή οδηγεί σε επιθέσεις στα τραπεζικά πληροφοριακά συστήματα όπου το ύψος των ζημιών που σημειώνονται είναι τεράστιο. Η εσωτερική απειλή στα τραπεζικά συστήματα δημιουργεί τεράστια ζημιά στις τράπεζες λόγω της σημασίας και της ελκυστικότητας των περιουσιακών στοιχείων που διαθέτουν (Aljawarneh, 2016).

Η δεύτερη κατηγορία είναι η εξωτερική απειλή η οποία προέρχεται κυρίως από εξωτερικούς κακόβουλους χρήστες, που έχουν ως στόχο τη διαδικτυακή επίθεση των τραπεζικών πληροφοριακών συστημάτων. Αυτού του είδους αθέμιτης επεξεργασίας των τραπεζικών προσωπικών δεδομένων μπορεί να προκαλέσει ανεπανόρθωτη ζημία, όσον αφορά τη διαρροή των δεδομένων των πελατών της τράπεζας. Σε κάθε περίπτωση, την ευθύνη για την προστασία των προσωπικών δεδομένων την έχει ο υπεύθυνος της επεξεργασίας, ο οποίος στην προκειμένη περίπτωση είναι η ίδια η τράπεζα. Τί συμβαίνει όμως στην περίπτωση που η αποθήκευση των δεδομένων προσωπικού χαρακτήρα των πελατών της τράπεζας γίνεται στο σύννεφο (cloud);

Η τεχνολογία του υπολογιστικού νέφους (cloud computing), στηρίζεται στη διατήρηση των δεδομένων σε απομακρυσμένους διακομιστές, οι οποίοι έχουν ως στόχο την άμεση διάθεση των πληροφοριών στα τραπεζικά πληροφοριακά συστήματα. Η υποδομή υπολογιστικού νέφους χρησιμοποιεί νέες τεχνολογίες και υπηρεσίες, οι περισσότερες από τις οποίες δεν έχουν αξιολογηθεί πλήρως όσον αφορά την ασφάλεια. Η υποδομή του υπολογιστικού νέφους, εγείρει σοβαρούς προβληματισμούς σε επίπεδο ασφάλειας δεδομένων, εμπιστοσύνης, κανονισμών και αποδόσεων. Ένα ζήτημα με τις υπηρεσίες νέφους είναι ότι η διαχείριση των δεδομένων ενδέχεται να μην είναι πλήρως αξιόπιστη. Ο κίνδυνος διαρροής εμπιστευτικών δεδομένων στο σύννεφο και η αποτυχία των υπηρεσιών του, έχουν λάβει μεγάλη προσοχή από πολλές εταιρείες (Arora et al., 2013).

Αν και υπάρχει μεγάλη έρευνα και πρόοδος στον τομέα του υπολογιστικού νέφους, πολλά έργα έχουν υψηλό ποσοστό αποτυχίας ειδικά όταν πρόκειται για έργα

τραπεζικών πληροφοριακών συστημάτων. Οι αρχές της διαχείρισης κινδύνων έχουν εισαχθεί στο υπολογιστικό νέφος για να βοηθήσουν στην τεκμηρίωση, να προβλέψουν ορισμένους κινδύνους και να διασφαλίσουν την επιτυχία εκτέλεσης των έργων τραπεζικών πληροφοριακών συστημάτων με υποδομή υπολογιστικού νέφους (Elzamly et al., 2017).

Ο Γενικός Κανονισμός Προστασίας Δεδομένων έχει ρυθμίσει αρκετά ζητήματα σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα των υποκειμένων, όμως δεν έχει ορίσει ακριβώς τον τρόπο με τον οποίο αντιμετωπίζονται ζητήματα προστασίας κι ασφαλείας δεδομένων στο υπολογιστικό νέφος. Αυτό πολλές φορές προκαλεί συγχύσεις στους οργανισμούς ως προς την ευθύνη της επεξεργασίας των δεδομένων. Τα χρηματοπιστωτικά ιδρύματα διαδραματίζουν σημαντικό ρόλο στην προετοιμασία πιο αξιόπιστων συστημάτων ασφαλείας που μπορούν να ικανοποιήσουν τις προσδοκίες των πελατών και να προσελκύσουν νέους πελάτες ώστε να χρησιμοποιούν με εμπιστοσύνη τις υπηρεσίες τους για να διατηρούν τα προσωπικά τους δεδομένα, τις εμπιστευτικές πληροφορίες και τα χρήματά τους ασφαλή. Παρόλο που η τεχνολογία εξελίσσεται και δημιουργεί νέες τάσεις αποθήκευσης, διαχείρισης και διατήρησης δεδομένων όπως είναι το υπολογιστικό νέφος, το τραπεζικό σύστημα θα πρέπει να έχει ένα εφεδρικό σχέδιο ή άλλες ασπίδες για να χειριστεί οποιαδήποτε κακόβουλη συμπεριφορά, η οποία σκοπεύει να παραβιάσει τις πληροφορίες του πελάτη. Βέβαια το παραπάνω εγχείρημα βασίζεται και στην συμμόρφωση του τραπεζικού συστήματος με το ισχύον θεσμικό πλαίσιο και ειδικότερα τον Γενικό Κανονισμό Προστασίας Δεδομένων, ο οποίος έχει ως στόχο τη διαμόρφωση των τραπεζικών διεργασιών με γνώμονα την προάσπιση των συμφερόντων του υποκειμένου των δεδομένων.

## 1.2 Κίνητρα και Στόχοι Έρευνας

Κίνητρο για την εκπόνηση της παρούσας διπλωματικής εργασίας, αποτέλεσε η εκτεταμένη χρήση τεχνολογιών υπολογιστικού νέφους από τους οργανισμούς, ως μέσο αποθήκευσης σημαντικών πληροφοριών που αφορούν δεδομένα προσωπικού χαρακτήρα. Οι οργανισμοί πλέον, εξαιτίας του πλήθους των δεδομένων, δεν μπορούν να φιλοξενήσουν στα πληροφοριακά τους συστήματα τον μεγάλο όγκο πληροφοριών που δέχονται καθημερινά, με αποτέλεσμα να χρησιμοποιούν διαφορετικές λύσεις. Επίσης, το νέο είδος αποθήκευσης δεδομένων στο σύννεφο διευκολύνει την εκτέλεση των

επιχειρηματικών διαδικασιών παρέχοντας γρηγορότερες και καλύτερες υπηρεσίες προς τους πελάτες τους.

Ενδιαφέρον παρουσιάζεται στον τρόπο με τον οποίον τα τραπεζικά πληροφοριακά συστήματα, που χρησιμοποιούν υποδομές υπολογιστικού νέφους, μπορούν να προστατεύσουν και να ασφαλίσουν τα δεδομένα των πελατών τους εφαρμόζοντας πάντα τον Γενικό Κανονισμό Προστασίας Δεδομένων. Η εφαρμογή του ΓΚΠΔ σε συνδυασμό με την ασφάλεια των τραπεζικών πληροφοριακών συστημάτων με υποδομή υπολογιστικού νέφους, ανοίγει το δρόμο για ένα νέο πεδίο έρευνας, το οποίο θα έχει ως απώτερο στόχο την βαθιά κατανόηση της λειτουργίας του υπολογιστικού νέφους και της προστασίας των δεδομένων προσωπικού χαρακτήρα στο τραπεζικό σύστημα.

Η επέκταση των δραστηριοτήτων των τραπεζικών πληροφοριακών συστημάτων στο υπολογιστικό νέφος, έχει δημιουργήσει προβληματισμούς ως προς την ακεραιότητα, την αυθεντικότητα, την εμπιστευτικότητα και την εν γένει ασφάλεια των προσωπικών δεδομένων προς επεξεργασία. Στόχος μας είναι να διερευνήσουμε τη λειτουργία των τραπεζικών πληροφοριακών συστημάτων στη διαχείριση των προσωπικών δεδομένων τα οποία είναι αποθηκευμένα στο νέφος (cloud). Αποτέλεσμα της μελέτης αυτής, είναι ο εντοπισμός του προβληματισμού και η ανεύρεση ενδεχόμενων λύσεων για την αποδοτικότερη διασφάλιση της προστασίας των προσωπικών δεδομένων στο τραπεζικό σύστημα ώστε ν' αναδείξει ότι η χρήση του υπολογιστικού νέφους ως μέθοδος αποθήκευσης, μπορεί να εξασφαλίσει τον αποδοτικό διαμοιρασμό κι επεξεργασία δεδομένων οικονομικής συμπεριφοράς των πελατών.

Οι στόχοι της έρευνας σχετίζονται με την παρουσίαση των τραπεζικών πληροφοριακών συστημάτων και την διαχείριση δεδομένων προσωπικού ή οικονομικού χαρακτήρα μέσω υποδομής υπολογιστικού νέφους. Συγκεκριμένα οι στόχοι της έρευνας είναι:

- Η παρουσίαση της αρχιτεκτονικής σχεδίασης των τραπεζικών πληροφοριακών συστημάτων και η λειτουργία των τοπικών διακομιστών βάσεων δεδομένων.
- Η ανάλυση της ασφάλειας των τραπεζικών πληροφοριακών συστημάτων και ο τρόπος επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
- Ο ορισμός του υπολογιστικού νέφους ως μέθοδος αποθήκευσης και διαχείρισης δεδομένων προσωπικού χαρακτήρα.
- Η παρουσίαση της αρχιτεκτονικής σχεδίασης των τραπεζικών πληροφοριακών συστημάτων με υποδομή υπολογιστικού νέφους. Ο τρόπος με τον οποίον το

τραπεζικό σύστημα συλλέγει κι επεξεργάζεται τα δεδομένα στο σύννεφο και ποια μοντέλα ασφαλείας χρησιμοποιεί το τραπεζικό σύστημα για την προστασία των δεδομένων των πελατών.

- Η εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων στα τραπεζικά πληροφοριακά συστήματα που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα με τη χρήση τεχνολογίας υπολογιστικού νέφους.
- Η ανάδειξη προβληματισμών και υποθέσεων για περαιτέρω έρευνα του θέματος.

## 1.3 Ερωτήματα – Προβληματισμοί

Το θέμα της παρούσας διπλωματικής εργασίας γεννά διάφορα ερωτήματα και προβληματισμούς σχετικά με την ασφάλεια των τραπεζικών πληροφοριακών συστημάτων. Επίσης η εφαρμογή του υπολογιστικού νέφους (cloud computing) ως μέθοδος αποθήκευσης και διαχείρισης προσωπικών δεδομένων, ανοίγει την πόρτα για τη διερεύνηση ενός νέου ερευνητικού πεδίου, αυτού της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων σε νέα μοντέλα επεξεργασίας τραπεζικών δεδομένων όπως είναι το σύννεφο. Κατ' αυτό τον τρόπο, ερευνητές προσπαθούν να θέσουν προβληματισμούς κι ερωτήματα διαμορφώνοντας μία κοινά αποδεκτή άποψη σχετικά με τη σημασία της εξέτασης του ερευνητικού πεδίου της ασφάλειας και της προστασίας των δεδομένων προσωπικού χαρακτήρα στα τραπεζικά πληροφοριακά συστήματα με την τεχνολογική υποδομή υπολογιστικού νέφους.

Η προστασία των δεδομένων προσωπικού χαρακτήρα σε συνδυασμό με την ασφάλεια που παρέχει το υπολογιστικό νέφος στα τραπεζικά πληροφοριακά συστήματα, δημιουργεί διάφορα ερωτήματα, κάποια από τα οποία αφορούν νομικές ρυθμίσεις και διατάξεις, μέτρα ασφαλείας των τραπεζικών πληροφοριακών συστημάτων στα χρηματοπιστωτικά ιδρύματα που αφορούν την επεξεργασία δεδομένων των πελατών (Μυλώση, 2018) και μεθόδους ενσωμάτωσης κι εφαρμογής του υπολογιστικού νέφους στα τραπεζικά δεδομένα. Με βάση τα παραπάνω, τα ερωτήματα μπορούν να διαμορφωθούν ως εξής:

- Με ποιον τρόπο τα χρηματοπιστωτικά ιδρύματα μπορούν να ελέγξουν τη ροή των δεδομένων κατά την επεξεργασία τους, από τα τραπεζικά πληροφοριακά συστήματα;

- Οι τράπεζες χρησιμοποιούν κάποιου είδους κώδικα δεοντολογίας που να ρυθμίζει ζητήματα εκτέλεσης εργασιών που σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα των πελατών;
- Η αρχιτεκτονική υποδομή των τραπεζικών πληροφοριακών συστημάτων, μπορεί να διαθέτει τα κατάλληλα μέτρα ασφαλείας κατά την επεξεργασία των δεδομένων στο σύννεφο;
- Η μέθοδος αποθήκευσης δεδομένων προσωπικού χαρακτήρα στο σύννεφο, αποτελεί εγγύηση για την προστασία τους από επιθέσεις κακόβουλων χρηστών του διαδικτύου;
- Σε περίπτωση που σημειωθεί διαρροή τραπεζικών δεδομένων ποιός θα έχει την ευθύνη, ο πάροχος του υπολογιστικού νέφους ή το ίδιο το χρηματοπιστωτικό ίδρυμα; Ποιός είναι ο υπεύθυνος επεξεργασίας δεδομένων από τη στιγμή που η επεξεργασία τους πραγματοποιείται είτε σε τοπικούς διακομιστές είτε σε απομακρυσμένους με τη χρήση υπολογιστικού νέφους;
- Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) επιλύει ζητήματα που αφορούν την προστασία δεδομένων προσωπικού χαρακτήρα στα τραπεζικά πληροφοριακά συστήματα με υποδομή υπολογιστικού νέφους; Κι εάν δεν περιέχει ρυθμιστικό πλαίσιο για τη χρήση του υπολογιστικού νέφους από τους φορείς επεξεργασίας δεδομένων, μπορεί ο ΓΚΠΔ να τα επιλύσει χρησιμοποιώντας τους ήδη υπάρχοντες κανονισμούς οι οποίοι θέτουν τα θεμέλια για τη σωστή επεξεργασία των δεδομένων;

Αυτά κι πολλά άλλα ερωτήματα, προσπαθεί η παρούσα διπλωματική εργασία να απαντήσει μέσα από διάφορες επιστημονικές προσεγγίσεις επί του θέματος. Όπως θα δούμε και παρακάτω, η διαδικασία της δημιουργίας προβληματισμών στο εν λόγω ερευνητικό πεδίο, θέτει τις βάσεις για την καλύτερη κι αποτελεσματικότερη επεξεργασία των δεδομένων , έχοντας ως κύριο στόχο την προστασία και την ασφάλεια αυτών από νέες μεθόδους και διαδικασίες επεξεργασίας.

## 1.4 Συνεισφορά και περιορισμοί της έρευνας

Η θεματική ενότητα της παρούσας διπλωματικής εργασίας, όπως αναφέραμε και παραπάνω, αποτελεί μία ξεχωριστή προσέγγιση της προστασίας των προσωπικών δεδομένων από νέες μορφές αποθήκευσης και διαχείρισης τραπεζικών πληροφοριών. Το

τραπεζικό σύστημα είναι αναγκασμένο ανά πάσα στιγμή, ν' αναβαθμίζει και να επικαιροποιεί την ασφάλεια των πληροφοριακών συστημάτων που χρησιμοποιούνται από τα χρηματοπιστωτικά ιδρύματα, ώστε να είναι συμβατή με τις νέες τεχνολογικές εξελίξεις.

Τα τραπεζικά δεδομένα έχουν απασχολήσει κατά καιρούς διάφορους ερευνητές, οι οποίοι μέσα από την επιστημονική τους συμβολή επί του θέματος, κατάφεραν να σημειώσουν προόδους ως προ τη νομική προσέγγιση του ερευνητικού πεδίου. Αυτό έχει σαν αποτέλεσμα τα τραπεζικά ιδρύματα να έχουν την τάση να συμμορφώνονται σε κανόνες και μεθόδους ως προς τον τρόπο επεξεργασίας δεδομένων των υποκειμένων. Βέβαια, ο δρόμος για την τελειοποίηση της ασφάλειας των τραπεζικών πληροφοριακών συστημάτων είναι ακόμα πολύ μακρύς καθώς οι τραπεζικές διεργασίες που εκτελούνται από τα χρηματοπιστωτικά ιδρύματα θα πρέπει να προσαρμοστούν στον κώδικα δεοντολογίας του τραπεζικού συστήματος περί προστασίας δεδομένων προσωπικού χαρακτήρα (Aljawarneh, 2016).

Η παρούσα μεταπτυχιακή διατριβή θα συνεισφέρει στη διεύρυνση του συγκεκριμένου ερευνητικού πεδίου, προκειμένου να διευκρινιστούν οι παράγοντες οι οποίοι επηρεάζουν την ασφάλεια των τραπεζικών πληροφοριακών συστημάτων με υποδομή υπολογιστικού νέφους για την προστασία των προσωπικών δεδομένων των πελατών των χρηματοπιστωτικών ιδρυμάτων. Τα ευρήματα της έρευνας έχουν σα στόχο την θεωρητική προσέγγιση σε επίπεδο εφαρμογής της τεχνολογίας υπολογιστικού νέφους για τη διαχείριση και αποθήκευση προσωπικών δεδομένων και την ασφάλεια των τραπεζικών πληροφοριακών συστημάτων από μη εξουσιοδοτημένους χρήστες. Πιο συγκεκριμένα, μετά την ανάγνωση της διπλωματικής εργασίας ο αναγνώστης θα είναι σε θέση να κατανοήσει:

1. Τον ρόλο των τραπεζικών πληροφοριακών συστημάτων στη διαχείριση και στην επεξεργασία των προσωπικών δεδομένων των πελατών.
2. Τη σημαντικότητα της ασφάλειας των πληροφοριακών συστημάτων που χρησιμοποιούν τα χρηματοπιστωτικά ιδρύματα για την προστασία των προσωπικών δεδομένων των πελατών τους.
3. Τους κινδύνους που παρουσιάζονται κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

4. Την έννοια του υπολογιστικού νέφους και τον τρόπο με τον οποίο τα τραπεζικά πληροφοριακά συστήματα τον χρησιμοποιούν για τη διαχείριση των τραπεζικών δεδομένων.
5. Την ασφάλεια των τραπεζικών πληροφοριακών συστημάτων με υποδομή υπολογιστικού νέφους. Η σημασία της προστασίας των προσωπικών δεδομένων των πελατών του χρηματοπιστωτικού ιδρύματος, χρησιμοποιώντας υπηρεσίες υπολογιστικού νέφους.
6. Την ευθύνη του παρόχου υπολογιστικού νέφους ως προς την παροχή των υπηρεσιών του στο τραπεζικό σύστημα και τον ορισμό του υπεύθυνου επεξεργασίας δεδομένων στα τραπεζικά πληροφοριακά συστήματα.
7. Το νομικό πλαίσιο περί προστασίας προσωπικών δεδομένων και η εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) στα χρηματοπιστωτικά ιδρύματα σχετικά με την επεξεργασία προσωπικών δεδομένων με τη χρήση της τεχνολογίας υπολογιστικού νέφους.

Κατά την εκπόνηση της παρούσας διπλωματικής εργασίας αντιμετωπίσαμε διάφορους περιορισμούς που αφορούσαν τη θεωρητική προσέγγιση του ερευνητικού πεδίου. Συγκεκριμένα, ήταν δύσκολη η εύρεση αποφάσεων της Αρχής Προστασίας Δεδομένων με αποτέλεσμα να μην έχουμε πλήρη εικόνα της λειτουργίας του υπολογιστικού νέφους σε συνδυασμό με τη χρήση των τραπεζικών πληροφοριακών συστημάτων όσον αφορά την ασφάλεια και την προστασία των προσωπικών δεδομένων των πελατών. Επίσης αντιμετωπίσαμε πρόβλημα στη βιβλιογραφία σχετικά με τον περιορισμένο όγκο πληροφοριών επί του θέματος με αποτέλεσμα η προσαρμογή της παρούσας διπλωματικής εργασίας στα ελληνικά δεδομένα να είναι δύσκολη.

## 1.5 Βασική Ορολογία

Στην παρούσα υπό-ενότητα παρουσιάζεται η βασική ορολογία για να γίνουν εξαρχής κατανοητοί οι ορισμοί βασικών εννοιών που χρησιμοποιούνται κατά την εκπόνηση της διπλωματικής εργασίας. Συγκεκριμένα:

- **Πληροφοριακά Συστήματα:** Ένα Πληροφοριακό Σύστημα (Information System) αποτελεί ένα σύνολο αλληλένδετων στοιχείων, τα οποία συλλέγουν, επεξεργάζονται, αποθηκεύουν και διανέμουν πληροφορίες που υποστηρίζουν, πολλές φορές, τη λήψη αποφάσεων και τον έλεγχο σ' έναν οργανισμό. Πέρα από

την υποστήριξη στη λήψη αποφάσεων, τα πληροφοριακά συστήματα μπορούν επίσης να βοηθήσουν στελέχη και προσωπικό στην ανάλυση προβλημάτων και στην επεξεργασία δεδομένων όπως τα προσωπικά δεδομένα (Laudon, K., & Laudon, J., 1999).

- **Τραπεζικά Πληροφοριακά Συστήματα:** Τα Τραπεζικά Πληροφοριακά Συστήματα (Banking Information System) είναι τα πληροφοριακά συστήματα τα οποία διαχειρίζονται τα δεδομένα των πελατών των χρηματοπιστωτικών ιδρυμάτων (Georgescu & Jeflea, 2015). Ένα τέτοιο σύστημα αποτελεί το Σύστημα Διαχείρισης Πελατειακών Σχέσεων (Customer Relationship Management – CRM) της τράπεζας κατά το οποίο οι υπάλληλοι του ιδρύματος αποθηκεύουν κι επεξεργάζονται τα δεδομένα των πελατών τους.
- **Ασφάλεια Τραπεζικών Πληροφοριακών Συστημάτων:** Με τον όρο ασφάλεια νοούνται οι τεχνικές εκείνες οι οποίες έχουν ως απώτερο σκοπό την προστασία των πληροφοριακών συστημάτων από κακόβουλες επιθέσεις μη εξουσιοδοτημένων χρηστών. Η ασφάλεια των τραπεζικών πληροφοριακών συστημάτων είναι σημαντική ως προς την προστασία των προσωπικών δεδομένων των πελατών των χρηματοπιστωτικών ιδρυμάτων (Ula, Ismail & Sidek, 2011). Η ασφάλεια, στη παρούσα διπλωματική εργασία, συνδέεται επίσης με τα μέτρα πρόληψης που λαμβάνει ο πάροχος του υπολογιστικού νέφους για τη προστασία των τραπεζικών δεδομένων.
- **Υπολογιστικό Νέφος:** Το Υπολογιστικό Νέφος (Cloud Computing) είναι ένα μοντέλο αποθήκευσης και διαχείρισης πληροφοριών με γρήγορη κι εύκολη πρόσβαση του δικτύου σ' ένα κοινόχρηστο σύνολο διαμορφωμένων υπολογιστικών πόρων (π.χ., δίκτυα, διακομιστές, αποθηκευτικοί χώροι, εφαρμογές και υπηρεσίες), που μπορούν να παρέχονται στον χρήστη ανεξαρτήτως τοποθεσίας (Mell & Grance, 2009). Ο χρήστης έχει την ικανότητα να επεξεργάζεται δεδομένα στο σύννεφο (cloud) παρέχοντας του τη δυνατότητα σύνδεσης σε απομακρυσμένους διακομιστές.
- **Προσωπικά Δεδομένα:** Τα Προσωπικά Δεδομένα (Personal Data) είναι η κάθε πληροφορία που σχετίζεται με ένα φυσικό πρόσωπο που έχει ταυτοποιηθεί ή μπορεί να προσδιοριστεί («υποκείμενο των δεδομένων»)[6] (Αλεξανδροπούλου-Αιγυπτιάδου, 2016). Το υποκείμενο των δεδομένων είναι το φυσικό πρόσωπο

[6] ΓΚΠΔ αρ. 4 (Ορισμοί) παρ. 1

που μπορεί να αναγνωριστεί, άμεσα ή έμμεσα, ιδίως με αναφορά σε ένα αναγνωριστικό όπως ένα όνομα, έναν αριθμό ταυτοποίησης, δεδομένα τοποθεσίας, ένα διαδικτυακό αναγνωριστικό ή με διάφορους παράγοντες που αφορούν, τη γενετική, τη διανοητική, την οικονομική, την πολιτιστική ή την κοινωνική ταυτότητα του φυσικού προσώπου (Politou, Alepis & Patsakis, 2018).

- **Δεδομένα Οικονομικής Συμπεριφοράς:** Τα δεδομένα οικονομικής συμπεριφοράς είναι δεδομένα πελατών των χρηματοπιστωτικών ιδρυμάτων για την πιστοποίηση της ταυτότητας τους ως φυσικά πρόσωπα. Τα δεδομένα αυτά μπορεί να αφορούν φορολογικά, οικονομικά και λοιπά στοιχεία, καθώς επίσης και αντίστοιχα αξιόπιστα έγγραφα τεκμηρίωσης των εν λόγω στοιχείων. Η επεξεργασία των δεδομένων πραγματοποιείται από τα τραπεζικά πληροφοριακά συστήματα και αποθηκεύονται σε βάσεις δεδομένων οι οποίες διαχειρίζονται από το τραπεζικό σύστημα.
- **Ιδιωτικότητα:** Η έννοια της ιδιωτικότητας (Privacy) χρησιμοποιείται συχνά όταν αναφερόμαστε στην προστασία των προσωπικών δεδομένων. Η ιδιωτικότητα σχετίζεται με το δικαίωμα ενός ατόμου ή μιας ομάδας ατόμων, να αποφασίσουν από μόνοι τους για το πότε, πως και μέχρι ποιο σημείο τα προσωπικά τους δεδομένα ή οι πληροφορίες που διαθέτουν σε φορέα επεξεργασίας δεδομένων, θα μπορούν να διαβιβαστούν σε τρίτους πέρα από την αρχική τους συμφωνία. Είναι τα δικαιώματα της προστασίας της προσωπικότητας και του ιδιωτικού βίου που ορίζεται ως το δικαίωμα του υποκειμένου των δεδομένων (De Hert & Gutwirth, 2006).

## 1.6 Διάρθρωση της μελέτης

Η διάθρωση της παρούσας διπλωματικής εργασίας, αποτελείται από έξι θεματικές ενότητες οι οποίες έχουν σα στόχο την ανάδειξη της ασφάλειας των τραπεζικών πληροφοριακών συστημάτων και της προστασίας των προσωπικών δεδομένων των πελατών του τραπεζικού συστήματος. Όπως θα αναλύσουμε και παρακάτω, η πρώτη θεματική ενότητα αναφέρεται στον ορισμό και τη σημασία των πληροφοριακών συστημάτων για τα χρηματοπιστωτικά ιδρύματα. Η δεύτερη θεματική ενότητα περιγράφει τον ρόλο του υπολογιστικού νέφους στη διαχείριση κι αποθήκευση πληροφοριών στους φορείς επεξεργασίας δεδομένων και συγκεκριμένα των

χρηματοπιστωτικών ιδρυμάτων, ενώ στη τρίτη θεματική ενότητα γίνεται λόγος για την εφαρμογή του υπολογιστικού νέφους από τα τραπεζικά πληροφοριακά συστήματα. Στην τέταρτη θεματική ενότητα, θα αναλύσουμε τη σημασία της ασφάλειας των τραπεζικών πληροφοριακών συστημάτων με απώτερο σκοπό την προστασία των προσωπικών δεδομένων των πελατών και στην πέμπτη θεματική ενότητα θα εξετάσουμε το νομικό και κανονιστικό πλαίσιο σχετικά με την επεξεργασία δεδομένων στο τραπεζικό σύστημα. Τέλος, στην έκτη θεματική ενότητα θα συνοψίσουμε την έρευνά μας και θα προτείνουμε μελλοντικές εξελίξεις της εφαρμογής τεχνολογιών υπολογιστικού νέφους στο τραπεζικό σύστημα.

Αναλυτικότερα, στο κεφάλαιο 2 θα περιγράψουμε τον ορισμό των πληροφοριακών συστημάτων και θα εξετάσουμε τον ρόλο τους στο τραπεζικό σύστημα. Επίσης θα αναπτύξουμε την αρχιτεκτονική σχεδίαση των τραπεζικών πληροφοριακών συστημάτων ώστε ο αναγνώστης να μπορεί να κατανοήσει τον ρόλο και τη σημασία της ασφάλειας των πληροφοριακών συστημάτων στην προστασία των προσωπικών δεδομένων των πελατών.

Στο κεφάλαιο 3 θα ορίσουμε την έννοια του υπολογιστικού νέφους και θα περιγράψουμε τον τρόπο λειτουργίας του ως προς τη διαχείριση κι επεξεργασία των προσωπικών δεδομένων. Σκόπιμο είναι, σ' αυτό το κεφάλαιο, να αναλύσουμε τον ρόλο του υπολογιστικού νέφους στους φορείς επεξεργασίας δεδομένων και να καταγράψουμε τα οφέλη που μπορεί να προσφέρει ως μία νέα μορφή αποθήκευσης και διαχείρισης δεδομένων.

Στο κεφάλαιο 4 θα περιγράψουμε τα τραπεζικά πληροφοριακά συστήματα που βασίζονται σε υποδομή υπολογιστικού νέφους. Επίσης θα εξετάσουμε τη σημασία της χρήσης της τεχνολογίας του υπολογιστικού νέφους από τα χρηματοπιστωτικά ιδρύματα και πως τα τραπεζικά δεδομένα επηρεάζονται από τη λειτουργία του σύννεφου (cloud). Τέλος θα αναλύσουμε τα οφέλη του υπολογιστικού νέφους στη διαχείριση κι αποθήκευση των προσωπικών δεδομένων καθώς και στη μετέπειτα επεξεργασία τους από τα πληροφοριακά συστήματα των χρηματοπιστωτικών ιδρυμάτων.

Στο κεφάλαιο 5 θα μελετήσουμε τη σημασία της ασφάλειας της τεχνολογίας υπολογιστικού νέφους και πως τα τραπεζικά πληροφοριακά συστήματα μπορούν να προστατεύσουν τα προσωπικά δεδομένα των πελατών του χρηματοπιστωτικού ιδρύματος. Έπειτα θα εξετάσουμε τους κινδύνους και τις απειλές της τεχνολογίας του

υπολογιστικού νέφους για το τραπεζικό σύστημα και θα προσπαθήσουμε ν' απαριθμήσουμε τους τρόπους αντιμετώπισής τους.

Στο κεφάλαιο 6 θα μελετήσουμε τις νομικές ρυθμίσεις σχετικά με την τεχνολογία του υπολογιστικού νέφους καθώς επίσης θα προσπαθήσουμε να εφαρμόσουμε τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) για την εφαρμογή τεχνολογιών νέφους στο τραπεζικό σύστημα. Τέλος στο κεφάλαιο 7 θα συνοψίσουμε την έρευνά μας, εξετάζοντας μελλοντικές εξελίξεις και προοπτικές εισαγωγής νέων μορφών διαχείρισης κι αποθήκευσης προσωπικών δεδομένων στο τραπεζικό σύστημα.

# 2 Τραπεζικά Πληροφοριακά Συστήματα

## 2.1 Εισαγωγή

Με την εξέλιξη της τεχνολογίας, πολλές επιχειρήσεις κι οργανισμοί θεώρησαν ότι η διαχείριση της πληροφορίας στο πλαίσιο εφαρμογής των επιχειρηματικών διεργασιών που εκτελούταν κατά τη διεκπεραίωση σημαντικών υπηρεσιών τους, αποτέλεσε αναγκαίο αγαθό για τη συλλογή κι επεξεργασία προσωπικών δεδομένων των πελατών τους. Η επιστήμη που ασχολείται με τη διαχείριση των πληροφοριών σ' έναν οργανισμό ονομάζεται Τεχνολογία Πληροφοριών (ΤΠ). Η τεχνολογία των πληροφοριών αποτελείται από το υλικό (hardware) και το λογισμικό (software) ενός συστήματος για την πλήρη προσαρμογή της τεχνολογίας στις επιχειρηματικές διαδικασίες ενός οργανισμού.

Η τεχνολογία των πληροφοριών έχει σα στόχο τη διαχείριση κι επεξεργασία όλων των διαθέσιμων πληροφοριών που συλλέγει ένας οργανισμός. Πως όμως ο φορέας επεξεργασίας των πληροφοριών θα μπορέσει να συλλέξει αποτελεσματικά τα δεδομένα των πελατών που εισρέουν στις επιχειρηματικές του διαδικασίες; Το ερώτημα αυτό προβλημάτισε κατά καιρούς τους ερευνητές προσπαθώντας να δώσουν λύσεις οι οποίες δε μπορούσαν να εφαρμοστούν στη διαχείριση μεγάλου όγκου πληροφοριών. Η ανάγκη των επιχειρήσεων για την αποδοτική εφαρμογή των διεργασιών τους ως προς τις απαιτήσεις των πελατών τους, τους οδήγησε στη χρήση της επιχειρηματικής τεχνολογίας.

Η δομημένη εφαρμογή της τεχνολογίας στις επιχειρηματικές διαδικασίες ενός οργανισμού αποτέλεσε ένα δύσκολο έργο των υπεύθυνων διαχείρισης κι επεξεργασίας πληροφοριών. Κατ' αυτόν τον τρόπο, οι υπεύθυνοι διαχείρισης δεδομένων, θεώρησαν ότι η τεχνολογία που μπορεί να χρησιμοποιηθεί θα πρέπει να ικανοποιεί την αρχιτεκτονική σχεδίαση των επιχειρηματικών λειτουργιών του οργανισμού, ώστε να ανταποκρίνεται αποτελεσματικά στη συλλογή κι επεξεργασία νέων πληροφοριών των πελατών. Αυτήν την εργασία την ανέθεσαν στα πληροφοριακά συστήματα, τα οποία με την εγκατάστασή τους, ο οργανισμός μπορούσε πλέον να διαχειριστεί έναν μεγάλο όγκο πληροφοριών που εισέρχονταν στην επιχείρηση.

Τα πληροφοριακά συστήματα εφαρμόζονται εντός του οργανισμού με σκοπό τη βελτίωση της αποτελεσματικότητας και της αποδοτικότητας του. Οι δυνατότητες των πληροφοριακών συστημάτων σε συνδυασμό με τα χαρακτηριστικά ενός οργανισμού

όπως είναι, τα συστήματα εργασίας, το ανθρώπινο δυναμικό και των μεθοδολογιών ανάπτυξης και εφαρμογής επιχειρηματικών διαδικασιών, καθορίζουν από κοινού το βαθμό στον οποίο επιτυγχάνεται ο σκοπός της συλλογής κι επεξεργασίας αναγκαίων πληροφοριών (Silver et al., 1995). Πολλοί ερευνητές του κλάδου των Πληροφοριακών Συστημάτων (Information System - IS), σημείωσαν ότι η περαιτέρω γνώση βοηθά στην παραγωγική εφαρμογή της τεχνολογίας των πληροφοριακών συστημάτων σε επιχειρήσεις κι οργανισμούς και τη διαχείρισή τους από τους υπαλλήλους των φορέων επεξεργασίας δεδομένων. Η γνώση σχετικά με τη διαχείριση των πληροφοριακών συστημάτων και η χρήση της τεχνολογίας αυτής έχει σα στόχο την ανάπτυξη διαχειριστικών κι οργανωτικών διαδικασιών συλλογής κι επεξεργασίας πληροφοριών.

Η απόκτηση γνώσεων σχετικά με την αρχιτεκτονική σχεδίαση των πληροφοριακών συστημάτων περιλαμβάνει δύο συμπληρωματικά αλλά ξεχωριστά παραδείγματα, την συμπεριφορική επιστήμη[7] και την επιστήμη του σχεδιασμού[8] (March & Smith, 1995). Η συμπεριφορική επιστήμη επιδιώκει να αναπτύξει και να δικαιολογήσει θεωρίες (δηλαδή, αρχές και νόμους) που εξηγούν ή προβλέπουν οργανωτικά και ανθρώπινα φαινόμενα που περιλαμβάνουν την ανάλυση, το σχεδιασμό, την εφαρμογή, τη διαχείριση και τη χρήση συστημάτων πληροφοριών για την αποτελεσματικότερη επεξεργασία δεδομένων των πελατών ενός οργανισμού. Τέτοιες θεωρίες ενημερώνουν τελικά τους ερευνητές και τους επαγγελματίες για τις αλληλεπιδράσεις μεταξύ ανθρώπων, τεχνολογίας και οργανισμών που πρέπει να γνωρίζουν εάν ένα σύστημα πληροφόρησης πρόκειται να επιτύχει τον δηλωμένο σκοπό του, συγκεκριμένα τη βελτίωση της αποτελεσματικότητας και της αποδοτικότητας ενός οργανισμού. Αυτές οι θεωρίες επηρεάζονται από αποφάσεις σχεδιασμού που λαμβάνονται σε σχέση με τη μεθοδολογία ανάπτυξης του συστήματος που χρησιμοποιείται, τις λειτουργικές δυνατότητες, το περιεχόμενο πληροφοριών και τις ανθρώπινες διεπαφές που εφαρμόζονται στο σύστημα πληροφοριών (Hevner et al., 2004).

[7] Οι Συμπεριφορικές επιστήμες έχουν ως κύριο αντικείμενο έρευνας και μελέτης, τις πάσης φύσεως δραστηριότητες και αλληλεπιδράσεις οποιουδήποτε πληροφοριακού συστήματος, σε σχέση με το περιβάλλον με το οποίο αλληλεπιδρά.

[8] Η Επιστήμη του σχεδιασμού πληροφοριακών συστημάτων έχει ως στόχο την αποτελεσματική δημιουργία διεπαφών του συστήματος. Αποτελεί κατασταλτικό παράγονται για την εύκολη διαχείριση κι επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Στην παρούσα ενότητα, γίνεται λόγος για τα τραπεζικά πληροφοριακά συστήματα. Πρόκειται για οργανωτικά συστήματα τα οποία έχουν ως απώτερο σκοπό την εύρυθμη λειτουργία του τραπεζικού συστήματος. Τα χρηματοπιστωτικά ιδρύματα με τις νέες νομικές διατάξεις περί προστασίας προσωπικών δεδομένων των υποκειμένων (πελατών), θα πρέπει να σχεδιάσουν τις τραπεζικές τους διαδικασίες με τέτοιο τρόπο ώστε να προστατεύονται τα συμφέροντα του υποκειμένου των δεδομένων. Όπως θα δούμε και παρακάτω τα τραπεζικά πληροφοριακά συστήματα θα πρέπει να σχεδιάζονται έτσι ώστε να πληρούν κάθε κριτήριο ασφάλειας πληροφοριών για την αποτελεσματική προστασία των προσωπικών δεδομένων των πελατών τους. Εδώ να σημειώσουμε ότι, το τραπεζικό σύστημα ήταν από τους πρώτους φορείς επεξεργασίας δεδομένων ο οποίος προσπάθησε να εναρμονίσει στις επιχειρηματικές του διατάξεις τα νομικά πρότυπα του κράτους και κατ' επέκταση της Ευρωπαϊκής Ένωσης (ΕΕ). Στόχος του κεφαλαίου είναι ο ορισμός των Τραπεζικών Πληροφοριακών Συστημάτων (ΤΠΣ) ως μέσω διαχείρισης κι επεξεργασίας προσωπικών δεδομένων καθώς και η ανάλυση του ρόλου των ΤΠΣ για την αποδοτική λειτουργία των χρηματοπιστωτικών ιδρυμάτων.

## 2.2 Η έννοια των Τραπεζικών Πληροφοριακών Συστημάτων

Τα χρηματοπιστωτικά ιδρύματα σε όλο τον κόσμο παρέχουν τραπεζικές υπηρεσίες μέσω συστημάτων πληροφοριών, όπως: αυτόματες ταμειολογιστικές μηχανές (ATM), διαδικτυακές συναλλαγές (internet banking) και τηλεφωνικές τραπεζικές υπηρεσίες, σε μια προσπάθεια να παραμείνουν ανταγωνιστικές καθώς και να βελτιώσουν την εξυπηρέτηση των πελατών τους. Ωστόσο παλαιότερα, η αποδοχή τέτοιων τραπεζικών συστημάτων εισροής πληροφοριών, ακόμα και στις αναπτυσσόμενες χώρες, αποτελούσε πρόβλημα προσαρμογής των παραδοσιακών τρόπων εκτέλεσης τραπεζικών υπηρεσιών με την τεχνολογία (Reid & Levy, 1970). Το κλασικό μοντέλο προσαρμογής της τεχνολογίας στις τραπεζικές διαδικασίες για την διεκπεραίωση σημαντικών υπηρεσιών των χρηματοπιστωτικών ιδρυμάτων, έχει επικυρωθεί καλά σε εκατοντάδες μελέτες τις τελευταίες δύο δεκαετίες. Οι μελέτες αυτές συνέβαλαν στην εκτεταμένη έρευνα της αποδοχής της τεχνολογίας από τα χρηματοπιστωτικά ιδρύματα, προσπαθώντας να επικυρώσουν την ενσωμάτωση των τραπεζικών διεργασιών με την τεχνολογία, σύμφωνα με το κλασικό μοντέλο προσαρμογής των πληροφοριακών συστημάτων στα τραπεζικά ιδρύματα. Ωστόσο, τα αποτελέσματα έδειξαν ότι η

διαχείριση των προσωπικών δεδομένων των πελατών είναι πράγματι ένας σημαντικός παράγοντας που επηρεάζει, τόσο την εφαρμογή των πληροφοριακών συστημάτων στις τράπεζες όσο και τη διαμόρφωση των υπηρεσιών του τραπεζικού συστήματος ανάλογα με την εξέλιξη της τεχνολογίας.

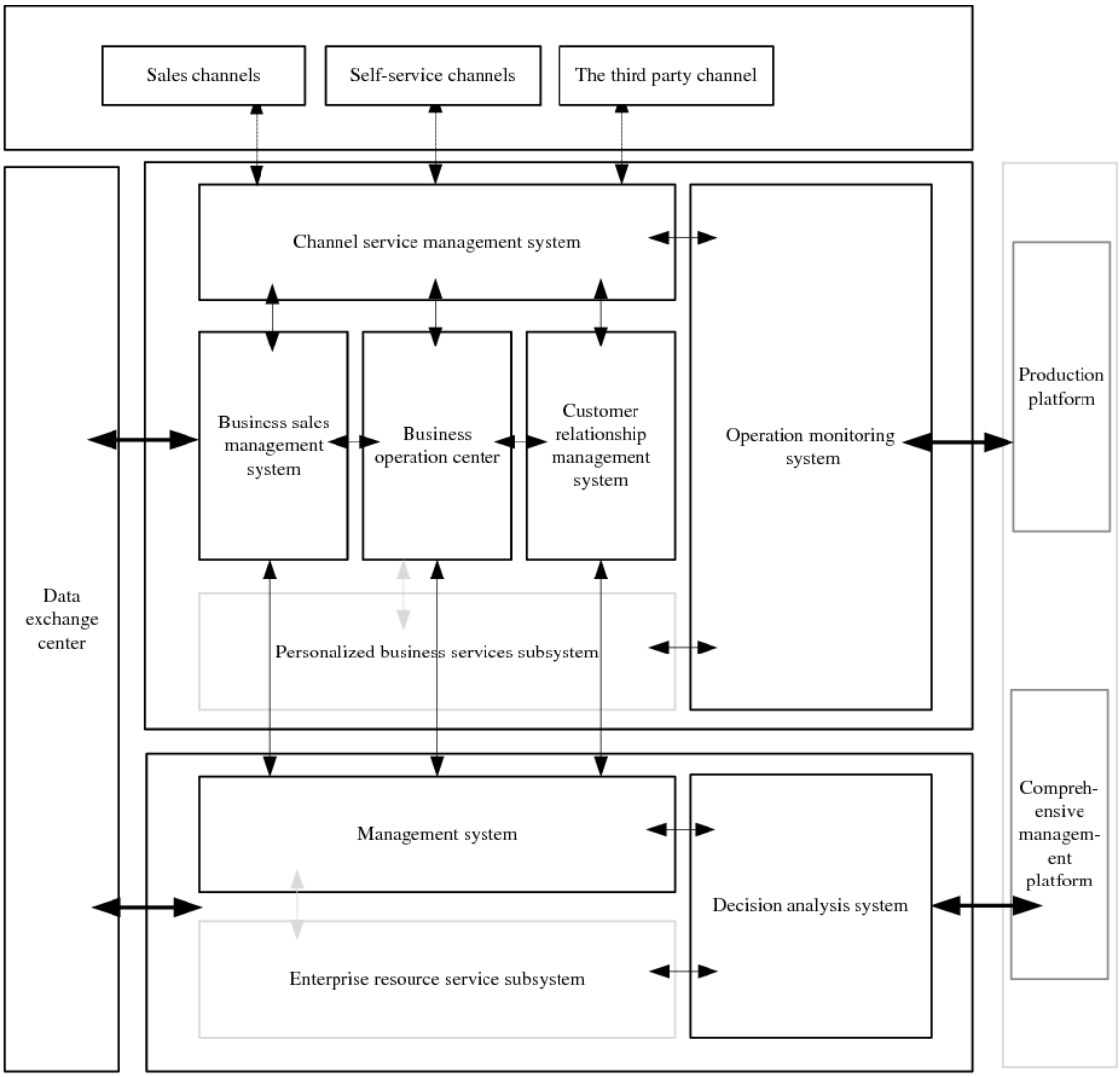
Όπως αναφέραμε και παραπάνω, η διαχείριση των πληροφοριών που εισέρχονται σε μία επιχείρηση αποτελεί έναν κρίσιμο παράγοντα στη διαμόρφωση των επιχειρηματικών του λειτουργιών. Στο τραπεζικό σύστημα τα προσωπικά δεδομένα των πελατών, για την αποτελεσματική κι αποδοτική διαχείρισή τους, απαιτείται η εγκατάσταση των πληροφοριακών συστημάτων. Τι είναι όμως ένα πληροφοριακό σύστημα και πως η αρχιτεκτονική του σχεδίαση εφαρμόζεται στο τραπεζικό σύστημα;

Ένα πληροφοριακό σύστημα είναι ένα σύνολο αλληλοσχετιζόμενων στοιχείων που έχουν σαν κύριο στόχο τη συλλογή, την αποθήκευση, τη διαχείριση κι την επεξεργασία κρίσιμων πληροφοριών. Η αρχιτεκτονική δομή των συστημάτων αυτών τους επιτρέπει την ταυτόχρονη προσπέλαση των πόρων από διάφορους χρήστες, με αποτέλεσμα τα δεδομένα να διαμοιράζονται ομοιόμορφα εντός της επιχείρησης για διοικητικούς και οργανωτικούς σκοπούς. Τα πληροφοριακά συστήματα περιέχουν πληροφορίες πελατών, τόπων και περιουσιακών στοιχείων μέσα από τον οργανισμό ή από το περιβάλλον με το οποίο αλληλεπιδρά.

Τα τραπεζικά πληροφοριακά συστήματα συλλέγουν αυτοματοποιημένα ή μη σημαντικές πληροφορίες των πελατών για την αποδοτική εκτέλεση των υπηρεσιών ενός χρηματοπιστωτικού ιδρύματος. Το τραπεζικό σύστημα δίνει περισσότερο έμφαση στην ασφάλεια των πληροφοριακών συστημάτων για την προστασία των προσωπικών δεδομένων των πελατών. Η ασφάλεια αυτή, όπως θα δούμε και σ' επόμενο κεφάλαιο, προκύπτει από την μεταφορά κρυπτογραφημένων δεδομένων[9] μεταξύ των χρηστών των τραπεζικών πληροφοριακών συστημάτων (οι τραπεζικοί υπάλληλοι), τον διαχωρισμό εξουσιοδοτημένων χρηστών ή μη για την συγκεκριμένη πρόσβαση τους σε μερικά ή ολικά τμήματα του συστήματος (ορισμός σύνθετων κωδικών πρόσβασης ανά χρήστη) και την ασφάλεια που διαθέτει η βάση δεδομένων όπως αποθηκεύονται οι εισερχόμενες

[9] Η τεχνική της κρυπτογράφησης έχει ως στόχο την απόκρυψη του περιεχομένου, δηλαδή των πληροφοριών ή των δεδομένων, ενός συστήματος αρχείων. Τα ιδιωτικά δεδομένα που περιέχονται στο σύστημα αρχείων, πρέπει να προστατευθούν από πιθανές επιθέσεις κακόβουλων χρηστών, οι οποίοι με διάφορες τεχνικές έχουν αποκτήσει πρόσβαση στον υπολογιστή (ως φυσικό μέσο) ή στο δίκτυο της τράπεζας.

πληροφορίες του χρηματοπιστωτικού ιδρύματος. Με όσα αναφέρθηκαν παραπάνω, προκύπτει το συμπέρασμα ότι για τη δημιουργία και την ανάπτυξη των τραπεζικών πληροφοριακών συστημάτων απαιτείται λεπτομερής σχεδιασμός, ώστε να περιλαμβάνει όλες τις προδιαγραφές για την προστασία των προσωπικών δεδομένων των πελατών, βάση των οποίων εκτελούνται οι τραπεζικές διεργασίες.




**Εικόνα 1:** Αρχιτεκτονική ενός πληροφοριακού συστήματος[10]

Στην παραπάνω εικόνα απεικονίζεται η αρχιτεκτονική ενός πληροφοριακού συστήματος που έχει ως στόχο την αποτελεσματική επεξεργασία των πληροφοριών που εισέρχονται στον οργανισμό. Τα πληροφοριακά συστήματα μετασχηματίζουν τις

[10] Πηγή: Study on Information System Architecture Based on Service-Dominant Logic. *Intelligent Information Management*, *7*(02), 53.

πληροφορίες σε χρήσιμα δεδομένα κι έπειτα εξάγονται ως εκροές εκτελώντας κατ' αυτόν τον τρόπο τις επιχειρηματικές διαδικασίες (Wu et al., 2015). Η αρχιτεκτονική δομή των τραπεζικών πληροφοριακών συστημάτων είναι παρόμοια με αυτήν της Εικόνας 1. Στόχος των συστημάτων αυτών είναι η επεξεργασία των προσωπικών δεδομένων των πελατών για την άμεση εκτέλεση των τραπεζικών διεργασιών.

Είναι γενικά αποδεκτό ότι ένας από τους βασικούς παράγοντες για τον επιτυχημένο σχεδιασμό και υλοποίηση των τραπεζικών πληροφοριακών συστημάτων είναι η στενή σύνδεση της στρατηγικής αυτών των συστημάτων με την τραπεζική στρατηγική. Ωστόσο, στην πράξη, η σύνδεση της φιλοσοφίας των πληροφοριακών συστημάτων με την τραπεζική στρατηγική αποτελεί έναν δύσκολο παράγοντα υλοποίησης μίας ενιαίας οργανικής στρατηγικής (Baets, 1992). Με την εξέλιξη της τεχνολογίας και την εισαγωγή νέων μεθόδων εταιρικής διακυβέρνησης στο τραπεζικό σύστημα, η εκτέλεση των διεργασιών έχει αυξήσει την πολυπλοκότητα τους με αποτελέσματα την άμεση εφαρμογή των πληροφοριακών συστημάτων για τη διαχείριση ενός μεγάλου όγκου πληροφοριών. Κατ' αυτόν τον τρόπο δημιουργήθηκαν διαφορετικά είδη τραπεζικών πληροφοριακών συστημάτων, το καθένα από τα οποία εκτελεί συγκεκριμένες διεργασίες[11].

## 2.3 Τα είδη των Τραπεζικών Πληροφοριακών Συστημάτων

Η άνοδος του Διαδικτύου και η χρήση νέων μεθόδων προσπέλασης δεδομένων, δημιούργησε την ανάγκη για την εφαρμογή συστημάτων διαχείρισης των πληροφοριών ανάλογα του σκοπού της επεξεργασίας δεδομένων. Το τραπεζικό σύστημα χρησιμοποιεί διάφορα είδη συστημάτων για να διαμορφώσει κατάλληλα τις τραπεζικές διεργασίες στις ανάγκες των πελατών. Έτσι έχουμε Συστήματα Διαχείρισης Επιχειρηματικών Πόρων (Enterprise Resource Planning - ERP), Συστήματα Διαχείρισης Πελατειακών Σχέσεων (Customer Relationship Management - CRM), Πληροφοριακά Συστήματα Διοίκησης (Management Information System - MIS) και Συστήματα Διαχείρισης Ανθρώπινου Δυναμικού (Human Resources Management - HRM).

[11] Βλ. πληροφοριακά συστήματα ΤΕΙΡΕΣΙΑΣ Α.Ε.

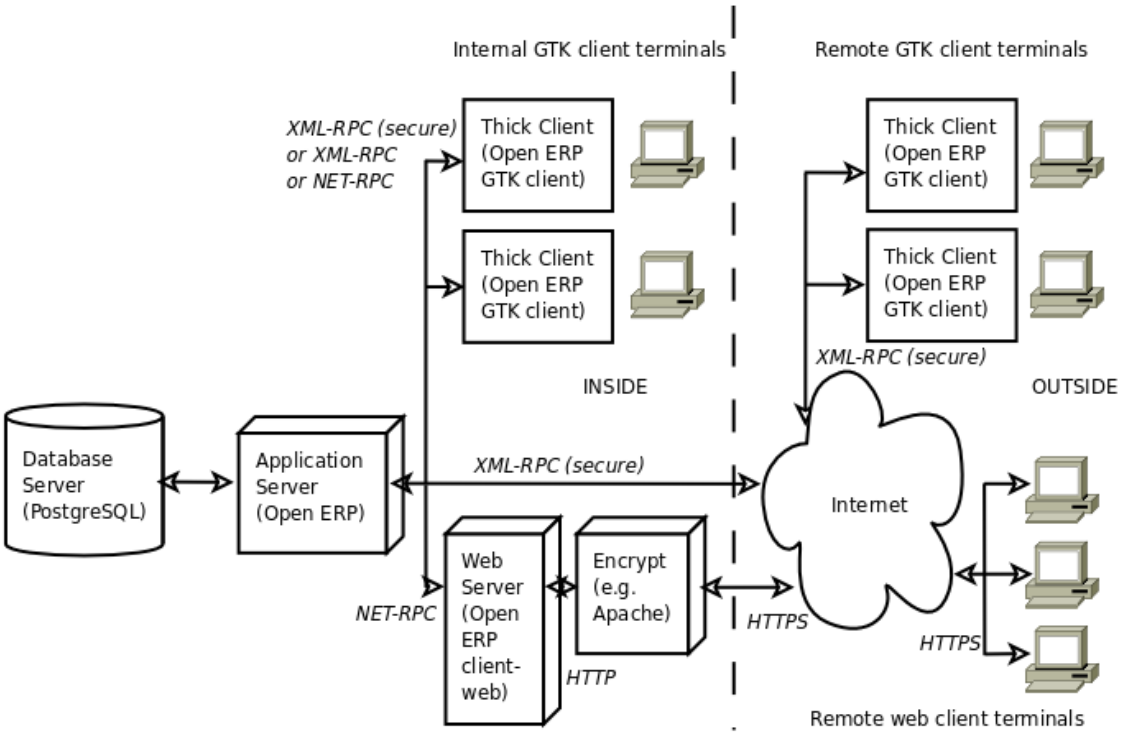
### *2.3.1 Συστήματα Διαχείρισης Επιχειρηματικών Πόρων (ERP)*

Η Τεχνολογία της Πληροφορίας έχει βαθιά επίδραση στα σημερινά τραπεζικά ιδρύματα. Τα χρηματοπιστωτικά ιδρύματα και οι πελάτες τους, αναγκάζονται να προσαρμοστούν σε αυτήν τη νέα πραγματικότητα εφαρμόζοντας λύσεις βάσει της τεχνολογίας των πληροφοριών που έχουν αποδειχθεί αποτελεσματικές στην επιτάχυνση της λειτουργίας των τραπεζικών ιδρυμάτων, βελτιώνοντας παράλληλα την παραγωγικότητα τους. Επομένως, για την εφαρμογή των συστημάτων που βασίζονται στην τεχνολογία της πληροφορίας, πρέπει να εφαρμοστούν ολοκληρωμένα Συστήματα Διαχείρισης Επιχειρηματικών Πόρων (ERP).

Η εφαρμογή των συστημάτων διαχείρισης επιχειρηματικών πόρων, υποστηρίζει διάφορες προσεγγίσεις στη διαχείριση των τραπεζικών δεδομένων και μπορεί να διαφέρει από το ένα χρηματοπιστωτικό ίδρυμα στο άλλο, ανάλογα με τις δυνατότητες και τις απαιτήσεις του. Οι προσεγγίσεις υλοποίησης περιλαμβάνουν: την ολοκληρωμένη εφαρμογή, την πιλοτική εφαρμογή και τη σταδιακή εφαρμογή του συστήματος. Η τράπεζα χρησιμοποιεί μια προσέγγιση που ταιριάζει καλύτερα στις επιχειρηματικές ανάγκες και τις δραστηριότητές της, καθώς τα τραπεζικά συστήματα χρησιμοποιούν σχεδόν όλες τις δυνατότητες ενός ΠΣ ERP (Ahmad, Ibrahim & Garba, 2015).

Στο εννοιολογικό πλαίσιο ενός συστήματος ERP, κάθε τραπεζική λειτουργία που δημιουργείται από το σύστημα, μπορεί να συνδεθεί και με άλλα τραπεζικά πληροφοριακά συστήματα του χρηματοπιστωτικού ιδρύματος. Η λειτουργία της διεπαφής του χρήστη, χρησιμεύει ως εργαλείο επικοινωνίας μεταξύ του τραπεζικού υπαλλήλου και του συστήματος ERP. Οι τραπεζικές λειτουργίες που εκτελεί ένα τραπεζικό σύστημα διαχείρισης επιχειρηματικών πόρων μπορεί να αφορούν περιουσιακά στοιχεία της τράπεζας, δεδομένα οικονομικού χαρακτήρα του χρηματοπιστωτικού ιδρύματος, οικονομικά αποθέματα, τραπεζικά και λογιστικά έγγραφα καθώς και δεδομένα πελατών τα οποία μπορούν ν’ αντληθούν από ένα σύστημα διαχείρισης πελατειακών σχέσεων (CRM) (Akram, Kewley, & Allan, 2006).

Στην Εικόνα 2, παρουσιάζεται η αρχιτεκτονική δομή ενός συστήματος διαχείρισης επιχειρηματικών πόρων. Τα δεδομένα οικονομικής συμπεριφοράς που έχει συλλέξει το τραπεζικό ίδρυμα από τους πελάτες του, εξάγονται στο σύστημα ERP μέσω της βάσης δεδομένων της τράπεζας. Έπειτα πραγματοποιούνται τεχνικές ασφάλειας, όπως είναι η κρυπτογράφηση δεδομένων και στη συνέχεια τα δεδομένα παρουσιάζονται σε αναγνώσιμη μορφή στον χρήστη του τραπεζικού συστήματος ERP.

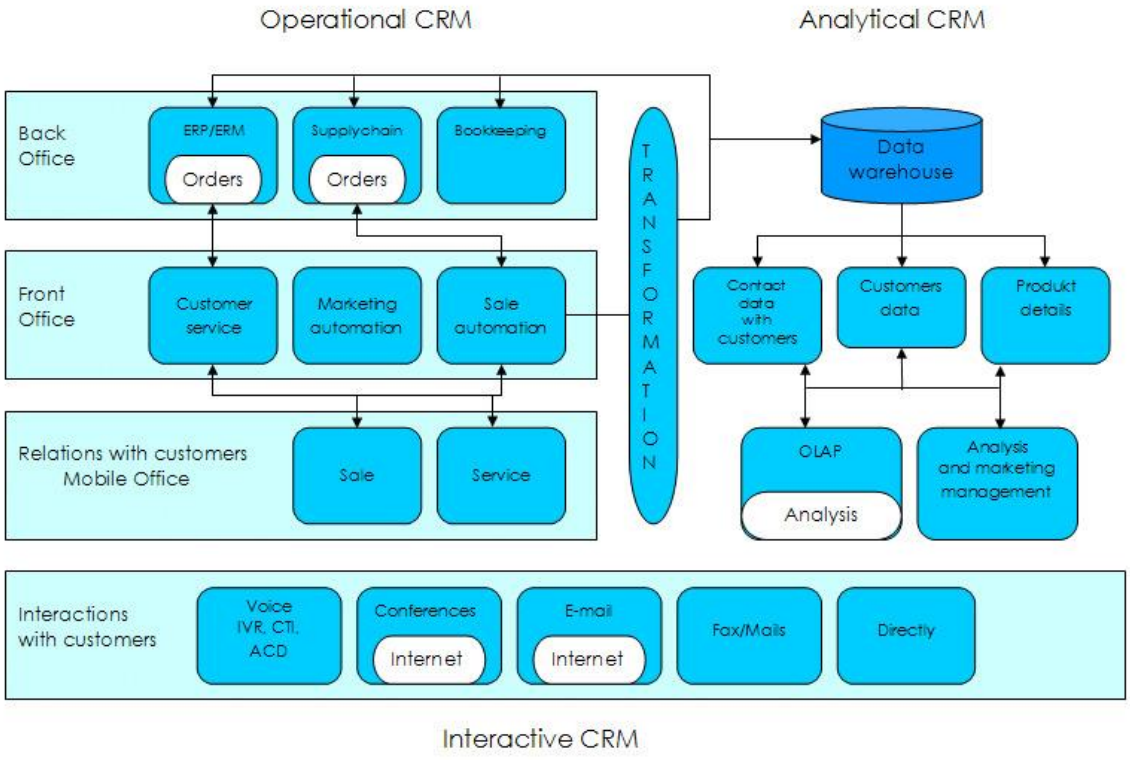



**Εικόνα 2:** Αρχιτεκτονική δομή ενός συστήματος ERP[12]

### *2.3.2 Συστήματα Διαχείρισης Πελατειακών Σχέσεων (CRM)*

Η ικανότητα αναγνώρισης κερδοφόρων πελατών και, στη συνέχεια, προσαρμογής του μάρκετινγκ με βάση την αξία τους, επέτρεψε σε πολλές τράπεζες να ξεπεράσουν του προβληματισμούς τους ως προς τη διαχείριση των πληροφοριών των πελατών τους, με αποτέλεσμα να μπορέσουν να επιβιώσουν σ' ένα ανταγωνιστικό περιβάλλον. Σε κάθε περίπτωση, οι τράπεζες έχουν αποκτήσει ανταγωνιστικό πλεονέκτημα μέσω των δυνατοτήτων που σχετίζονται με τα δεδομένα που εισρέουν στο τραπεζικό σύστημα από τους πελάτες, βασισμένες σ' ένα μεγάλο βαθμό στα **Συστήματα Διαχείρισης Πελατειακών Σχέσεων (CRM)**. Δεν προκαλεί έκπληξη το γεγονός ότι οι υπεύθυνοι των χρηματοπιστωτικών ιδρυμάτων επισημαίνουν ότι, διαθέτοντας πόρους σε τεχνολογίες διαχείρισης πελατειακών σχέσεων, όλες οι εταιρείες στον τομέα των χρηματοοικονομικών υπηρεσιών μπορούν να δημιουργήσουν νέες μορφές ανταγωνιστικού πλεονεκτήματος (Coltman, 2007).

[12] Πηγή: https://doc.odoo.com/5.0/pt_BR/book/1/1_1_Inst_Config/1_1_Inst_Config_architecture/




**Εικόνα 3:** Αρχιτεκτονική δομή ενός συστήματος CRM[13]

Στην Εικόνα 3, απεικονίζεται η αρχιτεκτονική δομή ενός συστήματος Διαχείρισης Πελατειακών Σχέσεων (CRM), η οποία βοηθάει την ομαλή ροή των δεδομένων εντός του τραπεζικού ιδρύματος. Οι πελάτες διαθέτουν τα απαραίτητα δεδομένα στη τράπεζα η οποία με τη σειρά της μέσω του συστήματος διαχείρισης των πελατών, επεξεργάζεται τα δεδομένα αυτά και δημιουργεί συγκεκριμένες τραπεζικές υπηρεσίες. Με τα δεδομένα που εισρέουν στο τραπεζικό σύστημα διαχείρισης πελατών, το χρηματοπιστωτικό ίδρυμα επιτρέπει (Kotarba, 2016):

1. τη διαχείριση δεδομένων πελατών (κύρια δεδομένα, συναλλαγές, προφίλ, μοτίβα), την τμηματοποίηση πελατών και τη μέτρηση της αξίας τους, την πρόβλεψη και παρακολούθηση του κύκλου ζωής των πελατών και τα προσαρμοσμένα και τυποποιημένα προϊόντα και πακέτα υπηρεσιών που μπορούν να τους προσφέρουν,

[13] Πηγή: CRM architecture. Source: A. Mazur, K. Jaworska, D. Mazur, CRM Zarządzanie kontaktami z klientami [CRM Customer Relationship Management], Madar, Zabrze, p. 23.

2. τη διαχείριση προτιμήσεων, την κοινή ανάπτυξη προϊόντων (τράπεζα-πελάτης), τη διασφάλιση των επιπέδων υπηρεσιών σε αναλογία τιμής και οφέλους, τη δημιουργία γνώσεων πελατών (τραπεζική νοημοσύνη) και τη χρήση τους σε επιχειρηματικές διαδικασίες,
3. τη διαχείριση στρατηγικών πωλήσεων μέσα από τη:
    - Σύνδεση της κοινότητας των πελατών(οικογένειες, κοινωνικοί κύκλοι πελατών, επιχειρηματικές-ιδιωτικές σχέσεις).
    - Τη συνεχή προβολή των κινήσεων των πελατών, συμπεριλαμβανομένων της κερδοφορίας τους, των προτιμήσεών τους, και του ιστορικού επαφών τους.
    - Τον προσδιορισμό της πελατειακής εμπειρίας (ανάγκες/απαιτήσεις) σε συνδυασμό με την παρακολούθηση των καταναλωτικών συνηθειών του πελάτη σε πραγματικό χρόνο.
    - Την ενσωμάτωση διαδικτυακών υπηρεσιών στο τραπεζικό σύστημα για την εύκολη πρόσβαση τους από τους πελάτες του χρηματοπιστωτικού ιδρύματος

Παράγοντες που προκαλούν αλλαγές στη διαχείριση των σχέσεων του πελάτη με το τραπεζικό σύστημα οφείλονται στη (Kotarba, 2016):

1. Διαχείριση πιστότητας και επιβράβευση των πελατών.
2. Διαχείριση ποιότητας και αξιώσεων.
3. Μέτρηση ικανοποίησης και συλλογής σχολίων σχετικά με τις τραπεζικές υπηρεσίες.
4. Ασφάλεια των προσωπικών δεδομένων των πελατών, προστασία των πληροφοριακών συστημάτων από κακόβουλους χρήστες, γρήγορη ανάλυση του κινδύνου, προγραμματισμένες ειδοποιήσεις από βλάβες συστήματος.

### *2.3.3 Πληροφοριακά Συστήματα Διοίκησης (MIS)*

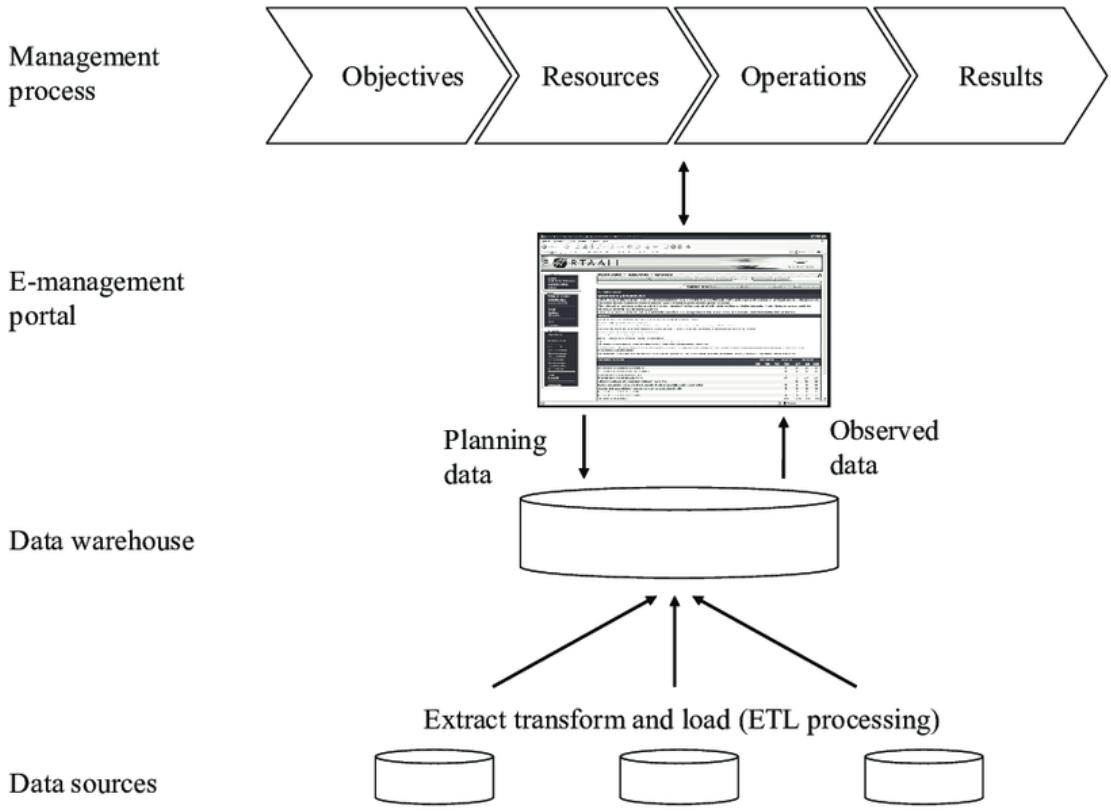
Η διαχείριση της τεχνολογίας των πληροφοριών διαδραματίζει καθοριστικό ρόλο, ιδίως σε τομείς υπηρεσιών όπως τις τραπεζικές υπηρεσίες, οι οποίες στηρίζουν το ανταγωνιστικό τους πλεονέκτημα στην αξιοπιστία και την πληροφόρηση των πελατών. Τεράστια κεφάλαια έχουν επενδυθεί σε συστήματα πληροφοριών, με τα **Πληροφοριακά Συστήματα Διοίκηση (MIS)**, να αποτελούν σημαντικό μέρος αυτής της δαπάνης.

Παρά την απουσία ενός τυπικού ορισμού των Πληροφοριακών Συστημάτων Διοίκησης, οι Davis και Olsen πρότειναν έναν ορισμό, σύμφωνα με τον οποίο τα πληροφοριακά συστήματα διοίκησης αποτελούν έναν ολοκληρωμένο μηχανισμό εκτέλεσης διεργασιών που παρέχουν τις απαραίτητες πληροφορίες για την υποστήριξη βασικών επιχειρηματικών λειτουργιών όπως διοικητικές λειτουργίες, διαχείριση προσωπικών δεδομένων και λήψη διοικητικών αποφάσεων. Αυτά τα συστήματα χρησιμοποιούν συνήθως λογισμικό και υλικό υπολογιστή, μη αυτοματοποιημένες διαδικασίες, μοντέλα χρηματοοικονομικής ανάλυσης, έλεγχο σχεδιασμού, λήψη στρατηγικών αποφάσεων και διαχείριση βάσης δεδομένων.

Η Εικόνα 4, παρουσιάζει μία αρχιτεκτονική δομή ενός τυπικού Πληροφοριακού Συστήματος Διοίκησης (MIS). Όπως παρατηρείται από το σχεδιάγραμμα, τα τραπεζικά δεδομένα εισέρχονται στη βάση δεδομένων που διαθέτει το χρηματοπιστωτικό ίδρυμα κι αποθηκεύονται εκεί μέχρι ο χρήστης του συστήματος να δημιουργήσει αίτηση επεξεργασίας συγκεκριμένων προσωπικών δεδομένων. Έπειτα τα δεδομένα αυτά συλλέγονται σ’ ένα ενιαίο αποθετήριο πληροφοριών τα οποία είναι διαθέσιμα ανά πάσα στιγμή μέσω της χρήσης της βάσης δεδομένων της τράπεζας. Τα προσωπικά δεδομένα που συλλέγονται από τους πελάτες της τράπεζας, επεξεργάζονται από του χρήστες των συστημάτων αυτών, επιτρέποντας την άμεση προσπέλασή τους μόνο από αυτούς που είναι εξουσιοδοτημένοι από το χρηματοπιστωτικό ίδρυμα. Στην προκειμένη περίπτωση τα δεδομένα των πελατών που συλλέγονται από τα Πληροφοριακά Συστήματα Διοίκησης έχουν ως στόχο τη διαμόρφωση των τραπεζικών λειτουργιών, ώστε τα τραπεζικά ιδρύματα να έχουν τη δυνατότητα να παρέχουν εξειδικευμένες υπηρεσίες στους πελάτες τους.

Η αξιολόγηση ενός πληροφοριακού συστήματος διοίκησης, έχει τεθεί στην κορυφή της ατζέντας τόσο των ακαδημαϊκών όσο και των διευθυντικών στελεχών, ιδιαίτερα την εποχή της οικονομικής κρίσης. Παρά το γεγονός ότι ο ορισμός και η μέτρηση της αποδοτικότητας αυτών των συστημάτων είναι σχετικά εύκολη, η αποτελεσματική εφαρμογή στα τραπεζικά ιδρύματα αποτελεί ένα δύσκολο έργο της διοίκησης (Trivellas & Santouridis, 2013). Τα χρηματοπιστωτικά ιδρύματα χρησιμοποιούν τέτοιου είδους πληροφοριακά συστήματα διότι αποτελούν τον συνδετικό κρίκο των συστημάτων που λειτουργούν εντός του τραπεζικού ιδρύματος. Τα δεδομένα συλλέγονται από συστήματα διαχείρισης πελατειακών σχέσεων και μαζί με τα υπόλοιπα συστήματα συλλογής προσωπικών δεδομένων, οι πληροφορίες αυτές επεξεργάζονται

από πληροφοριακά συστήματα διοίκησης, διαμορφώνοντας τη λειτουργία των τραπεζικών διεργασιών. Κατ' αυτόν τον τρόπο πραγματοποιείται ο διαμοιρασμός των προσωπικών δεδομένων εντός του τραπεζικού ιδρύματος, δημιουργώντας ένα δίκτυο διαχείρισης τραπεζικών πληροφοριών.

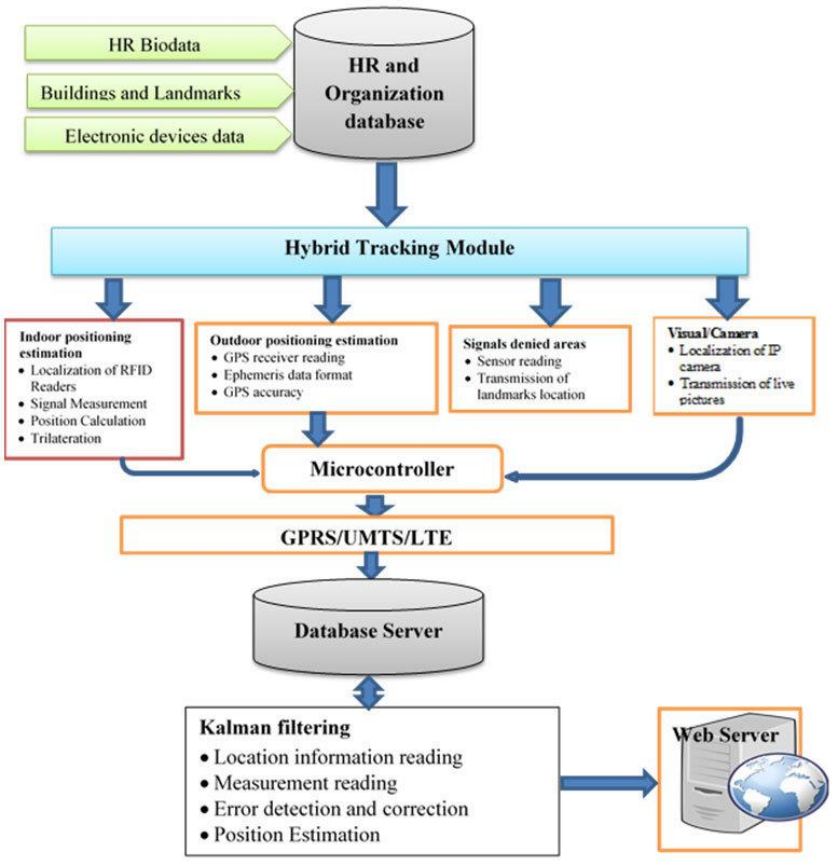



**Εικόνα 4:** Αρχιτεκτονική δομή ενός συστήματος MIS[14]

### *2.3.4 Συστήματα Διαχείρισης Ανθρώπινου Δυναμικού (HRM)*

Η στρατηγική διαχείρισης του ανθρώπινου δυναμικού μίας επιχείρησης αναφέρεται στο σχεδιασμό προγραμματισμένων εγκαταστάσεων και δραστηριοτήτων των ανθρωπίνων πόρων, που αποσκοπούν στην επιτυχία των στόχων του οργανισμού (Wright, & McMahan, 1992). Περιλαμβάνει όλες τις δραστηριότητες που υλοποιούνται από έναν οργανισμό για να επηρεάσουν τη συμπεριφορά των ατόμων σε μια προσπάθεια υλοποίησης των στρατηγικών αναγκών της επιχείρησης (Nishii & Wright, 2007).

[14] Πηγή: Kettunen, J. (2011). Management Information System in Higher Education. In *Global Business: Concepts, Methodologies, Tools and Applications* (pp. 1281-1289). IGI Global.




**Εικόνα 5:** Αρχιτεκτονική δομή ενός συστήματος HRM[15]

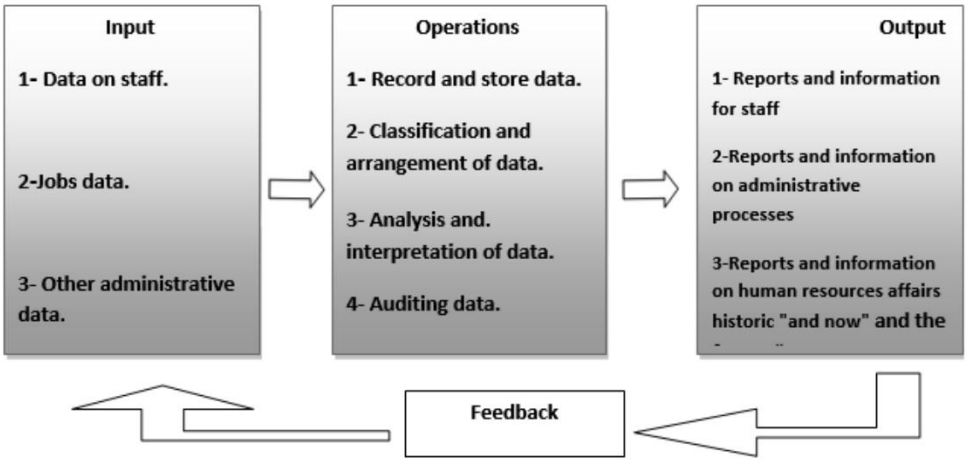
Στην Εικόνα 5, απεικονίζεται η αρχιτεκτονική δομή ενός συστήματος διαχείρισης ανθρώπινου δυναμικού. Τα δεδομένα που συλλέγονται από το ανθρώπινο δυναμικό του χρηματοπιστωτικού ιδρύματος, εισέρχονται στη βάση δεδομένων που χρησιμοποιεί η τράπεζα. Έπειτα τα δεδομένα επεξεργάζονται από το σύστημα κι εξάγονται σε μία ενιαία βάση δεδομένων όπου χρησιμοποιείται από το σύνολο των χρηματοπιστωτικών ιδρυμάτων. Κατ' αυτόν τον τρόπο τα προσωπικά δεδομένα των υπαλλήλων του τραπεζικού ιδρύματος είναι ανά πάσα στιγμή διαθέσιμα από διαδικτυακούς διακομιστές οι οποίοι έχουν σα στόχο τη διασύνδεση των τραπεζικών συστημάτων διαχείρισης ανθρώπινου δυναμικού.

Τα χρηματοπιστωτικά ιδρύματα διαχειρίζονται τα προσωπικά δεδομένα των υπαλλήλων τους μέσα από τα Συστήματα Διαχείρισης Ανθρώπινου Δυναμικού (HRM). Τα συστήματα αυτά επιτρέπουν στην τράπεζα να δημιουργεί το προφίλ των εργαζομένων της, συλλέγοντας πληροφορίες σχετικά με τα προσωπικά τους στοιχεία, τις

[15] Πηγή: Adewole, D. B., Akinyokun, O. C., & Babatunde, I. G. (2019). Hybrid human resources localization and tracking system. *Artif. Intell. Research*, *8*(1), 1.

ικανότητές τους, το μορφωτικό τους επίπεδο, τη μισθολόγια τους κ.ά. Τα δεδομένα αυτά αποτελούν καίριας σημασίας και χρήζουν προστασίας μέσα από την ασφάλεια που παρέχουν τα πληροφοριακά συστήματα του τραπεζικού ιδρύματος. Η σύνδεση με άλλα συστήματα της τράπεζας είναι απαραίτητη προϋπόθεση για την εύρυθμη λειτουργία των τραπεζικών υπηρεσιών της. Τα συστήματα διαχείρισης ανθρώπινου δυναμικού και τα συστήματα διαχείρισης πελατειακών σχέσεων έχουν άμεση σχέση καθώς οι υπάλληλοι του χρηματοπιστωτικού ιδρύματος είναι και πελάτες της τράπεζας με αποτέλεσμα τα προσωπικά τους δεδομένα να συλλέγονται αυτόματα από συστήματα διαχείρισης ανθρώπινου δυναμικού.

Η τράπεζα διαθέτει σύστημα διαχείρισης ανθρώπινου δυναμικού με στόχο την καινοτομία και την εξυπηρέτηση των πελατών της. Η δομή του συστήματος ανθρώπινου δυναμικού σ' ένα τραπεζικό ίδρυμα, αφορά τις πολιτικές διαχείρισης των ανθρωπίνων πόρων, χρησιμοποιώντας μεθόδους πρόσληψης νέου προσωπικού αλλά κι ανακατανομής του υπάρχοντος σε διαφορετικά τμήματα του ιδρύματος. Για παράδειγμα, η τράπεζα χρησιμοποιεί εταιρικούς ιστότοπους, πρακτορεία προσλήψεων, συμβούλους αναζήτησης έμπειρων στελεχών και διαφημίσεις στα κοινωνικά μέσα, τα οποία αποτελούν πηγή διοχέτευσης προσωπικών δεδομένων υποψήφιων υπαλλήλων της τράπεζας (Bartel, 2004). Όπως παρατηρείται στην Εικόνα 6, η διαδικασία που απεικονίζεται πραγματοποιείται από ένα σύστημα διαχείρισης ανθρωπίνου δυναμικού, έχοντας ως εισροή τα δεδομένων των υποψήφιων και ως εκροή σχετικές αναφορές του χρηματοπιστωτικού ιδρύματος.




**Εικόνα 6:** Ανάλυση δεδομένων για πρόσληψη προσωπικού[16]

[16] Πηγή: Majeed, Z. A., & Özyer, S. T. (2016). Implementation of the Human Resources Information Systems and Comparative Study of Various Platforms.

## 2.4 Ο ρόλος των Πληροφοριακών Συστημάτων στις τράπεζες

Τα τελευταία 20 χρόνια, οι τράπεζες προσπαθούν να αυτοματοποιήσουν τις τραπεζικές τους διαδικασίες. Αυτό είχε ως αποτέλεσμα την εφαρμογή πολλών πληροφοριακών συστημάτων ακόμα και σ' ένα χρηματοπιστωτικό ίδρυμα. Ενώ τα πληροφοριακά συστήματα μπόρεσαν να βοηθήσουν τις τράπεζες να διαχειριστούν καλύτερα τις διαδικασίες και τους πόρους τους, παρατηρήθηκε ότι δημιουργήθηκαν προβλήματα ως προς τον τρόπο διαχείρισης των προσωπικών δεδομένων των πελατών τους. Ένα σημαντικό μειονέκτημα των πληροφοριακών συστημάτων, είναι ότι είχε ως αποτέλεσμα τη δημιουργία τεράστιων όγκων δεδομένων και πληροφοριών, με αποτέλεσμα ν' αναπτυχθεί το φαινόμενο της έκρηξης πληροφοριών ή η υπερφόρτωση των συστημάτων. Με την εξέλιξη της τεχνολογίας, το σενάριο της σχεδίασης των συστημάτων αυτών έχει αλλάξει. Πλέον απαιτούνται περισσότερες προσπάθειες και πόροι για την αποτελεσματική εφαρμογή τους στο τραπεζικό σύστημα, καθώς στις σύγχρονες τραπεζικές συναλλαγές, οι πληροφορίες και οι γνώσεις αποτελούν πολύτιμα περιουσιακά στοιχεία για τα χρηματοπιστωτικά ιδρύματα (Tanaji, 2012).

Ο ρόλος των πληροφοριακών συστημάτων ποικίλει ανάλογα του τρόπου εφαρμογής τους από το τραπεζικό σύστημα. Τα συστήματα που χρησιμοποιούνται από τα τραπεζικά ιδρύματα παρουσιάζουν συγκεκριμένες ιδιαιτερότητες, καθώς τα συστήματα αυτά είναι παραμετροποιημένα αποκλειστικά για τις ανάγκες που δημιουργούνται από ένα χρηματοπιστωτικό ίδρυμα. Ποιοι είναι όμως οι παράγοντες εκείνοι που οδήγησαν τις τράπεζες να υιοθετήσουν παραμετροποιημένα πληροφοριακά συστήματα[17]; Το ερώτημα αυτό απασχόλησε πολλούς ερευνητές και διευθυντικά στελέχη των ιδρυμάτων, φτάνοντας στο συμπέρασμα ότι τα τραπεζικά συστήματα, με τη ραγδαία ανάπτυξη της τεχνολογίας, μπόρεσαν να διαχειριστούν και να επεξεργαστούν έναν τεράστιο όγκο δεδομένων.

Το κομβικό σημείο στην ανάπτυξη των πληροφοριακών συστημάτων είναι η ασφάλεια που παρέχει στον χρήστη σχετικά με την προστασία των προσωπικών του δεδομένων. Επειδή τα χρηματοπιστωτικά ιδρύματα συλλέγουν δεδομένα οικονομικής

[17] Τα παραμετροποιημένα πληροφοριακά συστήματα, είναι τα συστήματα τα οποία προγραμματίζονται έτσι ώστε να μπορούν να εφαρμοστούν πλήρως στα διάφορα τμήματα του χρηματοπιστωτικού ιδρύματος. Αυτή η σχεδίαση επιτρέπει στις τράπεζες να διαμορφώσουν τα συστήματα αυτά ανάλογα με τις τραπεζικές διεργασίες που εκτελούνται, δίνοντας τη δυνατότητα στα πληροφοριακά συστήματα να καλύψουν τις ανάγκες του ιδρύματος.

συμπεριφοράς αλλά και δεδομένα προσωπικού χαρακτήρα, πρέπει να εξασφαλίσουν την ομαλή ροή των δεδομένων αυτών στα πληροφοριακά συστήματα που διαθέτουν. Κατ' αυτόν τον τρόπο τα τραπεζικά συστήματα μπορούν, α) να διαχειριστούν έναν τεράστιο όγκο δεδομένων, β) να εξασφαλίσουν την προστασία των δεδομένων αυτών μέσα από μεθόδους και τεχνικές ασφάλειας που παρέχει η τράπεζα και δ) να εξασφαλίσουν τη μέγιστη δυνατή διαχείριση της γνώσης, που προσπαθούν μανιωδώς να επιτύχουν οι οργανισμοί του 21$^{ου}$ αιώνα.

### *2.4.1 Οφέλη από τη χρήση των Πληροφοριακών Συστημάτων*

Τα πληροφοριακά συστήματα έχουν σα στόχο τη δημιουργία ενός μηχανισμού διαχείρισης πληροφοριακών που εισέρχονται στο τραπεζικό σύστημα. Οι πληροφορίες αυτές αποτελούν πηγή γνώσης για ένα χρηματοπιστωτικό ίδρυμα, αφού παρέχουν επαρκή πληροφόρηση σχετικά με τραπεζικές κινήσεις των πελατών τους. Η διαχείριση της γνώσης αποτελεί τον κατασταλτικό παράγοντα που μετατρέπει ένα πληροφοριακό σύστημα σε πηγή εκμετάλλευσης σημαντικών δεδομένων. Έτσι τα οφέλη που παρέχει ένα πληροφοριακό σύστημα στις τράπεζες, περιγράφονται με βάση τον βαθμό εκμετάλλευσης της γνώσης ενός τραπεζικού ιδρύματος.

Σε ένα οργανωτικό περιβάλλον, τα οφέλη μπορούν να προκύψουν σε δύο επίπεδα, σε ατομικό κι οργανωτικό (Cong & Pandya, 2003). Σε ατομικό επίπεδο, η διαχείριση της γνώσης παρέχει στους υπαλλήλους ευκαιρίες, ώστε να βελτιώσουν τις δεξιότητες και την εμπειρία τους στη διαχείριση πολύπλοκων πληροφοριακών συστημάτων. Αυτές οι γνώσεις μπορούν να εκμεταλλευτούν στο έπακρο, εντός του τραπεζικού δικτύου που μπορεί να διαμορφωθεί από τη χρήση των τραπεζικών πληροφοριακών συστημάτων. Κατ' αυτόν τον τρόπο οι υπάλληλοι μπορούν να μεταφέρουν γνώσεις και σε άλλους υπαλλήλους του τραπεζικού ιδρύματος, βελτιώνοντας έτσι τόσο την προσωπική απόδοση, όσο και τη συνολική απόδοση της τράπεζας.

Σε οργανωτικό επίπεδο, η διαχείριση γνώσης παρέχει σημαντικά οφέλη για ένα χρηματοπιστωτικό ίδρυμα. Τα οφέλη αυτά είναι (Tanaji, 2012):

- Η βελτίωση της απόδοσης του ιδρύματος μέσω της αυξημένης αποδοτικότητας, παραγωγικότητας, ποιότητας και καινοτομίας.

- Η αύξηση της οικονομικής αξίας του οργανισμού, αντιμετωπίζοντας τις γνώσεις των ανθρώπων ως πλεονέκτημα.
- Η αντιμετώπιση των ριζικών αλλαγών μέσα από τη διαχείριση των δεδομένων από τα τραπεζικά πληροφοριακά συστήματα. Η γνώση από μόνη της μπορεί να επιταχύνει την καινοτομία των τραπεζικών υπηρεσιών και να ενισχύσει τα κέρδη.
- Η αποτελεσματική υποστήριξη διοικητικών αποφάσεων των χρηματοπιστωτικών ιδρυμάτων. Η ανταλλαγή γνώσεων για προηγούμενες επιτυχίες, αποτυχίες, έργα και πρωτοβουλίες, διαμορφώνει καλύτερες διοικητικές αποφάσεις δημιουργώντας μεγαλύτερη οικονομική αξία για τις τράπεζες. Τα δεδομένα οικονομικής συμπεριφοράς αποτελούν σημαντική πηγή πληροφοριών και κατ' επέκταση γνώσης για τα τραπεζικά ιδρύματα.
- Η αποτελεσματικότερη διαμόρφωση των τραπεζικών διεργασιών βάση των πληροφοριακών συστημάτων διαχείρισης προσωπικών δεδομένων. Τα τραπεζικά ιδρύματα εξελίσσουν τις υπηρεσίες τους με αποτέλεσμα οι πελάτες να δείχνουν περισσότερο εμπιστοσύνη στην επεξεργασία των δεδομένων τους.

Οι τράπεζες έχουν συνειδητοποιήσει τον κρίσιμο ρόλο της διαχείρισης της γνώσης στην απόκτηση πλεονεκτήματος σ' ένα ανταγωνιστικό περιβάλλον, αλλά υπήρξαν καθυστερήσεις στην εφαρμογή των συστημάτων αυτών, διότι τα τραπεζικά ιδρύματα δε γνώριζαν ποια θα ήταν τα πραγματικά οφέλη ή οι κίνδυνοι των πληροφοριακών συστημάτων ως προς τη διαχείριση των προσωπικών δεδομένων των πελατών τους. Σύμφωνα με έρευνα της International Data Corporation (IDC) που διενεργήθηκε σε περισσότερες από 600 τράπεζες στη Δυτική Ευρώπη, μόνο το 20% των τραπεζών εφάρμοσε από τη πρώτη στιγμή πληροφοριακά συστήματα διαχείρισης τραπεζικών δεδομένων. Αυξημένη τάση της εφαρμογής των πληροφοριακών συστημάτων, παρατηρήθηκε κυρίως στα μεγάλα χρηματοπιστωτικά ιδρύματα. Με μεγαλύτερη επίγνωση της σημασίας της διαχείρισης της γνώσης, η IDC αναμένει ότι η κατάσταση αυτή θα αλλάξει στο εγγύς μέλλον και ότι η διαχείριση των δεδομένων μέσω των τραπεζικών πληροφοριακών συστημάτων θα καταστεί προτεραιότητα για τον τραπεζικό τομέα (Tanaji, 2012).

## 2.5 Θέματα ασφαλείας των τραπεζικών πληροφορικών συστημάτων

Καθώς το σύγχρονο τραπεζικό σύστημα βασίζεται όλο και περισσότερο στο διαδίκτυο και στις τεχνολογίες διαχείρισης των πληροφοριών, για τη λειτουργία των χρηματοπιστωτικών ιδρυμάτων και των αλληλεπιδράσεων τους με την αγορά, οι απειλές και οι παραβιάσεις της ασφάλειας αυξάνονται ιδιαίτερα τα τελευταία χρόνια. Οι επιθέσεις εσωτερικού και εξωτερικού χαρακτήρα έχουν προκαλέσει τεράστιες οικονομικές απώλειες στους οργανισμούς. Επομένως, αυτή είναι η ανάγκη για ένα κατάλληλο πλαίσιο που να διέπει την ασφάλεια των πληροφοριακών συστημάτων στο τραπεζικό σύστημα (Ula, Ismail & Sidek, 2011).

Οι πρωταρχικές απειλές για το τραπεζικό σύστημα που οφείλονται στην έλλειψη πρακτικής διακυβέρνησης ασφάλειας πληροφοριών είναι (Ula, Ismail & Sidek, 2011):

- Η φυσική καταστροφή χώρων, υποδομών και δεδομένων από φυσικά αίτια. Η έλλειψη προετοιμασίας για μια κατάσταση έκτακτης ανάγκης μπορεί πράγματι να σημαίνει το οριστικό τέλος για μια τράπεζα σε περίπτωση πιθανής καταστροφής.
- Η ακούσια καταστροφή ή καταστροφή συστημάτων και δεδομένων λόγω ανθρώπινης αστοχίας που προκαλείται από πολλούς παράγοντες, όπως η καταλληλότητα των εργαλείων, η εκπαίδευση των εργαζομένων, ο φόρτος εργασίας, η εργασιακή ηθική και η εταιρική κουλτούρα.
- Η κατάχρηση της εμπιστοσύνης από υπαλλήλους ή στελέχη της τράπεζας για το χειρισμό ευαίσθητων δεδομένων, όπως μέσω της κατάχρησης πληροφοριών των πελατών ή επιχειρηματικών μυστικών ή μέσω της παράνομης απόκτησης πληροφοριών σχετικά με τους τραπεζικούς συνεργάτες.

Γενικά, στόχος μιας τράπεζας είναι να υιοθετήσει ένα προσαρμοσμένο σύνολο διαδικασιών και πρακτικών που επιτρέπουν τον έλεγχο επί των κρίσιμων πληροφοριών και των τεχνολογιών που επικυρώνουν την ύψιστη ασφάλεια των τραπεζικών πληροφοριακών συστημάτων. Το Ινστιτούτο Ανάπτυξης Λογισμικού (Software Development Institute) κατηγοριοποίησε μια ολοκληρωμένη προσέγγιση σε φυσικούς, τεχνικούς και διοικητικούς ελέγχους ασφάλειας προσωπικών δεδομένων ως εξής (Bhasin, 2007):

1. Το προληπτικό σύστημα ασφαλείας (κάρτες αναγνώρισης των υποκειμένων των δεδομένων, κρυπτογράφηση δεδομένων, λογισμικό υποκλοπής spyware, πολιτικές και τραπεζικές διαδικασίες προστασίας προσωπικών δεδομένων).
2. Το σύστημα παρακολούθησης (ηλεκτρονικές σφραγίδες, στοιχεία ελέγχου μηνυμάτων και τακτικοί ηλεκτρονικοί έλεγχοι)
3. Το αποτρεπτικό σύστημα (κάμερες κλειστού κυκλώματος, απόρριψη μετά από εσφαλμένη χρήση κωδικού πρόσβασης και εγκρίσεις πολλαπλών τμημάτων).
4. Το σύστημα διόρθωσης (απομόνωση και τακτικός έλεγχος διακομιστών, ενημερωμένα τείχη προστασίας και τμηματοποίηση της λειτουργίας των συστημάτων ανάλογα το είδος του τραπεζικού πληροφοριακού συστήματος)
5. Το σύστημα ανάκαμψης που έχει ως στόχο να υιοθετήσει ένα προσαρμοσμένο σύνολο διαδικασιών και πρακτικών που επιτρέπουν την άσκηση ελέγχου σε κρίσιμα περιουσιακά στοιχεία, στις τραπεζικές πληροφορίες και στα προσωπικά δεδομένα τόσο των πελατών όσο και των υπαλλήλων της τράπεζας.

### *2.5.1 Συλλογή προσωπικών δεδομένων*

Οι βασική λειτουργία των τραπεζικών πληροφοριακών συστημάτων είναι η συλλογή των προσωπικών δεδομένων τόσο των πελατών όσο και των υπαλλήλων του τραπεζικού ιδρύματος. Τα δεδομένα αυτά αποτελούν χρήσιμες πληροφορίες οι οποίες μπορούν να συλλεχθούν αυτοματοποιημένα ή μη από τα τραπεζικά συστήματα. Οι πληροφορίες που συλλέγονται από τα τραπεζικά συστήματα χωρίζονται σε πέντε κατηγορίες πληροφοριών, οι οποίες κρίνονται απαραίτητες για την αποτελεσματικότερη εκτέλεση των τραπεζικών υπηρεσιών. Συγκεκριμένα, οι κατηγορίες των πληροφοριών που συλλέγουν τα χρηματοπιστωτικά ιδρύματα είναι οι εξής (Bhasin, 2007):

1. **Πληροφορίες εμπιστευτικού χαρακτήρα**: Πληροφορίες που παρέχουν στους κατόχους της, το πλεονέκτημα στην αγορά και είναι κατάλληλες για τη διεξαγωγή σημαντικών τραπεζικών εργασιών που βασίζονται σε εμπιστευτικές πληροφορίες (για παράδειγμα: πρακτικά συνεδριάσεων του διοικητικού συμβουλίου, πληροφορίες για την κεφαλαιαγορά και εσωτερικά χρηματοοικονομικά δεδομένα ενός τραπεζικού ιδρύματος).

2. **Πληροφορίες του πελάτη**: Πληροφορίες που καθιστούν δυνατή τη δημιουργία της ταυτότητας του πελάτη (για παράδειγμα: όνομα, διεύθυνση, ημερομηνία γέννησης) συμπεριλαμβανομένου του προσδιορισμού των στοιχείων τραπεζικής επικοινωνίας του (αριθμός λογαριασμού, αριθμός κατάθεσης).
3. **Πληροφορίες τραπεζικού λογαριασμού του πελάτη**: Πληροφορίες πελάτη οικονομικού δικαιούχου ή συνδικαιούχου.
4. **Πληροφορίες υπολοίπου**: Πληροφορίες που αντιπροσωπεύουν τις εμπορικές αξιώσεις μεταξύ της τράπεζας και των πελατών ή των επιχειρηματικών εταίρων της (για παράδειγμα: υπόλοιπο λογαριασμού, και υπόλοιπο καταθέσεων).
5. **Πληροφορίες συναλλαγής**: Πληροφορίες που προκαλούν ή αντιπροσωπεύουν μια αλλαγή στις εμπορικές πράξεις μεταξύ τράπεζας, πελατών ή επιχειρηματικών εταίρων (για παράδειγμα: κινήσεις λογαριασμών και καταθέσεων).

Το τραπεζικό σύστημα έχει αναπτύξει κώδικες δεοντολογίας για την προσεκτική συλλογή των προσωπικών δεδομένων των πελατών τους. Τα τραπεζικά δεδομένα που συλλέγονται θα πρέπει να αποσκοπούν στην εκτέλεση των υπηρεσιών του χρηματοπιστωτικού ιδρύματος ώστε να μη πραγματοποιείται άσκοπη εκμετάλλευση των προσωπικών δεομένων των πελατών. Οι κώδικας δεοντολογίας[18] που χρησιμοποιούν οι τράπεζες θα πρέπει να πληρούν τις προϋποθέσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ), ώστε τα δεδομένα που συλλέγονται κι αποθηκεύονται στα τραπεζικά πληροφοριακά συστήματα να εφαρμόζονται αποτελεσματικά από τα χρηματοπιστωτικά ιδρύματα.

### *2.5.2 Βάσεις δεδομένων των ΠΣ*

Οι βάσεις δεδομένων αποτελούν αναπόσπαστο τμήμα των τραπεζικών πληροφοριακών συστημάτων. Σε γενικές γραμμές, μπορούμε να κατηγοριοποιήσουμε τα συστήματα συλλογής πληροφοριών σε διαδικτυακό σύστημα επεξεργασίας πληροφοριών (Online Transaction Processing - OLTP) και σε συστήματα διαδικτυακής αναλυτικής επεξεργασίας (Online Analytical Processing - OLAP). Ένα σύστημα OLTP

[18] Άρθρο 40 παρ.2 εδ.γ' Γενικός Κανονισμός Προστασίας Δεδομένων

χαρακτηρίζεται από έναν μεγάλο αριθμό σύντομων διαδικτυακών ερωτημάτων προς τη βάση δεδομένων όπως είναι η ανάγνωση, η εισαγωγή, η ενημέρωση και η διαγραφή των τραπεζικών πληροφοριών. Ο σκοπός αυτών των συστημάτων είναι η εκτέλεση βασικών τραπεζικών καθηκόντων. Τα συστήματα αυτά μπορούν να επεξεργάζονται δεδομένα οικονομικού χαρακτήρα σε περιβάλλον πολλαπλών χρηστών[19]. Τα τραπεζικά πληροφοριακά συστήματα που βασίζονται σε μία βάση δεδομένων OLTP, μπορούν να καταγράψουν και ν' αποθηκεύσουν λεπτομερή αρχεία συναλλαγών με την υποστήριξη ενός σχεσιακού μοντέλου δεδομένων[20].

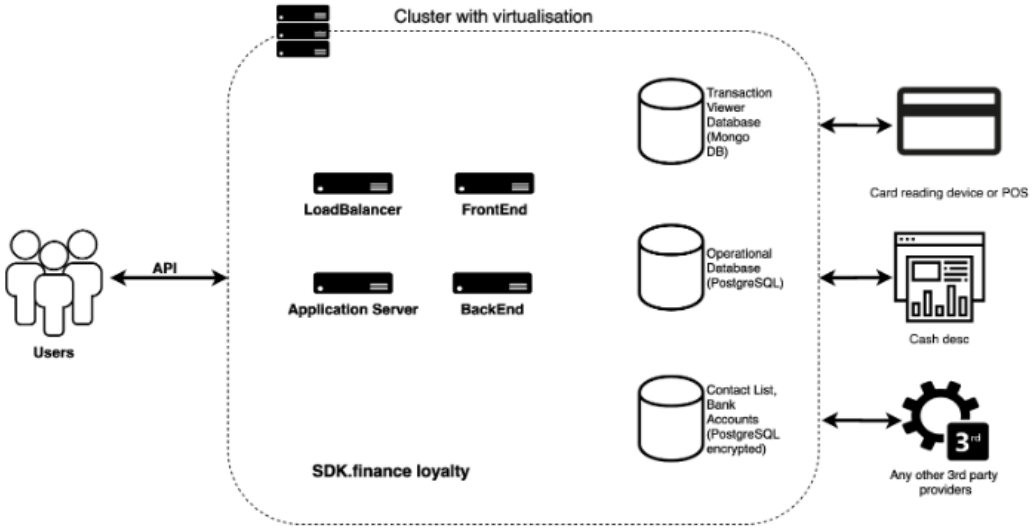
Αντιθέτως, ένα σύστημα OLAP χαρακτηρίζεται από σχετικά χαμηλό όγκο διαμοιρασμού δεδομένων. Ο σκοπός ενός συστήματος OLAP είναι να βοηθήσει τους υπεύθυνους λήψης αποφάσεων ενός τραπεζικού ιδρύματος, να σχεδιάσουν τις τραπεζικές διαδικασίες, να επιλύσουν προβλήματα, να πραγματοποιήσουν ανάλυση αποδόσεων και να έχουν την δυνατότητα για εξόρυξη δεδομένων. Μια βάση δεδομένων OLAP περιέχει συσσώρευση ιστορικών δεδομένων συναλλαγών, συγκεντρωτικά μέτρα και πολλαπλές διαστάσεις. Στα περισσότερα συστήματα OLTP και OLAP, τα υποκείμενα συστήματα βάσεων δεδομένων βασίζονται στο σχεσιακό μοντέλο δεδομένων, το οποίο υπάρχει από τις αρχές του 1970. Από το 2008 περίπου, σημειώθηκε μια έκρηξη νέων συστημάτων βάσης δεδομένων και κανένα από αυτά τα συστήματα δεν ακολούθησε τις παραδοσιακές σχεσιακές υλοποιήσεις. Αυτές οι νέες βάσεις δεδομένων, γνωστές και ως βάσεις δεδομένων NoSQL, σχεδιάστηκαν για να αποθηκεύουν και να επεξεργάζονται μια μεγάλη ποσότητα δεδομένων (Big Data). Οι βάσεις δεδομένων NoSQL θέτουν ευκαιρίες και προκλήσεις για τα τραπεζικά πληροφοριακά συστήματα του μέλλοντος (Ramakrishnan, Gehrke & Gehrke, 2003).

Στην Εικόνα 7, απεικονίζεται η αλληλεπίδραση του χρήστη με το πληροφοριακό σύστημα ενός τραπεζικού ιδρύματος. Οι χρήστες διαχειρίζονται τα δεδομένα από το σύστημα διαχείρισης των πληροφοριών, στέλνοντας ερωτήματα στη βάση δεδομένων. Η

[19] Εννοείται η διαχείριση των προσωπικών δεδομένων από πληροφοριακά συστήματα που είναι εγκατεστημένα σε διάφορα τμήματα του τραπεζικού ιδρύματος. Κατ' αυτόν τον τρόπο πραγματοποιείται η διαχείριση των δεδομένων οικονομικής συμπεριφοράς από πολλαπλούς χρήστες ταυτόχρονα.

[20] Με τον όρο **σχεσιακή βάση δεδομένων ή σχεσιακό μοντέλο δεδομένων** εννοείται μία συλλογή δεδομένων οργανωμένη σε πίνακες παρέχοντας έναν μηχανισμό για ανάγνωση, εγγραφή, τροποποίηση ή και πιο πολύπλοκες διαδικασίες επεξεργασίας δεδομένων. Ο σκοπός μιας βάσης δεδομένων είναι η οργανωμένη αποθήκευση πληροφορίας και η δυνατότητα εξαγωγής αυτής, ιδίως σε πιο οργανωμένη μορφή, σύμφωνα με ερωτήματα που τίθενται στη σχεσιακή βάση δεδομένων.

βάση δεδομένων απαντάει στο σύστημα με την εμφάνιση των εγγραφών που διαθέτει στους κατάλληλα διαμορφωμένους πίνακες. Οι εγγραφές αυτές αποτελούν τα δεδομένα που συλλέγει ένα τραπεζικό ίδρυμα. Με τις ενέργειες που έχει τη δυνατότητα να εκτελέσει μία βάση δεδομένων όπως είναι η αποθήκευση, η διαγραφή, η ενημέρωση και η τροποποίηση των στοιχείων, γίνεται λόγος για την επεξεργασία των δεδομένων οικονομικού χαρακτήρα που αφορούν τους πελάτες της τράπεζας.




**Εικόνα 7:** Η χρησιμότητα των τραπεζικών βάσεων δεδομένων[21]

## 2.6 Προστασία προσωπικών δεδομένων

Η πολιτική και τα ρυθμιστικά μέτρα που ακολουθούν τα χρηματοπιστωτικά ιδρύματα σχετικά με την προστασία των προσωπικών δεδομένων δεν μπορούν να εφαρμοστούν αποτελεσματικά χωρίς τη νομική εξουσία να ρυθμίζει και να εποπτεύει παρόχους συμπληρωματικών τραπεζικών υπηρεσιών, όπως φορείς εκμετάλλευσης δικτύων κινητής τηλεφωνίας και εταιρείες τεχνολογίας, που διαβιβάζουν ή διαχειρίζονται πληροφορίες συναλλαγών (Dias & McKee, 2010).

Ωστόσο, ο τραπεζικός κλάδος μπορεί να χρησιμοποιήσει ορισμένες βασικές μεθόδους προστασίας και συγκεκριμένα αμυντικά εργαλεία για να ελαχιστοποιήσει τους κινδύνους από ηλεκτρονικά εγκλήματα στον κυβερνοχώρο. Σε γενικές γραμμές, μια τράπεζα πρέπει να χρησιμοποιεί τους τραπεζικούς πόρους των πληροφοριακών συστημάτων που διαθέτει, αναπτύσσοντας παράλληλα μηχανισμούς προστασίας των

[21] Πηγή: SDK.finance

τραπεζικών δεδομένων Συγκεκριμένες ενέργειες που μπορούν να εφαρμοστούν για την προστασία των προσωπικών δεδομένων είναι: (Bhasin, 2007).

- Αναβάθμιση υπαρχόντων συστημάτων ελέγχου ταυτότητας ενός παράγοντα κωδικού, σε συστήματα δύο παραγόντων.
- Χρήση λογισμικού σάρωσης για να την ανίχνευση και την πρόληψη από το ηλεκτρονικό ψάρεμα (phishing[22]).
- Χρήση λογισμικού ανίχνευσης ηλεκτρονικής απάτης όπως ο εντοπισμός παραβίασης λογαριασμού.
- Ενίσχυση εκπαιδευτικών προγραμμάτων για τη σωστή χρήση των τραπεζικών πληροφοριακών συστημάτων από τους υπαλλήλους του χρηματοπιστωτικού ιδρύματος.
- Δημιουργία δικτύου ανταλλαγής πληροφοριών μεταξύ χρηματοπιστωτικών ιδρυμάτων, κυβερνητικών φορέων και παρόχων πληροφορικής.
- Δημιουργία συστημάτων κρυπτογράφησης δεδομένων σε μη αναγνώσιμη μορφή από κακόβουλους χρήστες.

## 2.7 Σύνοψη

Στις μέρες μας η διαχείριση της πληροφορίας παίζει σημαντικό ρόλο για την ανάπτυξη και την εξέλιξη ενός οργανισμούς ή μιας εταιρείας. Με την πρόοδο της τεχνολογίας και την εμφάνιση νέων μεθόδων επεξεργασίας δεδομένων, κρίθηκε επιτακτική η ανάγκη για αποτελεσματικότερη διαχείριση της πληροφορίας. Κατ' αυτόν τον τρόπο δημιουργήθηκαν τα πληροφοριακά συστήματα, τα οποία χρησιμοποιήθηκαν από πολλές επιχειρήσεις έχοντας ως στόχο την αποδοτική συλλογή κι επεξεργασία των δεδομένων του υποκειμένου.

Τα χρηματοπιστωτικά ιδρύματα εκμεταλλεύτηκαν τη γνώση των πληροφοριακών συστημάτων, εφαρμόζοντας μεθόδους και διαδικασίες προσαρμοσμένες στις ανάγκες του τραπεζικού συστήματος. Τα τραπεζικά πληροφοριακά συστήματα παρέχουν τη δυνατότητα επεξεργασίας δεδομένων προσωπικού χαρακτήρα και οικονομικής

[22] Το Ψάρεμα (Phishing) είναι ενέργεια εξαπάτησης των διαδικτυακών χρηστών, κατά την οποία ο κακόβουλος χρήστης υποδύεται μία αξιόπιστη οντότητα και σε συνδυασμό με την ελλιπή προστασία που παρέχουν τα ηλεκτρονικά μέσα, έχει ως σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων, όπως είναι ευαίσθητα ιδιωτικά στοιχεία και κωδικοί.

συμπεριφοράς των πελατών του ιδρύματος, ανάλογα με το είδος του συστήματος που χρησιμοποιεί. Σημαντικός παράγοντας για την εύρυθμη λειτουργία μίας τράπεζας είναι η προστασία των προσωπικών δεδομένων των πελατών της από μη εξουσιοδοτημένους χρήστες. Αυτό προϋποθέτει την ασφάλεια των τραπεζικών πληροφοριακών συστημάτων και συγκεκριμένα των βάσεων δεδομένων όπου αποθηκεύονται οι πληροφορίες οικονομικού χαρακτήρα που αφορούν το χρηματοπιστωτικό ίδρυμα.

Για την άμεση αντιμετώπιση των κινδύνων που αφορούν την ασφάλεια των τραπεζικών πληροφοριακών συστημάτων, σημαντικό ρόλο έχει και ο κώδικας δεοντολογίας του τραπεζικού ιδρύματος. Στόχος είναι να εφαρμόζεται αποτελεσματικά ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) σε συνδυασμό με τη χρήση εξειδικευμένων μηχανισμών ασφαλείας, διαμορφώνοντας με αυτόν τον τρόπο τις τραπεζικές διεργασίες. Οι μέθοδοι και οι διαδικασίες συλλογής κι επεξεργασίας δεδομένων από τα τραπεζικά πληροφοριακά συστήματα θα πρέπει να συμμορφώνονται στους κανονισμούς που θέτει ο ΓΚΠΔ, για την προστασία του υποκειμένου των δεδομένων.

# 3 Υπολογιστικό Νέφος και Προσωπικά Δεδομένα

## 3.1 Εισαγωγή

Η ανάγκη για αποδοτική αποθήκευση, επεξεργασία και μεταφορά πληροφορίας είναι επιτακτική σε μία σύγχρονη κοινωνία όπου ο τελικός χρήστης πρέπει να λαμβάνει γρήγορα και εύκολα την πληροφορία που χρειάζεται. Απαιτείται, ένας μηχανισμός διαφάνειας ώστε ο τελικός χρήστης να μην επικεντρώνεται στο λειτουργικό κομμάτι της υποδομής παρά μόνο στο αντικείμενο ενασχόλησής του. Για παράδειγμα, για την επεξεργασία κειμένου σε ένα τοπικό οικιακό μηχάνημα απαιτείται μία σειρά βημάτων για την εγκατάσταση και ρύθμιση αντίστοιχου προγράμματος. Πολλές φορές η διαδικασία αυτή είναι επίπονη ενώ δεν επιτρέπει τον τελικό χρήστη, με "άγνοια" στις ενέργειες αυτές, να ολοκληρώσει τον σκοπό του (δηλαδή την συγγραφή κειμένου). Ως ακόμα ένα παράδειγμα στον τομέα των επιχειρήσεων είναι η ύπαρξη ενός προγράμματος καταγραφής προϊόντων. Η επιχείρηση αφενός χρειάζεται κάποιον ειδικό ή ομάδα ειδικών για να προσαρμόσει το λογισμικό για την επιχείρηση και αφετέρου υπάρχει η ανάγκη για υπολογιστικούς πόρους και συστήματα ασφαλείας. Αυτή η διαδικασία για μία επιχείρηση μπορεί να αποβεί πολύ κοστοβόρα και επίσης να υπάρχουν ατέλειες στην υπηρεσία που επιθυμούν (καταγραφή προϊόντων). Εκτός από τα προβλήματα που παρουσιάζονται σε ατομικό επίπεδο, συλλογικά, αυτά τα προβλήματα δεν επιτρέπουν την εξέλιξη της κοινωνίας και των μελών που την απαρτίζουν.

Στη λύση τέτοιας φύσεως προβλημάτων βασίζεται το διαδίκτυο των υπηρεσιών. Αναλυτικά το διαδίκτυο των υπηρεσιών περιγράφει τη συνολική υποδομή που χρησιμοποιεί το Διαδίκτυο ως μέσο προσφοράς και διάθεσης υπηρεσιών (Βακάλη & Παπαμήτσιου, 2012). Η ιδέα της ύπαρξης διασυνδεδεμένων υπηρεσιών παροχής πληροφορίας έρχεται να λύσει σημαντικά προβλήματα στο σύγχρονο διαδίκτυο. Για παράδειγμα, οι εταιρείες ανάπτυξης λογισμικού δε θα χρειάζονται τοπικές εγκαταστάσεις για να αναπτύξουν τις υπηρεσίες τους καθώς το διαδίκτυο των υπηρεσιών θα επιτρέπει την ένταξη των υπηρεσιών τους σε αυτό καθώς και την προβολή των υπηρεσιών σε τελικούς χρήστες (Armbrust et. al., 2010). Επίσης, οι τελικοί χρήστες θα έχουν την δυνατότητα για αποθήκευση και επεξεργασία των δεδομένων τους που είναι αποθηκευμένα απομακρυσμένα και όχι σε κάποιο οικιακό μηχάνημα. Με αυτόν τον τρόπο, μειώνεται το κόστος ανά χρήστη, ενώ ταυτόχρονα τα δεδομένα των χρηστών βρίσκονται σε ασφαλείς τοποθεσίες (χωρίς τον φόβο διαρροής τους) με συστήματα

ανάκτησης δεδομένων σε περίπτωση απώλειας αυτών. Μία σημαντική υποδομή που έχει διακριθεί στο διαδίκτυο υπηρεσιών είναι το υπολογιστικό νέφος το οποίο είναι και αντικείμενο του συγκεκριμένου κεφαλαίου.

## 3.2 Η έννοια του Υπολογιστικού Νέφους

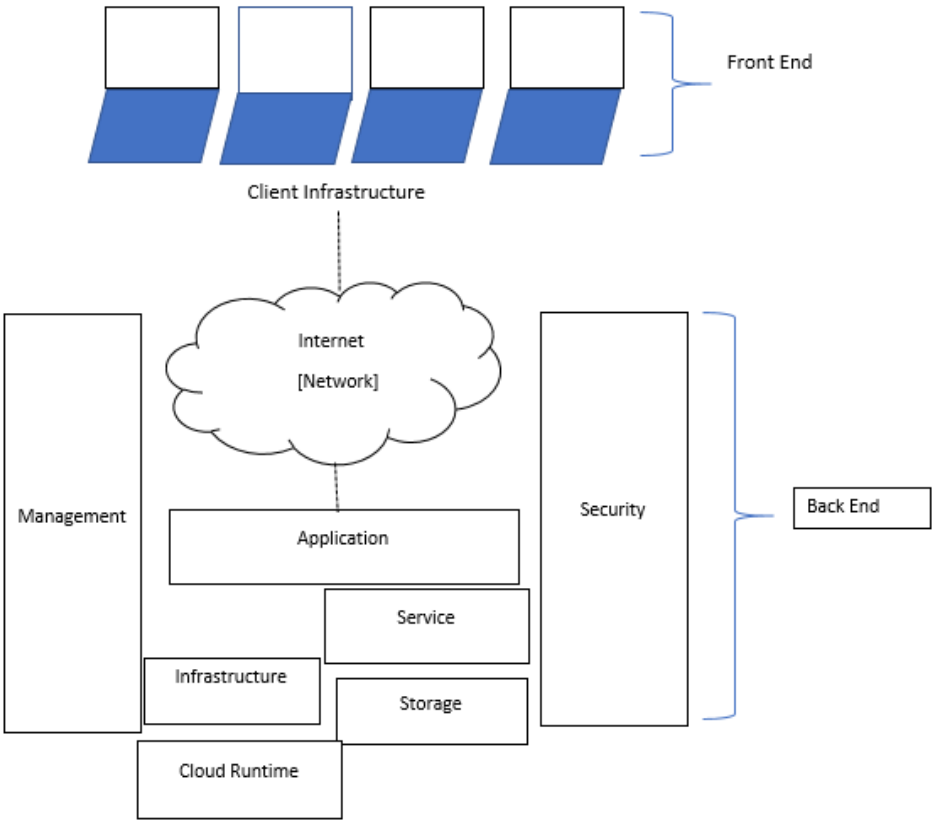
Ως υπολογιστικό νέφος ορίζεται ένα μοντέλο που επιτρέπει την κατ 'απαίτηση πρόσβαση δικτύου σε κοινόχρηστο σύνολο διαμορφώσιμων υπολογιστικών πόρων (π.χ. δίκτυα, διακομιστές, αποθηκευτικά μέσα, εφαρμογές και υπηρεσίες) που μπορούν να παρέχονται γρήγορα και να διανέμονται με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδραση παρόχου υπηρεσιών (Dillon κ.α., 2010). Το υπολογιστικό νέφος ουσιαστικά αποτελεί ένα σύνολο υπολογιστών πόρων που βρίσκονται απομακρυσμένοι από τον τελικό χρήστη και η εσωτερική λειτουργία του μοντέλου δεν είναι εμφανής στο ευρύ κοινό παρέχοντας με αυτόν τον τρόπο ασφάλεια στους χρήστες του. Οι χρήστες δεν γνωρίζουν, ούτε και χρειάζεται, αν κάποιοι διακομιστές του υπολογιστικού νέφους λειτουργούν ή όχι διότι η διαφάνεια που παρέχει το μοντέλο αυτό καθιστά αυτό το ζήτημα ανούσιο για τον χρήστη.

Κύριο μέλημα του υπολογιστικού νέφους είναι η οπτικοποίηση των υπηρεσιών και η βελτιστοποίηση πόρων επιτρέποντας έτσι τον τελικό χρήστη του μοντέλου αυτού να αποθηκεύει τεράστιους όγκους δεδομένων και ταυτόχρονα να τους επεξεργάζεται με ιδιαίτερη ευκολία. Σημαντικό είναι να αναφερθεί ότι οι χρήστες δεν χρειάζεται να δεσμεύουν από την αρχή τους πόρους που θα χρειαστούν, με αποτέλεσμα να φαντάζουν “άπειροι” και αυτή η υπηρεσία ελκύει τον τελικό χρήστη που δεν γνωρίζει την εσωτερική λειτουργία της υποδομής. Από την άλλη μεριά, οι πάροχοι του υπολογιστικού νέφους μπορούν να εξοικονομήσουν πόρους όταν αυτοί δεν χρειάζονται ή να τους αναθέσουν για άλλους σκοπούς.

### *3.2.1 Αρχιτεκτονική Υπολογιστικού Νέφους*

Η αρχιτεκτονική σχεδίαση του υπολογιστικού νέφους βασίζεται στον τρόπο με τον οποίο είναι διαμορφωμένες οι βάσεις δεδομένων των πληροφοριακών συστημάτων. Είναι σημαντικό να τονίσουμε ότι τα δεδομένα που εισέρχονται μέσα από τη χρήση των πληροφοριακών συστημάτων, αποθηκεύονται στο σύννεφο το οποίο αποτελείται από πολλούς απομακρυσμένους διακομιστές. Κατ’ αυτόν τον τρόπο μία επιχείρηση δεν

απαιτείται να έχει στις εγκαταστάσεις της δικούς της διακομιστές διότι τα δεδομένα πλέον δεν αποθηκεύονται στο τοπικό δίκτυο. Τα δεδομένα παραμένουν αποθηκευμένα στο σύννεφο και μπορούν να προσπελαστούν ανά πάσα στιγμή από ένα πληροφοριακό σύστημα μέσω της χρήσης του Διαδικτύου, όπως φαίνεται και στην παρακάτω εικόνα:




**Εικόνα 8:** Αρχιτεκτονική σχεδίαση Υπολογιστικού Νέφους[23]

Ένα πληροφοριακό σύστημα λαμβάνει δεδομένα από τον χρήση. Τα δεδομένα αυτά αποθηκεύονται, μέσω Διαδικτύου, σε απομακρυσμένους διακομιστές και παραμένουν εκεί. Όταν το πληροφοριακό σύστημα κάνει αίτημα για επεξεργασία δεδομένων τότε τα δεδομένα μεταφέρονται, μέσω του πρωτοκόλλου ασφαλείας SSL, από τους διακομιστές στο σύννεφο με αποτέλεσμα να μπορεί να πραγματοποιηθεί η διαχείρισή τους. Βασική προϋπόθεση για την ανάπτυξη ενός λογισμικού υπολογιστικού νέφους είναι η ασφάλεια που παρέχει για την προστασία των δεδομένων. Επίσης η διεπαφή του χρήστη είναι σημαντική για την εκτέλεση των υπηρεσιών του νέφους καθώς μέσα από εκεί ο χρήστης θα έχει τη δυνατότητα διαγραφής, επεξεργασίας, τροποποίησης και μεταφοράς των δεδομένων ανά πάσα στιγμή.

[23] Πηγή: https://www.educba.com/cloud-computing-architecture/

## 3.3 Μοντέλα Ανάπτυξης Υπολογιστικού Νέφους

Τα τέσσερα μοντέλα ανάπτυξης νέφους που έχουν καθοριστεί από την κοινότητα υπολογιστικού νέφους είναι (Dillon, Wu, & Chang, 2010):

1. Ιδιωτικό σύννεφο (Private Cloud) - Η υποδομή νέφους λειτουργεί αποκλειστικά σε έναν οργανισμό και τη διαχειρίζεται ο οργανισμός ή τρίτος ανεξάρτητα από το εάν βρίσκεται εντός ή εκτός εγκαταστάσεων. Το κίνητρο για τη δημιουργία ενός ιδιωτικού νέφους σε έναν οργανισμό έχει διάφορες πτυχές. Πρώτον, η μεγιστοποίηση και η βελτίωση της αξιοποίησης των υπαρχόντων εσωτερικών πόρων. Δεύτερον, οι ανησυχίες σχετικά με την ασφάλεια, συμπεριλαμβανομένου του απορρήτου των δεδομένων και της εμπιστοσύνης, καθιστούν επίσης το ιδιωτικό νέφος μια επιλογή για πολλές εταιρείες. Τρίτον, το κόστος μεταφοράς δεδομένων από την τοπική υποδομή πληροφορικής σε ένα δημόσιο σύννεφο εξακολουθεί να είναι αρκετά σημαντικό.
2. Σύννεφο κοινότητας (Community cloud) - Αρκετοί οργανισμοί από κοινού κατασκευάζουν και μοιράζονται την ίδια υποδομή υπολογιστικού νέφους. Η κοινότητα του νέφους δημιουργείται σε ένα βαθμό οικονομικής κλιμάκωσης και δημοκρατικής ισορροπίας. Η υποδομή ενός κοινοτικού σύννεφου θα μπορούσε να φιλοξενείται από έναν τρίτο προμηθευτή ή σε έναν από τους οργανισμούς της κοινότητας (π.χ. για έναν όμιλο επιχειρήσεων).
3. Δημόσιο σύννεφο (Public cloud) - Αυτή είναι η κυρίαρχη μορφή του τρέχοντος μοντέλου ανάπτυξης υπολογιστικού νέφους. Το δημόσιο σύννεφο χρησιμοποιείται από το ευρύ κοινό των καταναλωτών νέφους και ο πάροχος υπηρεσιών υπολογιστικού νέφους έχει την πλήρη ιδιοκτησία του δημόσιου σύννεφου με τη δική του πολιτική, την αξία και το μοντέλο κέρδους, κοστολόγησης και χρέωσης.
4. Υβριδικό σύννεφο (Hybrid cloud) – Αυτή η υποδομή ανάπτυξης υπολογιστικού νέφους είναι ένας συνδυασμός δύο ή περισσότερων σύννεφων (ιδιωτικών, κοινοτικών ή δημόσιων) που παραμένουν μοναδικές οντότητες, αλλά συνδέονται μεταξύ τους με τυποποιημένη ή ιδιόκτητη τεχνολογία που επιτρέπει τη φορητότητα δεδομένων και εφαρμογών. Οι οργανισμοί χρησιμοποιούν το υβριδικό μοντέλο νέφους για να βελτιστοποιήσουν τους πόρους τους και για να αυξήσουν τις βασικές τους ικανότητες,

περιθωριοποιώντας τις περιφερειακές επιχειρησιακές λειτουργίες στο σύννεφο, ενώ ελέγχουν τις βασικές δραστηριότητες τους μέσω ιδιωτικού νέφους.

### *3.3.1 Χαρακτηριστικά Υπολογιστικού Νέφους*

Η Cloud Security Alliance έχει συνοψίσει βασικά χαρακτηριστικά που απεικονίζουν τη σχέση και τις διαφορές από το παραδοσιακό τρόπο διαχείρισης δεδομένων στη διαχείρισης δεδομένων στο νέφος (Xiao, Z., & Xiao, Y., 2012).

- Αυτό-εξυπηρέτηση: Ένας πελάτης νέφους μπορεί μονομερώς να αποκτήσει υπολογιστικές δυνατότητες, όπως η χρήση διαφόρων διακομιστών και αποθήκευση δικτύου χωρίς να αλληλεπιδρά με τον πάροχο.
- Ευρεία πρόσβαση στο δίκτυο: Οι υπηρεσίες που παρέχονται μέσω Διαδικτύου με τη χρήση ενός τυπικού μηχανισμού, επιτρέπει στους πελάτες να έχουν πρόσβαση στις υπηρεσίες ετερογενών εργαλείων (π.χ. υπολογιστές, κινητά τηλέφωνα και PDA).
- Συγκέντρωση πόρων: Ο πάροχος του νέφους χρησιμοποιεί ένα μοντέλο πολλαπλών συνομιλιών για την εξυπηρέτηση πολλαπλών πελατών συγκεντρώνοντας υπολογιστικούς πόρους, οι οποίοι είναι φυσικοί και εικονικοί πόροι που εκχωρούνται δυναμικά ή εκ νέου ανάλογα με τη ζήτηση των πελατών.
- Μετρημένη υπηρεσία: Η υπηρεσία που αγοράζουν οι πελάτες μπορεί να ποσοτικοποιηθεί και να μετρηθεί. Τόσο για τον πάροχο όσο και για τους πελάτες, η χρήση πόρων θα παρακολουθείται, θα ελέγχεται, θα μετριέται και θα αναφέρεται.

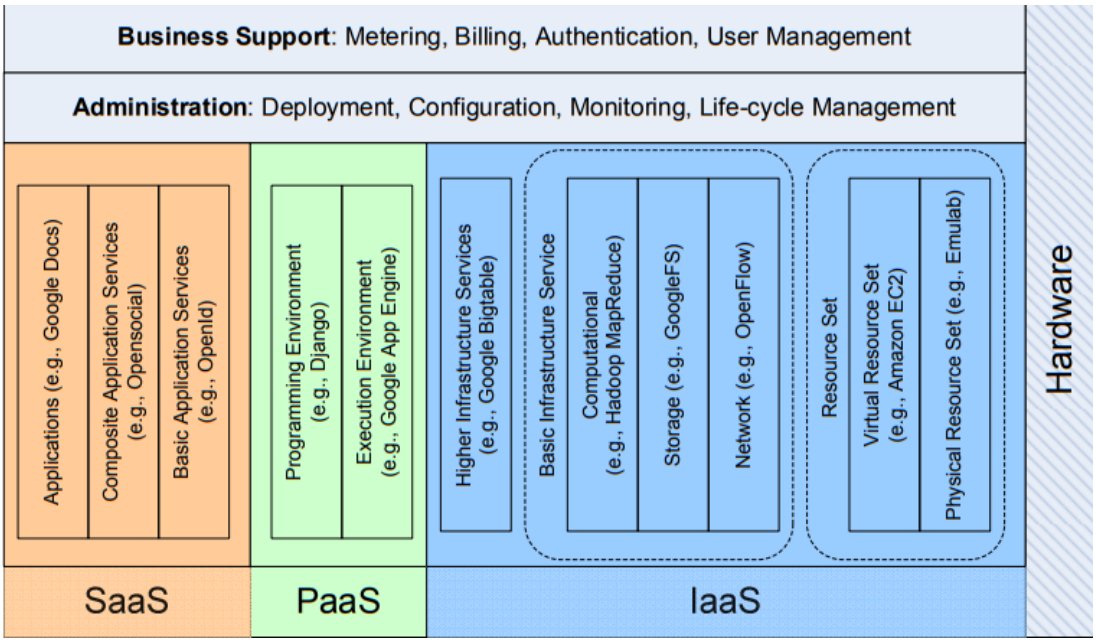
### *3.3.2 Μοντέλα Υπηρεσιών*

Για την εφαρμογή και τη χρήση των υπηρεσιών υπολογιστικού νέφους, θα πρέπει να εξεταστούν τα μοντέλα υπηρεσιών νέφους. Τα μοντέλα αυτά παίζουν σημαντικό ρόλο στην επεξεργασία των δεδομένων και αποτελούν το μέσω της εξακρίβωσης του υπεύθυνου επεξεργασίας και του εκτελών της επεξεργασία σε μία επιχείρηση. Τα μοντέλα υπηρεσιών υπολογιστικού νέφους είναι:

1. **Λογισμικό ως υπηρεσία (Software as a Service - SaaS)**: Οι καταναλωτές στο νέφος αποθηκεύουν τα δεδομένα τους σε περιβάλλον φιλοξενίας, στο οποίο έχουν πρόσβαση μέσω ενός δικτύου εφαρμογών. Οι καταναλωτές νέφους δεν έχουν τον έλεγχο της υποδομής του σύννεφου που συχνά χρησιμοποιεί αρχιτεκτονική συστήματος πολλαπλής κατανάλωσης υπολογιστικών πόρων, δηλαδή, διαφορετικές εφαρμογές καταναλωτών νέφους οργανώνονται σε ένα λογικό περιβάλλον στο νέφος SaaS για να επιτύχουν οικονομίες κλίμακας και για να βελτιώσουν τη ταχύτητα, την ασφάλεια, τη διαθεσιμότητα, την αποκατάσταση καταστροφών και τη συντήρηση των δεδομένων. Παραδείγματα εφαρμογών SaaS είναι το SalesForce.com, το Gmail και τα Έγγραφα Google (Dillon, Wu, & Chang, 2010).
2. **Πλατφόρμα ως υπηρεσία (Platform as a Service - PaaS)**: Το PaaS είναι μια πλατφόρμα ανάπτυξης που επιτρέπει στους καταναλωτές νέφους να αναπτύσσουν υπηρεσίες σύννεφου και εφαρμογές (π.χ. SaaS) απευθείας στο νέφος PaaS. Η διαφορά μεταξύ SaaS και PaaS είναι ότι η υποδομή SaaS φιλοξενεί μόνο ολοκληρωμένες εφαρμογές νέφους, ενώ το PaaS προσφέρει μια πλατφόρμα ανάπτυξης που φιλοξενεί ολοκληρωμένες και σε εξέλιξη εφαρμογές υπολογιστικού νέφους. Αυτό απαιτεί το PaaS, εκτός από την υποστήριξη περιβάλλοντος φιλοξενίας εφαρμογών, να διαθέτει υποδομή ανάπτυξης, όπως περιβάλλον προγραμματισμού και εργαλεία ανάπτυξης προγραμμάτων. Ένα παράδειγμα PaaS είναι το Google AppEngine (Dillon, Wu, & Chang, 2010).
3. **Υποδομή ως υπηρεσία (Infrastructure as a Service - IaaS)**: Οι καταναλωτές νέφους χρησιμοποιούν απευθείας υποδομές πληροφορικής (επεξεργασία, αποθήκευση και διαχείριση υπολογιστικών πόρων) που παρέχονται στο νέφος IaaS. Η εικονικοποίηση χρησιμοποιείται εκτενώς στην υποδομή IaaS για την ενσωμάτωση φυσικών πόρων καλύπτοντας την αυξανόμενη ή συρρικνωμένη ζήτηση των πόρων από τους καταναλωτές. Η βασική στρατηγική της εικονικοποίησης είναι η δημιουργία ανεξάρτητων εικονικών μηχανών που είναι απομονωμένες τόσο από το υποκείμενο υλικό όσο και από άλλες εικονικές μηχανές. Ένα παράδειγμα του IaaS είναι το EC2 του Amazon (Dillon, Wu, & Chang, 2010).

4. **Αποθήκευση δεδομένων ως υπηρεσία (Data storage as a Service - DaaS)**: Η παράδοση εικονικοποιημένου χώρου αποθήκευσης κατ 'απαίτηση γίνεται ξεχωριστή υπηρεσία νέφους για την αποθήκευση δεδομένων. Το κίνητρο είναι ότι τα εταιρικά συστήματα βάσεων δεδομένων απαιτούν ένα τεράστιο κόστος εγκατάστασης αποκλειστικού διακομιστή, άδεια λογισμικού, υπηρεσίες μετά την παράδοση και εσωτερική συντήρηση της τεχνολογίας. Η υποδομή DaaS επιτρέπει στους καταναλωτές να πληρώνουν για ότι χρησιμοποιούν στην πραγματικότητα και όχι για την άδεια ιστότοπου και για ολόκληρη τη βάση δεδομένων. Παραδείγματα DaaS είναι το Amazon S3, το Google BigTable και το Apache HBase (Dillon, Wu, & Chang, 2010).

Η εικόνα 9 απεικονίζει τη γενική αρχιτεκτονική μιας πλατφόρμας υπολογιστικού νέφους, η οποία ονομάζεται επίσης στοίβα νέφους. Με βάση τις εγκαταστάσεις υλικού, οι υπηρεσίες νέφους μπορούν να προσφέρονται σε διάφορες μορφές από το κατώτερο έως το ανώτερο επίπεδο. Στη στοίβα νέφους, κάθε επίπεδο αντιπροσωπεύει ένα μοντέλο ανάπτυξης. Η υποδομή ως ανάπτυξης (IaaS) προσφέρεται στο κατώτερο επίπεδο, όπου οι πόροι συγκεντρώνονται και διαχειρίζονται φυσικά (π.χ. Emulab και Amazon EC2),




**Εικόνα 9:** Αρχιτεκτονική του Υπολογιστικού Νέφους[24]

[24] Πηγή: Xiao, Z., & Xiao, Y. (2012). Security and privacy in cloud computing. *IEEE communications surveys & tutorials*, *15*(2), 843-859.

Το μεσαίο επίπεδο παρέχει την υποδομή πλατφόρμας ως υπηρεσία (PaaS), στο οποίο οι υπηρεσίες παρέχονται ως περιβάλλον για προγραμματισμό (π.χ. Django) ή για την εκτέλεση λογισμικού (π.χ. Google App Engine). Το λογισμικό ως υπηρεσία (SaaS) εντοπίζεται στο ανώτερο επίπεδο, στο οποίο ένας πάροχος υπολογιστικού νέφους περιορίζει περαιτέρω την ευελιξία των πελατών, προσφέροντας απλώς εφαρμογές λογισμικού ως υπηρεσία. Εκτός από την παροχή υπηρεσιών, ο πάροχος διατηρεί μια σουίτα εργαλείων και εγκαταστάσεων διαχείρισης του περιβάλλοντος υπολογιστικού νέφους για τη διαχείριση ενός μεγάλου συστήματος νέφους (Xiao, Z. & Xiao, Y., 2012).

## 3.4 Προστασία προσωπικών δεδομένων στο νέφος

Το υπολογιστικό νέφος αποτελεί πλέον τον σύγχρονο τρόπο αποθήκευσης πληροφοριών μέσω των πληροφοριακών συστημάτων που εκτελούν την επεξεργασία δεδομένων. Ωστόσο, εξακολουθούν να υπάρχουν ορισμένα προβλήματα σχετικά με την αποθήκευση και την επεξεργασία των δεδομένων που πρέπει να λυθούν για τους χρήστες των ΠΣ και τις επιχειρήσεις ανάπτυξης εφαρμογών σε περιβάλλον νέφους. Ένα από τα πιο σημαντικά εμπόδια στην υιοθέτηση των υπηρεσιών υπολογιστικού νέφους είναι η ασφάλεια των δεδομένων, η οποία συνοδεύεται από διάφορα θέματα όπως η κανονιστική συμμόρφωση, η ιδιωτικότητα, η εμπιστοσύνη και τα νομικά ζητήματα (Shah, Swaminathan, & Baker, 2008). Η ανάπτυξη των συστημάτων με υποδομή υπολογιστικού νέφους, θα πρέπει να έχει ως κύριο γνώμονα την προστασία της ιδιωτικής ζωής του υποκειμένου καθώς και την ασφάλεια των δεδομένων του (Kshetri, 2013).

Η ανάγκη για την ανάπτυξη κατάλληλων μέτρων ασφαλείας για την προστασία των δεδομένων στο νέφος, οδήγησε πολλές επιχειρήσεις στην υιοθέτηση ενός κώδικα δεοντολογίας σχετικά με την αποτελεσματική χρήση των υπηρεσιών υπολογιστικού νέφους στις επιχειρηματικές τους διαδικασίες. Το σχέδιο ενός κώδικα δεοντολογίας για την προστασία των προσωπικών δεδομένων για παρόχους υπηρεσιών νέφους, εκπονήθηκε από την Cloud Select Industry (C-SIG) και υποβλήθηκε επισήμως στην ομάδα εργασίας του άρθρου 29 (WP29) στις 27 Φεβρουαρίου 2014. Το άρθρο 29 είχε συνοψίσει μια σειρά σχολίων σε επιστολή που εστάλη στο C-SIG τον Ιούνιο του 2014, ενώ μία νέα έκδοση του κώδικα δεοντολογίας, λαμβάνοντας υπόψη ορισμένα επίσημα και ουσιαστικά σχόλια που έγιναν στην επιστολή, υποβλήθηκε στην ομάδα εργασίας του άρθρου 29 στις 21 Ιανουαρίου 2015 (EUROPEIA, 2015).

Κατά την αναθεώρησή του, ο στόχος της ομάδας του άρθρο 29 ήταν να διασφαλίσει ότι το σχέδιο του κώδικα δεοντολογίας θα επιτρέψει στα άτομα να αισθάνονται ασφάλεια ως προς την προστασία των προσωπικών τους δεδομένων και ότι οι υπηρεσίες υποδομής υπολογιστικού νέφους θα συμμορφώνονταν με την οδηγία για την προστασία δεδομένων (οδηγία 95/46 / ΕΚ) και μετέπειτα με τον Γενικό Κανονισμό Προστασίας Δεδομένων ((ΕΕ) 2016/679) (ΓΚΠΔ)[25]. Με τη θέσπιση του κώδικα δεοντολογίας σχετικά με την εφαρμογή του υπολογιστικού νέφους θα επιταχυνόταν:

1. Η προστασία των προσωπικών δεδομένων, διότι η επεξεργασία τους στο νέφους θα πληρούσε τις νομικές και ρυθμιστικές διατάξεις της Οδηγίας.
2. Η ομαλή λειτουργία των πληροφοριακών συστημάτων σχετικά με την επεξεργασία των προσωπικών δεδομένων εξαιτίας της αύξησης των μέτρων ασφαλείας που θα έπρεπε να λάβει η επιχείρηση.
3. Ο διαχωρισμός της ευθύνης μεταξύ του υπεύθυνου και του εκτελούντος την επεξεργασία.
4. Η ανάδειξη των δικαιωμάτων του υποκειμένου σχετικά με την προστασία των προσωπικών του δεδομένων.

Η γνώμη της ομάδας άρθρου 29 (γνώμη 05/2012 για την αποτελεσματική εφαρμογή του υπολογιστικού νέφους) σχετικά με τη χρήση των υπηρεσιών υπολογιστικού νέφους, υπογράμμισε ότι είναι σημαντικό να αποσαφηνιστεί ο ρόλος κάθε μέρους προκειμένου να καθοριστούν οι συγκεκριμένες υποχρεώσεις τους σε σχέση με τη νομοθεσία περί προστασίας δεδομένων και να ανατεθεί η ευθύνη για πιθανή παραβίαση αυτών των κανόνων (EUROPEIA, 2015). Όπως θα δούμε και στο κεφάλαιο 6, ο διαχωρισμός των ρόλων για την ευθύνη της επεξεργασίας των προσωπικών δεδομένων στο νέφος, γίνεται πλέον σαφής με την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ).

### *3.4.1 Προβλήματα ασφαλείας στο σύννεφο*

Τα παρακάτω είναι τα μεγαλύτερα προβλήματα που σχετίζονται με δημόσιες λύσεις υπολογιστικού νέφους:

[25]https://www.technologylawdispatch.com/2018/04/privacy-data-protection/article-29-working-party-makes-recommendations-following-submission-of-code-of-conduct-for-cloud-infrastructure-service-providers/

1. Η ασφάλεια των συμμετρικών κι ασύμμετρων κλειδιών και των διαπιστευτηρίων πρόσβασης χρήστη στο νέφος. Στα διαπιστευτήρια πρόσβασης, που παρέχονται από ορισμένους δημόσιους προμηθευτές νέφους, πρέπει να γίνεται ορθή διαχείριση και να εξασφαλίζεται η μέγιστη δυνατή προστασία. Σημαντικές επιθέσεις που προβλέπονται στη διαδικασία ελέγχου ταυτότητας, είναι (Nagaraju & Parthiban, 2015):
    a. Τα διαπιστευτήρια σύνδεσης και ελέγχου ταυτότητας χρήστη δεν αποκαλύπτονται στους διακομιστές νέφους και τράπεζας.
    b. Ένας εισβολέας μπορεί να παρακολουθεί το κανάλι επικοινωνίας διαπιστευτηρίων και μπορεί να χρησιμοποιήσει επανάληψη επίθεσης.
    c. Μερικές φορές, ένας εισβολέας μπορεί να αλλάξει την διεύθυνση IP δικτύου του εξουσιοδοτημένου χρήστη, έτσι ώστε το αίτημα που προέρχεται από το τροποποιημένο σύστημα να μη φαίνεται ότι είναι ένα αίτημα που προέρχεται από έναν κακόβουλο χρήστη.
2. Η εφαρμογή των υπηρεσιών νέφους διαφέρει από χώρα σε χώρα, διότι ορισμένοι νόμοι ενδέχεται να επηρεάζουν την πολιτική που ακολουθεί ένα κράτος σχετικά με την προστασία προσωπικών δεδομένων των πολιτών τους. Τα τραπεζικά πληροφοριακά συστήματα είναι ευάλωτα σε τέτοιου είδους καταστάσεις. Επομένως, υπάρχει ανάγκη λήψης κατάλληλων μέτρων για να διασφαλιστεί ότι οι τραπεζικές πληροφορίες παραμένουν ιδιωτικές, ανεξάρτητα από το εάν φιλοξενούνται σε οποιαδήποτε πάροχο ή όχι.

Από την άποψη των τραπεζικών οργανισμών, διάφοροι κίνδυνοι σχετίζονται με λύσεις δημόσιου νέφους. Μερικοί από τους βασικούς κινδύνους συνοψίζονται παρακάτω (Nagaraju & Parthiban, 2015):

1. Πολυπλοκότητα στην τραπεζική διακυβέρνηση, τη συμμόρφωση και τη διαχείριση του ελέγχου
2. Δυσκολίες στη διατήρηση προτύπων ασφαλείας και θεσμοθέτησης ρυθμιστικού πλαισίου περί απορρήτου και πράξεων πληροφόρησης.
3. Οι τραπεζικές υπηρεσίες θα εγκλωβισθούν στο νέφος και είναι δύσκολο να επανέλθουν στο εσωτερικό, εάν απαιτείται.
4. Δυνητικά νέφη API δεν διαθέτουν φορητότητα, επομένως οι ενδιαφερόμενοι δεν μπορούν να μετακινηθούν από τον ένα πάροχο υπηρεσιών νέφους στον άλλο.

## 3.5 Σύνοψη

Το απόρρητο των δεδομένων είναι μια ακόμη κρίσιμη ανησυχία όσον αφορά την εφαρμογή του υπολογιστικού νέφους από τις επιχειρήσεις, λόγω του γεγονότος ότι τα δεδομένα των πελατών και η επιχειρηματική λογική βρίσκονται μεταξύ των δύσπιστων διακομιστών νέφους, οι οποίοι ανήκουν και συντηρούνται από τον πάροχο. Επομένως, υπάρχουν πιθανοί κίνδυνοι ότι τα εμπιστευτικά δεδομένα (π.χ. οικονομικά δεδομένα) ή προσωπικά στοιχεία (π.χ., προσωπικό προφίλ) αποκαλύπτονται σε δημόσιους ή επιχειρηματικούς ανταγωνιστές. Το απόρρητο των δεδομένων υπήρξε ζήτημα ύψιστης προτεραιότητας (Liu, Xiao, Li, Liang & Chen, 2012).

Μερικά χαρακτηριστικά ασφαλείας επηρεάζουν άμεσα ή έμμεσα τη διατήρηση της ιδιωτικής ζωής, συμπεριλαμβανομένης της εμπιστευτικότητας, της ακεραιότητας, της λογοδοσίας κ.λπ. Προφανώς, προκειμένου να διατηρηθεί η αποκάλυψη ιδιωτικών δεδομένων, η εμπιστευτικότητα καθίσταται απαραίτητη σε συνδυασμό με την ακεραιότητα η οποία διασφαλίζει ότι τα δεδομένα δεν είναι κατεστραμμένα και κατά κάποιον τρόπο διατηρείτε το απόρρητο. (Xiao, Z., & Xiao, Y., 2012).

# 4 Τραπεζικά Πληροφοριακά Συστήματα με υποδομή Υπολογιστικού Νέφους

## 4.1 Εισαγωγή

Στις μέρες μας, σχεδόν κάθε επιχειρηματικός τομέας επενδύει στις υπηρεσίες που παρέχει το υπολογιστικό νέφος. Επιπλέον, λαμβάνοντας υπόψη τα οφέλη που υπόσχεται το νέφος και τον τρόπο με τον οποίο εξελίσσεται η τεχνολογία, τα χρηματοπιστωτικά ιδρύματα πλέον είναι σε θέση να εφαρμόσουν τις υπηρεσίες του υπολογιστικού νέφους στις τραπεζικές διεργασίες. Οι τράπεζες και οι εταιρείες χρηματοοικονομικών υπηρεσιών μπορούν να επωφεληθούν από το γεγονός ότι το υπολογιστικό νέφος βοηθά στη δημιουργία ενός πιο ευέλικτου επιχειρηματικού μοντέλου για την κάλυψη των αυξανόμενων επιχειρηματικών αναγκών σε ένα δυναμικό και ανταγωνιστικό περιβάλλον (Awadallah, 2016).

Αυτή η ενότητα εξετάζει πώς τα χρηματοπιστωτικά ιδρύματα έχουν προσεγγίσει τα πλεονεκτήματα των υπηρεσιών υπολογιστικού νέφους. Καλύπτει τόσο την οργανική χρήση του νέφους στον τραπεζικό τομέα, όσο και τις επίσημες στρατηγικές νέφους, συμπεριλαμβανομένων των διαδικασιών διαχείρισης του. Στη συνέχεια, η ενότητα εξετάζει ποιους τύπους υπηρεσιών νέφους χρησιμοποιούν τα τραπεζικά ιδρύματα όσον αφορά τα μοντέλα υπηρεσιών και ανάπτυξης.

## 4.2 Η εξέλιξη των Τραπεζικών υπηρεσιών με την εισαγωγή υποδομής Υπολογιστικού Νέφους

Η τεχνολογία υπολογιστικού νέφος επιτρέπει στις τράπεζες να επεξεργάζονται τα δεδομένα τους πιο αποτελεσματικά με μια αποδοτικότερη διαχείριση και κατανομή των υπολογιστικών πόρων (Apostu, Rednic & Puican, 2012). Το υπολογιστικό νέφος βοηθά τις τράπεζες να αλλάξουν τις επιχειρηματικές τους διαδικασίες και να βελτιώσουν την ικανότητά τους να αναπτύσσονται σε νέους τομείς διαχείρισης δεδομένων χωρίς το χρόνο και το κόστος που απαιτείται από τις φυσικές εγκαταστάσεις των διακομιστών. Επιπλέον η εφαρμογή του νέφους βοηθάει στη δημιουργία νέων αγορών και υπηρεσιών για τη διαφοροποίηση από τον ανταγωνισμό και τη δημιουργία νέων τρόπων πρόσβασης και χρήσης των προϊόντων και των υπηρεσιών της τράπεζας.

Με τη χρήση του υπολογιστικού νέφους, οι τράπεζες θα έχουν καλύτερη ικανότητα να παρέχουν σταθερή εξυπηρέτηση πελατών σε όλα τα καταστήματα, σε διάφορες γεωγραφικές περιοχές και επίσης να ενσωματώνουν μια πληθώρα πληροφοριών και αναλυτικών στοιχείων για τους πελάτες. Με την εισαγωγή του υπολογιστικού νέφους στις τραπεζικές διεργασίες, οι πελάτες του χρηματοπιστωτικού ιδρύματος έχουν τη δυνατότητα μέσα από τις υπηρεσίες του νέφους:

- Να εκτελέσουν με αποτελεσματικό και γρήγορο τρόπο τις χρηματικές τους συναλλαγές.
- Να μεταφέρουν τα δεδομένα τους σε άλλο τραπεζικό ίδρυμα, χωρίς να απαιτείται η φυσική παρουσία του πελάτη στις εγκαταστάσεις του.
- Να δημιουργήσουν μία κοινοτική ομάδα με επιχειρήσεις και προμηθευτές για την άμεση αλληλεπίδραση μεταξύ τους, παρέχοντας γρήγορη πρόσβαση σε προσωπικά και οικονομικά δεδομένα.
- Να εκτελούν συναλλαγές οποτεδήποτε και από οποιοδήποτε μέρος με το πάτημα ενός κουμπιού.

Το νέφος παρέχει πολλές υπηρεσίες που είναι απολύτως κατάλληλες όταν πρόκειται για τραπεζικές συναλλαγές. Με αυτόν τον τρόπο θα βοηθήσει το τραπεζικό επιχειρηματικό μοντέλο στη διαμόρφωση αποτελεσματικότερων υπηρεσιών για τους πελάτες τους (Rani & Gangal, 2012).

## 4.3 Χρήση του Υπολογιστικού Νέφους στα Τραπεζικά Πληροφοριακά Συστήματα

Οι τράπεζες της Ευρωπαϊκής Ένωσης (ΕΕ) φαίνεται να αρχίζουν να χρησιμοποιούν τις υπηρεσίες υπολογιστικού με δύο βασικούς τρόπους (Hon & Millard, 2018):

- Μέσω του **νέφους σκιάς (shadow cloud)** όπου άτομα ή ομάδες αρχίζουν να χρησιμοποιούν υπηρεσίες νέφους χωρίς τη συμμετοχή προσωπικού πληροφορικής ή την αντιμετώπιση πιθανών νομικών επιπτώσεων και συμμόρφωσης. Με το νέφος σκιάς (shadow cloud), οι εργαζόμενοι εγγράφονται απευθείας σε υπηρεσίες νέφους χωρίς τη γνώση των υπηρεσιών της τεχνολογίας της πληροφορικής ή των τμημάτων του τραπεζικού ιδρύματος, με αποτέλεσμα να προμηθεύονται υπηρεσίες υπολογιστικού

νέφους χωρίς να συμβουλευτούν το νομικό τμήμα σχετικά με την προστασία των δεδομένων της Τράπεζας (Hon & Millard, 2018). Ενώ το κίνητρο είναι συνήθως η βελτίωση της διεκπεραίωσης των τραπεζικών υπηρεσιών, το αποτέλεσμα ήταν ότι πολλές υπηρεσίες νέφους χρησιμοποιούνταν χωρίς τη γνώση των τραπεζικών λειτουργιών, ιδιαίτερα των δωρεάν υπηρεσιών, όπως την αποθήκευση δεδομένων στο Dropbox ή στο Google Drive.

- Μέσω του **νέφους μανιταριών (mushrooming cloud)** με την αποσπασματική οργανική ανάπτυξη, ακολουθούμενη συχνά από μια επίσημη στρατηγική υπολογιστικού νέφους. Μόλις οι υπεύθυνοι επεξεργασίας δεδομένων του τραπεζικού ιδρύματος ανακαλύψουν την έκταση και τη φύση της χρήσης του νέφους σκιάς ή εντοπίσουν κίνδυνο στην ασφάλεια των δεδομένων τότε χρησιμοποιούν εφεδρικά συστήματα νέφους για την αποτροπή της απώλειας των δεδομένων. Το νέφος μανιταριών έχει σα στόχο την υιοθέτηση του υπολογιστικού νέφους σε μία μικρή κλίμακα δεδομένων του τραπεζικού ιδρύματος. Κατ' αυτόν τον τρόπο επιτυγχάνεται αποτελεσματικότερα η εφαρμογή του νέφους στις τραπεζικές υπηρεσίες. Η πιλοτική χρήση του νέφους κλιμακώνεται γρήγορα με αποτέλεσμα να εφαρμόζεται μία μικρή περίπτωση χρήσης[26] του υπολογιστικού νέφους από το τραπεζικό ίδρυμα. Επομένως είναι σημαντικό για τις τράπεζες να εφαρμόζουν συστήματα ειδοποιήσεων ή μέτρα ασφαλείας για την αποφυγή της υπέρβασης της χρήσης ορισμένων σημείων του νέφους (Hon & Millard, 2018).

Η διαμόρφωση, η εφαρμογή, η δημοσιοποίηση, η επιβολή και η ενημέρωση μιας εσωτερικής πολιτικής υπολογιστικού νέφους, όπως η απαγόρευση της χρήσης του νέφους σκιάς[27], είναι σύνηθες φαινόμενο στην πολιτική που ακολουθούν τα χρηματοπιστωτικά ιδρύματα. Κατ' αυτόν τον τρόπο, οι τράπεζες πολλές φορές απαγορεύουν τη χρήση δημόσιου σύννεφου για σημαντικές λειτουργίες (όπως για παράδειγμα την επεξεργασία προσωπικών δεδομένων των πελατών τους), δίνοντας

[26] Το τραπεζικό ίδρυμα δοκιμάζει μία μικρή κλίμακα εφαρμογής υπολογιστικού νέφους χωρίς τη διαχείριση ευαίσθητων δεδομένων.

[27] Όπου οι υπάλληλοι εγγράφονται απευθείας σε υπηρεσίες νέφους χωρίς τη γνώση των τμημάτων πληροφορικής ή της νομικής συμμόρφωσης.

περισσότερη έμφαση στην εφαρμογή υποδομής του ιδιωτικού νέφους (Hon & Millard, 2018).

### *4.3.1 Πλεονεκτήματα χρήσης υπηρεσιών Υπολογιστικού Νέφους στην Τράπεζα*

Τα πλεονεκτήματα χρήσης των υπηρεσιών υπολογιστικού νέφους για ένα τραπεζικό σύστημα είναι τα εξής: (Awadallah, 2016)

1. Μείωση του κόστους διαχείρισης δεδομένων: Με το υπολογιστικό νέφος οι τράπεζες δε θα χρειαστούν να επενδύσουν, σε μεγάλο βαθμό, σε ειδικό υλικό, λογισμικό και ανθρώπινο δυναμικό. Είναι πολύ πιο εύκολο για αυτές να ενημερώσουν την υποδομή των πληροφοριακών τους συστημάτων και το αρθρωτό μοντέλο επί πληρωμής (pay on demand) του νέφους, όπου η τράπεζα χρειάζεται να πληρώσει μόνο για το υλικό και το λογισμικό που χρειάζονται.
2. Βελτίωση της ευελιξίας και της επεκτασιμότητας: Το νέφος δίνει στις τράπεζες τη δυνατότητα να ανταποκρίνονται γρήγορα στις μεταβαλλόμενες ανάγκες της αγοράς, των πελατών και των νέων τεχνολογιών. Μπορούν να κλιμακώσουν και να μειώσουν την τεχνολογία σύμφωνα με τις απαιτήσεις του τραπεζικού ιδρύματος.
3. Αύξηση της αποδοτικότητας: Η τυποποίηση που υπάρχει στο υπολογιστικό νέφος θα μπορούσε να διευκολύνει την ενσωμάτωση νέων τεχνολογιών κι εφαρμογών στο μέλλον. Επειδή η λειτουργία της τεχνολογίας και των τραπεζικών ιδρυμάτων μπορούν να συνδυαστούν σε υψηλό επίπεδο, το σύννεφο δίνει στις τράπεζες μια ευκαιρία να απομακρύνουν την πολυπλοκότητα στη διαχείριση των δεδομένων των πελατών τους.
4. Ταχύτερη εξυπηρέτηση πελατών: Το υπολογιστικό νέφος καθιστά ευκολότερη την ανάπτυξη και την κυκλοφορία νέων και ομαδοποιημένων προϊόντων και υπηρεσιών στην αγορά. Επιπλέον, εξαλείφει τις καθυστερήσεις προμηθειών για υλικό και λογισμικό. Οι τράπεζες θα είναι σε θέση να ενισχύσουν την υπολογιστική τους ισχύ για να καλύψουν την αιχμή της ζήτησης και να παρέχουν τις τελευταίες λύσεις χρηματοπιστωτικών συναλλαγών χωρίς να χρειάζεται να ανησυχούν για το αν η τεχνολογία είναι ενημερωμένη. Οι εταιρείες πλέον έχουν τη δυνατότητα πρόσβασης σε

τραπεζικά συστήματα χρησιμοποιώντας προγράμματα περιήγησης ιστού από οπουδήποτε και οποτεδήποτε.

5. Δημιουργία ισχυρότερων σχέσεων με πελάτες: Ο συνδυασμός πολλών δεδομένων και απεριόριστης υπολογιστικής ισχύος θα επιτρέψει στις τράπεζες να αναπτύξουν συστήματα ικανά να παρέχουν καλύτερη εικόνα για τους πελάτες τους και να λαμβάνουν καλύτερες αποφάσεις για λογαριασμό τους. Οι τραπεζικές υπηρεσίες με τη χρήση του νέφους θα μπορούσαν να γίνουν πιο προσαρμοσμένες στις απαιτήσεις των πελατών.
6. Ευκολία διεκπεραίωσης τραπεζικών συναλλαγών: Οι τραπεζικές συναλλαγές διευκολύνουν τις πληρωμές μεταξύ αγοραστών και πωλητών. Προς το παρόν, οι δραστηριότητες που απαιτούνται για τη διεκπεραίωση πληρωμών είναι εγγενώς αναποτελεσματικές, επειδή χρησιμοποιούν διαφορετική τεχνολογία. Ωστόσο, οι αγοραστές και οι πωλητές θα μπορούσαν να συγκεντρωθούν σε κοινόχρηστες εφαρμογές στο νέφος.

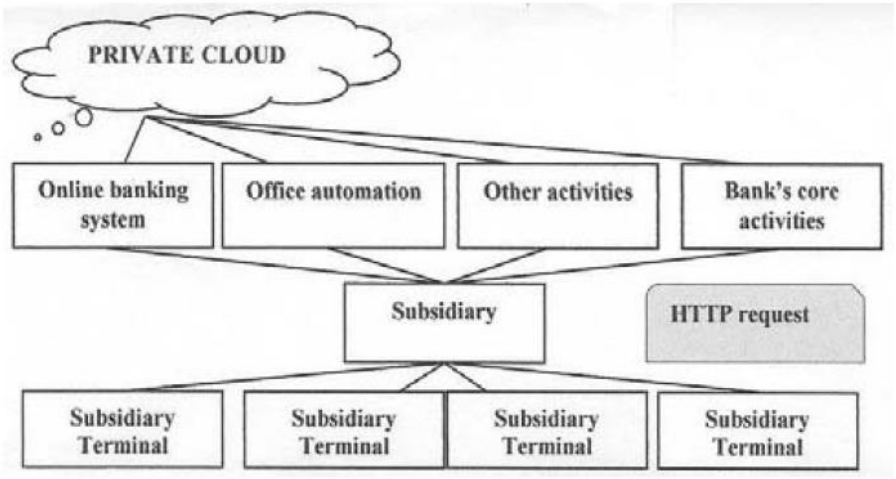
## 4.4 Η αρχιτεκτονική των Τραπεζικών ΠΣ με υποδομή Υπολογιστικού Νέφους

Το λογισμικό υπολογιστικού νέφους θα πρέπει να είναι σχεδιασμένο για επαναχρησιμοποίηση, διαλειτουργικότητα και συντήρηση. Η λειτουργικότητα του λογισμικού θα πρέπει να αξιοποιεί κατανεμημένους, εικονικοποιημένους παράλληλους και αξιόπιστους υπολογιστικούς μηχανισμούς και να παρέχει τη δυνατότητα διαμόρφωσης, και προσαρμογής των διεργασιών στους επιχειρηματικούς κανόνες, τη διεπαφή χρήστη και τα επίπεδα ασφαλείας.

Λαμβάνοντας υπόψη τη φύση και την ποικιλομορφία των δραστηριοτήτων που ασκούν τα τραπεζικά ιδρύματα, τα συστήματα πληροφοριών που παρέχουν υποστήριξη έχουν υψηλό βαθμό πολυπλοκότητας καθιστώντας δύσκολη την οριοθέτηση της αρχιτεκτονικής τους. Μια αποδεικτική προσέγγιση της βιβλιογραφίας, οριοθετεί γενικά τα χαρακτηριστικά μοντέλα των τραπεζικών ιδρυμάτων βάσει κριτηρίων σχετικά με τον εντοπισμό εφαρμογών, το επίπεδο και τον τύπο συνδεσιμότητας με το περιβάλλον λειτουργίας (Georgescu & Jeflea, 2015).

Μια οριοθέτηση που βασίζεται στον εντοπισμό του συστήματος εφαρμογών λαμβάνει υπόψη την ανάγκη μαζικής συγκέντρωσης δεδομένων στο σύννεφο, ειδικά για

τα τραπεζικά και τα κρατικά ιδρύματα, αποθηκεύοντας πληροφορίες στη βάση δεδομένων, μεταξύ των οποίων πραγματοποιείται συγχρονισμός. Επομένως, το αρχιτεκτονικό μοντέλο που βασίζεται στη συγκέντρωση πληροφοριών σε ένα κέντρο δεδομένων, επιτρέπει εύκολες προσαρμογές, αναβαθμίσεις και αλλαγές στο λογισμικό που εφαρμόζονται γρήγορα, με σημαντικά χαμηλό κόστος. Ταυτόχρονα, στην περίπτωση του κεντρικού μοντέλου, η πρόσβαση στη βάση δεδομένων, σε επίπεδο τερματικών, θυγατρικών και τοπικών κέντρων δεδομένων, καθίσταται δύσκολη λόγω του μεγάλου όγκου δεδομένων που διαβιβάζονται (Georgescu & Jeflea, 2015). Η κατάσταση είναι διαφορετική στην περίπτωση του μοντέλου αποκέντρωσης που προσφέρει το πλεονέκτημα της διευκόλυνσης της μετάδοσης δεδομένων. Επομένως, πλαισιώνεται ένα συγκεκριμένο αρχιτεκτονικό μοντέλο, βασισμένο στη συγκέντρωση δεδομένων, όπως απεικονίζεται στο παρακάτω σχήμα:




**Εικόνα 10:** Αρχιτεκτονική υποδομή υπολογιστικού νέφους στις τράπεζες[28]

Μέσα σε αυτό το μοντέλο, τα συστήματα εφαρμογών για διακομιστές μπροστινού-μέρους (front-end) θεωρούνται το κεντρικό σύστημα τραπεζικών δραστηριοτήτων και τα δεδομένα σχετικά με τη βασική λειτουργία έχουν πρόσβαση σύμφωνα με την ακόλουθη σειρά: τερματικό - κέντρο δεδομένων - διακομιστή (ιδιωτικό υπολογιστικό νέφος). Κατά γενικό κανόνα, χρησιμοποιείται μια δομή πελάτη σε διακομιστή (Client to Server) και η επικοινωνία με απομακρυσμένους διακομιστές

[28] Πηγή: Mingfei, Y. (2008), "Next Generation Information System for the Banking and Finance Sector. A guide to ADN Planning", F5 Networks, Beijing, p. 10.

πραγματοποιείται μέσω πρωτοκόλλου TCP και SSL για την ασφάλεια των συναλλαγών (Georgescu & Jeflea, 2015).

## 4.5 Η σύνδεση των Τραπεζικών ΠΣ με το Υπολογιστικό Νέφος

Ορισμένες τράπεζες έχουν ήδη αναθέσει εξ ολοκλήρου τη διαμόρφωση του υπολογιστικού νέφους σε εξωτερικούς συνεργάτες, ή μόνο λειτουργίες προγραμματισμού υπολογιστικού νέφους, σε σημαντικούς πάροχους λογισμικού όπως το Accenture, η HP ή η IBM. Όπως αναφέρεται παρακάτω, οι τράπεζες της Ευρωπαϊκής Ένωσης χρησιμοποιούν όλους τους τύπους υπηρεσιών νέφους, από το SaaS έως το IaaS, και με μοντέλα ανάπτυξης που κυμαίνονται από ιδιωτικά εσωτερικά σύννεφα έως δημόσια και υβριδικά, για ένα ευρύ φάσμα υπηρεσιών.

Τα συστήματα των χρηματοπιστωτικών ιδρυμάτων περιλαμβάνουν εφαρμογές για την επεξεργασία και την καταχώρηση των συναλλαγών που σχετίζονται με πληρωμές, λογαριασμούς ταμιευτηρίου, δάνεια και χρεόγραφα (π.χ. λογαριασμός τρεχουσών συναλλαγών και καταθέσεων, διατήρηση λογαριασμών δανείων, κατοχή τίτλων και εκκαθάριση πληρωμών) ή back-end εφαρμογές επεξεργασίας δεδομένων για την διαχείριση όλων των συναλλαγών που πραγματοποιούνται σε μια ημέρα και την ανάρτηση ενημερωμένων δεδομένων σχετικά με τα υπόλοιπα λογαριασμών[29].

Οι τραπεζικές εφαρμογές τείνουν να βασίζονται σε προσαρμοσμένες πλατφόρμες τεχνολογίας, που συνήθως κατασκευάζονται εσωτερικά από μια τράπεζα με την πάροδο των ετών, συμπεριλαμβανομένου του λογισμικού ενός πληροφοριακού συστήματος που μπορεί να είναι προγενέστερο του Διαδικτύου. Ωστόσο, όλο και περισσότερο, διατίθενται πλατφόρμες για τραπεζικές εφαρμογές, τις οποίες ένας τραπεζικός πελάτης μπορεί να χορηγήσει άδεια. Το λογισμικό μπορεί να αναπτυχθεί μέσω εγκατάστασης σ' ένα κέντρο δεδομένων που διαχειρίζεται τρίτο μέρος, όπως τα μοντέλα ανάπτυξης υπολογιστικού νέφους SaaS ή PaaS επιστρωμένο σε IaaS εξωτερικού παρόχου νέφους (Hon & Millard, 2018). Συνοψίζοντας, μια τράπεζα μπορεί να εκχωρήσει άδεια για μια κεντρική τραπεζική πλατφόρμα διαχείρισης πληροφοριών και να την εγκαταστήσει στο δικό της ιδιωτικό σύννεφο.

[29] Συνήθως περιλαμβάνουν επεξεργασία λογαριασμού, επεξεργασία δανείων και πιστώσεων, διεπαφές με το γενικό καθολικό σύστημα και εργαλεία αναφοράς.

### *4.5.1 Διαπραγματεύσεις παρόχου υπολογιστικού νέφους με την τράπεζα*

Ένας πάροχος κρίνει ότι οι διαπραγματεύσεις με τα χρηματοπιστωτικά ιδρύματα πρέπει να επικεντρώνονται στο κόστος της δημιουργίας του λογισμικού υπολογιστικού νέφους κι όχι στον τρόπο ανάπτυξης του, ώστε να ικανοποιεί όλα κριτήρια ασφαλείας για την προστασία των δεδομένων. Η σχετική ισχύς στην αγορά και το μέγεθος του παρόχου και της τράπεζας είναι προφανώς σημαντικοί παράγοντες στη διαμόρφωση του τελικού έργου. Για παράδειγμα αν μια τράπεζα θελήσει ένα πολύπλοκο σύστημα υπολογιστικού νέφους, η Amazon μπορεί να μην είναι σε θέση να το παραδώσει, θεωρώντας ότι η ανάπτυξη του τραπεζικού λογισμικού θα ήταν προτιμότερο να γίνει με το μοντέλο ανάπτυξης νέφους SaaS παρά με το IaaS ή το PaaS (Hon & Millard, 2018).

Οι ειδικές συμβάσεις ανάπτυξης έργου υπολογιστικού νέφους των χρηματοπιστωτικών ιδρυμάτων ήταν διαπραγματεύσιμες με ορισμένους παρόχους τηλεπικοινωνιών της Ευρωπαϊκής Ένωσης. Τα χρηματοπιστωτικά ιδρύματα για την εφαρμογή νέων μεθόδων επεξεργασίας δεδομένων, πραγματοποιούν αναλύσεις κινδύνου με το νομικό τους τμήμα και όχι με τους παρόχους υπολογιστικού νέφους. Ένα παράδειγμα διαπραγμάτευσης της τράπεζας με έναν μεγάλο πάροχο νέφους ήταν η απροθυμία του παρόχου να διαπραγματευτεί τη γλώσσα που η τράπεζα θεώρησε απαραίτητη για να συμμορφωθεί με τις κανονιστικές απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (Hon & Millard, 2018).

Ορισμένοι μεγάλοι πάροχοι χρησιμοποιούν εξωτερικούς σύμβουλους για τη διαχείριση τραπεζικών έργων, αλλά σε τέτοιες περιπτώσεις οι διαπραγματεύσεις με την τράπεζα γίνονται πιο δύσκολες διότι ο εξωτερικός σύμβουλος ενδέχεται να μην ενστερνίζεται τα οφέλη ενός έργου υπολογιστικού νέφους στον τραπεζικό τομέα[30] (Hon & Millard, 2018). Κατά συνέπεια, οι πάροχοι που χρησιμοποιούν εξωτερικούς δικηγόρους θα πρέπει να διασφαλίζουν ότι τους δίνουν σαφείς οδηγίες σχετικά με το τι επιτρέπεται και τι όχι, ώστε οι συμβάσεις ενός έργου να συμφέρει τόσο το χρηματοπιστωτικό ίδρυμα όσο και τον πάροχο υπολογιστικού νέφους.

[30] Αυτό συμβαίνει διότι ο πολύπλοκος μηχανισμός της επεξεργασίας δεδομένων στα τραπεζικά ιδρύματα, αποτρέπει την εκμάθηση των εξωτερικών συμβούλων σχετικά με τη διαδικασία λειτουργίας των τραπεζικών διεργασιών, με αποτέλεσμα να μην κατανοούν τη σημασία της εφαρμογής των υπηρεσιών υπολογιστικού νέφους στον τραπεζικό τομέα.

## 4.6 Σύνοψη

Τα τραπεζικά πληροφοριακά συστήματα που αντλούν δεδομένα από το σύννεφο, είναι δομημένα σε διαφορετικό αρχιτεκτονικό σχήμα καθώς οι διακομιστές βάσεων δεδομένων της τράπεζας δεν είναι εγκατεστημένοι στο τοπικό δίκτυο, αλλά σε απομακρυσμένη τοποθεσία. Η ενοποίηση μοντέλων διαχείρισης κινδύνων υπολογιστικού νέφους θεωρείται ένα νέο φαινόμενο σε τραπεζικούς οργανισμούς, όπου απαιτεί από τους διαχειριστές και τους προγραμματιστές υπολογιστικού νέφους να συμμετέχουν στη δημιουργία ενός έργου από τη φάση του προσδιορισμού του κινδύνου έως τη φάση της αντιμετώπισης του.

Η ανάγκη τήρησης της εμπιστευτικότητας και της ασφάλειας, έχουν εμποδίσει τις επιχειρήσεις να αποδεχτούν πλήρως τις πλατφόρμες νέφους. Για την προστασία των σύννεφων, οι πάροχοι πρέπει πρώτα να ασφαλίσουν πόρους εικονικού κέντρου δεδομένων, να διασφαλίσουν το απόρρητο των χρηστών και να διατηρήσουν την αυθεντικότητα και την εμπιστευτικότητα των δεδομένων. Οι οργανισμοί χρηματοοικονομικών υπηρεσιών αρχίζουν να χρησιμοποιούν τεχνολογίες υπολογιστικού νέφους σε διάφορους τομείς, ιδίως για εφαρμογές για κινητές συσκευές, δοκιμές καινοτομίας και τραπεζικές συναλλαγές. Οι τράπεζες πρέπει να γνωρίζουν ότι πρόκειται για μεταμόρφωση επιχειρηματικού μοντέλου και για να επιτύχουν επιχειρηματική ευελιξία για το επόμενο επίπεδο ανάπτυξης, το κλειδί είναι να διασφαλιστεί ότι κάθε τράπεζα αρχίζει να εργάζεται σε μια αρχιτεκτονική αναφοράς νέφους, η οποία θα καθορίσει τη στρατηγική νίκη (Awadallah, 2016).

# 5 Προστασία προσωπικών δεδομένων κι ασφάλεια στα Τραπεζικά Πληροφοριακά Συστήματα με υποδομή Υπολογιστικού Νέφους

## 5.1 Εισαγωγή

Η ασφάλεια, το απόρρητο και η εμπιστοσύνη διαδραματίζουν πρωταρχικό και κεντρικό ρόλο τόσο στις υπηρεσίες υπολογιστικού νέφους όσο και στις τραπεζικές υπηρεσίες. Σε κάποιο βαθμό, η ασφάλεια στο νέφος είναι παρόμοια με τα στοιχεία ελέγχου ασφαλείας σε διαδικτυακά τραπεζικά συστήματα. Και στις δύο περιπτώσεις θα πρέπει να ενσωματωθούν τεχνολογικά μέσα, όπως τείχη προστασίας (firewalls), συστήματα εντοπισμού/πρόληψης εισβολών, anti-virus, έλεγχο ταυτότητας, εγκεκριμένη εξουσιοδότηση χρήστη, κρυπτογράφηση, κ.λπ., για τον έλεγχο ταυτότητας τραπεζικών πληροφοριών σε διαφορετικές ρυθμίσεις (Bose, Luo, & Liu, 2013).

Σε μεγάλο βαθμό, το υπολογιστικό νέφος είναι παρόμοιο με τα τραπεζικά συστήματα. Υπήρχε μια εποχή που χρήματα και άλλα πολύτιμα περιουσιακά στοιχεία διατηρήθηκαν σε μυστικά μέρη, επειδή οι άνθρωποι δεν εμπιστεύονταν τις τράπεζες για την κατάθεση του πλούτου τους. Η αμφίδρομη διαδικασία ανταλλαγής πληροφορικών μεταξύ των ανθρώπων και της τράπεζας, χρειάστηκε σχεδόν μισό αιώνα για να χτίσει την εμπιστοσύνη των χρηστών στην τράπεζα. Σήμερα οι τράπεζες θεωρούνται συχνά ως τα πιο ασφαλή ιδρύματα στον κόσμο, επειδή οι άνθρωποι εμπιστεύονται στις τράπεζες τα χρήματά τους. Υποστηρίζεται ότι το υπολογιστικό νέφος θα εξελιχθεί επίσης με παρόμοιο τρόπο με την έννοια της δημιουργίας της εμπιστοσύνης των χρηστών με το τραπεζικό ίδρυμα (Bose, Luo, & Liu, 2013).

Πριν από την έλευση του υπολογιστικού νέφους, οι πελάτες έπρεπε να αποθηκεύσουν τα πολύτιμα δεδομένα τους στα τερματικά τους συστήματα και συχνά δεν μπορούσαν να έχουν πρόσβαση στα δεδομένα τους κατά παραγγελία. Σήμερα, οι πάροχοι νέφους αποθηκεύουν δεδομένα με μεγαλύτερη ασφάλεια από ό, τι οι πελάτες μεμονωμένα, όπως οι τράπεζες αποθηκεύουν χρήματα με μεγαλύτερη ασφάλεια από ό, τι οι ίδιοι οι πελάτες. Επιπλέον, τόσο το σύννεφο όσο και η τράπεζα παρέχουν πρόσβαση σε δεδομένα και υπηρεσίες στους πελάτες τους όλο το 24ωρο με αποτέλεσμα η προσπέλαση σε αυτά να μπορεί να πραγματοποιηθεί ανά πάσα στιγμή (Bose, Luo, & Liu, 2013). Οι άνθρωποι σήμερα δίνουν έμφαση στη χρήση του πλαστικού χρήματος για

την ελαχιστοποίηση της χρηματικής τους απώλειας. Καθώς οι τράπεζες δραστηριοποιούνται αποτελεσματικά στη διαφύλαξη των δεδομένων των πελατών τους, παρά τις απάτες, τις κλοπές και τις κακές πρακτικές, το υπολογιστικό νέφος θα πρέπει να εξελίσσεται και να αναπτύσσει νέες μεθόδους ασφαλείας κι εμπιστευτικότητας για την άμεση αντιμετώπιση απειλών που ενδέχεται να προκύψουν. Με επαρκή εμπιστοσύνη που χτίζεται με τους παρόχους υπηρεσιών, οι πελάτες μπορούν να αποθηκεύουν τα δεδομένα τους στο σύννεφο, με την ίδια αυτοπεποίθηση όπως διατηρούν χρήματα και άλλα πολύτιμα περιουσιακά στοιχεία στα χρηματοπιστωτικά ιδρύματα.

## 5.2 Το αμφιλεγόμενο ζήτημα ασφάλειας του Υπολογιστικού Νέφους

Τα τραπεζικά συστήματα ασφαλείας αποτελούνται από διάφορα επίπεδα ασφαλείας, όπως φυσική ασφάλεια (π.χ. θησαυροφυλάκιο και θυρίδες ασφαλείας), ασφάλεια συναλλαγών (π.χ. ATM, κάμερες παρακολούθησης, συστήματα ήχου) και ηλεκτρονική ασφάλεια (π.χ. σύστημα συναγερμού, CCTV / DVR συστήματα, υπηρεσίες παρακολούθησης). Αυτά τα συστήματα σε συνδυασμό με άλλες υπερσύγχρονες τεχνολογίες έχουν τεθεί σε εφαρμογή για την πρόληψη πιθανής απάτης και την προστασία των περιουσιακών στοιχείων των πελατών.

Οι υπηρεσίες νέφους από την άλλη πλευρά παρέχονται σε ένα ανοιχτό εικονικό περιβάλλον, το οποίο αποτελεί εύκολο στόχο για παράνομη πρόσβαση μη εξουσιοδοτημένων χρηστών. Οι κακόβουλοι χρήστες μπορούν να εκμεταλλευτούν κενά ασφαλείας του λογισμικού για να κλέψουν πολύτιμα δεδομένα των επιχειρήσεων ή των οργανισμών (Bose, Luo & Liu 2013). Για τις επιχειρήσεις, τα δεδομένα των πελατών είναι το πιο πολύτιμο περιουσιακό στοιχείο και η ποιότητα της ασφάλειας που παρέχεται για την προστασία τους, σχετίζεται άμεσα με τη λειτουργία και τη φήμη τους στο κοινό.

Επομένως, είναι ζωτικής σημασίας τα τραπεζικά ιδρύματα να λαμβάνουν προληπτικά μέτρα στα θέματα ασφαλείας, ώστε να μπορούν να προγραμματιστούν και να σχεδιαστούν πρόσθετα μέτρα προστασίας δεδομένων στο πλαίσιο δημιουργίας νέων συστημάτων και λογισμικών υπολογιστικού νέφους, για την αποτροπή μη εγκεκριμένων μεθόδων επεξεργασίας δεδομένων. Τα χρηματοπιστωτικά ιδρύματα πρέπει ν' αναγνωρίσουν τις πιθανές απειλές και να καθιερώσουν διαδικασίες ασφάλειας για την προστασία των τραπεζικών υπηρεσιών και των πληροφοριακών συστημάτων από επιθέσεις. Αυτή η κριτική σκέψη ασφαλείας που βασίζεται στη χρήση τεχνολογίας και

στρατηγικής θα βοηθήσει τις υπηρεσίες υπολογιστικού νέφους να είναι πιο αξιόπιστες, ανάλογα με τους μετασχηματισμούς που πέρασαν τα τελευταία χρόνια στο τραπεζικό σύστημα (Bose, Luo & Liu 2013)

### *5.2.1 Κίνδυνοι για προσωπικά δεδομένα σε περιβάλλον υπολογιστικού νέφους*

Κάποιους από τους κινδύνους των τραπεζικών ιδρυμάτων σχετικά με την εξασφάλιση της προστασίας των προσωπικών δεδομένων των πελατών τους στο υπολογιστικό νέφος είναι (Rani & Gangal, 2012):

- **Προνομιακή πρόσβαση χρήστη**: Υπάρχουν ευαίσθητα δεδομένα που υποβάλλονται σε επεξεργασία εκτός του οργανισμού, γεγονός που ενέχει τον κίνδυνο μη διατήρησης των δεδομένων, επειδή οι υπηρεσίες εξωτερικής ανάθεσης παρακάμπτουν τα φυσικά και λογικά στοιχεία ελέγχου των πληροφοριακών συστημάτων.
- **Συμμόρφωση με τους κανονισμούς**: Τα τραπεζικά ιδρύματα είναι υπεύθυνα για την ασφάλεια των δεδομένων των πελατών τους. Οι παραδοσιακοί πάροχοι υπηρεσιών υπόκεινται σε εξωτερικούς ελέγχους και πιστοποιήσεις ασφαλείας.
- **Τοποθεσία δεδομένων**: Όταν οι χρήστες χρησιμοποιούν το νέφος, δεν έχουν καμία γνώση σχετικά με τα φιλοξενούμενα δεδομένα. Η κατανεμημένη αποθήκευση δεδομένων είναι ο κύριος λόγος για τον οποίο οι πάροχοι υπολογιστικού νέφους μπορούν να προκαλέσουν έλλειψη ελέγχου και αυτό είναι επικίνδυνο για τους πελάτες.
- **Διαχωρισμός δεδομένων**: Καθώς το σύννεφο βρίσκεται συνήθως σε κοινόχρηστο περιβάλλον στο οποίο μπορεί να γίνει κοινή χρήση δεδομένων, υπάρχει ο κίνδυνος της απώλειάς τους από μη εξουσιοδοτημένους χρήστες. Η κρυπτογράφηση είναι διαθέσιμη σε όλα τα στάδια σχεδίασης και ελέγχου των τραπεζικών πληροφοριακών συστημάτων;
- **Ανάκτηση**: Είναι πολύ σημαντικό για ένα χρηματοπιστωτικό ίδρυμα ν' ανακτήσει τα δεδομένα των πελατών του, όταν εντοπισθεί κάποιο πρόβλημα ή κενά ασφαλείας των πληροφοριακών συστημάτων. Έτσι, το κύριο ερώτημα που προκύπτει εδώ είναι αν μπορεί ο πάροχος υπολογιστικού νέφους να επαναφέρει πλήρως τα δεδομένα ή όχι.

- **Ερευνητική υποστήριξη**: Οι υπηρεσίες νέφους είναι ιδιαίτερα δύσκολο να διερευνηθούν, διότι η καταγραφή των δεδομένων πολλών πελατών, ενδέχεται να εξαπλωθούν σε ένα συνεχώς μεταβαλλόμενο σύνολο κεντρικών υπολογιστών και βάσεων δεδομένων με αποτέλεσμα τα προσωπικά δεδομένα των πελατών της τράπεζας να είναι πιο επιρρεπείς από τους εισβολείς κακόβουλων χρηστών.
- **Μακροπρόθεσμη βιωσιμότητα**: Στην ιδανική περίπτωση, ο πάροχος υπολογιστικού νέφους έχει σαν κύριο στόχο την εξασφάλιση της προστασίας των πελατών τους, με αποτέλεσμα να θεωρούνται εμπιστευτικοί φορείς επεξεργασίας δεδομένων. Υπάρχει όμως ο φόβος ότι οι πάροχοι υπολογιστικού νέφους μπορούν οποτεδήποτε να πάψουν τη συνεργασία τους με την τράπεζα. Στην προκειμένη περίπτωση τα τραπεζικά ιδρύματα θα πρέπει να είναι σίγουρα ότι τα δεδομένα των πελατών τους θα παραμείνουν διαθέσιμα ακόμη και μετά από ένα τέτοιο συμβάν.

Άλλοι κίνδυνοι των τραπεζικών δεδομένων στο υπολογιστό νέφος πέρα των βασικών είναι οι εξής (Rani & Gangal, 2012):

- **Διαρροή δεδομένων**: Επειδή τα δεδομένα δεν αποθηκεύονται στους τοπικούς ηλεκτρονικούς υπολογιστές του χρηματοπιστωτικού ιδρύματος κι επειδή το υπολογιστικό νέφους χρησιμοποιείται σε περιβάλλον πολλαπλών παραγόντων, ενδέχεται να δημιουργηθεί πρόβλημα διαρροής δεδομένων στο σύννεφο (cloud).
- **Ασφάλεια βάσης δεδομένων και διακομιστή**: Δεδομένου ότι η ασφάλεια της βάσης δεδομένων και του διακομιστή αποτελεί προτεραιότητα για το τραπεζικό ίδρυμα διότι χρησιμοποιούνται κατά τη χρήση του υπολογιστικού νέφους, οι τράπεζες έχουν τη δυνατότητα να εκμεταλλευτούν ένα εύρος υπηρεσιών νέφους (εισαγωγή, διαγραφή, τροποποίηση, επεξεργασία και διαχείριση δεδομένων). Κατ' αυτόν τον τρόπο οι τράπεζες που αποθηκεύουν τα δεδομένα των πελατών τους από απόσταση δεν χρειάζεται να ανησυχούν για τις υλοποιήσεις υλικού ή εξοπλισμού που παρέχει ο πάροχος υπολογιστικού νέφους. Το σημαντικό μέλημα είναι ότι πρέπει να υπάρχει εμπιστευτικότητα, εξουσιοδότηση και αυθεντικότητα ως προς τον πάροχο του νέφους.
- **Έλεγχος ταυτότητας χρήστη**: Για όλες τις επιχειρήσεις, η διαχείριση του λογαριασμού χρήστη και το αντίστοιχο εξουσιοδοτημένο δικαίωμα πρόσβασης είναι πολύ σημαντικό και πρέπει να ορίζεται με αυστηρά κριτήρια. Πολλές επιχειρήσεις συνήθως αντιμετωπίζουν το πρόβλημα του λογαριασμού χρήστη,

όπως η υιοθέτηση της ενιαίας σύνδεσης ή τη δημιουργία πολλαπλών χρηστών για την πρόσβασή τους στα τραπεζικά πληροφοριακά συστήματα. Έτσι, η πολλαπλή πιστοποίηση για κάθε υπάλληλο αποτελεί αναγκαίο μέτρο για τη δημιουργία ενός συστήματος τραπέζης.

## 5.3 Οι κυριότερες απειλές για την ασφάλεια των προσωπικών δεδομένων στο σύννεφο

Οι κυριότερες απειλές για την ασφάλεια των προσωπικών δεδομένων στο σύννεφο είναι (Mahalle, Yong, Tao & Shen, 2018):

1. **Backdoor**: Εάν κάποιος μπορεί να παρακάμψει την εξουσιοδοτημένη πρόσβαση στο σύστημα λόγω κακής διαμόρφωσης του ΠΣ, ο χρήστης του ΠΣ μπορεί να έχει πρόσβαση τόσο σε προσωπικές όσο και σε οικονομικές πληροφορίες. Αυτές οι προσωπικές πληροφορίες μπορούν να χρησιμοποιηθούν για το άνοιγμα λογαριασμών και την πραγματοποίηση οικονομικών συναλλαγών. Η φύση της συναλλαγής μπορεί να φαίνεται γνήσια και είναι δύσκολο να εντοπιστεί. Επίσης, όταν η συναλλαγή εντοπιστεί ως μη εξουσιοδοτημένη, οι ένοχοι ενδέχεται να διαφύγουν από τον έλεγχο του τραπεζικού ιδρύματος, με αποτέλεσμα νομικές και οικονομικές κυρώσεις.
2. **Επιθέσεις άμεσης πρόσβασης**: Ένας μη εξουσιοδοτημένος χρήστης που αποκτά φυσική πρόσβαση σε έναν υπολογιστή είναι πιθανότατα σε θέση να αντιγράψει απευθείας δεδομένα από αυτόν. Μπορεί επίσης να θέσει σε κίνδυνο την ασφάλεια του τραπεζικού πληροφοριακού συστήματος κάνοντας τροποποιήσεις του λειτουργικού συστήματος, εγκαθιστώντας σκουλήκια λογισμικού, καταγραφικά κλειδιών, κρυφές συσκευές ακρόασης ή χρησιμοποιώντας ασύρματα ποντίκια. Η μη εξουσιοδοτημένη πρόσβαση μπορεί να οδηγήσει σε δημιουργία κενών ασφαλείας στα πληροφοριακά συστήματα, τα οποία με τη σειρά τους θα οδηγήσουν σε συνεχείς διαρροές και απώλεια εμπιστευτικών δεδομένων.
3. **Υποκλοπές**: Η υποκλοπή είναι η πράξη της κρυφής ακρόασης μιας ιδιωτικής συνομιλίας, συνήθως μεταξύ των κεντρικών υπολογιστών σε ένα δίκτυο (ή δύο συμβαλλόμενων μερών). Εάν η επικοινωνία μεταξύ του κεντρικού

υπολογιστή και του δικτύου περιλαμβάνει αποκάλυψη προσωπικών στοιχείων, αριθμών λογαριασμού, στοιχείων πιστωτικής κάρτας κ.λπ. και εντοπισθεί πρόσβαση από μη εξουσιοδοτημένο χρήστη, οι πληροφορίες μπορούν να χρησιμοποιηθούν στο μέλλον για την πραγματοποίηση της οικονομικής συναλλαγής ή την κλοπή ταυτότητας του ατόμου. Αυτό θα οδηγήσει σε απώλεια πληροφοριών πελατών και οικονομικών κυρώσεων σε τράπεζες και χρηματοοικονομικές υπηρεσίες.

4. **TCP / IP spoofing**: Σε αυτόν τον τύπο απειλής, αποστέλλεται ένα μήνυμα ηλεκτρονικού ταχυδρομείου στο χρήστη (πελάτης τράπεζας) που εμφανίζεται από την αυθεντική πηγή που είναι το τραπεζικό ίδρυμα. Αυτή η τεχνική είναι ισχυρή καθώς παρακάμπτει το τείχος προστασίας και η διεύθυνση IP φαίνεται να είναι εξωτερική. Αυτή η μέθοδος παρέχει πρόσβαση στο χρηματοπιστωτικό σύστημα (διακομιστή) σε εξωτερικούς μη εξουσιοδοτημένους χρήστες, που μπορεί να καταστρέψουν το σύστημα ή να κλέψουν πληροφορίες.
5. **Privilege κλιμάκωση**: Η Privilege κλιμάκωση περιγράφει μια κατάσταση όπου ένας εισβολέας με κάποιο επίπεδο περιορισμένης πρόσβασης είναι σε θέση, χωρίς εξουσιοδότηση, να αυξήσει τα προνόμιά του ή το επίπεδο πρόσβασης του στα τραπεζικά πληροφοριακά συστήματα. Για παράδειγμα, ένας τυπικός χρήστης υπολογιστή μπορεί να είναι σε θέση να «ξεγελάσει» το σύστημα ώστε να έχει πρόσβαση σε περιορισμένα δεδομένα ή να έχει απεριόριστη πρόσβαση σε ένα σύστημα.
6. **Phishing**: Μέσω του ηλεκτρονικού ψαρέματος (phishing), μπορεί να ζητηθεί από έναν πελάτη της τράπεζας να εισαγάγει διαπιστευτήρια του λογαριασμού που μπορούν να αποθηκευτούν στο σύστημα και να χρησιμοποιηθούν στο μέλλον για την πραγματοποίηση οικονομικών συναλλαγών. Λόγω του ηλεκτρονικού ψαρέματος, ο πελάτης της τράπεζας μπορεί να χάσει προσωπικά και οικονομικά στοιχεία που θα μοιάζουν αυθεντικά τόσο για τον πελάτη όσο και για την τράπεζα με αποτέλεσμα να μην μπορούν να εντοπιστούν τα κενά ασφαλείας του συστήματος.

### *5.3.1 Ανησυχίες και προβληματισμοί*

Το υπολογιστικό νέφος αποτελεί ένα επιτυχημένο και δημοφιλές επιχειρηματικό μοντέλο λόγω των μοναδικών του χαρακτηριστικών. Εκτός από τα πλεονεκτήματα που έχει το τραπεζικό ίδρυμα στη διάθεσή του, οι απειλές μη εγκεκριμένης χρήσης των υπηρεσιών του νέφους, έχουν ως αποτέλεσμα την πρόκληση σοβαρών ζητημάτων ασφαλείας, ειδικά για τις υπηρεσίες νέφους προς τα χρηματοπιστωτικά ιδρύματα. Η ανησυχία των χρηστών, που συνίσταται στην ασφάλεια του σύννεφου, έχει ως αποτέλεσμα την αποτροπή της μεταφοράς των δεδομένων της επιχείρησής στο σύννεφο. Τα ζητήματα ασφαλείας αποτέλεσαν το κυρίαρχο εμπόδιο στην ανάπτυξη και την ευρεία χρήση του υπολογιστικού νέφους. Υπάρχουν τρεις κύριες προκλήσεις για τη δημιουργία ενός ασφαλούς και αξιόπιστου συστήματος νέφους (Xiao, Z., & Xiao, Y., 2012):

- Εξωτερική ανάθεση - Η εξωτερική ανάθεση μειώνει τόσο τις κεφαλαιουχικές όσο και τις λειτουργικές δαπάνες για τους πελάτες υπολογιστικού νέφους. Ωστόσο, η εξωτερική ανάθεση σημαίνει ότι τα χρηματοπιστωτικά ιδρύματα χάνουν φυσικά τον έλεγχο των δεδομένων και των εργασιών τους. Η απώλεια του ελέγχου έχει γίνει μία από τις βασικές αιτίες της ανασφάλειας των τραπεζικών ιδρυμάτων στο σύννεφο. Για την αντιμετώπιση ζητημάτων ασφάλειας εξωτερικής ανάθεσης, ο πάροχος του νέφους πρέπει να είναι αξιόπιστος, παρέχοντας εμπιστοσύνη και ασφαλή διαχείριση των τραπεζικών δεδομένων. Επίσης, τα εξωτερικά δεδομένα πρέπει να είναι επαληθεύσιμα στους πελάτες όσον αφορά την εμπιστευτικότητα, την ακεραιότητα και άλλες υπηρεσίες ασφαλείας. Επιπλέον, η εξωτερική ανάθεση ενδέχεται να προκαλέσει παραβιάσεις απορρήτου, λόγω του γεγονότος ότι τα ευαίσθητα δεδομένα είναι εκτός ελέγχου.
- Multi-tenancy - Multi-tenancy σημαίνει ότι η πλατφόρμα υπολογιστικού νέφους είναι κοινόχρηστη και χρησιμοποιείται από πολλούς πελάτες. Επιπλέον, σε ένα εικονικοποιημένο περιβάλλον, δεδομένα που ανήκουν σε διαφορετικούς πελάτες μπορούν να τοποθετηθούν στον ίδιο φυσικό υπολογιστή με συγκεκριμένη πολιτική κατανομής πόρων. Ανταγωνιστικές εταιρείες ή οργανισμοί που ενδέχεται να είναι νόμιμοι πελάτες στο σύννεφο μπορούν να εκμεταλλευτούν το ζήτημα της συν-ιδιοκτησίας. Κατ' αυτόν τον τρόπο, προέκυψαν μια σειρά ζητημάτων ασφαλείας όπως παραβίαση δεδομένων, παραβίαση υπολογιστικών συστημάτων, επιθέσεις πλημμύρας

κ.λπ. (Ristenpart, Tromer, Shacham & Savage, 2009). Παρόλο που το Multi-tenancy είναι μια σταθερή επιλογή των προμηθευτών νέφους λόγω της οικονομικής του αποτελεσματικότητας, παρέχει κενά ασφαλείας στην πλατφόρμα του νέφους.

- Μαζικά δεδομένα- Το υπολογιστικό νέφος είναι ικανό να επεξεργάζεται μαζική αποθήκευση δεδομένων και έντονες υπολογιστικές εργασίες. Επομένως, οι παραδοσιακοί μηχανισμοί ασφαλείας ενδέχεται να μην επαρκούν λόγω της εξάντλησης των υπολογιστικών πόρων ή των γενικών επικοινωνιών. Για παράδειγμα, για να επαληθεύσει το τραπεζικό ίδρυμα την ακεραιότητα των δεδομένων που αποθηκεύονται εξ' αποστάσεως, δεν είναι πρακτικό να κατακερματίσει ολόκληρο το σύνολο δεδομένων. Για το σκοπό αυτό, αναμένονται νέες στρατηγικές και πρωτόκολλα διαχείρισης δεδομένων στο υπολογιστικό νέφος από τα χρηματοπιστωτικά ιδρύματα.

## 5.4 Αντιμετώπιση απειλών από την τράπεζα

Η Τράπεζα θα μπορούσε να χρησιμοποιήσει ένα υβριδικό μοντέλο υπολογιστικού νέφους για τις συναλλαγές με τους πελάτες της, με την εφαρμογή του ιδιωτικού νέφους το οποίο θα εξασφάλιζε τις ασφαλείς συναλλαγές και του δημόσιου νέφους για το ανώτερο επίπεδο διαμοίρασης των τραπεζικών δεδομένων. Μέτρα ασφαλείας που έχουν παρθεί από χρηματοπιστωτικά ιδρύματα είναι:

- Το πρωτόκολλο Kerberos το οποίο αποτελεί την αρχιτεκτονική δομή για ασφαλές υπολογιστικό νέφος ως τραπεζικό πρωτόκολλο ελέγχου ταυτότητας εφαρμογών που λειτουργεί βάσει εξειδικευμένων τεχνικών αναγνώρισης χρηστών, για τον ασφαλή έλεγχο ταυτότητας με το οποίο αποδεικνύεται η γνησιότητα της εξουσιοδότησης των διαχειριστών του υπολογιστικού νέφους. Το πρωτόκολλο αυτό χρησιμοποιεί κρυπτογραφία συμμετρικού κλειδιού και απαιτεί ένα αξιόπιστο τρίτο μέρος κατά τη διάρκεια ορισμένων φάσεων ελέγχου της ταυτότητας του χρήστη (Zhu & Tung, 2006).
- Το Dynamic Firewall το οποίο χρησιμοποιείται για την προστασία των επιθέσεων μη εξουσιοδοτημένων χρηστών μέσω Διαδικτύου. Το τείχος προστασίας (firewall) χρησιμοποιείται από τα τραπεζικά πληροφοριακά συστήματα κατά τη διάρκεια αλληλεπίδρασης του με το υπολογιστικό νέφος.

Κατ' αυτόν τον τρόπο ένας κακόβουλος χρήστης που επιθυμεί να εισβάλει στο τραπεζικό δίκτυο θα αναχαιτιστεί από το τείχος προστασίας των συστημάτων.

- Το Honey Pot το οποίο χρησιμοποιείται για την ανίχνευση μη εξουσιοδοτημένης χρήσης δεδομένων. Το συγκεκριμένο λογισμικό δεν προσθέτει άμεση αξία στην ασφάλεια των τραπεζικών πληροφοριακών συστημάτων. Αντίθετα, εφαρμόζεται για τη μελέτη των επιθέσεων για λογαριασμό της τράπεζας και χρησιμοποιείται για την προστασία από αυτές (Rani, & Gangal, 2012).
- Το Intrusion Detection System (IDS), δηλαδή το σύστημα ανίχνευσης εισβολής, το οποίο χρησιμοποιείται για την παρακολούθηση των παραβιάσεων του δικτύου και την παροχή αναφορών στο κέντρο διαχείρισης δεδομένων του χρηματοπιστωτικού ιδρύματος (Scarfone & Mell, 2012).

## 5.5 Προσωπικά δεδομένα και ιδιωτικότητα στο σύννεφο

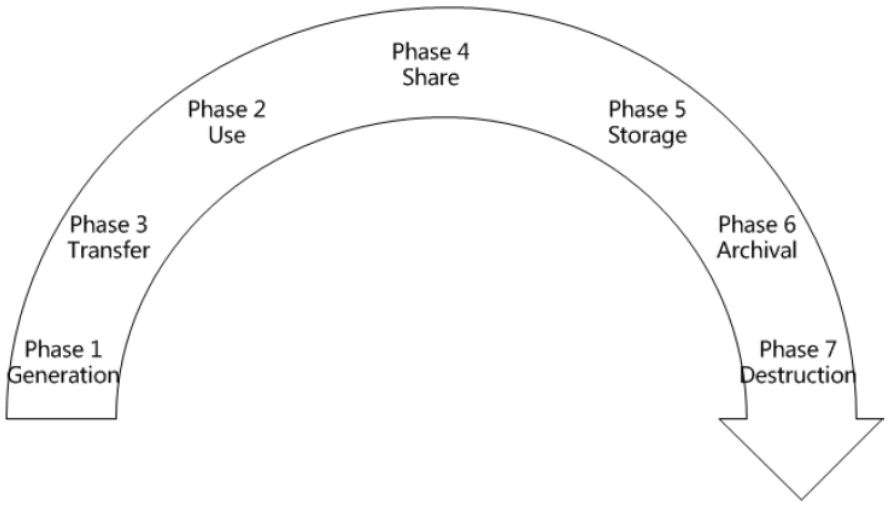
Οι οργανισμοί δεν πρέπει να αποκαλύπτουν τα ευαίσθητα δεδομένα τους, όπως προσωπικά ή οικονομικά δεδομένα σε μη εξουσιοδοτημένους χρήστες. Οι πάροχοι υπηρεσιών νέφους, θα πρέπει να ασκούν ισχυρούς ελέγχους πρόσβασης στα δεδομένα των πελατών τους. Η διαδικασία ελέγχου πρόσβασης περιλαμβάνει συνήθως εξουσιοδότηση και έλεγχο ταυτότητας. Λόγω του αυξημένου αριθμού οντοτήτων και σημείων πρόσβασης σε περιβάλλον υπολογιστικού νέφους, ο έλεγχος της ταυτότητας και η εξουσιοδότηση γίνονται όλο και πιο σημαντικοί παράγοντες για την προστασία των δεδομένων των πελατών. Υπάρχουν πολλά στοιχεία ελέγχου πρόσβασης στα συστήματα ασφαλείας τραπεζών, για παράδειγμα ένα PIN σε ένα σύστημα ATM επιτρέπει μόνο στους εξουσιοδοτημένους χρήστες την πρόσβαση στον λογαριασμό τους για ανάληψη χρηματικού ποσού από το τερματικό ATM. Ένας μηχανισμός πρόσβασης για διαδικτυακές τραπεζικές συναλλαγές με κωδικούς πρόσβασης και ερωτήσεις ασφαλείας μπορεί να παρέχει έναν αυστηρό έλεγχο πρόσβασης (Bose, Luo & Liu, 2013).

Για τις περισσότερες από τις τράπεζες, ακόμη και ο διαχειριστής δε θα μπορεί να ανοίξει την πόρτα του θησαυροφυλακίου μόνος του. Αντ' αυτού, πρέπει να υπάρχουν δύο άτομα σωματικά παρόν για να ανοίξουν την πόρτα. Υποστηρίζεται ότι ο μηχανισμός κρυπτογράφησης δύο κλειδιών μπορεί να εφαρμοστεί και στην υπηρεσία του

υπολογιστικού νέφους, ώστε τα δεδομένα των πελατών να είναι ασφαλή και διαθέσιμα ανά πάσα στιγμή. Με τον όρο διαθεσιμότητα δεδομένων εννοούμε ότι οι πόροι υπηρεσιών και η αποθήκευση δεδομένων μέσα σε ένα σύννεφο καθίστανται προσβάσιμα και μπορούν να χρησιμοποιηθούν κατόπιν αιτήματος από εξουσιοδοτημένη οντότητα. Είναι σημαντικό οι πάροχοι να διαθέτουν πόρους, λογισμικό, πληροφορίες και υψηλή αξιοπιστία δικτύου μέσω Διαδικτύου. Οι πελάτες που έχουν εγγραφεί σε υπηρεσίες νέφους, δικαιούνται να λαμβάνουν τις υπηρεσίες του ανά πάσα στιγμή και από οποιοδήποτε μέρος. Στο ίδιο πνεύμα, τα χρήματα των τραπεζικών πελατών είναι προσβάσιμα από ATM, τηλεφωνικά κέντρα και προγράμματα περιήγησης Διαδικτύου, σχεδόν από οπουδήποτε στον κόσμο κι ανά πάσα στιγμή. Επιπλέον, οι πελάτες υπολογιστικού νέφους χρειάζονται μεγαλύτερη πρόσβαση στα δεδομένα τους με μια ποικιλία διαφορετικών μεθόδων και υπολογιστών πόρων (Bose, Luo & Liu, 2013).

### *5.5.1 Ο κύκλος ζωής των δεδομένων οικονομικού χαρακτήρα*

Ο κύκλος ζωής των δεδομένων αναφέρεται σε ολόκληρη τη διαδικασία από τη δημιουργία έως την καταστροφή των δεδομένων. Ο κύκλος ζωής των δεδομένων χωρίζεται σε επτά στάδια τα οποία απεικονίζονται στην παρακάτω εικόνα.




**Εικόνα 11:** Κύκλος ζωής δεδομένων[31]

[31] Πηγή: Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. In *2012 International Conference on Computer Science and Electronics Engineering* (Vol. 1, pp. 647-651). IEEE.

Ο κύκλος ζωής των δεδομένων στο υπολογιστικό νέφος διακρίνεται σε επτά φάσεις οι οποίες είναι (Chen & Zhao, 2012):

*Φάση 1: Δημιουργία δεδομένων*

Η παραγωγή δεδομένων καθορίζει το ιδιοκτησιακό τους καθεστώς. Στο παραδοσιακό περιβάλλον πληροφορικής, συνήθως οι χρήστες ή οι οργανισμοί κατέχουν και διαχειρίζονται τα δεδομένα. Σε περίπτωση που τα δεδομένα πρόκειται να μετεγκατασταθούν στο υπολογιστικό νέφος, θα πρέπει να ληφθεί υπόψη η διατήρηση της ιδιοκτησίας τους. Οι κάτοχοι των δεδομένων έχουν το δικαίωμα να γνωρίζουν τις προσωπικές πληροφορίες που συλλέγονται και, σε ορισμένες περιπτώσεις, να σταματήσουν τη συλλογή και την επεξεργασία των προσωπικών τους δεδομένων.

*Φάση 2: Μεταφορά δεδομένων*

Μέσα στα όρια του τραπεζικού ιδρύματος, η μεταφορά των δεδομένων συνήθως δεν απαιτεί κρυπτογράφηση ή απλώς έχει ένα απλό μέτρο κρυπτογράφησης δεδομένων. Για τη μεταφορά δεδομένων πέρα από τα όρια της τράπεζας, πρέπει να διασφαλιστεί τόσο η εμπιστευτικότητα όσο και η ακεραιότητα των δεδομένων προκειμένου να αποφευχθεί η αξιοποίηση και η παραβίαση των δεδομένων από μη εξουσιοδοτημένους χρήστες. Με άλλα λόγια, μόνο η κρυπτογράφηση δεδομένων δεν είναι αρκετή. Επομένως, πρέπει να διασφαλιστεί η ακεραιότητα και η εμπιστευτικότητα των πρωτόκολλων μεταφοράς των δεδομένων (για παράδειγμα το πρωτόκολλο έμπιστης μεταφοράς δεδομένων SSL).

*Φάση 3: Χρήση των δεδομένων*

Οι εφαρμογές που βασίζονται σε μοντέλο υπολογιστικού νέφους PaaS ή SaaS, δεν μπορούν να κρυπτογραφήσουν στατικά δεδομένα. Επειδή η κρυπτογράφηση των δεδομένων θα οδηγήσει σε προβλήματα ευρετηρίασης, τα στατικά δεδομένα που χρησιμοποιούνται από εφαρμογές που βασίζονται στο σύννεφο δεν είναι κρυπτογραφημένα.

*Φάση 4: Διαμοιρασμός δεδομένων*

Η κοινή χρήση πληροφοριών επεκτείνει το εύρος χρήσης των δεδομένων και καθιστά τα δικαιώματα τους πιο περίπλοκα. Οι κάτοχοι δεδομένων μπορούν να εξουσιοδοτήσουν την πρόσβασή τους σε ένα αποθηκευτικό μέσο υπολογιστικού νέφους και με τη σειρά του το μέσο αυτό μπορεί να κοινοποιήσει περαιτέρω τα δεδομένα σε άλλους χρήστες χωρίς τη συγκατάθεση των κατόχων δεδομένων.

*Φάση 5: Αποθήκευση δεδομένων*

Τα δεδομένα στο σύννεφο μπορούν να χωριστούν σε: (1) Δεδομένα σε περιβάλλον IaaS, όπως το Simple Storage Service της Amazon και σε (2) δεδομένα σε περιβάλλον PaaS ή SaaS που σχετίζονται με το νέφος. Τα δεδομένα που αποθηκεύονται στις αποθήκες νέφους είναι παρόμοια με αυτά που είναι αποθηκευμένα σε άλλα μέρη και πρέπει να ληφθούν υπόψη τρεις πτυχές της ασφάλειας πληροφοριών: εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα.

*Φάση 6: Αρχείο δεδομένων*

Εάν τα δεδομένα αποθηκεύονται σε φορητά μέσα και στη συνέχεια τα μέσα είναι εκτός ελέγχου, τα δεδομένα ενδέχεται να διατρέχουν τον κίνδυνο διαρροής. Εάν οι πάροχοι υπηρεσιών υπολογιστικού νέφους δεν παρέχουν αρχειοθέτηση εκτός ιστότοπου, η διαθεσιμότητα των δεδομένων θα απειληθεί.

*Φάση 7: Καταστροφή δεδομένων*

Λόγω των φυσικών χαρακτηριστικών του μέσου αποθήκευσης, τα διαγραμμένα δεδομένα ενδέχεται να εξακολουθούν να υπάρχουν και να μπορούν να αποκατασταθούν. Αυτό μπορεί να οδηγήσει σε ακούσια αποκάλυψη ευαίσθητων πληροφοριών.

## 5.6 Σύνοψη

Ως προσέγγιση για την αντιμετώπιση ζητημάτων κινδύνου και ευθύνης στο υπολογιστικό νέφος, οι Pieters και Van Cleeff (2009) πρότειναν την αρχή της προφύλαξης προσωπικών δεδομένων στο σύννεφο. Υποστηρίζουν ότι λόγω των πολύπλοκων διεργασιών που μπορεί να εκτελέσει ένας οργανισμός, στο πλαίσιο της εφαρμογής νέων τεχνολογιών, θα πρέπει να λάβουν τα κατάλληλα μέτρα για την ασφάλεια των πληροφοριακών τους συστημάτων (Pieters, 2009). Η αρχή της προφύλαξης των δεδομένων, καθορίζεται για την αποφυγή βλάβης από άγνωστες αιτίες χωρίς να παρεμποδίζεται εντελώς η πρόοδος και η καινοτομία. Επίσης η αρχή της προφύλαξης δηλώνει ότι οι οργανισμοί θα πρέπει να απέχουν από ενέργειες επιστημονικών αβεβαιοτήτων σχετικά με σοβαρές ή μη αναστρέψιμες βλάβες στα πληροφοριακά συστήματα.

Επιπλέον, το βάρος της απόδειξης για τη εξασφάλιση της ασφάλειας μιας δράσης βαρύνει εκείνους που την προτείνουν (Pieters, 2009). Πολλές ανεπιθύμητες ενέργειες και απειλές των πληροφοριακών συστημάτων με υποδομή υπολογιστικού νέφους (cloud computing), δεν μπορούν ακόμη να εντοπιστούν ακόμα κι από έμπειρους

προγραμματιστές. Αυτό δε σημαίνει ότι η ανάπτυξη και η εφαρμογή του νέφους στα χρηματοπιστωτικά ιδρύματα θα πρέπει να ακυρωθεί εντελώς. Αντίθετα, η αρχή της προφύλαξης καλεί τα εμπλεκόμενα μέρη να προβλέψουν τις απειλές του υπολογιστικού νέφους οι οποίες μπορεί να μην είναι προβλέψιμες. Επιπλέον, οι τράπεζες δεν πρέπει να λειτουργούν με γνώμονα την αβεβαιότητα για να απέχουν από το σχεδιασμό και την παροχή υπηρεσιών υπολογιστικού νέφους, αλλά αντιθέτως να υποστηρίζουν νέες μεθόδους διαχείρισης και επεξεργασίας δεδομένων, ακολουθώντας τους κανονισμούς που έχει θεσπίσει η Ευρωπαϊκή Ένωση για την προστασία των δεδομένων των φυσικών προσώπων (Pieters 2009).

# 6 Νομοθεσία για την προστασία προσωπικών δεδομένων στο υπολογιστικό νέφος

## 6.1 Εισαγωγή

Η προστασία των προσωπικών δεδομένων έχει τραβήξει τη προσοχή των νομοθετών, των επιχειρηματιών, των προγραμματιστών και των εποπτικών αρχών. Αυτό σχετίζεται με την αυξανόμενη υιοθέτηση υπηρεσιών που βασίζονται στο υπολογιστικό νέφος και στην προστασία των προσωπικών δεδομένων ως βασικό πλεονέκτημα στα σύγχρονα επιχειρηματικά μοντέλα. Το γεγονός ότι τα προσωπικά δεδομένα έχουν σημαντική οικονομική αξία αποδεικνύεται από την εμφάνιση πολλών υπηρεσιών υπολογιστικού νέφους. Το όφελος για μια εταιρεία που παρέχει τέτοιες υπηρεσίες (και αποτελούν τη μοναδική πηγή εσόδων της) προέρχεται από την επεξεργασία τέτοιων προσωπικών δεδομένων, ιδίως την πώληση σε τρίτους.

Το κύριο νομικό μέσο της Ευρωπαϊκής Ένωσης (ΕΕ) που καθορίζει τους γενικούς κανόνες για την επεξεργασία δεδομένων προσωπικού χαρακτήρα ήταν η οδηγία 95/46/ΕΚ, η οποία παρείχε στα υποκείμενα δεδομένων ένα σύνολο δικαιωμάτων σχετικά με την επεξεργασία των δεδομένων τους. Επίσης η οδηγία αυτή είχε ως στόχο τη δήλωση των υποχρεώσεων των υπεύθυνων επεξεργασίας δεδομένων, ενώ προέβλεπε τις αρχές και τους μηχανισμούς που αποσκοπούσαν στη διασφάλιση και τη τήρηση των κανόνων. Οι ίδιοι γενικοί κανόνες ισχύουν όταν τα δεδομένα αποθηκεύονται ή υφίστανται επεξεργασία με άλλο τρόπο στο σύννεφο (cloud). Ωστόσο, η ταχεία εξέλιξη της τεχνολογίας τις τελευταίες δύο δεκαετίες αποκάλυψε πολλές αδυναμίες του ισχύοντος νομικού πλαισίου, οδηγώντας στην προσαρμογή της νομοθεσίας. Κατ' αυτόν τον τρόπο κρίθηκε απαραίτητη μία μεταρρύθμιση για νέα νομοθεσία η οποία βρισκόταν υπό ανάπτυξη, έως ότου να φτάσει στα τελικά της στάδια (Bartolini, Gheorghe, Giurgiu, Sabetzadeh & Sannier, 2015).

Η μεταρρύθμιση αυτή αποτελείται από ένα σύνολο κανόνων και οδηγιών, οι οποίοι είχαν ως στόχο τη διαμόρφωση του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) 679/2016. Ο ΓΚΠΔ αντικατέστησε την οδηγία 95/46/ΕΚ. Ο κανονισμός βασίζεται στις αρχές και τους κανόνες της προϋπάρχουσας οδηγίας, αλλά στοχεύει στην ενίσχυση των δικαιωμάτων του υποκειμένου των δεδομένων. Επίσης, τονίζει την ευθύνη του υπεύθυνου επεξεργασίας δεδομένων και του εκτελούντος την επεξεργασία και αυξάνει τις κυρώσεις για παραβιάσεις των διατάξεών της. Ο νέος κανονισμός επιβαρύνει

σημαντικά τις επιχειρήσεις που εμπλέκονται στην επεξεργασία προσωπικών δεδομένων. (Bartolini, Gheorghe, Giurgiu, Sabetzadeh & Sannier, 2015). Τα τραπεζικά ιδρύματα, ιδίως όταν χρησιμοποιούν τρίτους φορείς για την επεξεργασία των δεδομένων των πελατών τους θα πρέπει να συμμορφωθούν με τον ΓΚΠΔ, για τη θέσπιση μίας συγκεκριμένης κατευθυντήριας γραμμής η οποία θα προσαρμόζεται στις νομικές απαιτήσεις της Ευρωπαϊκής Ένωσης (ΕΕ).

## 6.2 Η σημασία της νομοθετικής ρύθμισης των υπηρεσιών Υπολογιστικού Νέφους

Πριν από την εισαγωγή του Γενικού Κανονισμού Προστασίας Δεδομένων της ΕΕ (ΓΚΠΔ), εξετάστηκαν ορισμένα σημαντικά ζητήματα σχετικά με την εφαρμογή του υπολογιστικού νέφους (cloud computing) στο τραπεζικό σύστημα. Συγκεκριμένα, προέκυψαν προβλήματα ως προς τον έλεγχο των δεδομένων που ήταν αποθηκευμένα στο σύννεφο και την διατήρηση αποδεικτικών στοιχείων σχετικά με τη σωστή κι αποτελεσματική διαχείριση των προσωπικών δεδομένων του υποκειμένου. Η ανάπτυξη μηχανισμών ελέγχου ασφαλείας στο σύννεφο, είναι απαραίτητη προϋπόθεση για την αποδοτική εφαρμογή του στα χρηματοπιστωτικά ιδρύματα. Η πολύπλοκη φύση της αρχιτεκτονικής του υπολογιστικού νέφους, μπορεί να επιφέρει επιπλέον προβλήματα στην επίτευξη ασφάλειας στο σύννεφο με αποτέλεσμα να δημιουργούνται φόβοι ως προς την νόμιμη εφαρμογή του από τα τραπεζικά ιδρύματα.

Ιστορικά, πολλοί οργανισμοί και επιχειρήσεις είχαν την ανάγκη να εντοπίσουν το χρονικό διάστημα παραβίασης των συστημάτων τους, ώστε να καταλάβουν ποιά δεδομένα είχαν προσπελαστεί, τροποποιηθεί ή διαγραφεί από τα πληροφοριακά τους συστήματά. Συχνά, όταν μιλάμε για πληροφοριακά συστήματα βασισμένα σε υποδομή υπολογιστικού νέφους, δεν υπάρχει κατανόηση ως προς το ποιός διέπραξε την παραβίαση, πράγμα που σημαίνει ότι είναι δύσκολο να ποσοτικοποιηθεί ο κίνδυνος στον οποίο έχουν εκτεθεί τα συστήματα αυτά. Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) επιδιώκει να βελτιώσει αυτήν την κατάσταση, απαιτώντας να αναφερθούν όλες οι παραβιάσεις εντός εβδομήντα δύο ωρών από την εμφάνιση τους[32], συμπεριλαμβανομένης της πλήρους αναγνώρισης όλων των δεδομένων που έχουν

[32] ΓΚΠΔ αρ. 33 παρ. 1

παραβιαστεί, ελλείψει των οποίων το τραπεζικό ίδρυμα θα μπορούσε να υπόκειται σε ποινικά επίπεδα προστίμων (Weir, Aßmuth, Whittington & Duncan, 2017).

Όπως θα δούμε και σε επόμενη υπό ενότητα, η νομική ρύθμιση της τεχνολογίας του υπολογιστικού νέφους κρίθηκε απαραίτητη από πολλούς ερευνητές θέτοντας τον προβληματισμό της προσαρμογής του σύννεφου (cloud) στις τραπεζικές διεργασίες και κατ' επέκταση στα τραπεζικά πληροφοριακά συστήματα. Η πολύπλοκη αρχιτεκτονική σχεδίαση του υπολογιστικού νέφους σε συνδυασμό με τη διαδικασία λογοδοσίας[33] του τραπεζικού ιδρύματος προς την εποπτική αρχή, σχετικά με την προστασία των προσωπικών δεδομένων των πελατών, καθιστά δύσκολη την πλήρη ενσωμάτωση των υπηρεσιών του υπολογιστικού νέφους στα πληροφοριακά συστήματα των χρηματοπιστωτικών ιδρυμάτων. Έτσι κρίθηκε απαραίτητη η δημιουργία κανόνων προστασίας δεδομένων οι οποίοι θα διασφαλίζουν ότι οι φορείς επεξεργασίας θα διαχειρίζονται αποτελεσματικά και σύμφωνα με τα Ευρωπαϊκά πρότυπα τα δεδομένα των υποκειμένων.

Η Ευρωπαϊκή Ένωση (ΕΕ) θέσπισε τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ)[34] για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία αυτών. Με τον ΓΚΠΔ, τα τραπεζικά ιδρύματα έπρεπε να συμμορφωθούν προς τους κανονισμούς που έθεσε η ΕΕ στο πλαίσιο της προστασίας των προσωπικών δεδομένων των υποκειμένων. Έτσι τα χρηματοπιστωτικά ιδρύματα για να συμμορφωθούν με τον ΓΚΠΔ, έπρεπε:

1. Να διαμορφώσουν τον κώδικα δεοντολογίας[35] τους, ώστε όλες οι τραπεζικές διεργασίες που εκτελούνται για την αποτελεσματική λειτουργία των τραπεζικών υπηρεσιών, να συμβαδίζουν με τον νέο κανονισμό περί προστασίας προσωπικών δεδομένων.
2. Να λάβουν όλα τα μέτρα ασφαλείας[36], ιδίως στα τραπεζικά πληροφοριακά συστήματα, καθώς αποτελούν έναν μηχανισμό επεξεργασίας προσωπικών

[33] ΓΚΠΔ αρ. 5 παρ. 2 «*Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»)*»

[34] Κανονισμός Ευρωπαϊκής Ένωσης 679/2016 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016

[35] Άρθρο 40 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016

[36] Άρθρο 32 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016

δεδομένων. Ισχυρά μέτρα προστασίας δεδομένων πρέπει να λάβουν και για τις διαδικτυακές υπηρεσίες που προσφέρει το τραπεζικό ίδρυμα (π.χ. ηλεκτρονικές πλατφόρμες συναλλαγών, ηλεκτρονική αλληλογραφία με τους πελάτες, αυτοματοποιημένα συστήματα συλλογής κι επεξεργασίας δεδομένων προσωπικού χαρακτήρα μέσω διαδικτύου).

3. Να λογοδοτούν για τυχών παραλείψεις ή κακή διαχείριση των προσωπικών δεδομένων των πελατών από το τραπεζικό ίδρυμα[37]. Τα χρηματοπιστωτικά ιδρύματα θα πρέπει να αναφέρουν άμεσα τυχών παραβιάσεις των συστημάτων τους στην εποπτική αρχή[38] και να ειδοποιήσουν τα υποκείμενα των δεδομένων για την τρέχουσα κατάσταση.
4. Να λάβουν υπόψη τα δικαιώματα των υποκειμένων των δεδομένων που υπόκεινται σε επεξεργασία και να συνάπτουν μαζί τους συμβάσεις κατά τις οποίες θα ορίζεται ρητώς η πολιτική απορρήτου που ακολουθεί το τραπεζικό ίδρυμα[39].
5. Να γνωστοποιούν τους λόγους συλλογής κι επεξεργασίας των προσωπικών δεδομένων των πελατών και να οριοθετούν την ευθύνη τους ως προς την επεξεργασία των δεδομένων[40].

Με την εισαγωγή νέων μορφών διαχείρισης και αποθήκευσης δεδομένων, όπως είναι το υπολογιστικό νέφος, δεν υπήρχαν επαρκείς νομικές ρυθμίσεις όπου θα ξεδιάλυναν το τοπίο, σχετικά με τον ρόλο του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία. Ο Γενικός Κανονισμός Προστασίας Δεδομένων προσπαθεί να δώσει λύσεις μέσα από τις γενικές διατάξεις του, θεωρώντας ότι το υπολογιστικό νέφος αποτελεί μία υπηρεσία που χρησιμοποιείται από οργανισμούς για τη διαχείριση των δεδομένων τους. Η αντιμετώπιση του εν λόγω θέματος, όπως θα δούμε και στη συνέχεια, αποτελεί ένα ενδιαφέρον ζήτημα που εγείρει την επιστημονική μελέτη σχετικά με τον ρόλο της τεχνολογίας του υπολογιστικού νέφους στη διαχείριση και επεξεργασία των προσωπικών δεδομένων των υποκειμένων, με αποτέλεσμα πολλοί

[37] Στην προκειμένη περίπτωση ένα χρηματοπιστωτικό ίδρυμα λειτουργεί σαν φορέας επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

[38] Άρθρο 33 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016

[39] Άρθρο 34 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016

[40] Άρθρο 30 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016

ερευνητές να προσπαθούν να προσαρμόσουν τις υπηρεσίες του υπολογιστικού νέφους στις απαιτήσεις του ΓΚΠΔ.

## 6.3 Υπολογιστικό Νέφος και ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) 679/2016

Η εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016, δε στηρίχθηκε σε μεμονωμένες τεχνολογίες για την διεξαγωγή ρυθμίσεων, όπως της υπηρεσίας του υπολογιστικού νέφους. Ο ΓΚΠΔ βασίστηκε κυρίως σε γενικές διατάξεις που όριζαν ακριβώς τον τρόπο με τον οποίο ένας φορέας επεξεργασίας δεδομένων πρέπει να εργαστεί για την εξασφάλιση της προστασίας των προσωπικών δεδομένων του υποκειμένου.

Ο ΓΚΠΔ άλλαξε τον τρόπο με τον οποίο πραγματοποιείται η συλλογή των δεδομένων και τον τρόπο σχεδιασμού και χρήσης εταιρικών βάσεων δεδομένων. Επίσης, διαμόρφωσε δυνητικά τον τρόπο διεξαγωγής της έρευνας και ανάπτυξης επηρεάζοντας τις πρακτικές ασφάλειας στον κυβερνοχώρο, καθώς και την εισαγωγή ενός πρακτικού φάσματος προκλήσεων που περιστρέφονται γύρω από ιστότοπους και αποθετήρια όπου οι ομάδες μοιράζονται σχόλια, πληροφορίες και άλλα δεδομένα. Ωστόσο, ο ΓΚΠΔ μεταφέρει αυτήν την ιδέα σε ένα νέο και μη δοκιμασμένο επίπεδο. Εκτός από το ότι παρέχει στα φυσικά πρόσωπα τον πλήρη έλεγχο των δεδομένων τους, μπορούν να αφαιρέσουν τις πληροφορίες τους από μια βάση δεδομένων ή μια διαδικτυακή πηγή ανά πάσα στιγμή ενώ για όσους πιστεύουν ότι έχουν αδικηθεί, ο κανονισμός τους παρέχει τη δυνατότητα της διεξαγωγής έρευνας κι άσκησης αγωγής εις βάρος αντίστοιχου φορέα επεξεργασίας δεδομένων (Greengard, 2018).

Οι αρχές προστασίας δεδομένων στην Ευρωπαϊκή Ένωση πρόσφατα έδωσαν ιδιαίτερη προσοχή στο υπολογιστικό νέφος (cloud computing), ως απάντηση σε έρευνες από προμηθευτές και υποψήφιους χρήστες της τεχνολογίας του νέφους που επιδιώκουν να διασφαλίσουν τη συμμόρφωση τους με τις απαιτήσεις της προστασίας προσωπικών δεδομένων της ΕΕ. Ορισμένες από τις κύριες νομικές εκτιμήσεις που σχετίζονται με τις υπηρεσίες υπολογιστικού νέφους στην Ευρωπαϊκή Ένωση περιγράφονται παρακάτω.

### *6.3.1 Υπεύθυνοι επεξεργασίας κι εκτελούντες την επεξεργασία*

Στην Ευρωπαϊκή Ένωση, το καθεστώς μιας οντότητας ως υπευθύνου επεξεργασίας δεδομένων ή εκτελούντος την επεξεργασία είναι ζωτικής σημασίας δεδομένου ότι η έκταση των υποχρεώσεων προστασίας δεδομένων των υποκειμένων εξαρτάται από τον ρόλο τους. Ο υπεύθυνος επεξεργασίας δεδομένων καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και είναι υπεύθυνος για τη συμμόρφωση με τη νομοθεσία περί προστασίας δεδομένων, ενώ ο εκτελών την επεξεργασία είναι το φυσικό ή νομικό πρόσωπο που επεξεργάζεται τα δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας (Sotto, Treacy, & McLellan, 2010).

Όσον αφορά το υπολογιστικό νέφος (cloud computing), ο χαρακτηρισμός μιας οντότητας ως υπεύθυνου ή εκτελούντος την επεξεργασία των δεδομένων, μπορεί να εξαρτάται από τον τύπο του συστήματος υπολογιστικού νέφους που χρησιμοποιείται ή από την τεχνική ρύθμιση του συστήματος. Αυτός ο χαρακτηρισμός θα καθορίσει την ευθύνη των αντίστοιχων μερών για συμμόρφωση με τις υποχρεώσεις προστασίας δεδομένων. Επιπλέον, ένας υπεύθυνος επεξεργασίας φέρει ευθύνη για την εκπλήρωση υποχρεώσεων προστασίας δεδομένων, ακόμη και όταν τα δεδομένα έχουν μεταφερθεί σε τρίτους φορείς επεξεργασίας ή έχουν μεταβιβαστεί σε παρόχους υπολογιστικού νέφους. Είναι επομένως σημαντικό για ένα τραπεζικό ίδρυμα να προβεί σε αυστηρή εκτίμηση της ευθύνης του για τα δεδομένα που υποβάλλονται σε επεξεργασία από τον πάροχο του σύννεφου (cloud) και να συνάψει συμφωνία επεξεργασίας δεδομένων που απαιτεί από τον πάροχο υπολογιστικού νέφους να ενεργεί σύμφωνα με τις οδηγίες του τραπεζικού ιδρύματος, για να διασφαλιστεί η τεχνική/οργανωτική ασφάλεια ώστε να συμμορφωθεί με τον ΓΚΠΔ (Sotto, Treacy, & McLellan, 2010).

Επομένως σημαντικό ρόλο στη διαμόρφωση των υποχρεώσεων και των ρόλων του υπεύθυνου ή του εκτελούντος την επεξεργασίας, είναι τα μοντέλα παροχής υπηρεσιών υπολογιστικού νέφους. Κατ' αυτόν τον τρόπο, ένας πάροχος υπολογιστικού νέφους που παρέχει μόνο το λογισμικό για τη διαχείριση των δεδομένων στο τραπεζικό ίδρυμα, διαφοροποιείται από εκείνον τον πάροχο που παρέχει την πλατφόρμα, τον χώρο φιλοξενίας ή την τεχνολογική υποδομή[41]. Όταν ένας πάροχος υπολογιστικού νέφους προσφέρει τις υπηρεσίες του απευθείας στο υποκείμενο των δεδομένων, τότε ο πάροχος

[41] https://ico.org.uk/media/fororganisations/documents/1540/cloud_computing_guidance_for_organisations.pdf σελ: 6.

χαρακτηρίζεται ως υπεύθυνος επεξεργασίας ενώ το υποκείμενο των δεδομένων ως εκτελών την επεξεργασία[42]. Τα τραπεζικά ιδρύματα συνήθως χρησιμοποιούν το μοντέλο ανάπτυξης της υποδομής ως υπηρεσίας (Infrastructure as a service - IaaS), για την εξασφάλιση υπολογιστικών πόρων και αποθηκευτικού χώρου για την καλύτερη και γρηγορότερη επεξεργασία των δεδομένων. Επίσης, τα χρηματοπιστωτικά ιδρύματα στηρίζονται στο ιδιωτικό ή στο κοινοτικό νέφος, το οποίο χρησιμοποιείται αποκλειστικά για την εξυπηρέτηση των τραπεζικών τους διεργασιών. Μ' αυτήν τη λογική ο πάροχος υπολογιστικού νέφους παρέχει μόνο υπολογιστικούς πόρους για τη διαχείριση των τραπεζικών δεδομένων χωρίς ο ίδιος ο πάροχος να προσφέρει οποιαδήποτε εφαρμογή ή λογισμικό ή πρόσβαση στο περιεχόμενο (άνευ γνώσεως του είδους των δεδομένων που θα αποθηκεύσει ο χρήστης). Αυτό έχει ως αποτέλεσμα ο υπεύθυνος επεξεργασίας δεδομένων να είναι το τραπεζικό ίδρυμα ενώ ο εκτελών την επεξεργασία να ορίζεται από τον υπεύθυνο, χωρίς να απαιτείται η διαμεσολάβηση του εξωτερικού παρόχου υπολογιστικού νέφους, αφού οι υπηρεσίες σύννεφου παράγονται από το ίδιο το χρηματοπιστωτικό ίδρυμα.

Έπειτα από μελέτη του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) εντοπίσαμε ότι από τα 99 άρθρα, μόνο τα ακόλουθα άρθρα επηρεάζουν τους παρόχους υπηρεσιών υπολογιστικού νέφους στο τραπεζικό σύστημα. Τα άρθρα αυτά για λογούς ευκολίας τα χωρίσαμε σε τις τρεις κατηγορίες ανάλογα με τις υπερχρεώσεις του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία.

#### *6.3.1.1 Υποχρεώσεις τράπεζας ως υπεύθυνου επεξεργασίας δεδομένων στο σύννεφο*

Ένα χρηματοπιστωτικό ίδρυμα θα πρέπει να προσαρμόσει τις λειτουργίες που παρέχουν τα πληροφοριακά του συστήματα, τα οποία επεξεργάζονται τα δεδομένα των πελατών, στο Γενικό Κανονισμό Προστασίας Δεδομένων. Τα τραπεζικά ιδρύματα είναι κυρίως υποχρεωμένα να ακολουθούν τους κανόνες του ΓΚΠΔ. Συγκεκριμένα οι κανόνες που θα πρέπει να δοθούν περισσότερο έμφαση για τις υπηρεσίες υπολογιστικού νέφους είναι (Elluri & Joshi, 2018):

[42] Βλ. και Ετήσια Έκθεση Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 2015: «Σε ερώτημα σχολείου σχετικά με το ζήτημα της χρήσης υπηρεσιών υπολογιστικού νέφους για τη διαχείριση δεδομένων που τηρεί το σχολείο, η Αρχή απάντησε τα εξής: β) εφόσον ο πάροχος υπηρεσιών υπολογιστικού νέφους παρέχει τα μέσα και την πλατφόρμα των υπηρεσιών, ενεργώντας εξ ονόματος του πελάτη, τότε θεωρείται εκτελών την επεξεργασία (σύμφωνα με το άρ. 2 στοιχ. η' του ν. 2472/1997).»

- **Άρθρο 5**: Επεξεργασία δεδομένων προσωπικού χαρακτήρα - Τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε επεξεργασία με νόμιμο, δίκαιο και διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Τα δεδομένα συλλέγονται για νόμιμο σκοπό και δεν πρέπει να υποβάλλονται σε επεξεργασία με τρόπο που δεν είναι συμβατός για το σκοπό αυτό. Το τραπεζικό ίδρυμα θα πρέπει να ενημερώνει πλήρως του πελάτες του για τον σκοπό της επεξεργασίας των δεδομένων του ακόμα και σε περιπτώσεις που χρησιμοποιεί υπηρεσίες υπολογιστικού νέφους εξασφαλίζοντας τις ευθύνες του υπευθύνου και του εκτελών την επεξεργασία.
- **Άρθρο 24**: Ευθύνη του υπεύθυνου επεξεργασίας – Το τραπεζικό ίδρυμα θα πρέπει να είναι υπεύθυνο για την εφαρμογή οποιωνδήποτε τεχνικών ή οργανωτικών μέτρων που απαιτούνται για τη συμμόρφωση του ΓΚΠΔ.
- **Άρθρο 25**: Προστασία δεδομένων ήδη από τον σχεδιασμό και εξ' ορισμού - Απαιτεί από το χρηματοπιστωτικό ίδρυμα να συλλέγει, να αποθηκεύει ή να επεξεργάζεται τα δεδομένα μόνο για τους απαιτούμενους σκοπούς με την εφαρμογή τεχνικών όπως ψευδωνυμοποίηση και ελαχιστοποίηση δεδομένων. Σε περίπτωση που απαιτείται εκ νέου επεξεργασία των δεδομένων, το τραπεζικό ίδρυμα θα πρέπει να ενημερώσει τον πελάτη για το είδος και τον σκοπό της επεξεργασίας, ζητώντας τη συγκατάθεσή του. Να σημειώσουμε ότι ο εκτελών την επεξεργασία ως πάροχος υπηρεσίας υπολογιστικού νέφους, είναι εκείνος που εφαρμόζει τεχνικά κι οργανωτικά μέτρα στο νέφος και διεξάγει την επεξεργασία κατά τρόπο που πληροί ο ΓΚΠΔ[43].
- **Άρθρο 26**: Από κοινού υπεύθυνοι επεξεργασίας - Σε περίπτωση περισσότερων από έναν υπεύθυνο επεξεργασίας δεδομένων, αυτό το άρθρο αναμένει ότι όλοι τους συμμορφώνονται με τον ΓΚΠΔ. Ανάλογα με την υπηρεσία υπολογιστικού νέφους που χρησιμοποιεί το τραπεζικό ίδρυμα, οι υπεύθυνοι επεξεργασίας μπορεί να είναι η τράπεζα και ο πάροχος υπολογιστικού νέφους.
- **Άρθρο 27**: Εκπρόσωποι υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μη εγκατεστημένων στην Ένωση - Είναι σημαντικό να διοριστεί ένας εκπρόσωπος που είναι φυσικό ή νομικό πρόσωπο εγκατεστημένο στην

[43] Άρθρο 25 ΓΚΠΔ 679/2016

Ευρωπαϊκή Ένωση εάν το τραπεζικό ίδρυμα ή ο πάροχος υπολογιστικού νέφους βρίσκεται εκτός ΕΕ. Τα τραπεζικά ιδρύματα αποφεύγουν να αναθέσουν σε τρίτο φορέα την επεξεργασία των δεδομένων τους λόγο ασφάλειας κι εμπιστευτικότητας, με αποτέλεσμα να καταφεύγουν σε υπηρεσίες ιδιωτικού ή κοινοτικού υπολογιστικού νέφους για την εξασφάλιση του ελέγχου των δεδομένων τους.

- **Άρθρο 34**: Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων – Απαιτείται από το χρηματοπιστωτικό ίδρυμα η ενημέρωση του υποκειμένου των δεδομένων σε σαφή και απλή γλώσσα σχετικά με την παραβίαση δεδομένων που ενδέχεται να επηρεάσει τα δικαιώματα και τις ελευθερίες του.

#### *6.3.1.2 Υποχρεώσεις παρόχου υπολογιστικού νέφους ως εκτελών την επεξεργασία*

Ο πάροχος υπολογιστικού νέφους ο οποίος διορίζεται από το τραπεζικό ίδρυμα, υποχρεούται να ακολουθεί τους κανόνες ΓΚΠΔ και συγκεκριμένα τα άρθρα (Elluri & Joshi, 2018):

- **Άρθρο 29**: Επεξεργασία υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία - Ο πάροχος υπολογιστικού νέφους πρέπει να επεξεργάζεται δεδομένα σύμφωνα με τις οδηγίες που παρέχονται από τον υπεύθυνο επεξεργασίας (δηλαδή το χρηματοπιστωτικό ίδρυμα), εκτός εάν υπάρχουν αιτήματα από τη νομοθεσία της Ευρωπαϊκής Ένωσης.
- **Άρθρο 37** Ορισμός του υπευθύνου προστασίας δεδομένων - Προτείνεται η πρόσληψη υπευθύνου προστασίας δεδομένων σε περίπτωση που συνεπάγεται συνεχή παρακολούθηση του υποκειμένου των δεδομένων σε μεγάλη κλίμακα. Ο υπεύθυνος επεξεργασίας δεδομένων (Data Protection Officer - DPO), δηλαδή το φυσικό πρόσωπο που διορίζεται από το τραπεζικό ίδρυμα, θα πρέπει να προσληφθεί με βάση την εξειδικευμένη κατανόηση των νόμων περί απορρήτου δεδομένων στην πράξη.
- **Άρθρο 44**: Γενικές αρχές για διαβιβάσεις - Υποχρεώσεις σχετικά με τις διασυνοριακές μεταφορές θα εφαρμοστούν στους παρόχους υπολογιστικού νέφους για τη διαβίβαση των δεδομένων του υποκειμένου εκτός Ευρωπαϊκής Ένωσης.

#### *6.3.1.3 Κοινές υποχρεώσεις παρόχου υπολογιστικού νέφους και τράπεζας*

Οι κοινές υποχρεώσεις του παρόχου υπολογιστικού νέφους με το τραπεζικό ίδρυμα ρυθμίζονται από τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ). Τα άρθρα αυτά είναι (Elluri & Joshi, 2018):

- **Άρθρο 3 (1):** Εδαφικό πεδίο εφαρμογής – Ο ΓΚΠΔ ρυθμίζει τη νομιμότητα της επεξεργασίας δεδομένων είτε η εγκατάσταση του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία είναι στην Ένωση, είτε είναι εκτός αυτής. Το εν λόγω πεδίο εφαρμογής είναι πολύ σημαντικό για την τεχνολογία νέφους (cloud) διότι τα δεδομένα διατηρούνται σε απομακρυσμένους διακομιστές με αποτέλεσμα η επεξεργασία τους, πολλές φορές, να πραγματοποιείται εκτός του πεδίου δράσεως του υπεύθυνου επεξεργασίας.
- **Άρθρο 30:** Αρχεία των δραστηριοτήτων επεξεργασίας – Ο ΓΚΠΔ ρυθμίζει τη διαδικασία τήρησης αρχείων σχετικά με τη δραστηριότητα επεξεργασίας των δεδομένων τόσο από τον υπεύθυνο όσο κι από τον εκτελών την επεξεργασία. Το τραπεζικό ίδρυμα θα πρέπει να διατηρεί αρχείο δραστηριοτήτων εξεργασίας όπως και ο εκτελών την επεξεργασία, που να σχετίζεται με τις υπηρεσίες υπολογιστικού νέφους της τράπεζας και τη διαχείριση των δεδομένων των πελατών τους.
- **Άρθρο 31:** Συνεργασία με την εποπτική αρχή – Το τραπεζικό ίδρυμα ως υπεύθυνος επεξεργασία και ο εκτελών την επεξεργασία, ο οποίος διαχειρίζεται δεδομένα οικονομικής συμπεριφοράς μέσω του υπολογιστικού νέφους, θα πρέπει να συνεργάζεται με την εποπτική αρχή του κράτους μέλους της ΕΕ που ανήκει το χρηματοπιστωτικό ίδρυμα.
- **Άρθρο 32:** Ασφάλεια επεξεργασίας – Ο ΓΚΠΔ πλέον αναγκάζει τα τραπεζικά ιδρύματα να χρησιμοποιούν τεχνολογίες ασφαλείας στα πληροφοριακά τους συστήματα. Το άρθρο αυτό παίζει σημαντικό ρόλο στην ασφάλεια των τραπεζικών πληροφοριακών συστημάτων και στην προστασία των δεδομένων των πελατών από την επεξεργασία τους στο σύννεφο. Τα θέματα ασφαλείας αλλά και οι διαδικασίες προστασίας των δεδομένων, θεσπίζονται από τον κώδικα δεοντολογίας που αναπτύσσεται στα πλαίσια των τραπεζικών υπηρεσιών

- **Άρθρο 33:** Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή – Το τραπεζικό ίδρυμα, εφόσον διαπιστώσει κενά ασφαλείας των πληροφοριακών του συστημάτων με αποτέλεσμα τη διαρροή των δεδομένων των πελατών, πρέπει εντός 72 ωρών να ειδοποιείται η εποπτική αρχή αλλά και το υποκείμενο των δεδομένων. Σε περίπτωση που η τράπεζα καθυστερήσει να ειδοποιήσει την αρχή τότε πρέπει να της αποστείλει την αιτιολόγηση της καθυστέρησης.
- **Άρθρο 82:** Δικαίωμα αποζημίωσης και ευθύνη – Το εν λόγο άρθρο του Γενικού Κανονισμού Προστασίας Δεδομένων, αναφέρει το δικαίωμα της αποζημίωσης του υποκειμένου σε περίπτωση διαρροής ή αθέμιτης επεξεργασίας των δεδομένων του, από το τραπεζικό ίδρυμα. Στην προκειμένη περίπτωση την ευθύνη της επεξεργασίας των δεδομένων φέρουν το τραπεζικό ίδρυμα ως υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία ο οποίος διαχειρίζεται τις πληροφορίες των πελατών στο σύννεφο.

### *6.3.2 Επεξεργασία προσωπικών δεδομένων*

Όπως είδαμε και παραπάνω τα δεδομένα των υποκειμένων υφίστανται επεξεργασία από το τραπεζικό ίδρυμα, το όποιο είναι υπεύθυνο για την προστασία τους από μη εγκεκριμένες τεχνικές διαχείρισης πληροφοριών. Η επεξεργασία των προσωπικών δεδομένων πολλές φορές πραγματοποιείται από το ίδιο το τραπεζικό σύστημα, ενώ τα τελευταία χρόνια συνηθίζεται η τάση της εξωτερικής ανάθεσης[44] της επεξεργασίας των δεδομένων των πελατών από άλλους φορείς που εκτελούν τέτοιου είδους υπηρεσίες για λογαριασμό τρίτων. Ένα σημαντικό στοιχείο στη διατήρηση της εμπιστοσύνης του πελάτη με το χρηματοπιστωτικό ίδρυμα είναι η σύναψη σύμβασης για την παροχή των τραπεζικών υπηρεσιών.

Οι συναλλαγές μεταξύ των τραπεζικών ιδρυμάτων, των πελατών τους και των εξωτερικών φορέων διαχείρισης των πληροφοριών που περιλαμβάνουν επεξεργασία δεδομένων, από μόνες τους, έχουν σημαντικές νομικές συνέπειες. Για παράδειγμα, η ευθύνη των μερών για τυχών ζημίες που οφείλονται σε μη εγκεκριμένες τεχνικές

[44] Η επεξεργασία των προσωπικών δεδομένων πραγματοποιείται από τρίτο φορέα επεξεργασίας κι όχι από το τραπεζικό ίδρυμα. Κατ' αυτόν τον τρόπο ο φορέας επεξεργάζεται τα προσωπικά δεδομένα των πελατών για λογαριασμό της τράπεζας

διαχείρισης δεδομένων, όπως η απροσεξία ή οι εκ προθέσεως κακόβουλες πράξεις, θα πρέπει να αποφασιστεί εκ των προτέρων και να δηλωθεί σε μια σύμβαση συνεργασίας. Κατ' αυτόν τον τρόπο τα μέρη της σύμβασης μπορούν να θεσπίσουν ειδικούς και σημαντικούς νομικούς κανόνες που να ισχύουν για τη νόμιμη επεξεργασία των τραπεζικών δεδομένων (Freed, 1963). Θα πρέπει να αξιοποιηθούν πλήρως αυτές οι ευκαιρίες για τη θέσπιση διατάξεων που θα βοηθήσουν στην επίλυση των συγκρούσεων, οι οποίες ενδέχεται να προκύψουν.

Σημαντικοί παράγοντες για την αποτελεσματική επεξεργασία προσωπικών δεδομένων αποτελούν, α) το καταστατικό το οποίο διαμορφώνει την εκτέλεση των τραπεζικών διεργασιών και β) η εποπτική αρχή η οποία έχει ως στόχο την προάσπιση των συμφερόντων του υποκειμένου των δεδομένων. Ο ορισμός του καταστατικού σε συνδυασμό με τις οδηγίες της εποπτικής αρχής, δεν επιτρέπουν την εξ' ολοκλήρου επεξεργασία των δεδομένων από τρίτο φορέα, προκειμένου να προστατεύσουν τους καταθέτες από τους κινδύνους απώλειας δεδομένων που μπορεί προκύψουν. Οι εσωτερικοί κίνδυνοι που ενέχει το τραπεζικό σύστημα είναι γνωστοί και μπορούν να προβλεφθούν ως ένα βαθμό. Οι εξωτερικοί κίνδυνοι είναι μεταβλητοί και συχνά έχουν άγνωστο μέγεθος και, ως εκ τούτου, δεν μπορούν να ληφθούν εκ των προτέρων επιπρόσθετα μέτρα ασφαλείας. Επομένως, για ένα τραπεζικό ίδρυμα, η παραχώρηση της επεξεργασίας δεδομένων σε τρίτο φορέα εγείρει θέματα ασφαλείας ή διαρροής προσωπικών δεδομένων[45] (Freed, 1963).

Οι νομικές συνέπειες της επεξεργασίας εκτός του χρηματοπιστωτικού ιδρύματος, είναι πιθανώς οι πιο ενδιαφέρουσες από όλες αυτές που προκύπτουν από την εισαγωγή των τραπεζικών πληροφοριακών συστημάτων. Το φαινόμενο της επεξεργασίας από τρίτο φορέα για λογαριασμό τραπέζης αποτελεί ένα ξεχωριστό ερευνητικό πεδίο που χρήζει μελέτης. Για πρώτη φορά οι παραδοσιακές τραπεζικές διαδικασίες επεξεργασίας προσωπικών δεδομένων, έχουν ανατεθεί σε τρίτους. Η πρακτική ήταν εντελώς απρόβλεπτη όταν οι υφιστάμενοι νομικοί κανόνες που ίσχυαν για τις τράπεζες

[45] Βλ. και Ετήσια Έκθεση Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 2018: «Η παρεχόμενη προστασία θα πρέπει να είναι εξίσου και όταν τα δεδομένα είναι αποθηκευμένα σε άλλο μέσο πέραν από τα μέσα τα οποία βρίσκονται στην απόλυτη σφαίρα επιρροής του χρήστη. Συνεπώς, μπορεί να είναι ο εξυπηρετητής του παρόχου ή το υπολογιστικό νέφος που αυτός χρησιμοποιεί για την αποθήκευση. Καθώς η θέση αυτή δεν φαίνεται να βρίσκει απήχηση στα κράτη μέλη της ΕΕ, η Αρχή επισήμανε ότι σε αυτήν την περίπτωση είναι απόλυτα απαραίτητο να ρυθμιστεί επαρκώς και συνεκτικά η προστασία κατά τη φάση της επικοινωνίας (in transit).»

θεσπίστηκαν νομοθετικά από τα δικαστήρια. Όπως και σε άλλους τομείς της οικονομίας, ένα πρακτικό μέσο για την παροχή τραπεζικών υπηρεσιών επεξεργασίας δεδομένων, με χαμηλότερο κόστος ή με μεγαλύτερη αποτελεσματικότητα, ήταν η εκχώρηση δικαιωμάτων επεξεργασίας σε τρίτο φορέα με χρήση της υποδομής υπολογιστικού νέφους. Σε πολλές περιπτώσεις, το χαμηλότερο κόστος επεξεργασίας επιτυγχάνεται με αυτήν την πρακτική επειδή, εκτός από οποιαδήποτε ελάχιστη χρέωση, η πληρωμή πραγματοποιείται μόνο για τις υπηρεσίες που χρησιμοποιούνται από τον φορέα επεξεργασίας δεδομένων. Κατά συνέπεια, υπάρχουν οικονομικοί λόγοι για την επίτευξη λύσεων σε νομικά ζητήματα που αφορούν την επεξεργασία εκτός του τραπεζικού ιδρύματος.

Σε γενικές γραμμές, δεν είναι απολύτως σαφές ότι οι φορείς επεξεργασίας δεδομένων μπορούν να παρέχουν τέτοιου είδους υπηρεσίες για τα τραπεζικά ιδρύματα. Οι εξειδικευμένες τραπεζικές υπηρεσίες, ενδέχεται να περιλαμβάνουν την επεξεργασία μισθοδοσίας, τον έλεγχο οικονομικού αποθέματος, τις οικονομικές προβλέψεις και υπολογιστικούς μηχανισμούς που διαθέτει το ίδρυμα. Όπως ήδη αναφέρθηκε, οι φορείς επεξεργασίας δεδομένων πρέπει να περιορίζονται στην εκτέλεση των τραπεζικών λειτουργιών και να μην παρέχουν υπηρεσίες επεξεργασίας δεδομένων σε άλλες επιχειρήσεις ή οργανισμούς, οι οποίοι ενδέχεται να επωφελούνται από το είδος των δεδομένων που συλλέγει ένα χρηματοπιστωτικό ίδρυμα (Freed, 1963). Αυτό συμβαίνει διότι, λόγω συμφερόντων, τα τραπεζικά δεδομένα ενδέχεται να μεταφέρνουν σε ανταγωνιστική εταιρεία με αποτέλεσμα να δημιουργηθούν κενά ασφαλείας και ως εκ τούτου να θέσουν σε κίνδυνο τα περιουσιακά στοιχεία των καταθετών του τραπεζικού ιδρύματος.

Οι φορείς επεξεργασίας δεδομένων ενδέχεται να μην εκτελούν απευθείας τραπεζικές υπηρεσίες για πελάτες που δεν είναι τράπεζες. Μπορούν να εκτελούν μόνο υπηρεσίες επεξεργασίας δεδομένων για λογαριασμό των χρηματοπιστωτικών ιδρυμάτων. Ωστόσο, ο ορισμός των τραπεζικών υπηρεσιών θα μπορούσε να ερμηνευθεί έτσι ώστε να τους επιτρέπει να κάνουν γενική επεξεργασία δεδομένων έμμεσα μέσω των τραπεζών που εξυπηρετούν. Οι επιτρεπόμενες υπηρεσίες δεν πρέπει να περιλαμβάνουν μόνο μια σειρά συγκεκριμένων δραστηριοτήτων που συνήθως σχετίζονται με τραπεζικές συναλλαγές, όπως ταξινόμηση επιταγών και καταθέσεων, αλλά και οποιαδήποτε άλλη λογιστική ή στατιστική πρόβλεψη ή παρόμοιες λειτουργίες που εκτελούνται από ένα τραπεζικό ίδρυμα (Freed, 1963).

Μία ασφαλή δίοδο για την επεξεργασία δεδομένων αποτελεί η χρήση του ιδιωτικού ή του κοινοτικού υπολογιστικού νέφους, όπου ο ρόλος του υπεύθυνου και του εκτελούντος την επεξεργασία είναι ξεκάθαρος και ορίζεται από το χρηματοπιστωτικό ίδρυμα. Αν και τέτοια συστήματα απαιτούν μεγάλο κόστος συντήρησης, η ασφάλεια και η προστασία των προσωπικών δεδομένων είναι έργο της τράπεζας η οποία ακολουθώντας τον κώδικα δεοντολογίας που έχει αναπτύξει, μπορεί να προσαρμόσει τις τραπεζικές της υπηρεσίες στον Γενικό Κανονισμό Προστασίας Δεδομένων.

### *6.3.3 Διασυνοριακή ροή δεδομένων*

Οι περιορισμοί που επιβάλλονται στη διεθνή μεταφορά προσωπικών δεδομένων από τα κράτη μέλη της ΕΕ δημιουργούν ζητήματα δικαιοδοσίας στο πλαίσιο της εφαρμογής των υπηρεσιών του υπολογιστικού νέφους. Απαγορεύεται η μεταφορά δεδομένων προσωπικού χαρακτήρα εκτός της Ευρωπαϊκής Ένωσης που προέρχονται από τον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ), εκτός εάν η χώρα παραλαβής προβλέπει επαρκές επίπεδο προστασίας δεδομένων. Η Ευρωπαϊκή Επιτροπή θεώρησε ότι μόνο λίγες χώρες παρείχαν επαρκές επίπεδο προστασίας δεδομένων και ότι οι Ηνωμένες Πολιτείες δεν ήταν μία από αυτές (Sotto, Treacy, & McLellan, 2010). Η μεταφορά προσωπικών δεδομένων σε μια χώρα που δεν θεωρείται ασφαλής ως προς την προστασία τους, μπορεί να εγκριθεί εάν ο παραλήπτης δεδομένων έχει εφαρμόσει έναν νομικό μηχανισμό που να προβλέπει συγκεκριμένα επίπεδα προστασίας δεδομένων (όπως η συμμόρφωση με το πρόγραμμα Safe Harbor των ΗΠΑ) ή εάν ο υπεύθυνος επεξεργασίας δεδομένων μπορεί να καλύψει όλες τις προδιαγραφές του Γενικού Κανονισμού Προστασίας Δεδομένων. Τέτοιοι μηχανισμοί είναι δύσκολο να εφαρμοστούν σ' ένα περιβάλλον υπολογιστικού νέφους και ενδέχεται να απαιτούν την έγκριση μιας εποπτικής αρχής για την προστασία δεδομένων της ΕΕ. Για να επιλύσουν αυτές τις ανησυχίες, ορισμένοι πάροχοι υπολογιστικού νέφους (cloud computing) χρησιμοποιούν συγκεκριμένες τεχνικές διαχωρισμού του σύννεφου ώστε να μπορούν να εμποδίζουν τη μεταφορά προσωπικών δεδομένων εκτός της Ευρωπαϊκής Ένωσης[46], κυρίως σε χώρες που δεν παρέχουν επαρκή νομοθεσία για την προστασία των προσωπικών δεδομένων.

Σύμφωνα με τη νομοθεσία περί προστασίας δεδομένων της ΕΕ, οι οργανισμοί που επεξεργάζονται δεδομένα, πρέπει να έχουν νομική βάση για να το πράξουν και η

[46] Βλ. αιτιολογική σκέψη 116 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ)

μεταφόρτωση δεδομένων στο σύννεφο αποτελεί ένα είδος επεξεργασίας στην Ευρωπαϊκή Ένωση. Αν και υπάρχει μια ποικιλία πιθανών νομικών βάσεων, στο πλαίσιο του υπολογιστικού νέφους, ένα χρηματοπιστωτικό ίδρυμα πιθανότατα βασίζεται στη συγκατάθεση των υποκειμένων των δεδομένων και στην εκπλήρωση της σύμβασης. Όμως, η απόκτηση συναίνεσης του υποκειμένου των δεδομένων αναπόφευκτα θα ήταν επαχθής και σε κάθε περίπτωση, εγείρει σημαντικά νομικά ζητήματα στην Ευρώπη. Για παράδειγμα, για να είναι έγκυρη βάσει της νομοθεσίας της ΕΕ, η συγκατάθεση πρέπει να παρέχεται ελεύθερα και να είναι συγκεκριμένη ως προς το είδος της επεξεργασίας δεδομένων (Sotto, Treacy, & McLellan, 2010).

### *6.3.4 Δικαιώματα Υποκειμένου Επεξεργασίας Δεδομένων*

Ο Γενικός Κανονισμός Προστασίας Δεδομένων ορίζει τα δικαιώματα του υποκειμένου σχετικά με την επεξεργασία των δεδομένων του από άλλους φορείς. Ο ΓΚΠΔ δεν περιλαμβάνει ειδική ρύθμιση σε περιπτώσεις επεξεργασίας των δεδομένων του υποκειμένου, μέσω του υπολογιστικού νέφους. Το τραπεζικό ίδρυμα πρέπει να γνωστοποιήσει τα δικαιώματα αυτά στους νέους πελάτες του και να τα ενσωματώσει στην πολιτική απορρήτου για την προστασία των δεδομένων που επεξεργάζονται. Τα δικαιώματα αυτά είναι:

1. Δικαίωμα ενημέρωσης[47]: Το τραπεζικό ίδρυμα είναι υποχρεωμένο να ενημερώσει το υποκείμενο των δεδομένων για τον σκοπό και τους λόγους της επεξεργασίας των δεδομένων του.
2. Δικαίωμα πρόσβασης[48]: Ο πελάτης έχει το δικαίωμα να ζητήσει από το τραπεζικό ίδρυμα επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που τον αφορούν υφίστανται επεξεργασία και, εάν συμβαίνει αυτό, έχει το δικαίωμα πρόσβασης σε αυτά.
3. Δικαίωμα διόρθωσης[49]: Ο πελάτης έχει το δικαίωμα της διόρθωσης των δεδομένων έπειτα από αίτηση στο τραπεζικό ίδρυμα.
4. Δικαίωμα διαγραφής «δικαίωμα «τη λήθη»[50]: Με την επιφύλαξη ορισμένων περιορισμών, τα άτομα έχουν θεμελιώδες δικαίωμα σύμφωνα με τη

[47] Άρθρο 12 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016

[48] Άρθρο 15 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016

[49] Άρθρο 16 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016

νομοθεσία περί προστασίας δεδομένων της Ευρωπαϊκής Ένωσης για πρόσβαση, αποκλεισμό, διόρθωση ή διαγραφή των προσωπικών τους δεδομένων. Λόγω της τεχνικής ρύθμισης μιας υποδομής υπολογιστικού νέφους, ενδέχεται να είναι δύσκολο να διασφαλιστεί ότι η διαχείριση των αιτημάτων πρόσβασης, αποκλεισμού, διόρθωσης ή διαγραφής γίνεται αποτελεσματικά και σωστά. Μια συμφωνία παροχής υπηρεσιών θα πρέπει να αντιμετωπίσει αυτό το ζήτημα συγκεκριμένα.

5. Δικαίωμα περιορισμού της επεξεργασίας[51]: Εφόσον συντρέχουν συγκεκριμένες προϋποθέσεις, ο πελάτης έχει το δικαίωμα του περιορισμού της επεξεργασίας από το τραπεζικό ίδρυμα.
6. Δικαίωμα εναντίωσης[52]: Ο πελάτης έχει το δικαίωμα να αντιταχθεί, ανά πάσα στιγμή, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που τον αφορούν. Το χρηματοπιστωτικό ίδρυμα στην περίπτωση αυτή θα πρέπει να σταματήσει την επεξεργασία, εκτός και αν καταδείξει επιτακτικούς και νόμιμους λόγους οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του ως υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.
7. Δικαίωμα σε ανθρώπινη παρέμβαση στα πλαίσια απόφασης μέσω αυτοματοποιημένης διαδικασίας[53]: Ο πελάτης έχει το δικαίωμα να ζητήσει από την τράπεζα να μην υποβάλλετε, εφόσον συντρέχει περίπτωση, σε διαδικασία λήψης απόφασης αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που τον αφορούν ή τον επηρεάζει σημαντικά με παρόμοιο τρόπο.
8. Δικαίωμα φορητότητας[54]: Ο πελάτης έχει το δικαίωμα να ζητήσει από την τράπεζα να λάβει τα προσωπικά του δεδομένα, τα οποία έχει παράσχει, σε

[50] Άρθρο 17 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016

[51] Άρθρο 18 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016

[52] Άρθρο 21 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016

[53] Άρθρο 22 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016

[54] Άρθρο 20 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016

δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, ή να τα διαβιβάσει το τραπεζικό σύστημα σε άλλο πάροχο[55].

## 6.4 Ο ν. 4624/19: Προστασία προσωπικών δεδομένων και μέτρα εφαρμογής του ΓΚΠΔ

Η σημαντικότητα της ασφάλειας των πληροφοριακών συστημάτων είναι η διαφύλαξη του προσωπικού απορρήτου (privacy) των υποκειμένων των δεδομένων των οποίων οι εγγραφές διατηρούνται σε υπολογιστικά συστήματα των διαφόρων οργανισμών (Πάγκαλος & Μαυρίδης, 2002). Τα τραπεζικά πληροφοριακά συστήματα θα πρέπει να προσαρμόζονται σε πολιτικές προστασίας προσωπικών δεδομένων με κύριο γνώμονα την ασφάλεια των διαμοιραζόμενων πληροφοριών. Το γεγονός αυτό έφερε στο προσκήνιο την ανάγκη για τη θέσπιση μίας ρυθμιστικής αρχής, η οποία θα είχε ως απώτερο στόχο την προστασία των προσωπικών δεδομένων από με εγκεκριμένες μεθόδους επεξεργασίας τους. Για το σκοπό αυτό ιδρύθηκε στην Ελλάδα με τον Νόμο 2472/97 ως ανεξάρτητος διοικητικός φορέας η «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΧ)» που λειτουργεί από τον Νοέμβριο του 1997.

Στις 25 Μαΐου 2018 που τέθηκε σε εφαρμογή ο ΓΚΠΔ, άλλαξε το πλαίσιο προστασίας προσωπικών δεδομένων τόσο για τις επιχειρήσεις όσο και για τις τράπεζες. Έτσι κρίθηκε απαραίτητη η περαιτέρω ρύθμιση της προστασίας των προσωπικών δεδομένων με τη θέσπιση ενός νέου νόμου ο οποίος θα μπορούσε να αντικαταστήσει τον ν. 2472/97. Ο νέος νόμος 4624/19, θεσπίζει συμπληρωματικά μέτρα εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) και ενσωματώνει την οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου («Οδηγία LED»).

Ο νόμος 4624/19 προσδιορίζει το σκοπό και το πεδίο εφαρμογής του, ορίζοντας αυστηρώς τις υποχρεώσεις του υπεύθυνου επεξεργασίας δεδομένων καθώς επίσης και τις αρμοδιότητές του ως προς τους δημόσιους φορείς. Επιπλέον, ο νόμος αποτελείται από διατάξεις για την οργάνωση της Αρχής Προστασίας Προσωπικών Δεδομένων και θεσπίζει συμπληρωματικά μέτρα για την προστασία των υποκειμένων των δεομένων σε συναρτήσει με τον ΓΚΠΔ. Η επεξεργασία των προσωπικών δεδομένων από τα τραπεζικά ΠΣ της ΤΕΙΡΕΣΙΑΣ Α.Ε., πραγματοποιείται στο πλαίσιο τήρησης των διατάξεων τόσο του ΓΚΠΔ όσο και του εφαρμοστέου εθνικού ν. 4624/19. Κατ' αυτόν τον τρόπο τα

[55] Βλ. αιτιολογική σκέψη 68 του ΓΚΠΔ

πληροφοριακά συστήματα της ΤΕΙΡΕΣΙΑΣ Α.Ε. πρέπει να παρέχουν πρόσθετα μέτρα ασφαλείας για την προστασία των προσωπικών δεδομένων των υποκειμένων. Ο εν λόγω νόμος επιφέρει σημαντικούς περιορισμούς για τα δικαιώματα των υποκειμένων των δεδομένων και συγκεκριμένα περιορίζεται η άσκηση του δικαιώματος πρόσβασης[56] του υποκειμένου όταν δεν υφίσταται η υποχρέωση ενημέρωσης τους από τον υπεύθυνο επεξεργασίας δεδομένων. Βέβαια ο περιορισμός της ενημέρωσης και η παράλειψη της συγκατάθεσης του υποκειμένου σχετικά με το σκοπό επεξεργασίας των δεδομένων του, από τον υπεύθυνο επεξεργασίας,[57] πραγματοποιείται μόνο σε κρίσιμες καταστάσεις όπως για την προστασία των έννομων συμφερόντων τρίτων[58] προσώπων.

Για την προστασία των υποκειμένων από την αθέμιτη επεξεργασία των δεδομένων του, ο ν. 4624/19, ενίσχυσε τη θέση του ως προς την τήρηση των καθηκόντων της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και την επιβολή αυστηρών κυρώσεων σε φορείς επεξεργασίας προσωπικών δεδομένων μέσα από ποινικές (άρθρο 81) και διοικητικές κυρώσεις (άρθρο 82). Τέλος ο νέος νόμος παρέχει στο υποκείμενο των δεδομένων δικαστική προστασία έναντι του υπεύθυνου και του εκτελούντος την επεξεργασίας, δίνοντάς του τη δυνατότητα προσφυγής σε αρμόδιο δικαστήριο του τόπου διαμονής του.

## 6.5 Ασφάλεια και προστασία προσωπικών δεδομένων

Η νομοθεσία της Ευρωπαϊκής Ένωσης για την προστασία των δεδομένων απαιτεί από τους υπευθύνους επεξεργασίας δεδομένων να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των προσωπικών δεδομένων από (1) τυχαία ή παράνομη καταστροφή ή απώλεια των δεδομένων, (2) μη εξουσιοδοτημένη αλλοίωση, αποκάλυψη ή πρόσβαση (ιδίως όταν η επεξεργασία περιλαμβάνει τη μετάδοση δεδομένων μέσω δικτύου) και (3) όλες τις άλλες παράνομες μορφές επεξεργασίας. Κατά την εφαρμογή αυτής της ευρείας απαίτησης στο υπολογιστικού νέφος (cloud computing), υπάρχουν ορισμένα σημεία που πρέπει να λάβουν υπόψη τα χρηματοπιστωτικά

[56] Νόμος 4624/19 αρ. 55 (ενσωμάτωση των άρθρων 14 και 15 της Οδηγίας)

[57] Βλ. επίσης τα Συστήματα Αθέτησης Υποχρεώσεων (ΣΑΥ) της ΤΕΙΡΕΣΙΑΣ Α.Ε., όπου δεν είναι απαραίτητη η συγκατάθεση του υποκειμένου σχετικά με τη καταχώρηση τους στο εν λόγω σύστημα (Αλεξανδροπούλου-Αιγυπτιάδου & Μυλώση, 2015).

[58] Νόμος 4624/19 αρ. 54 (ενσωμάτωση του άρθρου 14 της Οδηγίας)

ιδρύματα, συμπεριλαμβανομένου του γεγονότος ότι η χρήση ενός παρόχου υπολογιστικού νέφους αυξάνει τις πιθανότητες μη εξουσιοδοτημένης αποκάλυψης ή πρόσβασης κακόβουλων χρηστών (Sotto, Treacy, & McLellan, 2010). Κατά συνέπεια, οι έλεγχοι ταυτότητας και πρόσβασης πρέπει να είναι ισχυροί και να παρέχουν κατάλληλο επίπεδο ασφάλειας, λόγω του αυξημένου επιπέδου πρόσβασης του κοινού στο σύννεφο, ο κίνδυνος παραβίασης της ασφάλειας πληροφοριών είναι αντίστοιχα υψηλότερος, επομένως ο πάροχος του νέφους είναι υποχρεωμένος, μέσω της σύμβασης, να ενημερώνει το τραπεζικό ίδρυμα για τυχόν περιστατικά παραβίασης δεδομένων.

## 6.6 Βιωσιμότητα Υπολογιστικού Νέφους και ρύθμιση

Ένα τραπεζικό ίδρυμα για τη μεταφορά των ενημερωτικών του πόρων στο σύννεφο, σημαντικό ρόλο παίζει η μακροζωία και η βιωσιμότητα του παρόχου υπολογιστικού νέφους. Στα τραπεζικά ιδρύματα, οι επιπτώσεις από την διακοπή της συνεργασίας με τον πάροχο υπολογιστικού νέφους μπορεί να επιφέρει καταστροφικά αποτελέσματα, εάν η σύμβαση παροχής υπηρεσιών λήξει απότομα ως αποτέλεσμα της αφερεγγυότητας του παρόχου. Χωρίς στρατηγική της τράπεζας, οι πελάτες θα είναι απρόθυμοι να μεταφέρουν τα δεδομένα τους στο σύννεφο (Bose, Luo & Liu, 2013). Το υπολογιστικό νέφος θα πρέπει να αντιμετωπίσει το ζήτημα της μακροπρόθεσμης βιωσιμότητας, όπως συμβαίνει με την πτώχευση του τραπεζικού ιδρύματος όπου οι πελάτες είναι εγγυημένοι ότι θα ανακτήσουν τα χρήματά τους .

Ανεξάρτητα από την πολιτιστική και πολιτική διακυβέρνηση, οι κανονισμοί σε όλο τον κόσμο αποκτούν ζωτική σημασία για τη δημιουργία ενός αξιόπιστου νομικού και ασφαλούς πλαισίου για τις τραπεζικές συναλλαγές, όπως οι γενικοί κανόνες για την ασφάλεια των τραπεζικών καταθέσεων και οι κανονισμοί για την ασφάλεια των διαδικτυακών τραπεζών. Σε σύγκριση με τον τραπεζικό τομέα, υπάρχουν λιγότεροι κανονισμοί και πρότυπα σχετικά με το τμήμα του υπολογιστικού νέφους. Πολλοί κανονισμοί, όπως οι Ομοσπονδιακοί Κανόνες Πολιτικής Δικονομίας, ο Νόμος περί Απορρήτου των Ηλεκτρονικών Επικοινωνιών, ο Ομοσπονδιακός Νόμος Διαχείρισης Ασφάλειας Πληροφοριών των ΗΠΑ, ο νόμος Gramm-Leach-Bliley, ο Γενικός Κανονισμός Προστασίας Δεδομένων για την προστασία δεδομένων της Ευρωπαϊκής Ένωσης και ούτω καθεξής, δεν έχουν ενημερωθεί ακόμη για την αντιμετώπιση των μοναδικών προβλημάτων ενός τομέα υπολογιστικού νέφους. Συγκεκριμένα, η έλλειψη

κοινών προτύπων ασφαλείας κάνει τους παρόχους υπηρεσιών να καταφεύγουν σε υπάρχοντα πρότυπα (π.χ. ISO 27001) που δεν είχαν καθοριστεί για τη χρήση του σύννεφου.

Για την προώθηση της ασφάλειας του σύννεφου και τη συμμόρφωση με τα βιομηχανικά πρότυπα, αναμένεται να καταβληθούν συντονισμένες προσπάθειες για τη δημιουργία κανονιστικών προτύπων του υπολογιστικού νέφους (cloud computing). Ενώ το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST) των ΗΠΑ δημιούργησε μια ομάδα ασφάλειας υπολογιστικού νέφους, άλλοι οργανισμοί όπως το ISO, το Cloud Security Alliance και το CloudAudit εργάζονται επίσης για τη δημιουργία ρυθμιστικών προτύπων της τεχνολογίας του σύννεφου. Τελικά, οι πάροχοι του υπολογιστικού νέφους θα καταλήξουν σε συμφωνίες για κρίσιμα ζητήματα, όπως πρότυπα, διαλειτουργικότητας και προγράμματα υποστήριξης τρίτων, κ.λπ. Με τη σειρά τους, τραπεζικά ιδρύματα θα πρέπει να είναι σε θέση να παρακολουθούν τους παρόχους υπηρεσιών νέφους, ώστε να πληρούν τις κανονιστικές απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) (Bose, Luo & Liu, 2013).

## 6.7 Αρχή Προστασίας των Προσωπικών Δεδομένων

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), λαμβάνει μέτρα εφαρμογής του κανονισμού 679/2016 (ΓΚΠΔ) με τον ν. 4624/19. Η εποπτική αρχή ορίζει τις υποχρεώσεις του υπεύθυνου και του εκτελών την επεξεργασία για την αποτελεσματική διαχείριση των δεδομένων των φυσικών προσώπων. Στην παρούσα υπό ενότητα θα εξετάσουμε μερικές από της αποφάσεις της αρχής σχετικά με την επεξεργασία των δεδομένων του υποκειμένου και την ασφάλεια των πληροφοριακών συστημάτων στον τραπεζικό τομέα. Η παρουσίαση των εν λόγω αποφάσεων έχει ως στόχο την κατανόηση των ευθυνών του υπεύθυνου και του εκτελούντος την επεξεργασία σε δεδομένα τα οποία είναι διαθέσιμα μέσω των τραπεζικών πληροφοριακών συστημάτων.

### *6.7.1 Αποφάσεις Αρχής*

Α Π Ο Φ Α Σ Η ΑΡ. 185 / 2014[59]

Με το υπ' αριθμ. πρωτ. ΓΝ/ΕΙΣ/1136/10-06-2014 έγγραφό της, η εταιρεία ΤΕΙΡΕΣΙΑΣ Α.Ε. γνωστοποιεί στην Αρχή τη λειτουργία του συστήματος με την ονομασία «Τειρεσίας Σύστημα Ελέγχου Κινδύνων» (ΤΣΕΚ)[60]. Η εταιρεία ΤΕΙΡΕΣΙΑΣ Α.Ε. παρέχει σε επιχειρηματίες φυσικά και νομικά πρόσωπα (αποδέκτες), τη δυνατότητα πρόσβασης σε δεδομένα οικονομικής συμπεριφοράς φυσικών και νομικών προσώπων.[61] Η αρχή έκρινε ότι σύμφωνα με το άρθρο 4 παρ. 1 στοιχ. α΄ του ν. 2472/1997, *«τα δεδομένα πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών».*

Επισημαίνεται δε ότι, σύμφωνα με την παρ. 4 της απόφασης 24/2004, «***Αποδέκτες των δεδομένων, σύμφωνα με τον σκοπό της επεξεργασίας δικαιολογείται να είναι μόνο οι τράπεζες, τα χρηματοπιστωτικά ιδρύματα και οι εταιρείες διαχείρισης πιστωτικών καρτών, καθώς και φορείς του δημόσιου τομέα, όχι τρίτοι μετέχοντες στις οικονομικές συναλλαγές και ακόμη λιγότερο μη μετέχοντες***. Ο διαμοιρασμός των δεδομένων από το διατραπεζικό πληροφοριακό σύστημα ΤΣΕΚ, επέκτεινε της δραστηριότητά του ΤΕΙΡΕΣΙΑ Α.Ε. με αποτέλεσμα τα δεδομένα να μεταβιβάζονται σε τρίτα φυσικά πρόσωπα τα οποία δεν περιλαμβανόταν στην ως άνω λίστα, με κύριο σκοπό την εξέταση, παρανόμως της πιστοληπτικής ικανότητας των

[59] https://www.dpa.gr/portal/page?_pageid=33%2C15453&_dad=portal&_schema=PORTAL&_piref33_15473_33_15453_15453.etos=2014&_piref33_15473_33_15453_15453.arithmosApofasis=185&_piref33_15473_33_15453_15453.thematikiEnotita=133&_piref33_15473_33_15453_15453.ananeosi=%CE%91%CE%BD%CE%B1%CE%BD%CE%AD%CF%89%CF%83%CE%B7

[60] Σκοπός του συστήματος αυτού είναι η παροχή πληροφοριών οικονομικής συμπεριφοράς για την διαπίστωση της πιστοληπτικής ικανότητας πάσης φύσεως επιχειρήσεων.

[61] Απόφαση αρ. 185/2014 – «*Πρόσβαση στα ως άνω δεδομένα μπορούν πλέον να έχουν, κατά δήλωση της αιτούσας, εκτός των νομικών προσώπων, και φυσικά πρόσωπα ή ενώσεις προσώπων του Αστικού Κώδικα που ασκούν εμπορική, βιομηχανική, βιοτεχνική, γεωργική ή άλλη επιχείρηση στην Ελληνική Επικράτεια ή σε άλλη χώρα του Ευρωπαϊκού Οικονομικού Χώρου και την Ελβετία, προκειμένου να αντλούν δεδομένα για τα φυσικά ή νομικά πρόσωπα, με τα οποία συναλλάσσονται με πίστωση και, συνεπώς, αναλαμβάνουν σχετικό πιστωτικό κίνδυνο, ώστε αφενός καθίσταται απαραίτητος ο έλεγχος της φερεγγυότητας των αντισυμβαλλομένων τους και αφετέρου είναι προφανές το έννομο συμφέρον πρόσβασης στην συγκεκριμένη υπηρεσία.*»

υποκειμένων των δεδομένων. Η αρχή σημείωσε ότι «*Επιπροσθέτως, στο αρχείο ΤΣΕΚ τηρούνται και διατίθενται προς εμπορία στοιχεία ακάλυπτων επιταγών/συναλλαγματικών κάνοντας χρήση των αρχείων ΣΑΥ και ΣΥΠ της εταιρείας, ενώ σύμφωνα με την απόφαση 71/2001 της Αρχής, μπορούν να διαβιβάζονται νόμιμα σε εταιρείες διαπίστωσης πιστοληπτικής ικανότητας μόνο τα στοιχεία που έχει η κάθε μία τράπεζα στο δικό της αρχείο και όχι αυτά που μπορεί να έχει πρόσβαση μέσω του διατραπεζικού συστήματος ΤΕΙΡΕΣΙΑΣ*[62]». Κατ' αυτόν τον τρόπο ο σκοπός της επεξεργασίας δεδομένων οικονομικής συμπεριφοράς του πληροφοριακού συστήματος ΤΣΕΚ είναι παράνομος διότι η αρχική του δήλωση περί επεξεργασίας δεδομένων δε συνάδει με τον τελικό σκοπό του συστήματος.

Εκτός από την παράνομη διαμοίραση των δεδομένων οικονομικής συμπεριφοράς σε τρίτα πρόσωπα, η εταιρεία ΤΕΙΡΕΣΙΑΣ Α.Ε. δεν ενημέρωσε εγκαίρως την αρχή και το υποκείμενο των δεδομένων: «*Η εν λόγω επεξεργασία γνωστοποιήθηκε στην Αρχή μετά την έναρξή της και, ειδικότερα, όσον αφορά επεξεργασία δεδομένων φυσικών προσώπων, έξι μήνες αργότερα (Ιούνιος 2014). Ως εκ τούτου, υπάρχει μη έγκαιρη γνωστοποίηση κατά παράβαση του άρθρου 6 του ν. 2472/1997*».

Έτσι, η αρχή απεφάνθη ότι:

1. με τη λειτουργία του συστήματος ΤΣΕΚ, η ΤΕΙΡΕΣΙΑΣ Α.Ε. διεύρυνε παρανόμως τον σκοπό επεξεργασίας των δεδομένων του αρχείου της, υπέβαλε τη σχετική γνωστοποίηση στην Αρχή με σημαντική χρονική καθυστέρηση και δεν ενημέρωσε προσηκόντως τα υποκείμενα των δεδομένων για τη μεταβολή αυτή
2. κι επιβάλλει στην ΤΕΙΡΕΣΙΑΣ Α.Ε., ως υπεύθυνο επεξεργασίας, πρόστιμο ύψους εβδομήντα πέντε χιλιάδων (75.000) Ευρώ για τις ως άνω διαπιστωθείσες παραβάσεις.

Συμπερασματικά η αρχή, με την εν λόγω απόφαση της, επαναλαμβάνει τις προϋποθέσεις λειτουργίας του πληροφοριακού συστήματος ΤΣΕΚ, σχετικά με τη

[62] Απόφαση αρ. 185/2014 – «*Ισχυρισμός της ΤΕΙΡΕΣΙΑΣ ΑΕ ότι ο σκοπός λειτουργίας του συστήματος «ΤΣΕΚ» είναι ο αυτός που η εταιρεία επιδιώκει ως διατραπεζική εταιρεία που λειτουργεί χάριν των πιστωτικών και χρηματοδοτικών ιδρυμάτων είναι αβάσιμος, όπως αβάσιμος είναι και ο περαιτέρω ισχυρισμός ότι νομίμως γίνεται διαχωρισμός μεταξύ των διαβιβαζόμενων πληροφοριών πιστοληπτικής ικανότητας στο χρηματοπιστωτικό σύστημα και των μη προβλεπομένων από τον σκοπό διαβιβαζομένων πληροφοριών σε νομικά και φυσικά πρόσωπα*».

συλλογή των δεδομένων και τον έλεγχο της ακρίβειάς τους, υπενθυμίζοντας την υποχρέωση του υπεύθυνου επεξεργασίας για ενημέρωση των υποκειμένων των δεδομένων όσον αφορά την αλλαγή του σκοπού επεξεργασίας των δεδομένων τους. Επίσης η Αρχή επισημαίνει τη λήψη των αναγκαίων μέτρων ασφαλείας για τη νόμιμη λειτουργία του αρχείου της ΤΕΙΡΕΣΙΑΣ Α.Ε. (Αλεξανδροπούλου-Αιγυπτιάδου & Μυλώση, 2015).

Α Π Ο Φ Α Σ Η ΑΡ. 64 / 2015[63]

Η Αρχή πραγματοποίησε επιτόπιο έλεγχο στην εταιρεία «ICAP GROUP ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΗ ΠΛΗΡΟΦΟΡΗΣΗ ΣΥΜΒΟΥΛΟΙ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΥΠΗΡΕΣΙΕΣ ΠΡΟΣ ΕΠΙΧΕΙΡΗΣΕΙΣ», αναφορικά με την προστασία των προσωπικών δεδομένων που επεξεργάζεται η εν λόγω εταιρεία για τον σκοπό του ελέγχου της πιστοληπτικής ικανότητας επιχειρήσεων. Η ICAP απέστειλε έγγραφο στην ΤΕΙΡΕΣΙΑΣ Α.Ε. ζητώντας πληροφορίες για είκοσι τρεις κωδικούς χρήστη με πρόσβαση στις εφαρμογές της εν λόγω εταιρείας που βρέθηκε να χρησιμοποιούνται από την ICAP[64].

Συγκεκριμένα η εταιρεία ICAP ζήτησε από την ΤΕΙΡΕΣΙΑΣ Α.Ε., για λογαριασμό της τράπεζας ALPHA BANK, αναλυτικά στοιχεία των προσβάσεων που πραγματοποιήθηκαν κατά το μήνα Μάρτιο του έτους 2013 σε δεδομένα Οικονομικών Μονάδων της Τειρεσίας Α.Ε. από όλους τους λογαριασμούς που είχαν αποδοθεί στην Alpha Bank και χρησιμοποιήθηκαν από την εταιρεία ICAP. Από τα στοιχεία αυτά προκύπτει πρόσβαση σε στοιχεία τόσο του συστήματος ΣΑΥ/ΣΥΠ όσο και του συστήματος ΣΣΧ. Συγκεκριμένα, σε σύνολο 11.190 προσβάσεων σε στοιχεία φυσικών προσώπων έγινε πρόσβαση σε στοιχεία ΣΣΧ σε 6.322 περιπτώσεις.

---

[63] https://www.dpa.gr/portal/page?_pageid=33%2C15453&_dad=portal&_schema=PORTAL&_piref33_15473_33_15453_15453.etos=2015&_piref33_15473_33_15453_15453.arithmosApofasis=64&_piref33_15473_33_15453_15453.thematikiEnotita=133&_piref33_15473_33_15453_15453.ananeosi=%CE%91%CE%BD%CE%B1%CE%BD%CE%AD%CF%89%CF%83%CE%B7

[64] Απόφαση Αρχής 65/2015 – *«Συγκεκριμένα: α) Τα πλήρη στοιχεία των χρηστών στους οποίους έχουν αποδοθεί οι κωδικοί και τυχόν ιστορικό αλλαγών. β) Τις ημερομηνίες ενεργοποίησης και τα αντίστοιχα αιτήματα για την ενεργοποίηση των κωδικών. γ) Τα αποδοθέντα δικαιώματα πρόσβασης για τους κωδικούς από την ημερομηνία ενεργοποίησής τους έως και σήμερα. δ) Στατιστικά στοιχεία για τον αριθμό των καταγεγραμμένων προσβάσεων που έχουν πραγματοποιηθεί από τους κωδικούς αυτούς για το χρονικό διάστημα από την αρχή του έτους έως και την ημέρα του εγγράφου».*

Έτσι η αρχή με βάση της τους νόμους:

1. Στο άρθρο 2 στοιχ. α΄, γ΄, ζ΄, η΄ και ι΄ του ν. 2472/1997, όπως ισχύει, ορίζονται οι έννοιες των «απλών» δεδομένων, του υποκειμένου αυτών, του υπεύθυνου επεξεργασίας, του εκτελούντος την επεξεργασία και του αποδέκτη αντίστοιχα. Τα μέτρα ασφάλειας πρέπει α) να διασφαλίζουν ότι τα δεδομένα χρησιμοποιούνται μόνον για τον εκάστοτε επιδιωκόμενο σκοπό και β) να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας.
2. Η πρόσβαση των τραπεζών στα δεδομένα του Συστήματος Συγκέντρωσης Χορηγήσεων (εφεξής «ΣΣΧ» - λευκή λίστα) της ΤΕΙΡΕΣΙΑΣ Α.Ε. επιτρέπεται μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων[65] σύμφωνα με το άρθρο 5 παρ. 1 σε συνδυασμό με τη διάταξη του άρθρου 40 του ν. 3259/2004 παρ. 2 εδ. β΄, όπως ισχύει.
3. Η πρόσβαση των τραπεζών στα δεδομένα του Συστήματος Αθέτησης Υποχρεώσεων & Συστήματος Υποθηκών – Προσημειώσεων (εφεξής «ΣΑΥ/ΣΥΠ» - μαύρη λίστα) επιτρέπεται χωρίς συγκατάθεση του υποκειμένου των δεδομένων, ως επεξεργασία απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος τους, σύμφωνα με το άρθρο 5 παρ. 2 στοιχ. ε΄ του ν. 2472/1997 σε συνδυασμό με τις Κανονιστικές Αποφάσεις 24/2004 και 25/2004 της Αρχής.
4. Οι υπάλληλοι της ICAP είχαν πρόσβαση στην ηλεκτρονική εφαρμογή της ΤΕΙΡΕΣΙΑΣ Α.Ε. για χρονικό διάστημα τουλάχιστον τριών ετών (2011 έως και τέλος του 2013, οπότε και διακόπηκε η πρόσβαση). Η πρόσβαση γινόταν με χρήση συγκεκριμένων κωδικών που έχουν εκδοθεί από την

[65] Απόφαση 65/2015 – «*Επιτρέπεται στα πιστωτικά και χρηματοδοτικά ιδρύματα η διαβίβαση προς καταχώριση δεδομένων επί των εκάστοτε ανεξόφλητων υπολοίπων δανείων ή και πιστώσεων, περιλαμβανομένων και των υφιστάμενων, που χορηγούν σε φυσικά ή νομικά πρόσωπα ή ενώσεις προσώπων, σε αρχείο δεδομένων οικονομικής συμπεριφοράς που λειτουργεί νόμιμα, χάριν αυτών, χωρίς την προϋπόθεση του άρθρου 5 παρ. 1 του ν. 2472/1997 (ΦΕΚ 50 Α΄). Η πρόσβαση των πιστωτικών και χρηματοδοτικών ιδρυμάτων στα ως άνω δεδομένα επιτρέπεται μόνο κατά τους όρους και προϋποθέσεις του ν. 2472/1997, όπως εκάστοτε ισχύει και εφαρμόζεται*».

ΤΕΙΡΕΣΙΑΣ Α.Ε. για την ALPHA BANK και αποδοθεί από την ALPHA BANK στην ICAP[66].

5. Στη φόρμα αίτησης νέου κωδικού για πρόσβαση στο σύστημα της ΤΕΙΡΕΣΙΑΣ δεν γίνεται διαφοροποίηση ως προς τις υπηρεσίες πρόσβασης στα στοιχεία ΣΑΥ/ΣΥΠ και ΣΣΧ[67].

Με βάση τα παραπάνω συμπεραίνουμε ότι η ΤΕΙΡΕΣΙΑΣ Α.Ε., δεν είχε λάβει τα κατάλληλα μέτρα προστασίας των πληροφοριακών της συστημάτων με αποτέλεσμα να υπάρχει ανεπιθύμητη πρόσβαση κι επεξεργασία των δεδομένων των φυσικών προσώπων που αφορούσαν τη συνεργασία τους με την ALPHA BANK. Επίσης η ΤΕΙΡΕΣΙΑΣ δεν προέβλεψε τον απόλυτο διαχωρισμό των δεδομένων ανάλογα τον σκοπό της επεξεργασίας με αποτέλεσμα η ICAP να έχει πρόσβαση και σε άλλα δεδομένα, όπου υπό κανονικές συνθήκες δε θα έπρεπε να είχε. Τέλος, Οι χειριστές της ICAP είχαν δικαιώματα για πλήρη πρόσβαση σε στοιχεία αναζήτησης οικονομικών μονάδων που περιλαμβάνουν και φυσικά πρόσωπα. Αυτό είχε ως συνέπεια, ο αριθμός των μοναδικών προσβάσεων των χρηστών της ICAP στο σύστημα της ΤΕΙΡΕΣΙΑΣ Α.Ε. να είναι μεγαλύτερος σε σχέση με τον αριθμό των πελατών της ALPHA BANK, για τους οποίους η Τράπεζα ζήτησε και έλαβε υπηρεσίες από την ICAP[68].

Στην προκειμένη περίπτωση η Αρχή, *«λαμβάνοντας υπόψη τη βαρύτητα των παραβάσεων των άρθρων 4, 5 και 10 του ν. 2472/1997 που αποδείχθηκαν, όπως αυτή εκτέθηκε αναλυτικά ανωτέρω, κρίνει ότι πρέπει να επιβληθούν στην ΤΕΙΡΕΣΙΑΣ Α.Ε., ως υπεύθυνο επεξεργασίας, για κάθε μία από τις παραβάσεις αυτές, οι προβλεπόμενες στο άρθρο 21 παρ. 1 εδαφ. α΄ και β΄ του ν. 2472/1997 κυρώσεις που αναφέρονται στο διατακτικό και οι οποίες τυγχάνουν ανάλογες με τη βαρύτητα ων παραβάσεων».*

Κατ' αυτόν τον τρόπο η Αρχή, επέβαλλε στην ΤΕΙΡΕΣΙΑΣ Α.Ε.:

1. Πρόστιμο ύψους 30.000 (τριάντα χιλιάδων) για παράλειψη λήψης μέτρων κατά τη διάθεση/χορήγηση δεδομένων των αρχείων ΣΑΥ/ΣΥΠ και ΣΣΧ στην ICAP (μέσω παροχής πρόσβασης στα αρχεία αυτά)

---

[66] *Εύρημα 1 Αρχής: Πρόσβαση της ελεγχόμενης σε δεδομένα προσωπικού χαρακτήρα που τηρούνται από την ΤΕΙΡΕΣΙΑΣ Α.Ε.. Καταχώριση και επεξεργασία αυτών χωρίς κάποια μορφή διαχωρισμού. Χρήση των δεδομένων για σκοπούς άλλους από τη σύμβαση με την Alpha Bank.*

[67] *Εύρημα 2 Αρχής: Μη διαφοροποίηση της πρόσβασης πληροφοριών ΣΑΥ – ΣΥΠ – ΣΣΧ (Ευθύνη της ΤΕΙΡΕΣΙΑΣ Α.Ε.)*

[68] Βλ. στοιχεία που απέστειλαν στην Αρχή η ΤΕΙΡΕΣΙΑΣ ΑΕ και η ALPHA BANK με τα υπ' αριθμ. πρωτ. Γ/ΕΙΣ/5639/03-09-2013 και Γ/ΕΙΣ/7234/14-11-2013 έγγραφά τους, αντίστοιχα

2. Προειδοποίηση να τροποποιήσει τα δικαιώματα πρόσβασης στα αρχεία ΣΑΥ/ΣΥΠ και ΣΣΧ εντός τριμήνου από τη λήψη της παρούσας σύμφωνα με τον τρόπο που περιγράφεται στο σκεπτικό της.

## 6.8 Σύνοψη

Το υπολογιστικό νέφος (cloud computing) ως νέο πρότυπο τεχνολογίας πληροφορικής, βρίσκεται ακόμη στο αρχικό στάδιο ανάπτυξής του. Τα πλεονεκτήματα του υπολογιστικού νέφους είναι προφανή, αλλά εξακολουθούν να υπάρχουν πολλές αμφιβολίες για την υιοθέτησή του για πρακτική εφαρμογή σε διαφορετικές βιομηχανίες. Ο κλάδος των χρηματοοικονομικών υπηρεσιών είναι ένας από τους κλάδους που μπορούν να δεχτούν την πιο πρόσφατη τεχνολογία, χάρη στην ευελιξία, τα κεφάλαια που διαθέτουν και την προθυμία τους να μειώσουν το κόστος σε τεχνολογίες διαχείρισης κι επεξεργασίας δεδομένων. Ωστόσο, αυτός ο κλάδος έχει τις αυστηρότερες απαιτήσεις για το απόρρητο των δεδομένων, την ασφάλεια και την αξιοπιστία, οι οποίες προειδοποιούν τα χρηματοπιστωτικά ιδρύματα για την αποτελεσματική εφαρμογή του νέφους στις τραπεζικές τους υπηρεσίες (Wenge, Lampe, Müller & Schaarschmidt, 2014).

Φαίνεται ότι τα χρηματοπιστωτικά ιδρύματα επικεντρώνονται τόσο σε νομικές όσο και σε τεχνικές λύσεις για την προστασία του απορρήτου των δεδομένων. Ωστόσο, οι δυνατότητες για την εφαρμογή του υπολογιστικού νέφους, εμφανίζονται σε όλες τις επιχειρηματικές διαδικασίες του χρηματοπιστωτικού κλάδου, δηλαδή στην επεξεργασία δεδομένων κι εάν αυτή προστατεύεται επαρκώς από διαρροές, απώλειες και υποκλοπή, όπως ορίζεται σε πολλές κανονιστικές απαιτήσεις της ΕΕ.

Στην Ευρωπαϊκή Ένωση, τα τραπεζικά συμβούλια πρέπει να ενημερώνονται για ζητήματα που επηρεάζουν τη προστασία των δεδομένων των πελατών, συμπεριλαμβανομένων θεμάτων που σχετίζονται με το απόρρητο των πελατών και την ασφάλεια των δεδομένων τους. Στις ευρωπαϊκές χώρες, πρέπει να συνάπτεται επίσημη συμφωνία μεταξύ του τραπεζικού ιδρύματος και του πελάτη για την εξασφάλιση της προστασίας των δεδομένων του από μη αθέμιτη επεξεργασία. Ανάλογα με τη δικαιοδοσία, τα χρηματοπιστωτικά ιδρύματα ενδέχεται να είναι ανθεκτικά στην εισαγωγή νέων τεχνολογιών (όπως το υπολογιστικό νέφος), που θα μπορούσαν να έχουν αντίκτυπο στην ιδιωτική ζωή των πελατών τους (Sotto, Treacy, & McLellan, 2010).

Τις παραπάνω ανησυχίες έρχεται να τις καλύψει ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ). Αν και οι διατάξεις του δεν ρυθμίζουν επακριβώς το θέμα του υπολογιστικού νέφους στις επιχειρήσεις ή στους οργανισμούς, παρέχει όμως τη δυνατότητα, μέσα από τις γενικές του διατάξεις, να ρυθμίσει τον τρόπο λειτουργίας των τραπεζικών ιδρυμάτων σχετικά με το απόρρητο και την προστασία των δεδομένων των πελατών τους.

# 7 Επίλογος

## 7.1 Συμπεράσματα

Το υπολογιστικό νέφος (cloud computing) είναι ένα μοντέλο επεξεργασίας πληροφοριών, αποθήκευσης και παράδοσης στο οποίο παρέχονται εξαιρετικά συγκεντρωτικοί φυσικοί πόροι σε απομακρυσμένους πελάτες κατόπιν αιτήματος στις τραπεζικές συναλλαγές. Αντί να αγοράζουν φυσικές συσκευές/διακομιστές, αποθηκευτικούς χώρους και εξοπλισμό δικτύωσης, οι πελάτες μισθώνουν αυτούς τους πόρους από έναν πάροχο υπολογιστικού νέφους ως υπηρεσία εξωτερικής ανάθεσης διαχείρισης δεδομένων. Με την κοινή χρήση της υποδομής μεταξύ των χρηστών του υπολογιστικού νέφους, ένας πάροχος νέφους μπορεί να εξισορροπήσει το φόρτο εργασίας, μειώνοντας το κόστος ανά μονάδα υπολογιστικού πόρου, δίνοντας στους πελάτες τη δυνατότητα κατανάλωσής τους. Το υπολογιστικό νέφος είναι ευέλικτο και φορητό, καθώς μπορεί να προσπελαστεί ανά πάσα στιγμή. Χρησιμοποιώντας ιστότοπους και εφεδρικό χώρο αποθήκευσης, οι πάροχοι υπολογιστικού νέφους μπορούν επίσης να παρέχουν μεγαλύτερη αξιοπιστία από τα τοπικά πληροφοριακά συστήματα (Shekhawat & Sharma, 2011).

Ωστόσο, πέρα από τα οφέλη του υπολογιστικού νέφους που παρέχει στους χρήστες του, στερεί από τους πελάτες τον άμεσο έλεγχο των συστημάτων που διαχειρίζονται τα δεδομένα τους, γεγονός που δημιουργεί ανησυχία στην επιλογή χρήσης του. Πώς μπορούν οι πελάτες της τράπεζας να εμπιστεύονται ότι ένας πάροχος νέφους θα προστατεύσει το απόρρητο των δεδομένων ή ότι θα λάβει τα κατάλληλα μέτρα ασφαλείας για την εμπόδιση ενδεχόμενης διαρροής δεδομένων; (Shekhawat & Sharma, 2011)

Υποστηρίζουμε ότι από μόνη της, η κρυπτογραφία και συνεπώς, οποιοδήποτε εργαλείο ασφάλειας προσωπικών δεδομένων, δεν μπορεί να λύσει το πρόβλημα διασφάλισης του απορρήτου δεδομένων στο νέφους. Ωστόσο, το μοντέλο διατήρησης της ιδιωτικότητας των φυσικών προσώπων, είναι ακριβώς αυτό, που τελικά χρειάζονται οι εφαρμογές υπολογιστικού νέφους για τη δημιουργία κοινοτικών ομάδων με δυνατότητες κοινωνικής δικτύωσης, κοινής χρήσης εγγράφων και ούτω καθεξής.

Στη παρούσα διπλωματική εργασία, διερευνήσαμε την προστασία της ιδιωτικής ζωής στις αρχιτεκτονικές υπολογιστικού νέφους σε συνδυασμό με τη χρήση των τραπεζικών πληροφοριακών συστημάτων. Ο Γενικός Κανονισμός Προστασίας

Δεδομένων (ΓΚΠΔ), έχει ως στόχο τη πλήρη διαμόρφωση του κώδικα δεοντολογίας των τραπεζικών ιδρυμάτων ώστε να συμβαδίζουν με τις κανονιστικές του διατάξεις. Με την εισαγωγή νέων μορφών επεξεργασίας δεδομένων, τα χρηματοπιστωτικά ιδρύματα άρχισαν να εφαρμόζουν το ιδιωτικό υπολογιστικό νέφος για την αποτελεσματικότερη προσπέλαση των δεδομένων. Ο διαχωρισμός του υπεύθυνου και του εκτελών την επεξεργασία, είναι εμφανής ανάλογα με το μοντέλο ανάπτυξης της αρχιτεκτονικής υπολογιστικού νέφους που εφαρμόζει το τραπεζικό ίδρυμα. Ο ΓΚΠΔ αν και δεν περιέχει σαφείς ορισμούς για την προστασία δεδομένων στο υπολογιστικό νέφος, μέσα από τις διατάξεις του, ρυθμίζει το ρόλο του τραπεζικού ιδρύματος είτε ως υπεύθυνος επεξεργασίας είτε ως εκτελών την επεξεργασία

## 7.2 Μελλοντικές Επεκτάσεις

Αν και υπάρχει μεγάλη έρευνα και πρόοδος στον τομέα του υπολογιστικού νέφους, πολλά έργα έχουν υψηλό ποσοστό αποτυχίας ιδιαίτερα όταν σχετίζεται με τον τραπεζικό τομέα. Ωστόσο, αρκετά σοβαρά ζητήματα ασφάλειας στο σύννεφο, όπως η προστασία δεδομένων, η ακεραιότητα, η ποιότητα των υπηρεσιών, η φορητότητα των δεδομένων και η διαλειτουργικότητα, πρέπει να ελεγχθούν πριν το υπολογιστικό νέφος εφαρμοστεί σε ευρεία κλίμακα από τα χρηματοπιστωτικά ιδρύματα (Elzamly, Hussin, Abu-Naser, Shibutani & Doheir, 2017). Επιπλέον, το σύννεφο έχει πολλά πλεονεκτήματα, αλλά η εφαρμογή του σε τραπεζικούς οργανισμούς πάσχει από πολλά προβλήματα ασφάλειας. Ο στόχος της διαχείρισης κινδύνου του νέφους είναι ο προσδιορισμός και η αξιολόγηση των θεμάτων ασφάλειας σε πρώιμο στάδιο για την αποτελεσματικότερη πρόβλεψη των κινδύνων που ενδέχεται να επηρεάσουν τα τραπεζικά πληροφοριακά συστήματα.

Οι εταιρείες ήδη εκφράζουν ανησυχίες ότι το Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ), θα μπορούσε να εμποδίσει την καινοτομία περιορίζοντας τον τρόπο χειρισμού των δεδομένων σε εφαρμογές, βάσεις δεδομένων και διαδικτυακές υπηρεσίες. Το ζήτημα θα μπορούσε να επηρεάσει τα αυτόνομα οχήματα, τη ρομποτική και ένα πλήθος συστημάτων που βασίζονται σε τεχνολογίες τεχνητής νοημοσύνης. Οι τραπεζικοί οργανισμοί ενδέχεται τελικά να χρειαστεί να διατηρήσουν δύο ξεχωριστές βάσεις δεδομένων μία για την Ευρωπαϊκή Ένωση και μία για χώρες έκτος Ευρώπης ή να βρουν τρόπους για να διαφοροποιήσουν τα αρχεία σε βάσεις δεδομένων (Greengard, 2018).

Η βασική πρόκληση για τα χρηματοπιστωτικά ιδρύματα, ως μελλοντικοί χρήστες υπολογιστικού νέφους, είναι η ικανοποίηση των κανονιστικών απαιτήσεων και η εκπλήρωση αυτών από τους εξωτερικούς παρόχους νέφους κι αυτό αποτελεί μία νομική, παρά τεχνική πρόκληση. Επομένως, απαιτείται επαρκής διαλειτουργικότητα μεταξύ των παρόχων υπολογιστικού νέφους και των τραπεζικών ιδρυμάτων με την ενοποίηση διαφορετικών νόμων περί απορρήτου δεδομένων (Armbrust et al., 2010).

# Βιβλιογραφία


Ahmad, M. K. A., Rosalim, R. V., Beng, L. Y., & Fun, T. S. (2010). Security issues on banking systems. *International Journal of Computer Science and Information Technologies*, *1*(4), 268-272.

Ahmad, S., Ibrahim, S., & Garba, S. (2015). Enterprise resource planning (ERP) systems in banking industry: Implementation approaches, reasons for failures and how to avoid them. *Journal of Computer Sciences and Applications*, *3*(2), 29-32.

Akram, A., Kewley, J., & Allan, R. (2006). Modelling WS-RF based Enterprise Applications. In *2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06)* (pp. 22-22). IEEE.

Albrecht, J. P. (2016). How the GDPR will change the world. *Eur. Data Prot. L. Rev.*, *2*, 287.

Aljawarneh, S. A. (Ed.). (2016). *Online banking security measures and data protection*. IGI Global.

Apostu, A., Rednic, E., & Puican, F. (2012). Modeling cloud architecture in banking systems. Procedia economics and finance, 3, 543-548.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50-58.

Arora, R., Parashar, A., & Transforming, C. C. I. (2013). Secure user data in cloud computing using encryption algorithms. *International journal of engineering research and applications*, *3*(4), 1922-1926.

Awadallah, N. (2016). Usage of cloud computing in banking system. *International Journal of Computer Science Issues (IJCSI)*, *13*(1), 49.

Baets, W. (1992). Aligning information systems with business strategy. *The Journal of Strategic Information Systems*, *1*(4), 205-213.

Bartel, A. P. (2004). Human resource management and organizational performance: Evidence from retail banking. *ILR Review*, *57*(2), 181-203.

Bartolini, C., Gheorghe, G., Giurgiu, A., Sabetzadeh, M., & Sannier, N. (2015). Assessing IT security standards against the upcoming GDPR for cloud systems.

Bhasin, M. (2007). Mitigating cyber threats to banking industry. *The chartered accountant*, *55*(10), 1618-1624.

Bose, R., Luo, X. R., & Liu, Y. (2013). The roles of security and trust: Comparing cloud computing and banking. *Procedia-Social and Behavioral Sciences*, *73*, 30-34.

Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. In *2012 International Conference on Computer Science and Electronics Engineering* (Vol. 1, pp. 647-651). IEEE.

Coltman, T. (2007). Can superior CRM capabilities improve performance in banking. *Journal of Financial Services Marketing*, *12*(2), 102-114.

Cong, X., & Pandya, K. V. (2003). Issues of knowledge management in the public sector. *Electronic journal of knowledge management*, *1*(2), 25-33.

De Hert, P., & Gutwirth, S. (2006). Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. *Privacy and the criminal law*, 61-104.

Dias, D., & McKee, K. (2010). Protecting branchless banking consumers: Policy objectives and regulatory options. *Focus Note*, *64*, 1-17.

Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: issues and challenges. In *2010 24th IEEE international conference on advanced information networking and applications* (pp. 27-33). Ieee.

Edge, K., Raines, R., Grimaila, M., Baldwin, R., Bennington, R., & Reuter, C. (2007, January). The use of attack and protection trees to analyze security for an online banking system. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 144b-144b). IEEE.

Elluri, L., & Joshi, K. P. (2018). A knowledge representation of cloud data controls for eu gdpr compliance. In *2018 IEEE World Congress on Services (SERVICES)* (pp. 45-46). IEEE.

Elzamly, A., Hussin, B., Abu-Naser, S. S., Shibutani, T., & Doheir, M. (2017). Predicting critical cloud computing security issues using Artificial Neural Network (ANNs) algorithms in banking organizations.

EUROPEIA, U. (2015). Article 29 Data Protection Working Party. *Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing (2588/15/EN, WP 232)*, *22*.

Freed, R. N. (1963). Some legal implications of the use of computers in the banking business. *Communications of the ACM*, *6*(12), 713-720.

Georgescu, M., & Jeflea, V. (2015). The particularity of the banking information system. *Procedia Economics and Finance*, *20*, 268-276.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59*(6), 703-705.

Greengard, S. (2018). Weighing the impact of GDPR.

Haeberlen, A. (2010). A case for the accountable cloud. *ACM SIGOPS Operating Systems Review*, *44*(2), 52-57.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 75-105.

Hon, W. K., & Millard, C. (2018). Banking in the cloud: Part 1–banks' use of cloud services. *Computer law & security review*, *34*(1), 4-24.

Kotarba, M. (2016). New factors inducing changes in the retail banking customer relationship management (CRM) and their exploration by the FinTech industry. *Foundations of management*, *8*(1), 69-78.

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, *37*(4-5), 372-386.

Laudon, K. C., & Laudon, J. P. (1999). *Management information systems*. Prentice Hall PTR.

Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. P. (2012). Cyber security and privacy issues in smart grids. *IEEE Communications Surveys & Tutorials*, *14*(4), 981-997.

Mahalle, A., Yong, J., Tao, X., & Shen, J. (2018). Data privacy and system security for banking and financial services industry based on cloud computing infrastructure. In *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD))* (pp. 407-413). IEEE.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision support systems*, *15*(4), 251-266.

Mell, P., & Grance, T. (2009). Draft nist working definition of cloud computing-v15. *21*. *Aug 2009*, *2*, 123-135.

Nagaraju, S., & Parthiban, L. (2015). Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. *Journal of Cloud Computing*, *4*(1), 22.

Nishii, L. H., & Wright, P. M. (2007). Variability within organizations: Implications for strategic human resource management.

Pieters, W., & van Cleeff, A. (2009). The precautionary principle in a world of digital dependencies. *Computer*, *42*(6), 50-56.

Pirvu, A. I., & Boghirnea, I. (2014). Issues Related to Personal Data Protection in the Banking System. *Supplement of*, 144.

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), tyy001.

Ramakrishnan, R., Gehrke, J., & Gehrke, J. (2003). *Database management systems* (Vol. 3). New York: McGraw-Hill.

Rani, S., & Gangal, A. (2012). Security issues of banking adopting the application of cloud computing. *International Journal of Information Technology*, *5*(2), 243-246.

Reid, M., & Levy, Y. (1970). Integrating Trust and Computer Self-Efficacy with TAM: An Empirical Assessment of CustomersÃ¢ Â Â Acceptance of Banking Information Systems (BIS) in Jamaica. *The Journal of Internet Banking and Commerce*, *13*(3), 1-18.

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In *Proceedings of the 16th ACM conference on Computer and communications security* (pp. 199-212).

Scarfone, K., & Mell, P. (2012). *Guide to intrusion detection and prevention systems (idps)* (No. NIST Special Publication (SP) 800-94 Rev. 1 (Draft)). National Institute of Standards and Technology.

Shah, M. A., Swaminathan, R., & Baker, M. (2008). Privacy-Preserving Audit and Extraction of Digital Contents. *IACR Cryptol. ePrint Arch.*, *2008*, 186.

Shekhawat, N. S., & Sharma, D. P. (2011). Cloud Computing Security through Cryptography for Banking Sector. In *Proceedings of the 5th National Conference*.

Silver, M. S., Markus, M. L., & Beath, C. M. (1995). The information technology interaction model: A foundation for the MBA core course. *MIS quarterly*, 361-390.

Sotto, L. J., Treacy, B. C., & McLellan, M. L. (2010). Privacy and Data Security Risks in Cloud Computing. *World Communications Regulation Report*, *5*(2), 38.

Tanaji, B. S. (2012). Benefits of knowledge management system for banking sector. *BENEFITS*, *3*(1), 133-137.

Timmermans, J., Stahl, B. C., Ikonen, V., & Bozdag, E. (2010). The ethics of cloud computing: A conceptual review. In *2010 IEEE second international Conference on cloud computing technology and science* (pp. 614-620). IEEE.

Trivellas, P. G., & Santouridis, I. (2013). The impact of Management Information Systems' Effectiveness on Task Productivity–The Case of the Greek Banking Sector. *International Journal of Computer Theory and Engineering*, *5*(1), 170-173.

Ula, M., Ismail, Z., & Sidek, Z. M. (2011). A Framework for the governance of information security in banking system. *Journal of Information Assurance & Cyber Security*, *2011*, 1-12.

Weir, G., Aßmuth, A., Whittington, M., & Duncan, B. (2017). Cloud accounting systems, the audit trail, forensics and the EU GDPR: how hard can it be?. In *British Accounting & Finance Association (BAFA) Annual Conference 2017*.

Wenge, O., Lampe, U., Müller, A., & Schaarschmidt, R. (2014). Data Privacy in Cloud Computing–An Empirical Study in the Financial Industry.

Wright, P. M., & McMahan, G. C. (1992). Theoretical perspectives for strategic human resource management. *Journal of management*, *18*(2), 295-320.

Wu, J., Xu, M., Mo, Z., & Liao, N. (2015). Study on Information System Architecture Based on Service-Dominant Logic. *Intelligent Information Management*, *7*(02), 53.

Xiao, Z., & Xiao, Y. (2012). Security and privacy in cloud computing. *IEEE communications surveys & tutorials*, *15*(2), 843-859.

Zhu, L., & Tung, B. (2006). Public key cryptography for initial authentication in Kerberos (PKINIT). RFC 4556, June.

Αλεξανδροπούλου-Αιγυπτιάδου Ε. & Μυλώση Μ (2015). *Προσωπικά δεδομένα οικονομικής συμπεριφοράς και ηλεκτρονική επεξεργασία τους από την ΤΕΙΡΕΣΙΑΣ ΑΕ,* Δίκαιο Μέσων Ενημέρωσης & Επικοινωνίας, 33(7), 25-36

Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). Προσωπικά δεδομένα, εκδ. Νομική Βιβλιοθήκη, Αθήνα

Βακάλη, Αθηνά Ι. (2012). Πληροφοριακά συστήματα παγκόσμιου ιστού / Αθηνά Ι. Βακάλη, Ζαχαρούλα Παπαμήτσιου. - 1η έκδ. - Αθήνα : Εκδόσεις Νέων Τεχνολογιών, -510σ. · 24x17εκ.

Μυλώση, Μ. (2018). Το θεσμικό πλαίσιο του συστήματος μητρώων τραπεζικών λογαριασμών και λογαριασμών πληρωμών, 7ο Πανελλήνιο Συνέδριο ΕΕΝ e-Θέμις, Πιστωτικά Ιδρύματα: Νομικές & Θεσμικές Όψεις, Θεσσαλονίκη, ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ σελ. 53-66

Πάγκαλος, Γ., & Μαυρίδης, Ι. (2002). Ασφάλεια πληροφοριακών συστημάτων και δικτύων. *Εκδόσεις Ανικούλα, Θεσσαλονίκη*.

# ΠΑΡΑΡΤΗΜΑ Ι – Αποφάσεις ΔΕΕ για τη χρήση νέφους

Απόφαση C-230/14

Η Weltimmo, εταιρία εγγεγραμμένη στα μητρώα εταιριών στη Σλοβακία, διαχειρίζεται μια ιστοσελίδα μεσιτείας ακινήτων με αγγελίες για ακίνητα που βρίσκονται στην Ουγγαρία. Στο πλαίσιο αυτό, η εταιρεία επεξεργαζόταν τα δεδομένα προσωπικού χαρακτήρα των δημοσιευόντων αγγελιών. Οι αγγελίες δημοσιεύονται δωρεάν για ένα μήνα και, στη συνέχεια, έναντι αμοιβής. Πολλοί δημοσιεύοντες αγγελιών ζήτησαν την απόσυρση των αγγελιών τους πριν από τη λήξη του χρονικού αυτού ορίου και επί της ευκαιρίας, τη διαγραφή προσωπικών τους δεδομένων. Εντούτοις, η Weltimmo δεν προέβη στη σχετική διαγραφή και χρέωσε τους ενδιαφερόμενους για τις υπηρεσίες της. Λόγω μη πληρωμής των σχετικών ποσών, η εταιρία αυτή διαβίβασε τα δεδομένα προσωπικού χαρακτήρα που τους αφορούσαν σε επιχειρήσεις εισπράξεως οφειλών.

Τα δεδομένα που είχε συλλέξει η ιστοσελίδα της Weltimmo, τα αποθήκευε αυτόματα σε απομακρυσμένους διακομιστές οι οποίοι βρισκόταν στις εγκαταστήσεις της εταιρείας, στην Σλοβακία. Ένα εκ των προδικαστικών ερωτημάτων που υποβλήθηκαν αφορούσε στο εάν η εθνική νομοθεσία της Ουγγαρίας που είχε ενσωματώσει την οδηγία για την προστασία δεδομένων, μπορούσε να εφαρμοστεί στην περίπτωση του διαχειριστή της ιστοσελίδας και υπεύθυνου επεξεργασίας που ήταν εγκατεστημένος σε άλλο κράτος μέλος, λαμβάνοντας υπόψη και την παράμετρο ότι και τα προσωπικά δεδομένα των χρηστών της ιστοσελίδας είχαν διαβιβαστεί σε διακομιστές εγκατεστημένους σε άλλο κράτος μέλος.

Ο διαχειριστής της ιστοσελίδας διέθετε εκπρόσωπο της εταιρείας στην Ουγγαρία, το όνομα του οποίο αναγραφόταν στο σλοβακικό μητρώο εταιρειών ο οποίος ήταν υπεύθυνος για όλες τις εργασίες που πραγματοποιούνταν στον πλαίσιο της λειτουργίας της εταιρείας στην Ουγγαρία. Το Ευρωπαϊκό Δικαστήριο απεφάνθη ότι η εξεργασία των δεδομένων μπορεί να είναι περιορισμένη[69] κατά την άσκηση πραγματικής

[69] «*Προκειμένου να προσδιορίσει, υπό περιστάσεις όπως αυτές της κύριας δίκης, αν συμβαίνει κάτι τέτοιο, το αιτούν δικαστήριο μπορεί να λάβει υπόψη, ιδίως, το γεγονός, αφενός, ότι η δραστηριότητα του υπευθύνου της εν λόγω επεξεργασίας, στο πλαίσιο της οποίας αυτή πραγματοποιείται, συνίσταται στη διαχείριση ιστοσελίδων αγγελιών ακινήτων σχετικά με ακίνητα που βρίσκονται στο έδαφος του κράτους μέλους αυτού, ιστοσελίδων συντεταγμένων στη γλώσσα του εν λόγω κράτους, και ότι η ανωτέρω δραστηριότητα συνδέεται, κατά συνέπεια, κυρίως, ή ακόμα και αποκλειστικώς, με το εν λόγω κράτος μέλος, και, αφετέρου, ότι ο υπεύθυνος αυτός έχει ορίσει εκπρόσωπο εντός του εν λόγω κράτους μέλους, επιφορτισμένο με την είσπραξη*

δραστηριότητας της εταιρείας. Το ΔΕΕ έκρινε ότι η φυσική παρουσία του εκπροσώπου στο κράτος μέλλος, εξυπηρετούσε την οδηγία περί προστασίας δεδομένων και ότι έπρεπε η υπόθεση να εκδικασθεί από το κράτος κατά το οποίο ασκείτε η δραστηριότητα της εταιρείας (την Ουγγαρία), ανεξάρτητα από την κύρια έδρα της (Σλοβακία). Στην προκειμένη περίπτωση η Weltimmo ως υπεύθυνος επεξεργασίας ο οποίος είναι εγκατεστημένος στο έδαφος περισσοτέρων του ενός κρατών μελών, θα πρέπει να λαμβάνει τα αναγκαία μέτρα ώστε να εξασφαλίζεται ότι κάθε εγκατάστασή του ,πληροί τις απαιτήσεις που προβλέπει η εφαρμοστέα εθνική νομοθεσία σε συνδυασμό με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ).

Απόφαση C-191/15

Η Amazon EU είναι εταιρία που εδρεύει στο Λουξεμβούργο, ανήκει σε διεθνή όμιλο εξ αποστάσεως πωλήσεων και, μεταξύ άλλων δραστηριοτήτων, απευθύνεται στους καταναλωτές που κατοικούν στην Αυστρία, μέσω ιστότοπου με την κατάληξη «.de», και συνάπτει με αυτούς συμβάσεις ηλεκτρονικών πωλήσεων. Η εταιρία δεν έχει ούτε έδρα ούτε εγκατάσταση στην Αυστρία. Τα προσωπικά δεδομένα των καταναλωτών, η Amazon τα μετέφερε απευθείας στους απομακρυσμένους διακομιστές του κι όχι σε τοπικά δίκτυα στην Αυστρία. Με τις ρήτρες των γενικών ορών της εταιρείας, έδινε τη δυνατότητα στην Amazon ανά πάσα στιγμή να μεταφέρει τα δεδομένα των καταναλωτών της σε άλλες επιχειρήσεις από τους δικούς της διακομιστές[70] μέσω υπηρεσιών υπολογιστικού νέφους που διαθέτει η εταιρεία.

Η VKI, φορέας που νομιμοποιείται να ασκήσει αγωγές παραλείψεως υπό την έννοια της οδηγίας 2009/22, άσκησε αγωγή ενώπιον αυστριακού δικαστηρίου κατά της

---

*των απαιτήσεων από τη δραστηριότητα αυτή, καθώς και με την εκπροσώπησή του σε διοικητικές και δικαστικές διαδικασίες σχετικές με την επεξεργασία των οικείων δεδομένων.*»

Πηγή:http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=6142798

[70] «*Σε περίπτωση πληρωμής επί πιστώσει, καθώς και σε διάφορες άλλες περιπτώσεις, όταν αυτό δικαιολογείται, η Amazon.de εξακριβώνει και αξιολογεί τα δεδομένα προσωπικού χαρακτήρα των πελατών και ανταλλάσσει δεδομένα με άλλες επιχειρήσεις εντός του ομίλου της Amazon, με γραφεία οικονομικών πληροφοριών και, κατά περίπτωση, με την Bürgel Wirtschaftsinformationen GmbH & Co. KG, Postfach 5001 66, 22701, Αμβούργο, Γερμανία.*»

Πήγη:http://curia.europa.eu/juris/document/document.jsf?text=&docid=182286&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=6242456

χρήσεως του συνόλου των ρητρών που περιλαμβάνονταν στους γενικούς όρους της Amazon για τους καταναλωτές και υπέβαλε συγχρόνως αίτημα δημοσιεύσεως της αποφάσεως που θα εκδιδόταν, φρονώντας ότι όλες αυτές οι ρήτρες ήταν αντίθετες στη νομοθεσία και τα συναλλακτικά ήθη.

Στην εν λόγω απόφαση αναφέρθηκε ότι η επεξεργασία των δεδομένων των καταναλωτών, δεν απαιτούσε να γινόταν από την οικεία εγκατάσταση της Amazon αλλά να γίνεται στα πλαίσια άσκησης των δραστηριοτήτων της. Το ΔΕΕ έκρινε ότι αρμόδιο δικαστήριο για την άσκηση της προστασίας των προσωπικών δεόμενων των φυσικών προσώπων, ήταν το εθνικό δικαστήριο απ' όπου πραγματοποιούνταν οι δραστηριότητες της Amazon[71]. Στην προκειμένη περίπτωση ο υπεύθυνος κι ο εκτελών την επεξεργασία ήταν η ίδια εταιρεία Amazon, ανεξάρτητα από τον τόπο άσκησης των δραστηριοτήτων της.

[71] «*Το άρθρο 4, παράγραφος 1, στοιχείο α΄, της οδηγίας 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, έχει την έννοια ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα από επιχείρηση ηλεκτρονικού εμπορίου διέπεται από το δίκαιο του κράτους μέλους προς το οποίο η επιχείρηση αυτή κατευθύνει τις δραστηριότητές της, εφόσον αποδεικνύεται ότι η εν λόγω επιχείρηση προβαίνει στην επεξεργασία των επίμαχων δεδομένων στο πλαίσιο των δραστηριοτήτων εγκαταστάσεως ευρισκόμενης στο συγκεκριμένο κράτος μέλος. Στο εθνικό δικαστήριο εναπόκειται να εκτιμήσει αν συντρέχει τέτοια περίπτωση.*»