ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

«ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟΝ ΤΡΑΠΕΖΙΚΟ ΤΟΜΕΑ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΝΕΦΟΥΣ»

Διπλωματική Εργασία

του

Πολυχρόνη Καζαντζίδη

Θεσσαλονίκη, 02/2022

«ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ
ΣΤΟΝ ΤΡΑΠΕΖΙΚΟ ΤΟΜΕΑ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΝΕΦΟΥΣ»

Πολυχρόνης Καζαντζίδης
Πτυχίο Νομικής, ΕΚΠΑ, 2016
Μεταπτυχιακό Νομικής, ΕΚΠΑ, 2021

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Κος Κομνηνός Κόμνιος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 25/02/2022

Κομνηνός Κόμνιος	Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου	Μαρία Μυλώση
.....	.....	.....

Πολυχρόνης Καζαντζίδης

Περίληψη

Με την παρούσα διπλωματική εργασία επιχειρείται η παρουσίαση των βασικών αξόνων του κανονιστικού πλαισίου συμμόρφωσης και των υποχρεώσεων των τραπεζικών ιδρυμάτων σε σχέση με το νομοθετικό και κανονιστικό πλαίσιο που διέπει την προστασία των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της ειδικής σχέσης εμπιστοσύνης ανάμεσα σε τράπεζες και τους πελάτες αυτών, όπως αυτό έχει διαμορφωθεί μετά την θέση σε ισχύ του Γενικού Κανονισμού για την Προστασία των Δεδομένων (ΕΕ) 2016/679 και του νόμου 4624/2019.

Στο πρώτο μέρος της διπλωματικής εργασίας αναλύεται η έννοια της ιδιωτικότητας στον οικονομικό και φορολογικό τομέα, ενώ εξετάζεται η σχέση του δικαιώματος στην ιδιωτικότητα με το δικαίωμα στην προστασία προστασίας των προσωπικών δεδομένων. Στη συνέχεια, εξετάζεται το ιστορικό πλαίσιο της νομοθεσίας προστασίας προσωπικών δεδομένων στον ευρωπαϊκό χώρο, ενώ παρουσιάζονται και γενικά στοιχεία που αφορούν τον Κανονισμό (ΕΕ) 2016/679 και το νόμο 4624/2019 και τις αλλαγές που επέφεραν, σε σχέση με το προϊσχύσαν πλαίσιο της Οδηγίας 95/46/ΕΚ και του νόμου 2472/1997.

Στο δεύτερο μέρος, αναλύεται η σχέση ανάμεσα σε τραπεζικά ιδρύματα και τους πελάτες τους, ενώ παρουσιάζονται και οι υποχρεώσεις που ενέχουν τα τραπεζικά ιδρύματα έναντι των πελατών τους στο πλαίσιο της σχέσης αυτής. Στη συνέχεια, γίνεται εκτενής αναφορά στις υποχρεώσεις των τραπεζών που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα των πελατών τους, αλλά και στη διαδικασία συλλογής και επεξεργασίας των προσωπικών δεδομένων των πελατών από τα τραπεζικά ιδρύματα. Περαιτέρω, θίγονται ειδικότερα ζητήματα εφαρμογής της νομοθεσίας προστασίας προσωπικών δεδομένων στα πιστωτικά ιδρύματα. Πιο συγκεκριμένα, αναλύεται η φύση του τραπεζικού απορρήτου, το οποίο πέραν της ειδικής του προστασίας, προστατεύεται και από τη νομοθεσία περί προσωπικών δεδομένων. Επιπροσθέτως, γίνεται αναφορά στα ζητήματα προστασίας προσωπικών δεδομένων που έχουν ανακύψει μετά την εισαγωγή των διαδικασιών πώλησης ή εκχώρησης της διαχείρισης των μη εξυπηρετούμενων δανείων σε Εταιρείες Ειδικού Σκοπού, βάσει του νόμου 4354/2015.

Τέλος, στο τρίτο μέρος, αναλύονται τα μοντέλα και οι τεχνολογίες υπολογιστικής νέφους που υιοθετούνται από τους χρηματοπιστωτικούς θεσμούς στο πλαίσιο του μετασχηματισμού των επιχειρηματικών δραστηριοτήτων τους. Το υπολογιστικό νέφος δύναται να αυξήσει την αποδοτικότητα και την ευελιξία αλλά και να επιφέρει σημαντική εξοικονόμηση σε κόστη που μπορούν να ανακατανεμηθούν σε προγράμματα προσανατολισμένα στους πελάτες και στις υπηρεσίες. Ωστόσο, η ευρεία υιοθέτησή του έχει εμποδιστεί από το αίσθημα ανασφάλειας και παραβίασης της ιδιωτικότητας στο σύχρονο επιγραμμικό περιβάλλον. Λαμβάνοντας υπόψιν τους περιορισμούς των υπαρχόντων ταξινομήσεων των απειλών ασφαλείας για τα συστήματα υπολογιστικού νέφους, στην παρούσα εργασία παρουσιάζεται μια εναλλακτική κατηγοριοποίηση που διακρίνει τους κινδύνους για τα συστήματα νέφους σε τρεις κατηγορίες. Αναλύεται, επίσης, η φύση των συμβάσεων παροχής υπηρεσιών νέφους, οι οποίες εντάσσονται σε ένα γενικότερο πλαίσιο διακυβέρνησης των συστημάτων αυτών.

Λέξεις Κλειδιά: προσωπικά δεδομένα**,** προστασία προσωπικών δεδομένων, ιδιωτικότητα, τραπεζικά ιδρύματα, τραπεζικό απόρρητο, μη εξυπηρετούμενα δάνεια, υπολογιστική νέφους, Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ)

Abstract

This Diploma Thesis attempts to present the major themes of the regulatory framework and the obligations of the banking institutions in conjunction with the legislative and regulatory framework which governs the protection of personal data in the context of the special trust relationship between banking institutions and their clients, as it has been reconfigured after the enactment of the General Data Protection Regulation (EU) 2016/679 (GDPR) and law 4624/2016.

In the first part of this Diploma Thesis the concept of privacy is analysed in the financial and tax sector, as well as the relation between the right to privacy and the right to the protection of personal data. Furthermore, the historical context of the protection of personal data in the European area is analysed, as well as additional elements concerning the General Data Protection Regulation (EU) 2016/679 (GDPR) and law 4624/2019 and the changes they implemented, in comparison to the legal context previously in force through the Directive 95/46/EC and Greek law 2472/1997.

The second part of this Diploma Thesis offers an analysis of the relationship between banking institutions and their clients, as well as the obligations that these banking institutions have to fulfil towards their respective clients in the context of their relationship. Moreover, the obligations of banking institutions regarding the protection of personal data of their clients as well as the processes of collection and processing of personal data of clients are analysed. Additionally, specific issues regarding the implementation of the data protection legislation by banking institutions are examined. Specifically, the nature of the banking institutions statutory duty of confidentiality is analysed, which beyond offering specialized protection, is also protected by the personal data legislation. In addition to all this, chapter six refers to the issues concerning the protection of personal data with regard to the introduction of the sale and subrogation of the management of non-performing loans to Special Purpose Vehicles, based on law 4354/2015.

The third part of this Diploma Thesis offers a detailed analysis of the cloud computing models and technologies, which are adopted by financial institutions in the context of the transformation of their business activities. Cloud computing has the ability to increase the efficiency and flexibility as well as bring about substantial savings in operational costs which can subsequently be redirected towards customers and services. Nevertheless, its wide adoption has been hampered by a sense of insecurity and violation of privacy in the modern online environment. Considering the limitations of existing classifications of security threats for cloud systems, which either consider the major cloud dependencies or utilize risk assessment tools, this thesis presents an alternative classification that distinguishes the risks into three categories. To conclude, an analysis of the nature of cloud computing service agreements which form part of a more generalized context of governance of these systems, is included.

Keywords: personal data, protection of personal data, privacy, banking institutions, duty of confidentiality, non-performing loans, cloud computing, General Data Protection Regulation (GDPR)

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ

Πρόλογος

Η ραγδαία ανάπτυξη της τεχνολογίας και η συνεχώς εντεινόμενη ψηφιοποίηση επηρεάζουν σήμερα κάθε τομέα της ανθρώπινης δραστηριότητας και καθιστούν πιο εύκολη την επικοινωνία και την πραγματοποίηση επιχειρηματικών δραστηριοτήτων σε παγκόσμιο επίπεδο. Παράλληλα, η καλπάζουσα τεχνολογική πρόοδος έδωσε τη δυνατότητα ανάπτυξης ψηφιακών πλατφορμών και εφαρμογών που μεταμορφώνουν τους παραδοσιακούς τομείς επιχειρηματικότητας και προωθούν την καινοτομία στο πεδίο της ψηφιακής οικονομίας. Η ψηφιοποίηση αυτή που διαπερνά κάθε τομέα της ανθρώπινης δραστηριότητας και ενσωματώνεται στις ψηφιακές πλατφόρμες, μειώνει την πληροφοριακή ασυμμετρία και το κόστος των συναλλαγών, ενώ παράλληλα ισχυροποιεί την ανάπτυξη νέων υπηρεσιών και συνεργατικών δικτύων σε μεγάλη κλίμακα. Στο πλαίσιο αυτό, εξέχουσα σημασία κατέχουν τα δεδομένα, που έχουν χαρακτηριστεί από πολλούς ως το «νέο πετρέλαιο», αποτυπώνοντας έτσι τον καθοριστικό τους ρόλο για την οικονομική ανάπτυξη και καινοτομία. Οι επιπτώσεις της χρήσης των δεδομένων και των τεχνικών ανάλυσης δεδομένων είναι πολυπληθείς και αναδιαμορφώνουν τις κοινωνικές δομές σε πολλαπλά επίπεδα. Σε ένα μικρό-επίπεδο για παράδειγμα, η εξέχουσα σημασία και αξία των δεδομένων επανακαθορίζει την παραδοσιακή σχέση μεταξύ καταναλωτών και παραγωγών. Ενώ στο παρελθόν οι παραδοσιακές συναλλακτικές σχέσεις περιορίζονταν στην πώληση προϊόντων με αντάλλαγμα κάποιο χρηματικό ποσό και κάποια αμελητέα δεδομένα, κάθε συναλλαγή που συντελείται στην εποχή μας και κάθε αλληλεπίδραση με κάποιον καταναλωτή, παράγει πολύτιμες πληροφορίες.[1]

Τα δεδομένα εντάσσονται έτσι στο πλαίσιο μιας ευρύτερης μετατόπισης, που καθιστά την αποτύπωση της καθημερινότητας υπό τη μορφή δεδομένων σε εγγενές στοιχείο της οργανωτικής και θεσμικής ζωής.[2]Στην μετατόπιση αυτή καθοριστικό ρόλο διαδραματίζουν και οι πρακτικές που ασκούν οι διαδικτυακές επιχειρήσεις, όπως η Google, η Amazon ,το Facebook και το Twitter, που μάχονται για τη διαδικτυακή ηγεμονία και είναι διατεθειμένες να προσφέρουν τις υπηρεσίες τους δωρεάν με απώτερο στόχο την απόκτηση περισσότερων δεδομένων. Κάθε ανθρώπινη δραστηριότητα συντελείται πλέον μέσω της ηλεκτρονικής διαμεσολάβησης και κάθε πτυχή του κόσμου μεταλλάσσεται οδηγώντας στη δημιουργία ενός «πολιτισμού της πληροφορίας». Τα δεδομένα επίσης οδηγούν σε ανακατατάξεις στο πεδίο του ανταγωνισμού και στην αναδιανομή της ισχύος στην αγορά. Η ικανότητα των εταιρειών μεγακλίμακας, όπως η Google και η Apple, να διαχειρίζονται τον τεράστιο όγκο των πληροφοριών, έχει προσφέρει ένα σημαντικό ανταγωνιστικό πλεονέκτημα τόσο στις ίδιες όσο και σε χώρες όπως η Κίνα και δίνει τη δυνατότητα για κινήσεις ισχύος στη σκακιέρα της παγκόσμιας πολιτικής οικονομίας. Οι προσπάθειες των εταιρειών και των κυβερνήσεων να δαμάσουν τη δύναμη και τα πλεονεκτήματα της τεχνολογίας για τη διαμόρφωση μιας οικονομίας που έχει ως γνώμονα τα δεδομένα (***data-driven economy***), καθίστανται εμφανείς και από τις επενδύσεις που πραγματοποιούνται στο πεδίο των υπερ-υπολογιστών και των κέντρων δεδομένων (***data centres***).[3]

---

[1] Mira Burri, *Big Data and Global Trade Law*, 1st ed. (repr., Cambridge University Press, 2021), 1.
[2] Μανώλης Πατινιώτης, *Εισαγωγή Στις Ψηφιακές Σπουδές*, 1η εκδ. (Θεσσαλονίκη: Εκδόσεις Ροπή, 2020), 355.
[3] "Ξεκινούν Οι Επενδύσεις Στα Data Center Νέας Γενιάς – Κόμβος Δεδομένων Η Ελλάδα", Capital.Gr, 2021, https://www.capital.gr/epixeiriseis/3559124/xekinoun-oi-ependuseis-sta-data-center-neas-genias-kombos-dedomenon-i-ellada.

Στην εποχή αυτή του «πληροφοριακού χρυσού», όπως την χαρακτήρισε ο Καθηγητής Σπύρος Σημίτης[4], οι πηγές των δεδομένων είναι ποικίλες. Μπορούν συνεπώς να προέρχονται από αισθητήρες που εντάσσονται στο οικοσύστημα του Διαδικτύου των Πραγμάτων (***IoT ecosystem***), από φορέσιμες συσκευές (***wearables***), νανοεξαρτήματα που έχουν ως κύριο στόχο τον εντοπισμό ενδείξεων ασθένειας, αυτό-οδηγούμενα οχήματα (***autonomous vehicles***), drones κ.λπ. Η αξία αυτού του «διαδικτύου των πάντων» ανέρχεται σύμφωνα με την σχετική έκθεση της Cisco στα 14,4 τρισεκατομμύρια δολάρια.[5]Τα δεδομένα μπορούν επίσης να προέρχονται από εταιρικές και κυβερνητικές βάσεις δεδομένων, στις οποίες συμπεριλαμβάνονται τράπεζες, μεσάζοντες εξόφλησης λογαριασμών, υπηρεσίες αξιολόγησης πίστης, αρχεία φορολογίας, απογραφής, αρχεία πιστωτικών καρτών, ασφαλειών και άλλα. Αποτελεί επίσης συχνό φαινόμενο η συγκέντρωση, ανάλυση, ομαδοποίηση και πώληση δεδομένων από μεταπράτες δεδομένων που ενεργούν εκτός του ισχύοντος νομικού πλαισίου προστασίας καταναλωτών και προσωπικών δεδομένων.[6] Ειδική μνεία θα πρέπει να γίνει για τα δεδομένα που προέρχονται και παράγονται από συστήματα παρακολούθησης τόσο σε μεγάλη κλίμακα (δορυφόροι, κάμερες παρακολούθησης) όσο και σε μικρή κλίμακα (έξυπνα τηλέφωνα).Τα τεχνολογικά εργαλεία που έχουν στη διάθεσή τους σήμερα οι εταιρείες και οι κυβερνητικές υπηρεσίες συμβάλλουν στην δημιουργία ενός καθεστώτος αόρατης επιτήρησης μέσω της ασταμάτητης ηλεκτρονικής καταγραφής προσωπικών δεδομένων που αφορούν κάθε πτυχή της δημόσιας και ιδιωτικής ζωής. Εν τέλει στο όνομα της ασφάλειας των πολιτών, η ηλεκτρονική παρακολούθηση των συμπεριφορών αποτελεί καθημερινό φαινόμενο και οδηγεί στη διαμόρφωση αυτού που ο Georgio Agamben ονόμασε «βιοπολιτικό τατουάζ» και περιλαμβάνει την αξιοποίηση πληθώρας πληροφοριών που αφορούν την ιδιωτική και δημόσια σφαίρα των υποκειμένων.[7]Το «βιοπολιτικό τατουάζ» οδηγεί σε εξατομίκευση της επιτήρησης, ενώ η συνεχώς αυξανόμενη γενίκευση της διασύνδεσης μεταξύ των βάσεων δεδομένων που περιέχουν πληροφορίες των πολιτών εντείνει την ασυμμετρία ανάμεσα στην ελευθερία και την ασφάλεια, απειλώντας σε τελική ανάλυση τα θεμελιώδη ανθρώπινα δικαιώματα.[8] Οδηγούμαστε εν τέλει στη διαμόρφωση ενός νέου ψηφιακού και εικονικού Πανοπτικού στο οποίο τον ρόλο των φυλάκων διαδραματίζουν οι κρατικοί μηχανισμοί και οι ιδιωτικές επιχειρήσεις που ιχνηλατούν την ανθρώπινη ζωή με τρόπο ανεπαίσθητο και αφανή. Στη νέα αυτή γιγαντιαία αγορά προσωπικών δεδομένων τα προσωπικά δεδομένα των υποκειμένων αποτελούν το νέο πολύτιμο εμπόρευμα.[9]

Αποτελεί επομένως πρόκληση για τον ενωσιακό και τον εθνικό νομοθέτη η ανάπτυξη και η διαμόρφωση ενός νομικού πλαισίου που διασφαλίζει ένα επαρκές επίπεδο προστασίας των προσωπικών δεδομένων των φυσικών προσώπων (εφεξής «υποκείμενα») ενώ παράλληλα εξασφαλίζει ισότιμους όρους ανταγωνισμού για τις επιχειρήσεις ώστε αυτές να αναπτύξουν καινοτόμες υπηρεσίες βασιζόμενες στα δεδομένα. Στις επιχειρήσεις αυτές εντάσσονται και οι Τράπεζες, οι οποίες στο πλαίσιο της άσκησης των συναλλακτικών τους δραστηριοτήτων συλλέγουν και επεξεργάζονται πληθώρα προσωπικών δεδομένων των πελατών τους (ευαίσθητων και μη) ώστε να εξασφαλίσουν την ομαλή εκτέλεση, υποστήριξη και παρακολούθηση των πάσης

---

[4] Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, *Προσωπικά Δεδομένα*, 1η εκδ. (Θεσσαλονίκη: Νομική Βιβλιοθήκη, 2016), 27.
[5] Cisco.com, 2013. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf.
[6] Μανώλης Πατινιώτης, *Εισαγωγή Στις Ψηφιακές Σπουδές*, 1η εκδ. (Θεσσαλονίκη: Εκδόσεις Ροπή, 2020), 362.
[7] Ξενοφών Κοντιάδης, *Πανδημία, Βιοπολιτική Και Δικαιώματα*, 1η εκδ. (Αθήνα: Εκδόσεις Καστανιώτη, 2020), 114.
[8] Θεώδορος Παπαθεωδόρου, *Επιτηρούμενη Δημοκρατία*, 1st εκδ. (Αθήνα: Βιβλιόραμα, 2009), 107.
[9] Ιγνάσιο Ραμονέ, *Αυτοκρατορία Της Επιτήρησης*, 1η εκδ. (Αθήνα: Εκδόσεις του εικοστού πρώτου, 2017), 15 επ.

φύσεως συναλλαγών και σχέσεων. Στη «χρυσή αυτή εποχή των προσωπικών δεδομένων» οι Τράπεζες με απώτερο στόχο την βελτιστοποίηση και επιτάχυνση των εργασιών τους, προχωρούν στην υιοθέτηση νέων τεχνολογιών. Για να ανταποκριθούν στην ανάγκη αυτή για χωρητικότητα και ταχύτητα, οι χρηματοπιστωτικοί οργανισμοί υιοθετούν τεχνολογικές λύσεις που βασίζονται στην υπολογιστική νέφους (cloud computing). Η τεχνολογία υπολογιστικής νέφους δύναται να προσφέρει στις τράπεζες ένα ανταγωνιστικό πλεονέκτημα καθώς επιτρέπει την προηγμένη ανάλυση δεδομένων των πελατών αλλά και την αποθήκευση δεδομένων σε πολλαπλά κέντρα δεδομένων ανά τον κόσμο, οδηγώντας σε αναλυτικότερες εξατομικευμένες οικονομικές προβλέψεις και εν τέλει στην παροχή βελτιωμένων υπηρεσιών και καταναλωτικών προϊόντων. Ωστόσο η υιοθέτηση επιχειρηματικών λύσεων από τις τράπεζες που βασίζονται στην τεχνολογία υπολογιστικής νέφους εγείρει ανησυχίες ως προς το θέμα της ασφάλειας των προσωπικών δεδομένων των πελατών και της ιδιωτικότητας αυτών. Στην εξελικτική αυτή διαδικασία ψηφιοποίησης της οικονομίας και των τραπεζικών υπηρεσιών συμμετέχουν και οι νεοφυείς επιχειρήσεις που αναπτύσσουν το επιχειρηματικό τους μοντέλο βάσει της οικονομικής τεχνολογίας (***financial start-ups, Fintech***). Στόχος τους είναι η ενίσχυση και η παροχή λύσεων σε οικονομικά προβλήματα με εύκολο και γρήγορο τρόπο. Επιπροσθέτως, πολλές εταιρείες Fintech χρησιμοποιούν προσωπικά δεδομένα πελατών για να παρέχουν εξατομικευμένες οικονομικές υπηρεσίες.[10]

Μπορούμε εύλογα επομένως να οδηγηθούμε στο συμπέρασμα ότι ο χρηματοπιστωτικός τομέας υφίσταται μια πρωτόγνωρη μεταμόρφωση χάρη στην επίδραση των νέων τεχνολογιών που εντάσσουν στις υποδομές τους τα τραπεζικά ιδρύματα. Η μεταμόρφωση αυτή δύναται να προσφέρει πολλαπλά οφέλη στους πελάτες των τραπεζικών ιδρυμάτων, ωστόσο επαυξάνει τις υποχρεώσεις των τελευταίων αναφορικά με την συμμόρφωσή τους με το ισχύον νομοθετικό και κανονιστικό πλαίσιο προστασίας των προσωπικών δεδομένων.

Το νομικό οπλοστάσιο προστασίας των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση (εφεξής η «Ε.Ε.») αναβαθμίστηκε το 2016 μέσω του Γενικού Κανονισμού Προστασίας Δεδομένων (**GDPR**)[11], ώστε να διευκολυνθεί η γρήγορη και αποτελεσματική ρυθμιστική απάντηση στις προκλήσεις που θέτουν οι τεχνολογικές εξελίξεις και να θωρακιστούν τα φυσικά πρόσωπα, αναφορικά με τη χρήση των προσωπικών δεδομένων τους, από παρεμβάσεις που θίγουν τον πυρήνα της ιδιωτικής, κοινωνικής και οικονομικής τους ζωής. Πριν τη θέση σε ισχύ του Κανονισμού, ο κατακερματισμός της προστασίας προσωπικών δεδομένων στην Ε.Ε. και η συνεπαγόμενη νομική αβεβαιότητα λογίζονταν ως εμπόδιο στην επιδίωξη των οικονομικών δραστηριοτήτων σε ευρωπαϊκό επίπεδο και οδηγούσαν σε διαστρέβλωση του ανταγωνισμού.[12] Σε αντίθεση με την προϊσχύσασα Οδηγία 95/46/ΕΚ[13], ο Κανονισμός εφαρμόζεται άμεσα και δεν απαιτούνται περαιτέρω εφαρμοστικές διατάξεις από τα κράτη-μέλη της Ε.Ε. Μέσω της

---

[10] Niels Pedersen, *Financial Technology: Case Studies in Fintech Innovation*, 1st ed. (repr., Kogan Page, 2020), 3-4.
[11] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση της οδηγίας 95/46/ΕΚ (General Data Protection Regulation), OJ L 119/1-88, 4.5.2016
[12] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)*, 1st ed. (repr., Cham: Springer International Publishing, 2017), 2.
[13] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, OJ L 281/31-50, 23.11.1995.

εναρμόνισης και της εξισορρόπησης των κανόνων προστασίας προσωπικών δεδομένων, ο Κανονισμός δύναται να άρει τα εμπόδια στην ελεύθερη διακίνηση των προσωπικών δεδομένων. Κατά τη θέσπιση του Κανονισμού, ο ενωσιακός νομοθέτης έλαβε υπόψιν τις προκλήσεις που θέτει η σύγχρονη παγκόσμιας οικονομία, οι νέες τεχνολογίες και τα νέα επιχειρηματικά μοντέλα και καθόρισε με αυτόν τον τρόπο ένα ευρύ πεδίο εφαρμογής του Κανονισμού ώστε οι επιχειρήσεις να προβούν με επιμέλεια σε αναδιοργάνωση των εσωτερικών διαδικασιών προστασίας προσωπικών δεδομένων με απώτερο στόχο την συμμόρφωση στις επιταγές του Κανονισμού.

Στόχοι και δομή της εργασίας

Στο πλαίσιο αυτό, η παρούσα εργασία επιχειρεί να εξετάσει το νομοθετικό πλαίσιο της προστασίας των προσωπικών δεδομένων στον ευρωπαϊκό χώρο κατά τη διάρκεια των τελευταίων δεκαετιών και να παρουσιάσει το πλαίσιο συμμόρφωσης και των υποχρεώσεων των χρηματοπιστωτικών ιδρυμάτων με βάση το ισχύον νομοθετικό και κανονιστικό πλαίσιο προστασίας των προσωπικών δεδομένων, όπως αυτό διαμορφώθηκε μετά την θέση σε ισχύ του Γενικού Κανονισμού Προστασίας προσωπικών δεδομένων (ΕΕ) 2016/679 και του εφαρμοστικού του νόμου 4624/2019.

Στο πρώτο κεφάλαιο παρουσιάζονται οι έννοιες της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων, ενώ τα αντίστοιχα δικαιώματα που πηγάζουν από αυτές αναλύονται περαιτέρω στο πλαίσιο του φορολογικού και του οικονομικού τομέα. Παράλληλα, διερευνώνται οι προκλήσεις και αναλύονται οι κίνδυνοι για την ιδιωτικότητα, που προκύπτουν από τη χρήση των νέων τεχνολογιών. Στη συνέχεια, εξετάζεται ένα νέο, εναλλακτικό μοντέλο που αποσκοπεί στην άμβλυνση των κινδύνων για την ιδιωτικότητα.

Στο δεύτερο κεφάλαιο, περιλαμβάνεται μια ιστορική-συγκριτική ανάλυση που εστιάζει στην ανάπτυξη των νομοθετημάτων προστασίας προσωπικών δεδομένων στον ευρωπαϊκό χώρο. Αρχικά, αναλύονται οι νόμοι προστασίας προσωπικών δεδομένων της Έσσης, της Σουηδίας και της Γαλλίας. Στη συνέχεια, γίνεται εκτενής αναφορά στις «Κατευθυντήριες γραμμές σχετικά με την προστασία της ιδιωτικότητας και των διασυνοριακών ροών προσωπικών δεδομένων», τις οποίες εξέδωσε ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) αλλά και στη Σύμβαση 108 του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων. Στη συνέχεια αναλύονται οι πρώτοι εθνικοί νόμοι προστασίας δεδομένων του Ηνωμένου Βασιλείου και του Βελγίου, οι οποίοι εφάρμοζαν την Σύμβαση 108. Τέλος, αναλύονται διεξοδικά οι νομοθετικές μεταβολές που επήλθαν μέσω της Οδηγίας 95/46/ΕΚ αλλά και του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (ΕΕ) 2016/679.

Στη συνέχεια, στο τρίτο κεφάλαιο αναλύεται διεξοδικά η σχέση ανάμεσα στα τραπεζικά ιδρύματα και τους πελάτες τους. Η έννομη αυτή σχέση βασίζεται στις περισσότερες περιπτώσεις σε συμβάσεις που συνάπτονται ανάμεσά τους, συνιστούν δηλαδή εκδήλωση της ιδιωτικής τους αυτονομίας. Επιπροσθέτως, από την σχέση αυτή απορρέουν υποχρεώσεις των τραπεζικών ιδρυμάτων για την μέριμνα των συμφερόντων των αντισυμβαλλόμενων τους και για την αποτροπή δυσανάλογα επαχθών συνεπειών στο πρόσωπό τους και την περιουσία τους.

Ακολούθως, στο τέταρτο κεφάλαιο εξετάζονται τα ζητήματα προστασίας δεδομένων προσωπικού χαρακτήρα τα οποία προκύπτουν στο πεδίο των τραπεζικών εργασιών. Τα σχετικά ζητήματα δεν περιορίζονται πλέον στην υποχρέωση εχεμύθειας των τραπεζών, αλλά έχουν τις τελευταίες δεκαετίες εξετασθεί υπό ευρύτερο πρίσμα, δεδομένης της αναδείξεως ενός νεοπαγούς δικαιώματος, της προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ερωτάται, ειδικότερα, τι είδους δεδομένα προσωπικού χαρακτήρα δύναται να συλλέγει η τράπεζα, από ποιες πηγές και υπό ποιες προϋποθέσεις, τι είδους χρήση μπορεί να κάνει και υπό ποιες προϋποθέσεις δικαιούται να τα διαβιβάζει περαιτέρω.

Στο πέμπτο κεφάλαιο εξετάζεται η φύση μιας γενικής υποχρέωσης των τραπεζών έναντι των πελατών τους, η οποία συνίσταται στην τήρηση εκ μέρους της τράπεζας του απορρήτου ως προς τις έννομες και γενικότερα συναλλακτικές της σχέσεις με την πελατεία της. Η υποχρέωση αυτή πηγάζει απευθείας από τον νόμο, ενώ το γενικό τραπεζικό απόρρητο είναι διαφορετικό κατά την έκταση και τις έννομες συνέπειες αφενός από το ειδικό απόρρητο των τραπεζικών καταθέσεων και αφετέρου από τις υποχρεώσεις που επιβάλλονται με βάση τη νομοθεσία για την προστασία των προσωπικών δεδομένων, ζητήματα για τα οποία γίνεται λόγος στην οικεία θέση.

Στο έκτο κεφάλαιο εξετάζεται το ζήτημα της πώλησης και μεταβίβασης «κόκκινων» δανείων από τα τραπεζικά ιδρύματα από τη σκοπιά της προστασίας των δεδομένων προσωπικού χαρακτήρα. Οι διαδικασίες διαχείρισης και μεταβίβασης των μη εξυπηρετούμενων δανείων, δημιουργούν σημαντικά ζητήματα επεξεργασίας προσωπικών δεδομένων των φυσικών προσώπων, καθώς τα πιστωτικά ιδρύματα υποχρεούνται να μεταβιβάσουν στους αποκτώντες πλήθος προσωπικών δεδομένων των οφειλετών φυσικών προσώπων, υπό την έννοια του άρθρου 4 αρ. 1 του Κανονισμού (ΕΕ) 2016/679, διότι οι πληροφορίες αυτές είναι αναγκαίες για την ενάσκηση των μεταβιβαζόμενων απαιτήσεων.

Τέλος, στο έβδομο κεφάλαιο γίνεται εκτενής αναφορά στις τεχνολογίες υπολογιστικής νέφους, οι οποίες υιοθετούνται με εκθετικό ρυθμό από τα χρηματοπιστωτικά ιδρύματα, στο πλαίσιο της αναβάθμισης των υπολογιστικών τους υποδομών. Ορίζεται επομένως η έννοια του υπολογιστικού νέφους και αναπτύσσεται η αρχιτεκτονική σχεδίαση των συστημάτων και των μοντέλων που βασίζονται στις τεχνολογίες υπολογιστικού νέφους. Εξετάζεται επίσης η σημασία της χρήσης των τεχνολογιών υπολογιστικού νέφους από τα χρηματοπιστωτικά ιδρύματα, αλλά και οι τρόποι που αυτά επηρεάζονται από τη λειτουργία του νέφους. Τέλος, αναλύονται οι κίνδυνοι και οι απειλές που αντιμετωπίζουν σήμερα τα συστήματα υπολογιστικής νέφους, τόσο σε επίπεδο υποδομών όσο και σε επίπεδο παροχής υπηρεσιών, ενώ εξετάζονται και τα αντίμετρα που μπορούν να υιοθετηθούν για να αντιμετωπιστούν οι εν λόγω κίνδυνοι και απειλές.

ΜΕΡΟΣ Α'

ΠΡΩΤΟ ΚΕΦΑΛΑΙΟ
Η ΑΝΑΔΥΣΗ ΤΗΣ ΝΟΜΟΘΕΣΙΑΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

1.1 Το Ιστορικό Πλαίσιο

Η προστασία των προσωπικών δεδομένων προέκυψε ως ζήτημα κανονιστικής διαρρύθμισης σε μια περίοδο σημαντικών κοινωνικών και οικονομικών μεταβολών. Οι μεταβολές αυτές εντάσσονται στο πλαίσιο μετάβασης της κοινωνίας από την βιομηχανική στη μετα-βιομηχανική οικονομία, καθώς πολλές ευρωπαϊκές χώρες τη δεκαετία του 1960 εισήγαγαν σημαντικές κοινωνικές μεταρρυθμίσεις. Οι μεταρρυθμίσεις αυτές αφορούσαν κυρίως τον δημόσιο τομέα, καθώς επέβαλλαν στις κυβερνήσεις να προχωρούν σε αθρόα συλλογή και επεξεργασία των δεδομένων των πολιτών. Στην διαδικασία αυτή σημαντική ήταν η συμβολή των επιτευγμάτων της τεχνολογικής προόδου, χάρη στα οποία οι κυβερνήσεις μπορούσαν πλέον να επεξεργάζονται τα δεδομένα με αυτοματοποιημένο τρόπο και μεγαλύτερη ταχύτητα. Αρχικά τα υπολογιστικά συστήματα περιορίζονταν στην εκτέλεση εργασιών που αφορούσαν την έρευνα και τον σχεδιασμό. Αργότερα, στα μέσα της δεκαετίας του 1960, οι υπολογιστές συνέβαλλαν στην καθημερινή διοίκηση οδηγώντας σταδιακά στη διαπίστωση ότι η τεχνολογία των πληροφοριών (information technology) μπορεί εν τέλει να μεταβάλλει ριζικά τη σχέση μεταξύ πολίτη και κράτους.[14]

Η συζήτηση αναφορικά με τη χρήση αυτοματοποιημένων τεχνικών επεξεργασίας για την επεξεργασία δεδομένων οξύνθηκε χάρη στην βούληση των κυβερνήσεων να αναπτύξουν κεντρικές υποδομές αυτοματοποιημένων τραπεζών δεδομένων (***databanks***) του πληθυσμού. Τα σχέδια αυτά πυροδότησαν μια σειρά από αντιδράσεις ανάμεσα στους πολίτες καθώς θεωρήθηκε ότι δύνανται να παραβιάσουν την ιδιωτικότητά τους μέσω διευρυμένων πρακτικών παρακολούθησης και καταγραφής κάθε λεπτομέρειας του ιδιωτικού τους βίου. Σχετικές με τις ανησυχίες αυτές είναι και οι προτάσεις για καθιέρωση και επέκταση των συστημάτων απόδοσης αριθμών προσωπικής ταυτοποίησης στους πολίτες.[15] Οι αριθμοί ταυτοποίησης κρίθηκε ότι διευκολύνουν την διασύνδεση των πληροφοριών που περιέχονται σε πολλαπλές βάσεις δεδομένων, εντείνοντας τις ανησυχίες ότι τα δεδομένα μπορεί να χρησιμοποιηθούν μετέπειτα από τις κυβερνήσεις. Στη συνέχεια τη δεκαετία του 1970, η διενέργεια δημόσιων απογραφών έφερε στο προσκήνιο πολλαπλά ζητήματα ιδιωτικότητας, καθώς η αδιάκριτη φύση των ερωτημάτων και ο αυτοματοποιημένος τρόπος διενέργειας δεν άφηναν περιθώρια για εφησυχασμό στους πολίτες.[16] Φυσικά, η χρήση και επεξεργασία προσωπικών δεδομένων δεν περιοριζόταν στο δημόσιο τομέα. Πολλές ιδιωτικές επιχειρήσεις εισήγαγαν στο επιχειρηματικό τους μοντέλο μέσα αυτοματοποιημένης επεξεργασίας, με στόχο την αύξηση της αποδοτικότητας των καθημερινών τους εργασιών. Συνεπώς, οι ιδιωτικές επιχειρήσεις έθεταν με τη σειρά τους ζητήματα αθέμιτης και αδιάκριτης επεξεργασίας των δεδομένων των πολιτών. Ωστόσο, προκρίθηκε η θέσπιση

[14] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 155.
[15] Colin Bennet, *Regulating Privacy: Data Protection and Public Policy in Europe and The United States*, eBook, 1st ed. (repr., Ithaca, London: Cornell University Press, 1992), 49, http://www.jstor.org/stable/10.7591/j.ctv2n7hxs.
[16] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 156.

κανόνων προστασίας προσωπικών δεδομένων που εστίαζαν στη δραστηριότητα του δημοσίου τομέα, με αποτέλεσμα οι πρώτες νομοθετικές προσπάθειες να εστιάζουν στην οριοθέτηση της αυτοματοποιημένης επεξεργασίας που λάμβανε χώρα στον δημόσιο τομέα.[17]

Η προστασία των προσωπικών δεδομένων συνδέθηκε έτσι άρρηκτα με την τεχνολογική πρόοδο και με την χρήση υπολογιστικών συστημάτων που εν δυνάμει μπορούσαν να θέσουν σε κίνδυνο τα θεμελιώδη δικαιώματα των φυσικών προσώπων και τις ελευθερίες τους και ειδικά το δικαίωμά τους στην ιδιωτικότητα. Τα υπολογιστικά συστήματα έχουν τη δυνατότητα να συλλέγουν και να αθροίζουν τεράστιες ποσότητες πληροφοριών. Μέχρι την εμφάνισή τους, τα αρχεία που περιείχαν δεδομένα προσωπικού χαρακτήρα παρέμεναν διασκορπισμένα σε διαφορετικές υπηρεσίες και διαφορετικά τμήματα υπηρεσιών, καθιστώντας την εύρεση και εξακρίβωσή τους δυσχερή. Τα πληροφοριακά συστήματα εισήγαγαν νέους, ευκολότερους και ταχύτερους τρόπους αναδίφησης και εξεύρεσης των δεδομένων. Ως αποτέλεσμα των εξελίξεων στον τομέα των υπολογιστικών συστημάτων, περισσότερα δεδομένα συγκεντρώνονταν και αποθηκεύονταν και καθίσταντο διαθέσιμα σε ποικίλους ενδιαφερόμενους που τα χρησιμοποιούσαν για διαφορετικούς σκοπούς. Συνδυαστικά αυτές οι εξελίξεις δημιούργησαν το όραμα ενός μέλλοντος στο οποίο η προσωπική ελευθερία και η πληροφοριακή αυτοδιάθεση θα εξαρτάται από την έκβαση αδιαφανών και αμφισβητήσιμων διαδικασιών επεξεργασίας δεδομένων.[18]

Ο πρωτεύον στόχος της νομοθεσίας περί προστασίας προσωπικών δεδομένων είναι η προστασία των ατόμων και κατ' επέκταση της κοινωνίας ενάντια σε βλάβες που είναι δυνατό να προκληθούν από την κατάχρηση των προσωπικών τους δεδομένων.[19] Οι σχετικοί νόμοι που έχουν θεσπιστεί για την επίτευξη αυτού του στόχου εισάγουν μια σειρά διαδικαστικών δικλείδων για να προστατέψουν τα υποκείμενα από πιθανές παραβιάσεις της ιδιωτικότητάς τους. Συνοπτικά, η νομοθεσία προστασίας προσωπικών δεδομένων αποσκοπεί στην προστασία της ιδιωτικότητας των υποκειμένων και των σχετικών με αυτήν κοινωνικών αξιών και ενισχύει την υποχρέωση λογοδοσίας όσων χειρίζονται, διατηρούν και χρησιμοποιούν προσωπικά δεδομένα. Παράλληλα βελτιώνουν την ακεραιότητα και την αποτελεσματικότητα των διαδικασιών λήψης αποφάσεων.[20]

1.2 Η αξία της ιδιωτικότητας

Ως έννοια, η ιδιωτικότητα χαρακτηρίζεται από έλλειψη σταθερότητας ως προς τον ορισμό της[21]. Με αφετηρία την ρήση «η οικία του καθενός είναι το κάστρο του», επιχειρήθηκε το 1604 να οριοθετηθεί η ιδιωτική ζωή των ατόμων στο πλαίσιο του οίκου τους και να θεμελιωθεί το δικαίωμά τους να μένουν ανεξάρτητοι από τη δημόσια ζωή. Έτσι, την ίδια χρονιά ο Sir Edward Coke στο King's Bench of England, εγκαθίδρυσε το δικαίωμα του ιδιοκτήτη ενός οίκου να προστατεύει την οικία του ενάντια σε κάθε εισβολή.[22] Η απόφαση στη σχετική υπόθεση οδήγησε

---

[17] Frits W. Hondius, *Emerging Data Protection in Europe*, 1st ed. (repr., American Elsevier Pub. Co, 1975), 22-23.
[18] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 157.
[19] P.J.A. de Hert de Hert and S. Gutwirth, "Privacy, Data Protection and Law Enforcement: Opacity of The Individual and Transparency of Power", in *Privacy and The Criminal Law*, 1st ed. (repr., Antwerp/Oxford: Intersentia,2006),76, https://www.researchgate.net/publication/254800085_Privacy_data_protection_and_law_enforcement_Opacity_of_the_individual_and_transparency_of_power.
[20] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 158.
[21] Lee Bygrave, Privacy and data protection in an international perspective. *Scandinavian Studies in Law* 56:169. Διαθέσιμο στο: https://scandinavianlaw.se/pdf/56-8.pdf.
[22]"Semayne's Case Definition", Duhaime.Org, 2021, Διαθέσιμο στο: http://www.duhaime.org/LegalDictionary/S/SemaynesCase.aspx.

στην θέσπιση μιας πρώιμης μορφής του δικαιώματος στην ιδιωτικότητα. Το δόγμα αυτό ήταν επαρκές για την εποχή εκείνη, καθώς η κοινωνική ζωή και οι τρόποι επικοινωνίας περιορίζονταν στις διαπροσωπικές επαφές. Έκτοτε, οι νομικές κατασκευές για την προστασία της ιδιωτικότητας έχουν μετεξελιχθεί χάρη στην ραγδαία ανάπτυξη της τεχνολογίας. Ο πολλαπλασιασμός των έντυπων εκδόσεων που συντελέστηκε από το 1850 μέχρι το 1900 και η αδιάκριτη φύση των φωτορεπόρτερ που πάσχιζαν να απαθανατίσουν τα μέλη των ανώτερων τάξεων, οδήγησαν στην επινόηση της φράσης «το δικαίωμα να μην δέχεται κανείς οχλήσεις» (***right to be left alone***), από τους Samuel Warren και Louis Brandeis.[23] Στον πυρήνα της ανάλυσής τους βρίσκονταν οι τρόποι με τους οποίους το δίκαιο αναγνωρίζει τις ανάγκες της κοινωνίας και πώς αυτό εξελίσσεται για να ανταποκριθεί σε αυτές τις ανάγκες (όπως για παράδειγμα η ανάπτυξη της νομικής έννοιας της ιδιοκτησίας επεκτάθηκε στην έννοια της κυριότητας άυλων αγαθών και εν τέλει επέκτεινε το δικαίωμα στη ζωή).[24] Η φράση δημοσιεύτηκε το 1890 και προέρχεται από μια πραγματεία του δικαίου περί των αδικοπραξιών του 1879. Αποτελεί έκτοτε ένα από τα πιο διάσημα νομικά άρθρα που αφορούν το δικαίωμα στην ιδιωτικότητα και νοείται ως διαχωρισμός από την δημόσια παρατήρηση και εισβολή.[25]Η εννοιολόγηση της ιδιωτικότητας ως «δικαίωμα να μην δέχεται κανείς οχλήσεις», ανταποκρινόταν έτσι στην ανάγκη μετεξέλιξης της κοινωνίας ώστε να προστατεύει τα υποκείμενα από παραβιάσεις της ιδιωτικής και οικιακής τους ζωής. Οι παραβιάσεις αυτές ήταν το αποτέλεσμα της εμφάνισης νέων εφευρέσεων και επιχειρηματικών μοντέλων που απειλούσαν την σφαίρα της ιδιωτικής ζωής των υποκειμένων.[26]

Το άρθρο των Warren και Brandeis, αναφορικά με την έννοια του δικαιώματος στην ιδιωτικότητα, επιχειρούσε να εξετάσει αν οι νόμοι της εποχής (1980) περιείχαν αρχές που μπορούσαν να γίνουν αντικείμενο επίκλησης ώστε να προστατευθεί η ιδιωτικότητα των πολιτών. Η έννοια του δικαιώματος στην ιδιωτικότητα όπως την όρισαν, αποτέλεσε τη βάση των νόμων περί προστασίας της ιδιωτικότητας των Η.Π.Α καθώς υιοθετήθηκε στην υπόθεση Katz v US[27] στην οποία κρίθηκε ότι ο Katz μπορούσε να τεθεί υπό το προστατευτικό καθεστώς της Τέταρτης Τροπολογίας του αμερικανικού Συντάγματος αναφορικά με τις συνομιλίες του και δεν απαιτούνταν να υπάρχει φυσική εισβολή στον χώρο που καταλάμβανε ώστε να επικαλεστεί την Τροπολογία. Η τέταρτη τροπολογία επισημαίνει ότι οι άνθρωποι έχουν το δικαίωμα, «να είναι ασφαλείς στα πρόσωπα, τα σπίτια, τα χαρτιά και τα αποτελέσματά τους, έναντι παράλογων αναζητήσεων και κατασχέσεων». Σύμφωνα με τον δικαστή Potter Stewart, «Η Τέταρτη Τροπολογία προστατεύει τους ανθρώπους και όχι μέρη». Η υπόθεση έθεσε τις βάσεις για την δοκιμή «εύλογης προσδοκίας της ιδιωτικής ζωής» που εξακολουθεί να χρησιμοποιείται σήμερα κατά τον προσδιορισμό του κατά πόσον η αστυνομία χρειαζόταν ένταλμα για να πραγματοποιήσει έρευνα. Επίσης, το αρμόδιο Δικαστήριο επεσήμανε την ανάγκη για επέκταση του καθεστώτος προστασίας της ιδιωτικής ζωής ενόψει της ραγδαίας τεχνολογικής ανάπτυξης.[28] Οι Warren και Brandeis, ισχυρίζονταν επίσης ότι το σχετικό

---

[23] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890), 4, *Harvard Law Review,* 193.
[24] Temilola Abdul, "The Concept of Privacy: Is Privacy Still a Useful Concept?", *SSRN Electronic Journal*, 2020, 3, doi:10.2139/ssrn.3668520.
[25] Sanjay Sharma, *Data Privacy and GDPR Handbook*, 1st ed. (repr., Newark, United States: John Wiley & Sons, Incorporated, 2020), 24.
[26] Erin K Coyle, 'E. L. Godkin's Criticism of the Penny Press: Antecedents to a Legal Right to Privacy' (2014) 31, *American Journalism*, 262.
[27] "Katz v. United States." Oyez. Accessed July 15, 2021. https://www.oyez.org/cases/1967/35.
[28] "Katz Κατά Ηνωμένων Πολιτειών: Ανώτατο Δικαστήριο, Επιχειρήματα, Επιπτώσεις", Greelane.Com, 2020, http://bit.ly/3yZKCIL.

δικαίωμα έβρισκε επίσης έκφραση στην γαλλική νομοθεσία και συγκεκριμένα στον νόμο σχετικά με τον τύπο (***Loi relative à la presse***) της 11ης Μαΐου 1868, που απαγόρευε την έκδοση γεγονότων που αφορούσαν την ιδιωτική ζωή των ατόμων (***vie privée***), εκτός αν τα δεδομένα ήταν ήδη δημόσια ή δημοσιευμένα βάσει της συγκατάθεσης του υποκειμένου.[29] Ο Daniel Solove, θεώρησε ότι η εννοιολόγηση των Warren και Brandeis απέτυχε να δώσει σαφείς κατευθύνσεις ως προς το περιεχόμενο της ιδιωτικότητας και αποτυπώνει αυτήν ως ένα είδος ανοσίας ή μια μορφή απομόνωσης.[30]

Παρά το γεγονός ότι η ιδιωτικότητα εισήχθη ως δικαίωμα το 1890 από τους Warren και Brandeis, η συζήτηση γύρω από αυτήν έχει λάβει έντονο χαρακτήρα τις τελευταίες τρείς δεκαετίες, λόγω της ραγδαίας ανάπτυξης των επιστημών της πληροφορικής και των πληροφοριών. Όπως χαρακτηριστικά αναφέρει ο Introna, η ιδιωτικότητα αναδύθηκε ως φιλοσοφικό ζήτημα κατά την δεκαετία του 1960 και έκτοτε έχει αποτελέσει το αντικείμενο εκτεταμένων αντιπαραθέσεων εντός των ακαδημαϊκών, νομικών και κοινωνικών κύκλων.[31] Παρ ’όλα αυτά δεν υπάρχει ένας κοινώς αποδεκτός ορισμός για τον προσδιορισμό της ιδιωτικότητας. Θεωρείται έτσι είτε ως το δικαίωμα να μένει κανείς μόνος του, είτε ως «η ισχύς του καθενός να αποκαλύπτει επιλεκτικά τον εαυτό του στον κόσμο», είτε ως ο έλεγχος επί των προσωπικών πληροφοριών ή ακόμα και η ελευθερία να μην υπάγεται κανείς σε κρίση από άλλους. Ο Post εξηγεί ότι: «η ιδιωτικότητα αποτελεί μια αξία τόσο περίπλοκη, τόσο μπλεγμένη σε ανταγωνιζόμενες και αντιτιθέμενες διαστάσεις, τόσο διεσταλμένη με ποικίλα και διακριτά νοήματα, που μερικές φορές απελπίζομαι αναφορικά με το αν μπορεί να αντιμετωπιστεί επαρκώς.» Ο ίδιος κατηγοριοποιεί την ιδιωτικότητα, ως δύο αντιτιθέμενα και ανταγωνιζόμενα δικαιώματα, την ιδιωτικότητα ως αξιοπρέπεια και την ιδιωτικότητα ως ελευθερία. Η ιδιωτικότητα ως αξιοπρέπεια διαφυλάττει τις κοινωνικοποιημένες πλευρές του εαυτού, ενώ η ιδιωτικότητα ως ελευθερία διαφυλάττει τις αυθόρμητες, ανεξάρτητες και μοναδικά ιδιαίτερες πλευρές του εαυτού. Κάθε μια μοιάζει να είναι απαραίτητη σε μια πολιτισμένη κοινωνία, αλλά κρίνονται επίσης και ως ασύμβατες μεταξύ τους.[32] Σύμφωνα με τον Solove, ο όρος «ιδιωτικότητα», αποτελεί όρο ομπρέλα και αναφέρεται σε ένα ευρύ και διασκορπισμένο σύνολο συσχετιζόμενων πραγμάτων, ενώ παράλληλα δεν μπορεί να κατανοηθεί ανεξάρτητα από την κοινωνία εφόσον η ιδιωτικότητα, στον πυρήνα της, αποτελεί ένα κοινωνικό τεχνούργημα και χωρίς το κοινωνικό πλαίσιο, δεν θα υπήρχε ανάγκη για ιδιωτικότητα. Επίσης, προτείνει μια ταξονομία των απειλών της ιδιωτικότητας, που εστιάζει στα διαφορετικά είδη δραστηριοτήτων που θίγουν την ιδιωτικότητα και υποδεικνύει τις διαφορετικές βλάβες και προβλήματα.[33]

Η ιδιωτικότητα επίσης θεωρείται κρίσιμη για την προστασία μιας σειράς συσχετιζόμενων κοινωνικών αξιών, όπως της ατομικότητας, της αυτονομίας και της αξιοπρέπειας. Ενώ δεν υπάρχει συναίνεση ως προς τον ορισμό του δικαιώματος στην ιδιωτικότητα, οι διάφορες εννοιολογήσεις

---

[29] Warren, Samuel, and Louis Brandeis. 1890. The right to privacy. *Harvard Law Review*, 4, (5): 214

[30] Temilola Abdul, "The Concept of Privacy: Is Privacy Still a Useful Concept?", *SSRN Electronic Journal*, 2020, 4, doi:10.2139/ssrn.3668520. Διαθέσιμο στο: bit.ly/3hFHRXc

[31] Eugenia Politou et al., *Privacy and Data Protection Challenges in The Distributed Era*, 1st ed. (repr., Cham: Springer International Publishing AG, 2021), 8.

[32]Robert C. Post, "Three Concepts of Privacy", *Faculty Scholarship Series* 185 (2001): 2087, https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1184&context=fss_papers.

[33] Daniel J. Solove, "A Taxonomy of Privacy", *University of Pennsylvania Law Review* 154, no. 3 (2006): 477, doi:10.2307/40041279.

έχουν εφαρμοστεί μέσω των προβλέψεων της νομοθεσίας της προστασίας των δεδομένων. Για παράδειγμα, τα δικαιώματα των υποκειμένων που αφορούν την διαγραφή ή τον περιορισμό της επεξεργασίας, μπορούν να θεωρηθούν ως (μερικές) εκφάνσεις ενός δικαιώματος για τον έλεγχο της κυκλοφορίας των προσωπικών πληροφοριών που αφορούν ένα υποκείμενο. Παρομοίως, η ειδική αντιμετώπιση ορισμένων τύπων «ευαίσθητων» δεδομένων (λ.χ. δεδομένων που σχετίζονται με την υγεία ή τη σεξουαλική ζωή), μπορούν να θεωρηθούν ως μια προσπάθεια για περιορισμό της πρόσβασης στις πιο ενδόμυχες προσωπικές λεπτομέρειες του υποκειμένου. Καμία από τις προαναφερθείσες εννοιολογήσεις της ιδιωτικότητας, ωστόσο, δεν μπορεί να καλύψει επαρκώς τα δικαιώματα και τις υποχρεώσεις που συναντώνται στην νομοθεσία της προστασίας των προσωπικών δεδομένων.[34]

1.3 Η ιδιωτικότητα στην ψηφιακή εποχή

Σε μια οικονομία που λειτουργεί με «γνώμονα τα δεδομένα» (***data-driven***), δίνεται η εντύπωση ότι η ιδιωτικότητα έχει περιοριστεί ή ακόμα και εξαλειφθεί. Ο ιδρυτής του Facebook, Mark Zuckerberg, ισχυρίστηκε ότι η ιδιωτικότητα έχει εξελιχθεί τα τελευταία χρόνια και δεν μπορεί πλέον να θεωρηθεί ως κοινωνική νόρμα. Παρά τον ισχυρισμό αυτό, η ιδιωτικότητα δεν έχει χάσει την ισχύ της. Αντιθέτως, αν λάβουμε υπόψιν τους νέους τύπους παραβιάσεων της ιδιωτικότητας που κάνουν συνεχώς την εμφάνισή τους, μπορούμε να κατανοήσουμε ότι η ιδιωτικότητα είναι πιο επίκαιρη και σχετική από ποτέ. Ο ίδιος ο Zuckerberg αποτελεί απόδειξη αυτής της πραγματικότητας. Σε μια φωτογραφία που κοινοποιήθηκε στο Twitter το καλοκαίρι του 2016, διακρίνεται ο υπολογιστής του, στον οποίο η κάμερα και η θύρα των ακουστικών είναι καλυμμένες με ταινία και το πρόγραμμα διαχείρισης αλληλογραφίας που χρησιμοποιεί είναι το Thunderbird, το οποίο φημίζεται για την πολιτική προστασίας της ιδιωτικότητας των χρηστών. Το παράδειγμα του Zuckerberg, αποτελεί μια ένδειξη μιας ευρύτερης τάσης, σύμφωνα με την οποία οι άνθρωποι αποδίδουν ολοένα και περισσότερη σημασία στην διατήρηση της ιδιωτικότητας της εργασίας και της προσωπικής τους ζωής.

Στην εποχή μας, αυτό που θέτει την ιδιωτικότητά μας σε κίνδυνο είναι το καθεστώς παρακολούθησης των δεδομένων μας (***dataveillance***). Η πρακτική της παρακολούθησης αυτής συνίσταται στην συστηματική χρήση συστημάτων προσωπικών δεδομένων για την έρευνα ή την παρακολούθηση των ενεργειών ή των επικοινωνιών ενός ή περισσότερων υποκειμένων. Στην οικονομία των δεδομένων, στην οποία η συμπεριφορά και όλες οι ενέργειες των υποκειμένων, δεδομενοποιούνται με ραγδαίους ρυθμούς, η πρακτική της παρακολούθησης των δεδομένων διεξάγεται με μεγάλη ευκολία και με μικρό κόστος. Ως αποτέλεσμα, περισσότερα άτομα και μεγαλύτεροι πληθυσμοί μπορούν να αποτελέσουν αντικείμενο παρακολούθησης. Αυτό κρίνεται ιδιαίτερα επικίνδυνο, καθώς επιτρέπει την παρεμβολή σχετικά με γεγονότα και πληροφορίες που οι περισσότεροι προτιμούν να μένουν κρυφά. Για παράδειγμα, ένα άτομο μπορεί να μοιραστεί πληροφορίες που αφορούν τα χόμπι του ή τα αγαπημένα του βιβλία αλλά όχι πληροφορίες που αφορούν το σεξουαλικό προσανατολισμό του. Παρ ‘όλα αυτά, μέσω της χρήσης τεχνικών μηχανικής μάθησης και μεγάλων δεδομένων, οι πληροφορίες αυτές μπορούν να προβλεφθούν έτσι και αλλιώς.[35] Οι Kosinski, Stillwell και Graepel, έχουν επισημάνει πώς μια σειρά ιδιαίτερα

[34] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 158.
[35] Helena U Vrabec, *Data Subject Rights Under The GDPR*, 1st ed. (repr., Oxford, United Kingdom: Oxford University Press, 2021), 4.

ευαίσθητων προσωπικών χαρακτηριστικών, όπως ο σεξουαλικός προσανατολισμός, η εθνικότητα, οι θρησκευτικές και πολιτικές πεποιθήσεις, τα χαρακτηριστικά της προσωπικότητας, η χρήση εθιστικών ουσιών κ.λπ., μπορούν να προβλεφθούν με μεγάλη ακρίβεια με βάση τα δεδομένα αρεσκείας στο Facebook.[36]

Δεν αποτελεί υπερβολή ο ισχυρισμός ότι η σημερινή οικονομία «επικεντρώνεται στην εξαγωγή και την χρήση ενός συγκεκριμένου τύπου βασικής πρώτης ύλης: των δεδομένων». Στην πιο βασική τους μορφή τα μεγάλα δεδομένα χαρακτηρίζονται από τον μεγάλο όγκο τους (***volume***), από την ποικιλομορφία των τύπων δεδομένων (***variety***) και από την ταχύτητα με την οποία τα δεδομένα αυτά επεξεργάζονται (***velocity***).[37] Στο πλαίσιο αυτό, ακόμα και τα ανωνυμοποιημένα δεδομένα δεν μπορούν να εγγυηθούν την ιδιωτικότητα. Στην πραγματικότητα, τα ανωνυμοποιημένα δεδομένα μπορούν να θεωρηθούν το ίδιο χρήσιμα με τα προσωπικά δεδομένα σε πολλές περιπτώσεις. Ένα τυπικό παράδειγμα μπορεί να αφορά μια εταιρεία που θέλει να εξατομικεύσει τις εκστρατείες μάρκετινγκ της, με τη βοήθεια των τεχνικών κατάρτισης προφίλ (***profiling***). Η χρήση προσωπικών δεδομένων, μπορεί στο πλαίσιο αυτό να φανεί χρήσιμη για να αξιολογήσει η εταιρεία ποιοι πελάτες ενδιαφέρονται δυνητικά να προβούν στην αγορά συγκεκριμένων προϊόντων ή υπηρεσιών, αλλά τα συγκεντρωτικά δεδομένα (***aggregated data***) σε ένα τοπικό επίπεδο, μπορεί να φανούν παρομοίως χρήσιμα και λιγότερο κοστοβόρα ως προς την επεξεργασία τους.[38] Η συναγωγή πληροφοριών από ομαδικά προφίλ, δύναται να οδηγήσει σε προβλέψεις που αφορούν τις προσωπικές περιστάσεις των ατόμων. Από τη στιγμή που τα διαθέσιμα δεδομένα για ένα συγκεκριμένο άτομο αντιστοιχήσουν στα συναχθέντα δεδομένα (π.χ. ένα προφίλ), που δεν απαιτούνται να είναι προσωπικά δεδομένα, καθίσταται δυνατό να προβλεφθούν με ακρίβεια τα χαρακτηριστικά των μεμονωμένων χρηστών.[39]

Η ροή των δεδομένων ανάμεσα στους δρώντες στην δεδομενοποιημένη οικονομία, κλιμακώνει το ρίσκο των παραβιάσεων της ιδιωτικότητας. Αυτός είναι και ο λόγος που η Nissenbaum πιστεύει ότι η ανταπόκριση στις προσωπικές προσδοκίες αναφορικά με την ροή των προσωπικών πληροφοριών, έγκειται στον πυρήνα της ιδιωτικότητας.[40] Τα προσωπικά δεδομένα συχνά αποκτώνται από μια σειρά πηγών δεδομένων, συμπεριλαμβανομένων και των μεσιτών δεδομένων (***data brokers***), μέσω του συνδυασμού των δεδομένων. Για παράδειγμα, οι βάσεις δεδομένων του Facebook, συγχωνεύτηκαν με αναλυτικούς φακέλους οι οποίοι αποκτήθηκαν από μεσίτες δεδομένων και αφορούσαν τις απογραμμικές ζωές των χρηστών. Με αυτόν τον τρόπο, το Facebook βελτιώνει τα δεδομένα που έχει στην κυριότητά του με κατηγορίες που οι χρήστες δεν διαμοιράστηκαν ή δεν θέλησαν να αποκαλύψουν κατά τη χρήση της πλατφόρμας.[41]

---

[36] Michal Kosinski, David Stillwell and Thore Graepel, "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior", *Proceedings of The National Academy of Sciences* 110, no. 15 (2013): 5802, doi:10.1073/pnas.1218772110.

[37] Ignas Kalpokas, *Algorithmic Governance: Politics and Law in The Post-Human Era*, 1st ed. (repr., Cham, Switzerland: Palgrave Pivot, 2019), 11.

[38] Helena U Vrabec, *Data Subject Rights Under The GDPR*, 1st ed. (repr., Oxford, 2021), 5.

[39] Ariel Porat and Lior Strahilevitz, "Personalizing Default Rules and Disclosure with Big Data", *SSRN Electronic Journal* 112 (2013): 1417,1440, doi:10.2139/ssrn.2217064.

[40] Helen Fay Nissenbaum, *Privacy in Context*, 1st ed. (repr., [S.l.]: Stanford University Press, 2010), 72.

[41] Julia Angwin, Terry Jr. Parris and Surya Mattu, "Facebook Is Quietly Buying Information from Data Brokers About Its Users' Offline Lives", Business Insider, 2016, https://www.businessinsider.com/facebook-data-brokers-2016-12#:~:text=Facebook%20is%20quietly%20buying%20information,about%20its%20users'%20offline%20lives&text=Nor%20does%20Facebook%20show%20users,the%20Center%20for%20Digital%20Democracy

Επιπροσθέτως, το διαχωριστικό όριο ανάμεσα στην πρόβλεψη μιας συμφωνίας για την παράδοση των δεδομένων ενός υποκειμένου και της έλλειψης αυτής καθίσταται ολοένα και πιο δυσδιάκριτο. Ενώ τα καταγραφόμενα δεδομένα (***captured data***) οφείλονται στις άμεσες και συστηματικές παρατηρήσεις και μετρήσεις και απαιτούν τουλάχιστον την οικειοθελή δημοσιοποίηση, η κυρίαρχη μορφή τύπων δεδομένων που ονομάζονται «δεδομένα-καυσαέρια» (***exhaust data***), αποτελούν το υποπροϊόν μιας διαδικασίας της οποίας ο πρωταρχικός σκοπός είναι κάτι διαφορετικό από την απλή καταγραφή δεδομένων και επομένως συλλέγονται αυτομάτως.[42]Τέτοιου είδους δεδομένα αποκτώνται, συγκεντρώνονται, καθαρίζονται, τεκμηριώνονται, αναλύονται, ομαδοποιούνται, πωλούνται, αναλύονται περαιτέρω και πωλούνται ξανά. Καθίσταται προφανές ότι από τη στιγμή που τα δεδομένα θα επαναπροσδιοριστούν ως άχρηστο υλικό, η εξαγωγή και η οικονομική τους αξιοποίηση δεν είναι πιθανό να συναντήσει εμπόδια.

Στο σημείο αυτό θα πρέπει να γίνει αναφορά στην Google, η οποία έγινε η μεγαλύτερη και πιο επιτυχημένη εταιρεία που διαχειρίζεται «μεγάλα δεδομένα», γιατί είναι ένας από τους ιστοτόπους με τη μεγαλύτερη επισκεψιμότητα και αυτό έχει ως αποτέλεσμα να έχει στη διάθεσή της τα περισσότερα «δεδομένα-καυσαέρια». Η Google αποτελεί μια από τις πολλές εκ γενετής ψηφιακές εταιρείες, που έσπευσαν να προλάβουν την απότομη αύξηση της ζήτησης που κατέκλυσε την ιδιωτική διαδικτυακή σφαίρα, τα πρώτα χρόνια του Παγκόσμιου Ιστού. Καθώς οι τεχνολογίες εξελίσσονταν και οι χρήστες αυξάνονταν, η πίεση για αύξηση του κέρδους μεγάλωνε και η διοίκηση της εταιρείας άρχισε να εξετάζει πιθανές επιπτώσεις που θα είχε στην αύξηση των χρηστών η χρέωση ανά υπηρεσία. Αντί για την χρέωση αυτή, επέλεξε το μοντέλο της διαφήμισης. Η προσέγγιση αυτή βασίζεται στη δυνατότητα απόκτησης των δεδομένων των χρηστών ως πρώτη ύλη, επί της οποίας διενεργούνται αναλύσεις και αναπτύσσονται αλγόριθμοι που έχουν τη δυνατότητα να εξειδικεύουν και να πωλούν τη διαφήμιση μέσω ενός εξειδικευμένου μοντέλου δημοπράτησης με μεγάλη ακρίβεια και επιτυχία. Η Google αφότου εφάρμοσε το μοντέλο αυτό, είδε τα έσοδά της να αυξάνονται ραγδαία, με αποτέλεσμα να εστιάζει πλέον στην επιστράτευση ακόμα πιο αποτελεσματικών μεθόδων για την συγκέντρωση των δεδομένων. Το Google AdWords, η αλγοριθμική μέθοδος δημοπρασιών της Google για διαδικτυακές υπηρεσίες διαφήμισης, αναλύει τεράστιες ποσότητες δεδομένων ώστε να καθορίσει ποιες διαφημιστικές κατέχουν πρωτεύουσα θέση στις σελίδες των αποτελεσμάτων αναζήτησης.[43]

1.4 Η σχέση ανάμεσα στο δικαίωμα στην ιδιωτικότητα και το δικαίωμα της προστασίας των προσωπικών δεδομένων

Η ιδιωτικότητα και η προστασία των προσωπικών δεδομένων από μια νομική σκοπιά αντιπροσωπεύουν δύο διακριτά θεμελιώδη δικαιώματα που υπάγονται στο ευρωπαϊκό δίκαιο, το οποίο καθορίζει την πρώτη ως ένα θεμελιώδες δικαίωμα που δημιουργείται για να εξασφαλίσει την προστασία και την προώθηση των συμφερόντων των ατόμων και της κοινωνίας, ενώ η δεύτερη λογίζεται ως διαδικαστική και επομένως λειτουργεί στο επίπεδο θέσπισης των κανόνων, των μεθόδων και των συνθηκών, μέσω των οποίων τα θεμελιώδη δικαιώματα εφαρμόζονται και

[42] John D Kelleher and Brendan Tierney, *Data Science*, 1st ed. (repr., Cambridge, MA: The MIT Press, 2018), 52.
[43] Shoshana Zuboff, "Ο Μεγάλος Άλλος: Ο Καπιταλισμός Της Επιτήρησης Και Οι Προοπτικές Ενός Πολιτισμού Της Πληροφορίας", in *Εισαγωγή Στις Ψηφιακές Σπουδές*, 1st ed. (repr., Θεσσαλονίκη: Εκδόσεις Ροπή, 2020), 365.

προστατεύονται αποτελεσματικά.[44] Το ξεχωριστό θεμελιώδες δικαίωμα στην προστασία των προσωπικών δεδομένων, είχε προβλεφθεί στην Σύμβαση 108/1981 του Συμβουλίου της Ευρώπης «Για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων», γνωστή και ως Σύμβαση 108, η οποία αποτέλεσε το πρώτο δεσμευτικό διεθνές κείμενο και σήμανε την απαρχή μιας δεύτερης περιόδου για την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων.[45] Το δικαίωμα αναγνωρίστηκε επίσης ως θεμελιώδες και αυτόνομο με βάση το άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, που τέθηκε σε ισχύ από την Συνθήκη της Λισαβώνας το 2009.[46] Έχει υποστηριχθεί ότι οι αρχές πάνω στις οποίες βασίζεται το ανθρώπινο δικαίωμα στην προστασία των προσωπικών δεδομένων, αντικατοπτρίζουν κάποιες πρωτεύουσες αξίες, εγγενείς στην ευρωπαϊκή νομική τάξη, όπως η ιδιωτικότητα, η διαφάνεια, η αυτονομία και η απαγόρευση των διακρίσεων. Συνεπώς, υπό το πρίσμα μιας καθοριστικής σύλληψης, μπορούμε να ισχυριστούμε ότι το δικαίωμα στην προστασία των προσωπικών δεδομένων, μπορεί να αποτελέσει μια δικλείδα ασφαλείας, όχι μόνο για την ιδιωτικότητα, αλλά και για όλα τα θεμελιώδη δικαιώματα. Το δικαίωμα στην ιδιωτικότητα, από την άλλη μεριά, αποτελεί επίσης ένα καθιερωμένο δικαίωμα με βάση την Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου (άρθρο 8), η οποία τέθηκε σε ισχύ το 1953.[47]

Το δικαίωμα στην προστασία των προσωπικών δεδομένων και το δικαίωμα στον «ιδιωτικό βίο» βρίσκονται σε στενή σχέση μεταξύ τους, αλλά δεν είναι εναλλάξιμα. Από πολλές απόψεις, το δικαίωμα στην προστασία των προσωπικών δεδομένων χαρακτηρίζεται από πιο περιορισμένο πεδίο εφαρμογής σε σχέση με το δικαίωμα στην ιδιωτικότητα. Η ιδιωτικότητα των δεδομένων βρίσκει εφαρμογή σε περιπτώσεις όπου δεν εφαρμόζεται η προστασία των προσωπικών δεδομένων, όπως για παράδειγμα στις περιπτώσεις των φυσικών παρεμβάσεων στην ιδιωτικότητα ή στις περιπτώσεις που τα δεδομένα είναι ανωνυμοποιημένα. Υπάρχουν όμως και περιπτώσεις στις οποίες η προστασία των προσωπικών δεδομένων έχει ευρύτερο πεδίο εφαρμογής σε σχέση με την (πληροφοριακή) ιδιωτικότητα. Αυτό συμβαίνει όταν τα προσωπικά δεδομένα έχουν εσκεμμένα δημοσιευτεί, υποδηλώνοντας κατά αυτόν τον τρόπο ότι έχει πραγματοποιηθεί παραίτηση από το δικαίωμα στην ιδιωτικότητα και συνεπώς η προστασία του άρθρου 7 του Χάρτη Θεμελιωδών δικαιωμάτων δεν θα πρέπει να παρέχεται πλέον. Σε τέτοιες περιπτώσεις, η προστασία των προσωπικών δεδομένων παραμένει ενεργή και εφαρμοστέα και επομένως παρέχει διευρυμένη προστασία. Οι δικαστές του Ευρωπαϊκού Δικαστηρίου των Ανθρωπίνων Δικαιωμάτων (ΕΔΔΑ), οι οποίοι μειοψήφησαν στην υπόθεση Magyar Helsinki Bizottsag κατά Ουγγαρίας, αναγνώρισαν επίσης ότι η προστασία των προσωπικών πληροφοριών, που βρίσκεται σε στενή σχέση με την έννοια του πληροφοριακού αυτοκαθορισμού, θα πρέπει να διασφαλίζεται ανεξάρτητα από το εάν τα δεδομένα είναι δημοσιοποιημένα ή παραμένουν εμπιστευτικά. Στις Η.Π.Α τα δημοσιοποιημένα

[44] Norberto Nuno Gomes de Andrade, "Oblivion: The Right to Be Different … From Oneself: Re-Proposing the Right to Be Forgotten", in *The Ethics of Memory in A Digital Age*, 1st ed. (repr., Palgrave Macmillan, 2014), 65-81.
[45] Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, *Προσωπικά Δεδομένα*, 1η εκδ. (Θεσσαλονίκη: Νομική Βιβλιοθήκη, 2016), 201.
[46] Charter of Fundamental Rights of the European Union, Charter of Fundamental Rights of the European Union, 2012/C 326/02 (2012)
[47] "European Convention on Human Rights, Convention for The Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, As Amended) (ECHR) (1950)", Echr.Coe. Int, 2021, https://www.echr.coe.int/documents/convention_ell.pdf.

δεδομένα δεν εμπίπτουν στην προβλεπόμενη από την Τέταρτη Τροπολογία προστασία της ιδιωτικότητας.[48]

Στην σύμφωνη γνώμη της στην υπόθεση Jones, η δικαστής του Ανωτάτου Δικαστηρίου των Η.Π.Α Sotomayor, αμφισβήτησε το δόγμα αυτό ως ένα βαθμό, αναφέροντας ότι: «στην ουσία, ίσως είναι απαραίτητο να επανεξετάσουμε την πρόβλεψη σύμφωνα με την οποία ένα άτομο δεν έχει εύλογη προσδοκία ιδιωτικότητας για πληροφορίες που έχουν εθελουσίως γνωστοποιηθεί σε τρίτα μέρη…η προσέγγιση αυτή δεν είναι κατάλληλη για την ψηφιακή εποχή, στην οποία οι άνθρωποι αποκαλύπτουν πληθώρα πληροφοριών για τους εαυτούς τους σε τρίτα μέρη, καθώς εκτελούν τα κοινότοπα καθήκοντά τους».[49] Στην Ευρωπαϊκή Ένωση, τέτοιες περιπτώσεις μπορούν να αντιμετωπιστούν ως ένα βαθμό μέσω των κανόνων προστασίας προσωπικών δεδομένων.

Πέρα από τη διαφορά τους όσον αφορά την εμβέλεια, η προστασία προσωπικών δεδομένων και η ιδιωτικότητα θα πρέπει να διακριθούν λόγω των διαφορετικών υποκείμενων στόχων τους. Η Lynskey επισημαίνει δύο στόχους που ανήκουν στην προστασία των προσωπικών δεδομένων ως δικαίωμα. Ο πρώτος στόχος αφορά την ανάπτυξη της ατομικής προσωπικότητας ενώ ο δεύτερος στόχος αφορά την μείωση της ισχύος και των πληροφοριακών ασυμμετριών ανάμεσα στα υποκείμενα και σε όσους επεξεργάζονται τα δεδομένα τους.[50] Σε ένα πιο πρακτικό επίπεδο, ο Kranenborg, αναγνωρίζει την μοναδική αποστολή του δικαιώματος της προστασίας των προσωπικών δεδομένων, η οποία έγκειται στην αντιμετώπιση των τεχνολογικών εξελίξεων και της ολοένα αυξανόμενης χρήσης των τεχνολογιών της πληροφορίας και της επικοινωνίας.[51]Το δικαίωμα αυτό εγκαθιδρύει ένα μοναδικό σύστημα «ελέγχων και ισορροπιών», που κρίνεται απαραίτητο στην σύγχρονη πραγματικότητα της επεξεργασίας των δεδομένων. Παρομοίως, ο Gellert, περιγράφει την προστασία των προσωπικών δεδομένων ως ένα μέσο ώστε να χαλιναγωγηθούν οι επιπτώσεις αυτών των τεχνολογιών στην κοινωνία αλλά και για να αντιμετωπιστούν οι κίνδυνοι για την ιδιωτικότητα και για άλλα θεμελιώδη δικαιώματα.[52] Σύμφωνα με την άποψη του, το δικαίωμα στην προστασία των δεδομένων ομοιάζει με νομοθετικές προσεγγίσεις που είναι προσανατολισμένες στους κινδύνους, όπως συμβαίνει με το δίκαιο περιβάλλοντος. Οι προσεγγίσεις που προαναφέρθηκαν, αναγνωρίζουν την προστιθέμενη αξία της προστασίας των δεδομένων εντός του συστήματος των ανθρωπίνων δικαιωμάτων. Δευτερευόντως, αναγνωρίζουν και παρέχουν εξηγήσεις για τους λόγους για τους οποίους το δικαίωμα αναδεικνύεται σε εξέχον στο πλαίσιο της οικονομίας που καθοδηγείται από τα δεδομένα.[53]

---

[48] Helena U Vrabec, *Data Subject Rights Under The GDPR*, 1st ed. (repr., Oxford, United Kingdom: Oxford University Press, 2021), 26

[49]United States v. Jones, No. 10–1259, 615 F. 3d 544 (Supreme Court of the United States, 2012). https://www.law.cornell.edu/supct/pdf/10-1259.pdf

[50] Orla Lynskey, "Deconstructing Data Protection: The "Added- Value" Of A Right to Data Protection in The EU Legal Order'", *International and Comparative Law Quarterly* 63, no. 3 (2014): 569, 589, doi:10.1017/s0020589314000244.

[51] Herke Kranenborg, "Protection of Personal Data", in *The EU Charter of Fundamental Rights: A Commentary*, 2nd ed. (repr., Bloomsbury Publishing, 2021), 264.

[52] Raphaël Gellert, "Understanding the Notion of Risk in The General Data Protection Regulation", *Computer Law & Security Review* 34, no. 2 (2018), 3,6. https://doi.org/10.1016/j.clsr.2017.12.003

[53] Helena U Vrabec, *Data Subject Rights Under The GDPR*, 1st ed. (repr., Oxford, United Kingdom: Oxford University Press, 2021), 27.

Θα πρέπει να σημειωθεί επίσης, ότι η έννοια του «ιδιωτικού βίου» έχει κατοχυρωθεί Συνταγματικά[54] και αφορά κυρίως στην προστασία της ιδιωτικής σφαίρας από κάθε είδους προσβολή. Πριν από την εισαγωγή της εν λόγω διάταξης με την αναθεώρηση του 2001, το άρθρο 9 του Συντάγματος, είχε προταθεί, σε συνδυασμό με τις διατάξεις για την ελεύθερη ανάπτυξη της προσωπικότητας, ως βάση και για την προστασία των προσωπικών δεδομένων. Σε κάθε περίπτωση, η έννοια «ιδιωτικός βίος» είναι ευρύτερη, όπως αποδεικνύεται και από τη σύγκριση των δύο διατάξεων, αφού συνάγεται ότι ο απλός νομοθέτης έχει υποχρέωση να διαμορφώσει ένα περιοριστικό και κατάλληλο νομικό πλαίσιο, εντός του οποίου θα προστατεύεται ο ιδιωτικός βίος και θα καθίσταται θεμιτή και νόμιμη η συλλογή, επεξεργασία και η χρήση των προσωπικών δεδομένων του εκάστοτε υποκειμένου. Η διάταξη του άρθρου 9^{A} δεν έχει την έννοια της απόλυτης και απαραβίαστης συλλογής, επεξεργασίας και χρήσης προσωπικών δεδομένων του ατόμου, εφόσον κάτι τέτοιο θα ερχόταν σε αντίθεση με τη διάταξη του άρθρου 5^{A} του Συντάγματος, αλλά περιέχει ως γενική εξαγγελία την «προστασία των προσωπικών δεδομένων» του ατόμου, χωρίς να διευκρινίζει το περιεχόμενό της. Σύμφωνα με άλλη άποψη, η διάταξη αυτή ουσιαστικά τυποποιεί σε συνταγματικό κείμενο προγενέστερες ρυθμίσεις διεθνών νομικών κειμένων. Επομένως, η διάταξη του άρθρου 9^{A} ανάγεται σε συνταγματικό κανόνα περιορισμού των δικαιωμάτων που παρέχονται με το άρθρο 5^{A} του Συντάγματος, δηλαδή της πληροφόρησης και συμμετοχής στην Κοινωνία της Πληροφορίας.[55]

Όσον αφορά την πρόσφατα εφαρμοσμένη νομοθεσία για την προστασία των προσωπικών δεδομένων στον ευρωπαϊκό χώρο, ο Γενικός Κανονισμός Προστασίας Δεδομένων, ρητά προσδιορίζει τα δικαιώματα, με το άρθρο 1 να αναφέρει ότι ο Κανονισμός «προστατεύει τα θεμελιώδη δικαιώματα και τις ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία δεδομένων προσωπικού χαρακτήρα».[56] Παρά το γεγονός ότι δεν εντοπίζεται κάποια αναφορά στο δικαίωμα στην ιδιωτικότητα στο κείμενο του Κανονισμού, η έννοια της ιδιωτικότητας υπονοείται στις περισσότερες αιτιολογικές σκέψεις και άρθρα.

1.5 Ιδιωτικότητα στον οικονομικό και φορολογικό τομέα

Η οικονομική ιδιωτικότητα συχνά λογίζεται ως το δικαίωμα των ατόμων να αποφασίσουν ποιες πληροφορίες οικονομικής φύσεως που τους αφορούν, θα πρέπει να γνωστοποιούνται σε άλλους και συχνά αναφέρεται στην διατήρηση της εμπιστευτικότητας των πληροφοριών των πελατών σε σχέση με τις οικονομικές συναλλαγές. Αντιθέτως, το δικαίωμα στην προστασία προσωπικών δεδομένων που προβλέπεται στους νόμους προστασίας προσωπικών δεδομένων, δεν αφορά απλά την εμπιστευτικότητα των δεδομένων που συλλέγονται και ανταλλάσσονται, αλλά παρέχει στο υποκείμενο των δεδομένων εκτεταμένα δικαιώματα, όπως το δικαίωμα τα προσωπικά του δεδομένα να συλλέγονται και να ανταλλάσσονται μόνο για νόμιμους και σαφώς καθορισμένους σκοπούς και να μην διατηρούνται για χρονικό διάστημα μεγαλύτερο από αυτό που είναι απαραίτητο για τον σκοπό της επεξεργασίας τους («αρχή του περιορισμού της περιόδου αποθήκευσης»).[57] Λαμβάνοντας υπόψιν τις αρχές προστασίας προσωπικών δεδομένων, η

[54] Βλ. Σ9§1: «…η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη…»
[55] Γεώργιος Γιαννόπουλος, *Εισαγωγή Στη Νομική Πληροφορική*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2018), 67-68.
[56] Άρθρο 1 παρ. 2 ΓΚΠΔ.
[57] Βλ. τις ΑΠΔΠΧ 24/2004, 25/2004 αποφάσεις για τον περιορισμό του χρόνου διατήρησης των δεδομένων αρχείων της ΤΕΙΡΕΣΙΑΣ Α.Ε.

φορολογική και οικονομική ιδιωτικότητα στην εποχή μας, έχουν αποκτήσει ένα ευρύτερο νόημα που περιλαμβάνει τις αντίξοες επιπτώσεις στην ιδιωτικότητα, οι οποίες οφείλονται στην εκτεταμένη συλλογή πληροφοριών, με στόχο την κατάρτιση λεπτομερών προφίλ της φορολογικής και οικονομικής συμπεριφοράς των ατόμων, είτε για την επίτευξη κέρδους είτε για ελέγχους. Ωστόσο, το δικαίωμα στην φορολογική και οικονομική ιδιωτικότητα δεν είναι απόλυτο, εφόσον ένα απόλυτο δικαίωμα στην ιδιωτικότητα θα καθιστούσε κάθε σύγχρονο φορολογικό σύστημα μη λειτουργικό. Επομένως, ο ισχυρισμός ότι η ιδιωτικότητα μπορεί να θιγεί ώστε να προστατευθούν άλλα δικαιώματα ή κοινωνικά συμφέροντα, κρίνεται θεμιτός. Πρέπει σε κάθε περίπτωση οι αρμόδιες αρχές να παρέχουν την κατάλληλη αιτιολόγηση ως προς τους λόγους για τους οποίους η ιδιωτικότητα πρέπει να αρθεί. Στο πλαίσιο της φορολόγησης, συγκεκριμένα, τα άτομα κατέχουν μόνο διαδικαστικές ασφαλιστικές δικλείδες (π.χ. ενημέρωση, παρέμβαση, διαβούλευση), και όχι ένα θεμελιώδες δικαίωμα στην ιδιωτικότητα. Η απουσία ωστόσο αυτών των διαδικαστικών δικαιωμάτων, μπορεί να αποτελεί παραβίαση του θεμελιώδους δικαιώματος της ιδιωτικότητας.[58]

1.5.1 Οι κίνδυνοι για την ιδιωτικότητα στο πλαίσιο της κατάρτισης προφίλ στο φορολογικό και οικονομικό τομέα

Πολλές εταιρείες μεγακλίμακας αλλά και φορολογικές αρχές που έχουν στη διάθεσή τους ανεπτυγμένα ψηφιακά συστήματα, έχουν πρόσβαση σε πολλά ψηφιακά δεδομένα, όπως όρους αναζήτησης, ιστολόγια, κοινωνικές διασυνδέσεις, αλλά και πληροφορίες που σχετίζονται με ψηφιακές και φορολογικές συναλλαγές. Μέσω της πρόσβασης σε εξειδικευμένες πληροφορίες που τελικά σκιαγραφούν με αναλυτικό τρόπο τη συμπεριφορά των φυσικών προσώπων, οι εταιρείες και οι αρχές έχουν τη δυνατότητα να αναπτύξουν αναλυτικά προφίλ, που αργότερα μπορούν να χρησιμοποιηθούν για να επηρεάσουν τη συμπεριφορά των καταναλωτών ή να προβλέψουν μελλοντικές νομικές και φορολογικές υποχρεώσεις. Ωστόσο, όπως αναφέρουν σχετικές μελέτες[59][60], ενώ πολλές κυβερνητικές υπηρεσίες διευρύνουν συνεχώς τη χρήση συστημάτων ανάλυσης δεδομένων (data analytics), ώστε να βελτιώσουν τη λειτουργία και τις υπηρεσίες τους, οι περισσότερες από αυτές τις υπηρεσίες υστερούν σε σχέση με τις ιδιωτικές επιχειρήσεις και αντιμετωπίζουν προκλήσεις που σχετίζονται με τις υποδομές και τους πόρους, αλλά και με τον αρχικό καθορισμό του πεδίου εφαρμογής.[61] Οι ελλείψεις αυτές, λαμβάνοντας

---

[58] Eugenia Politou et al., *Privacy and Data Protection Challenges in The Distributed Era*, 1st ed. (repr., Cham: Springer International Publishing AG, 2021), 11.

[59] Liran Einav and Jonathan Levin, "The Data Revolution and Economic Analysis", *Innovation Policy and The Economy* 14 (2014): 1-24, doi:10.1086/674019.

[60] Michael Veale, Max Van Kleek and Reuben Binns, "Fairness and Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision-Making", *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, 440, doi:10.1145/3173574.3174014.

[61] Σε πρόσφατη μελέτη που διεξήχθη ανάμεσα σε 27 δημόσιες υπηρεσίες που κάνουν χρήση συστημάτων μηχανικής μάθησης και οι οποίες ανήκουν σε 5 χώρες του ΟΟΣΑ, αποκάλυφθηκε ότι υπάρχει χάσμα ανάμεσα στις θεσμικές πραγματικότητες και στα αποτελέσματα των ερευνών, στο πλαίσιο της χρήσης διαφανών και αμερόληπτων συστημάτων μηχανικής μάθησης. Οι ερευνητές κατέληξαν στο συμπέρασμα ότι για να μεταφερθούν οι αξίες της δίκαιης και υπόλογης μηχανικής μάθησης στον δημόσιο τομέα, η εν λόγω διαδικασία θα πρέπει να μελετηθεί in vivo, στο αχανές κοινωνικό-τεχνικό πλαίσιο, στο οποίο αναπόφευκτα εντάσσεται, εφόσον ζητήματα όπως η ακεραιότητα, συνοδεύονται από τεχνικά ανυπέρβλητα αντισταθμίσματα. [Michael Veale, Max Van Kleek and Reuben Binns, "Fairness and Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision-Making", *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, 440, doi:10.1145/3173574.3174014.]

παράλληλα υπόψιν το γεγονός ότι οι ιδιωτικές επιχειρήσεις δεν υπόκεινται στις ίδιες υποχρεώσεις δημόσιας λογοδοσίας, οδήγησαν πολλούς ερευνητές στη διατύπωση του ισχυρισμού ότι οι επιτυχείς δραστηριότητες των ιδιωτικών επιχειρήσεων δεν μπορούν να μεταφερθούν στο πεδίο του φορολογικού ή δημοσίου τομέα.[62][63]

Οι ιδιωτικές επιχειρήσεις, εκμεταλλευόμενες τις δυνατότητες των μεγάλων δεδομένων και των τεχνικών μηχανικής μάθησης, προτείνουν εξατομικευμένα προϊόντα στους καταναλωτές, είτε με στόχο την αύξηση των κερδών τους, είτε για να αντικαταστήσουν υπάρχοντα προϊόντα με νέα. Ωστόσο, ακόμα και όταν γίνεται κατάρτιση του προφίλ τους για εμπορικούς ή διαφημιστικούς σκοπούς, οι περισσότεροι καταναλωτές δεν αρέσκονται στο να παρακολουθούνται ή να ταυτοποιούνται. Σύμφωνα με μια υπόθεση που έλαβε χώρα το 2015, η ολλανδική τράπεζα IGN, σχεδίαζε να «διερευνήσει εάν οι καταναλωτές θα ενδιαφέρονταν να λαμβάνουν εξατομικευμένες εκπτώσεις από τρίτα μέρη, με βάση την καταναλωτική τους συμπεριφορά». Η πρόθεση αυτή της τράπεζας, προκάλεσε πολλές αντιδράσεις από τους καταναλωτές και τα μέσα μαζικής ενημέρωσης, και υποχρεώθηκε εν τέλει να μην πραγματώσει τα σχέδιά της.[64] Οι πρακτικές κατάρτισης προφίλ μπορούν όμως να καταστούν και πιο διεισδυτικές, όπως συμβαίνει σε περιπτώσεις μείωσης των πιστωτικών ορίων των φυσικών προσώπων, βάσει αναλύσεων των ιστορικών ασυνεπών εξοφλήσεων άλλων φυσικών προσώπων που ήταν πελάτες στα ίδια μαγαζιά.[65]

Στον φορολογικό τομέα, η κατάρτιση προφίλ αναφέρεται στην κατηγοριοποίηση των φορολογούμενων σε κατηγορίες ρίσκου, μέσω της χρήσης τεχνολογικών που κάνουν χρήση των μεγάλων δεδομένων, τα οποία συλλέγονται από διάφορες πηγές.[66] Στην πραγματικότητα, οι φορολογικές πληροφορίες μπορούν να διασταυρωθούν από τις δημόσιες αρχές εισπράξεως εσόδων με άλλες ψηφιακές πληροφορίες προσωπικού χαρακτήρα, που τηρούνται από την εγχώρια ή τις διεθνείς κυβερνήσεις (π.χ. τελωνειακά, μεταναστευτικά, ποινικά δεδομένα) ή από τον ιδιωτικό τομέα (π.χ. αρχεία συναλλαγών των καταναλωτών), ώστε να διαμορφώνεται κατά αυτόν τον τρόπο ένα αναλυτικό προφίλ του κάθε φυσικού προσώπου από προηγουμένως διακριτά σώματα δεδομένων. Το αναλυτικό αυτό προφίλ μπορεί να χρησιμοποιείται επίσης για σκοπούς που δεν αφορούν το φορολογικό τομέα, όπως στο πλαίσιο ερευνών παράνομων χρηματοδοτήσεων της τρομοκρατίας.[67] Στις Η.Π.Α, η Εφορία (***Inland Revenue Service-IRS***) έχει το δικαίωμα να συλλέγει τεράστιες ποσότητες ιδιωτικών πληροφοριών, όπως αυτές που αφορούν τις συνήθειες κατά τον ύπνο, τις ασχολίες των υποκειμένων, τις θρησκευτικές πεποιθήσεις, τις ιατρικές

---

[62] Nicholas Diakopoulos, "Accountability in Algorithmic Decision Making", *Communications of The ACM* 59, no. 2 (2016): 56-62, doi:10.1145/2844110.

[63]Michael Hatfield, *Taxation and Surveillance: An Agenda*, 17 Yale J. L. & Tech. 319 (2015), https://digitalcommons.law.uw.edu/faculty-articles/365

[64] https://www.ing.com/About-us/ING-and-the-use-of-customer-data.htm.

[65] F.T. Commission et al., big data: a tool for inclusion or exclusion? Understanding the issues. FTC Report, (2016, January).

[66] Linnet Taylor, Ralph Schroeder and Eric Meyer, "Emerging Practices and Perspectives on Big Data Analysis in Economics: Bigger and Better or More of The Same?", *Big Data & Society* 1, no. 2 (2014): 3, doi:10.1177/2053951714536877.

[67] Arthur J. Cockfield, "Protecting Taxpayer Privacy Rights Under Enhanced Cross-Border Tax Information Exchange: Toward A Multilateral Taxpayer Bill of Rights", *SSRN Electronic Journal*, 2008, 447, doi:10.2139/ssrn.1356841.

καταστάσεις, τα ταξιδιωτικά σχέδια κ.α.[68] Αυτός είναι και ο λόγος που η εν λόγω υπηρεσία έχει χαρακτηριστεί από τον Επίτροπο της ως «μια εντατικά πληροφοριακή επιχείρηση» που βασίζεται «στην οργάνωση των πληροφοριών και τελικά στην γνώση και την πληροφόρηση που εξάγουμε από τις πληροφορίες αυτές». Σύμφωνα με την Houser και την Sanders, η αμερικανική εφορία χρησιμοποιεί επίσης αυτοματοποιημένα υπολογιστικά προγράμματα (γνωστά και ως «αράχνες»), αλλά και μεθόδους ανάλυσης μεγάλων δεδομένων, ώστε να φιλτράρει και να εξορύξει ιστοσελίδες κοινωνικών δικτύων, όχι μόνο για φορολογούμενους που ελέγχονται αλλά και για να εντοπιστούν πιθανοί παραβάτες που δεν έχουν επιλεγεί για έλεγχο.[69]

Θα πρέπει επομένως, ένα σημαντικό κομμάτι της ερευνητικής προσπάθειας που σχετίζεται με την φορολόγηση και την επιτήρηση, να επικεντρωθεί στον καθορισμό των τρόπων μέσω των οποίων θα μπορούν να συγκεντρώνονται και να αναλύονται φορολογικά δεδομένα χωρίς να απεμπολείται η ιδιωτικότητα των προσώπων. Πώς μπορεί, επομένως , να σχεδιαστεί ένα σύστημα ώστε να συλλέγει τις κατάλληλες πληροφορίες, ενώ παράλληλα θα σέβεται και θα τηρεί τις ζώνες ιδιωτικότητας εντός των οποίων οι φορολογούμενοι δεν καθίστανται ανίσχυροι; Η απάντηση σε τέτοιου είδους ερωτήματα καθίσταται δύσκολη καθώς οι πολιτιστικές νόρμες και οι ζώνες ιδιωτικότητας συνεχώς μεταμορφώνονται χάρη στην πληροφοριακή τεχνολογική επανάσταση. Στο πλαίσιο αυτό θα μπορούσε να διαμορφωθεί ένα διττό φορολογικό σύστημα, που θα επέτρεπε στους φορολογούμενους να επιλέγουν ανάμεσα σε αυτό που συλλέγει λιγότερες πληροφορίες αλλά οδηγεί σε μειωμένα οφέλη και προνόμια και σε αυτό που συλλέγει περισσότερες πληροφορίες αλλά παρέχει επιπλέον προνόμια. Επί παραδείγματι, στο πρώτο σύστημα μπορεί να παρέχονται λιγότερα οφέλη ως προς τις εκπαιδευτικές δαπάνες, αλλά παράλληλα δεν θα υπάρχει ανάγκη παρακολούθησης, για παράδειγμα, της προόδου προς απόκτηση πτυχίου του φορολογούμενου. Η θα μπορούσε να δοθεί επιλογή στον φορολογούμενο να μην υφίσταται παρακολούθηση σε ορισμένες περιπτώσεις, με την παράλληλη πρόβλεψη ότι δεν θα έχει φορολογικές διευκολύνσεις για πιθανά έξοδα. Τοποθετώντας τον φορολογούμενο σε θέση ελέγχου της παρακολούθησης των πληροφοριών που τον αφορούν, ο τελευταίος θα έχει τον έλεγχο των εν λόγω πληροφοριών και θα μπορεί να καθορίζει τις ζώνες ιδιωτικότητάς του. Το σχεδιαστικό πρόβλημα στην περίπτωση αυτή αφορά την εξισορρόπηση των επιλογών του φορολογούμενου με το συμφέρον του φορολογικού συστήματος να συλλέγει τις σχετικές πληροφορίες.

1.5.2 Πολιτικές για την διασφάλιση της διαφάνειας στον φορολογικό και οικονομικό τομέα

Ο αριθμός των ενωσιακών και διεθνών πολιτικών για την συλλογή και την ανταλλαγή μεγάλων ποσοτήτων προσωπικών φορολογικών και οικονομικών δεδομένων, ώστε να διευκολυνθεί η καινοτομία και να προωθηθεί η διαφάνεια στον οικονομικό και φορολογικό χώρο, έχει ουσιωδώς αυξηθεί τα τελευταία χρόνια. Παράλληλα, παρατηρείται η κλιμακούμενη κυριαρχία της αρχής της διαφάνειας επί των προσωπικών οικονομικών και φορολογικών πληροφοριών, εις βάρος της

[68]Michael Hatfield, *Taxation and Surveillance: An Agenda*, 17 Yale J. L. & Tech. 319 (2015), 325 https://digitalcommons.law.uw.edu/faculty-articles/365

[69] Kimberly A. Houser and Debra Sanders, "The Use of Big Data Analytics by the IRS: Efficient Solutions or The End of Privacy as We Know It?", *Vanderbilt Journal of Entertainment and Technology Law (Jetlaw)* 4, no. 4 (2017): 824.

ιδιωτικότητας. Πράγματι, μετά την παγκόσμια οικονομική κρίση του 2008, πολλοί υπεύθυνοι για τον σχεδιασμό πολιτικών, ισχυρίστηκαν ότι η ανάγκη για ελεύθερη και αδιατάρακτη πρόσβαση σε προσωπικά φορολογικά και οικονομικά δεδομένα, ώστε να καταπολεμηθεί η παράνομη τρομοκρατική οικονομική δραστηριότητα, υπερβαίνει την αρχή του δικαιώματος στην ιδιωτικότητα.[70]Υπό αυτήν την οπτική, η διαφάνεια στον δημόσιο τομέα παρουσιάστηκε ως η λύση και η ιδιωτικότητα ως εμπόδιο για την επιτυχία των πολιτικών.[71]Παρομοίως, στον ιδιωτικό τομέα, οι πολιτικές ιδιωτικότητας και οι κανονισμοί έχουν συνδεθεί επανειλημμένα με την παρεμπόδιση της καινοτομίας και τον άμεσο επηρεασμό της οικονομικής ανάπτυξης και της αποτελεσματικότητας των αναδυόμενων τεχνολογιών.[72] Στο πλαίσιο αυτό, οι φορολογικές αρχές κάνουν πλέον χρήση αυτοματοποιημένων μεθόδων ανταλλαγής πληροφοριών για την καταπολέμηση της απάτης και της φοροδιαφυγής, ενώ παράλληλα οι ιδιωτικές επιχειρήσεις εκμεταλλεύονται καινοτόμους τρόπους για να διατηρούν και να κεφαλαιοποιούν τις προσωπικές οικονομικές πληροφορίες. Όλα αυτά συμβαίνουν εντός της Ε.Ε. και με βάση το διεθνές ρυθμιστικό πλαίσιο.

Ειδικότερα, ο ΟΟΣΑ και τα αρμόδια όργανα της Ε.Ε., έχουν καταβάλλει άνευ προηγουμένου προσπάθειες για την διαμόρφωση του «Παγκόσμιου Προτύπου για την Αυτόματη Ανταλλαγή Πληροφοριών Χρηματοοικονομικών Λογαριασμών» («***Automatic Exchange of Information» - AEOI***)[73] που σχετίζεται με τα φορολογικά δεδομένα που διακινούνται στις δικαιοδοσίες τους. Παράλληλα, οι ενωσιακοί κανονισμοί για την ανοιχτή τραπεζική («open banking») και τις χρηματοοικονομικές υπηρεσίες θέτουν υπό αμφισβήτηση το ισχύον καθεστώς του παραδοσιακού τραπεζικού τομέα. Ο καταλύτης για την παγκόσμια επέκταση του προτύπου AEOI ήταν ένα νομοθέτημα που υιοθετήθηκε στις Η.Π.Α το 2010 και ονομάζεται «νόμος περί φορολογικής συμμόρφωσης αλλοδαπών λογαριασμών (***Foreign Account Tax Compliance Act - FATCA***).[74]Η θέση σε ισχύ του αμερικάνικου νόμου είχε ως αποτέλεσμα να ενταθούν οι προσπάθειες για την κοινή αναφορά και την καθιέρωση των προτύπων προσήκουσας επιμέλειας που θα συνέβαλαν στην καταπολέμηση της εξωχώριας φοροδιαφυγής.[75]

Στον ιδιωτικό τομέα, δύο από τις πιο εξέχουσες νομοθεσίες που επηρέασαν και διαμόρφωσαν το τοπίο των τραπεζικών υπηρεσιών και των υπηρεσιών πληρωμών, είναι η δεύτερη Οδηγία (ΕΕ) 2015/2366 για τις υπηρεσίες πληρωμών (***Payment Services Directive 2 – PSD2***)[76] και η δεύτερη Οδηγία 2014/65/33, για τις αγορές χρηματοπιστωτικών μέσων (***Markets in Financial Instruments Directive – MiFIDII***)[77]. Η Οδηγία για τις υπηρεσίες πληρωμών αποσκοπεί στην

---

[70] J.C. Sharman, "Privacy as Roguery: Personal Financial Information in An Age of Transparency", *Public Administration* 87, no. 4 (2009): 724, doi:10.1111/j.1467-9299.2009.01785. x.

[71]Michael Hatfield, "Privacy in Taxation", *Florida State University Law Review* 44, no. 2 (2018): 630, https://ir.law.fsu.edu/cgi/viewcontent.cgi?article=2579&context=lr.

[72] Liran Einav and Jonathan Levin, "The Data Revolution and Economic Analysis", *Innovation Policy and The Economy* 14 (2014): 20-21, doi:10.1086/674019.

[73]https://www.oecd.org/ctp/exchange-of-tax-information/standard-for-automatic-exchange-of-financial-account-information-for-tax-matters-9789264216525-en.htm

[74] Lisa De Simone, Rebecca Lester and Kevin Markle, "Transparency and Tax Evasion: Evidence from The Foreign Account Tax Compliance Act (FATCA)", *Journal of Accounting Research* 58, no. 1 (2020): 106-107, doi:10.1111/1475-679X.12293.

[75] Christiana HJI Panayi, "Current Trends on Automatic Exchange of Information", *SSRN Electronic Journal,* S-43, no. 43 (2016): 3, doi:10.2139/ssrn.2748659.

[76] Ενσωματώθηκε στην ελληνική έννομη τάξη με τον νόμο 4537/2018 και αντικατέστησε την Οδηγία 2007/64/ΕΚ.

[77] Ενσωματώθηκε στην ελληνική έννομη τάξη με τον νόμο 4514/2018.

αύξηση του πανευρωπαϊκού ανταγωνισμού και της συμμετοχής στην βιομηχανία πληρωμών ακόμα και από μη χρηματοοικονομικούς θεσμούς, αλλά και στην προώθηση της ανάπτυξης και της χρήσης καινοτόμων επιγραμμικών και κινητών υπηρεσιών πληρωμών, όπως συμβαίνει στην περίπτωση της ανοιχτής τραπεζικής. Ταυτοχρόνως, η Οδηγία για τις αγορές χρηματοπιστωτικών μέσων στοχεύει στην ενίσχυση της προστασίας των επενδυτών και στην βελτίωση της λειτουργίας των χρηματοπιστωτικών αγορών, με τον πιο αποδοτικό, ανθεκτικό, δίκαιο και διαφανή τρόπο.

1.6 Ιδιωτικότητα ως εμπιστοσύνη: ένα εναλλακτικό μοντέλο

Τα επιγραμμικά κοινωνικά δίκτυα βασίζονται στην εμπιστοσύνη. Αυτό εντάσσεται σε ένα πλαίσιο που εκτείνεται από τις καθημερινές δραστηριότητες, όπως η επικοινωνία με την οικογένεια, τους φίλους και τους συγγενείς, έως τον διαμοιρασμό πληροφοριών με αγνώστους που αλληλεπιδρούν με εμάς. Η εμπιστοσύνη αποτελεί την προσδοκία ότι οι αποδέκτες των πληροφοριών μας δεν θα τις διαμοιραστούν για δικούς τους σκοπούς και χρήσεις, δεν θα τις εμπορευματοποιήσουν ή θα τις διαμοιραστούν για την επίτευξη κακόβουλων σκοπών. Στην περίπτωση της εμπορευματοποίησης, οι πάροχοι πληροφοριών αναμένουν την είσπραξη εσόδων από τον διαμοιρασμό των πληροφοριών. Η εικασία της εμπιστοσύνης επομένως έγκειται στον πυρήνα των αποφάσεών μας να μοιραστούμε τις προσωπικές μας πληροφορίες με άλλους. Στο τεχνολογικά καθοδηγούμενο επιγραμμικό πλαίσιο, οι χρήσεις των πληροφοριών μας συμπεριλαμβάνουν την εθνική ασφάλεια και την επιβολή του νόμου, την αποθήκευση των δεδομένων μας για την παροχή υπηρεσιών διευκόλυνσης, την εμπορευματοποίηση των πληροφοριών και την αγοραπωλησία αυτών, την εισβολή στα δεδομένα ή την κλοπή αυτών αλλά και την επιρροή των σκέψεων μας και των αποφάσεών μας. Η έννοια του Μεγάλου Αδελφού, που γνωρίζει τα πάντα για εμάς, έχει διαιωνιστεί και έχει ενταθεί χάρη στην έκρηξη των επιγραμμικών συνδέσεων και των επικοινωνιών. Αρχικά, αποτέλεσε μέσο επιβολής του νόμου από της αρχές, ώστε να παρακολουθούν και να επιβεβαιώνουν την υποταγή στο κυρίαρχο καθεστώς. Το εργαλείο αυτό δεν ωραιοποιήθηκε υπό το μανδύα των δωρεάν υπηρεσιών που υποθάλπουν την εμπιστοσύνη. Ο κυβερνητικός Μεγάλος Αδελφός και οι μηχανισμοί παρακολούθησής του, προκύπτουν μέσω των κρατικών χρηματοδοτήσεων. Σε αντίθεση με τον κρατικό μηχανισμό, οι επιγραμμικοί συλλέκτες δεδομένων, όπως το Facebook, το Amazon και το Google, δεν χαρακτηρίζονται από την ύπαρξη ενός καταπιεστικού χαρακτήρα τύπου Μεγάλου Αδελφού. Υπό την πρόφαση ότι διευκολύνουν την ζωή των χρηστών, παρέχουν φαινομενικά φθηνές/δωρεάν υπηρεσίες.

Η ιδιωτικότητα ως εμπιστοσύνη βασίζεται στο δίκαιο των καταπιστευμάτων (***trust law***). Είναι πλέον κοινώς αποδεκτός ο ισχυρισμός ότι οι επιγραμμικοί συλλέκτες δεδομένων κατέχουν «ασύμμετρη ισχύ» έναντι του μέσου καταναλωτή. Επομένως, σύμφωνα με τις αρχές που αφορούν τα εμπιστεύματα, όπως αυτές συναντώνται στο κοινοδίκαιο, οι συλλέκτες δεδομένων θα πρέπει να εξασφαλίζουν υψηλότερα πρότυπα προστασίας όταν τους εμπιστευόμαστε με τα δεδομένα μας. Θα πρέπει να ενεργούν με βάση τις κοινές αρχές που ορίζονται για τα εμπιστεύματα. Σε αντίθεση με το δίκαιο των συμβάσεων ή το δίκαιο περί αδικοπραξιών, το δίκαιο των εμπιστευμάτων έχει ως κεντρικό άξονα κάποιες ιδιαίτερες σχέσεις στις οποίες ο εμπιστευματοδόχος έχει την υποχρέωση να δρα με γνώμονα το καλύτερο συμφέρον του άλλου μέρους. Παραδείγματα

εμπιστευματοδόχων αποτελούν οι σύμβουλοι επενδύσεων, οι διαχειριστές περιουσίας, οι δικηγόροι και οι γιατροί.

Οι εμπιστευματοδόχοι επωμίζονται την λήψη αποφάσεων που αφορούν την ζωή και την διαβίωση των πελατών τους. Όταν μοιραζόμαστε τις προσωπικές μας πληροφορίες, αναμένουμε αυτές να τύχουν υπεύθυνης και ισότιμης μεταχείρισης. Η εμπιστευματική σχέση ανάμεσα στους μεσίτες δεδομένων και τους χρήστες θα βοηθούσε στην καταπολέμηση της ανισότητας της ισχύος που παρατηρείται στις επιγραμμικές συνδιαλλαγές και συναναστροφές. Με βάση τη θεώρηση αυτή, οι εταιρείες μεγάλης κλίμακας, όπως το Facebook, η Google και το Uber, θα πρέπει να χαρακτηριστούν ως εμπιστευματοδόχοι, λόγω της ευαλωτότητας των χρηστών του διαδικτύου απέναντί τους. Οι χρήστες εξαρτώνται σε μεγάλο βαθμό από αυτές και εκείνες αυτοπροβάλλονται ως ειδήμονες στο πεδίο τους και ενδεχομενικά ως αξιόπιστες. Σε κάθε περίπτωση, η εταιρική στρατηγική περί ιδιωτικότητας θα πρέπει να στοχεύει στην διατήρηση της εμπιστοσύνης των χρηστών. Τα αρμόδια για την ιδιωτικότητα στελέχη θα πρέπει να εντάσσουν τις εταιρείες σε ένα πλαίσιο εμπιστοσύνης και υπευθυνότητας, αντί να δημιουργούν πολιτικές που είναι σχεδιασμένες να αποφεύγουν τις δικαστικές διενέξεις. Επομένως, θα πρέπει να αναθεωρούν τις πολιτικές τους τακτικά, ώστε να ανταποκρίνονται στις συνεχώς μεταβαλλόμενες ανάγκες και προσδοκίες των πελατών τους, λαμβάνοντας παράλληλα υπόψιν τις μεταβαλλόμενες πραγματικότητες της ιδιωτικότητας στο διαδίκτυο, ή της έλλειψης αυτής.

Πολλές πολιτικές που αφορούν την ιδιωτικότητα και συμπεριλαμβάνονται στις εταιρικές ιστοσελίδες, είναι δυσανάγνωστες και δύσκολα εντοπίζονται εντός τους, ενώ απαιτείται πολύς χρόνος για την εξέτασή τους. Η Google συνεχίζει να δέχεται κριτική για την ικανότητά της να εντοπίζει και να καταγράφει την τοποθεσία των χρηστών στην εφαρμογή χαρτών της, ακόμα και όταν το χαρακτηριστικό του ιστορικού τοποθεσίας είναι απενεργοποιημένο. Επίσης, η Google γνωρίζει που αναλώνουμε τον ελεύθερο χρόνο μας, επιτρέποντας στα πλησιέστερα καταστήματα να αγοράσουν διαφημίσεις που μας στοχεύουν ευθέως. Κατανοούμε επομένως ότι οι εταιρείες-εμπιστευματοδόχοι, θα πρέπει να έχουν επιπρόσθετες υποχρεώσεις έναντι των ατομικών παρόχων δεδομένων- πελατών και όχι να περιορίζονται στην διασάφηση των πολιτικών περί ιδιωτικότητάς τους. Θα πρέπει επίσης να συμφωνήσουν να τηρούν ένα σύνολο πρακτικών που αφορούν την χρηστή πληροφόρηση, αλλά και να εγγυώνται την ασφάλεια και την ιδιωτικότητα, καθώς και την έγκαιρη γνωστοποίηση των παραβιάσεων. Τέλος, θα πρέπει πρωτίστως να απαιτηθεί από τις εταιρείες αυτές να «υποσχεθούν» ότι δεν χρησιμοποιήσουν ως μηχανισμό μόχλευσης τα προσωπικά δεδομένα για να καταχραστούν την εμπιστοσύνη των τελικών χρηστών.[78]

[78] Sanjay Sharma, *Data Privacy and GDPR Handbook*, 1st ed. (repr., Newark, United States: John Wiley & Sons, Incorporated, 2019), 13-14.

ΔΕΥΤΕΡΟ ΚΕΦΑΛΑΙΟ
Η ΝΟΜΟΘΕΤΙΚΗ ΚΑΤΟΧΥΡΩΣΗ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

2.1 Εισαγωγικές παρατηρήσεις

Οι έννοιες του «υπευθύνου επεξεργασίας» και του «εκτελούντος την επεξεργασία» δεν δημιουργήθηκαν από το πουθενά. Πριν την Οδηγία 95/46/ΕΚ και τον Γενικό Κανονισμό Προστασίας Προσωπικών δεδομένων, πολλές άλλες πράξεις προστασίας των δεδομένων ενσωμάτωναν έννοιες με παρόμοιο νόημα και πεδίο δράσης. Ο στόχος του παρόντος κεφαλαίου είναι να ενισχύσει το νόημα πολλών εννοιών που συναντούμε στα σημερινά νομοθετήματα προστασίας δεδομένων, εντοπίζοντας την προέλευσή τους και την ανάπτυξή τους διαχρονικώς. Όταν κάποιος εξετάζει την ενωσιακή νομοθεσία προστασίας των δεδομένων υπό μια ιστορική σκοπιά, μπορεί να διακρίνει τέσσερις κύριες περιόδους. Η πρώτη αφορά την ανάδυση των εθνικών νόμων προστασίας δεδομένων (1970-1980), η δεύτερη την διεθνοποίηση (1980-1981), η Τρίτη την εφαρμογή σε εθνικό επίπεδο (1982-1994) και η τέταρτη την ευρωπαϊκή νομοθετική εναρμόνιση (1995-2016). Αναφορικά με την πρώτη περίοδο, επελέγησαν προς ανάλυση οι νόμοι προστασίας δεδομένων της Έσσης, της Σουηδίας και της Γαλλίας. Ειδικότερα, οι νόμοι της Έσσης και της Γαλλίας επελέγησαν διότι αποτελούν τους πρώτους εθνικούς νόμους προστασίας δεδομένων. Ο γαλλικός νόμος προστασίας δεδομένων επελέγη ώστε να γεφυρώσει το χάσμα ανάμεσα στα πρώτα νομοθετήματα προστασίας δεδομένων και τα κοινοτικά μέσα προστασίας δεδομένων. Στο πλαίσιο της δεύτερης περιόδου που αφορά τη διεθνοποίηση, αναλύονται η Σύμβαση 108 και οι Κατευθυντήριες Αρχές για την «προστασία της ιδιωτικότητας και τη διασυνοριακή αποστολή προσωπικών δεδομένων» (***Guidelines on the Protection of Privacy and Transborder Flows of Personal Data***) του ΟΟΣΑ. Η ανάλυση της Σύμβασης 108 θεωρήθηκε απαραίτητη καθώς παρέχει το κανονιστικό πλαίσιο για εθνικά νομοθετικά μέτρα εφαρμογής κατά την περίοδο που ακολούθησε. Η ανάλυση των Αρχών του ΟΟΣΑ επίσης κρίνεται επωφελής, καθώς οι εν λόγω Αρχές αναπτύχθηκαν παράλληλα με την Σύμβαση 108 και επομένως παρέχουν μια εκτενέστερη εικόνα των εννοιών που συμπεριλαμβάνονται στη Σύμβαση 108. Για την Τρίτη περίοδο επελέγησαν η αγγλική νομοθετική πράξη προστασίας δεδομένων του 1984 και η βελγική νομοθετική πράξη προστασίας δεδομένων του 1992. Η επιλογή αυτή βασίστηκε στην επιθυμία να διατηρηθεί η χρονολογική οπτική της ανάλυσης των νομοθετημάτων με βάση τις προηγούμενες περιόδους. Τέλος, η Οδηγία 95/46/ΕΚ και ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων επελέγησαν ως τα δύο νομοθετήματα που αντιπροσωπεύουν την περίοδο της ευρωπαϊκής νομοθετικής εναρμόνισης, αλλά και γιατί αποτελούν το εστιακό σημείο ανάλυσης της παρούσας εργασίας σε σχέση με το τραπεζικό σύστημα.

Προτού αναλυθούν οι συγκεκριμένοι εθνικοί νόμοι προστασίας δεδομένων, παρέχεται μια επισκόπηση του πλαισίου δημιουργίας των ενωσιακών νομοθετημάτων προστασίας δεδομένων. Στη συνέχεια, εξετάζονται οι Αρχές του ΟΟΣΑ και η Σύμβαση 108. Ακολουθεί η ανάλυση των πρώτων νομοθετημάτων προστασίας δεδομένων (Έσσης, Σουηδίας, Γαλλίας) και η ανάλυση δύο εθνικών νομοθετημάτων προστασίας δεδομένων που εφαρμόζουν την Σύμβαση 108 (Αγγλία, Βέλγιο). Τέλος, αναλύεται η Οδηγία 95/46/ΕΚ και ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων σε εθνικό και ενωσιακό επίπεδο.

2.2 Το ευρωπαϊκό και διεθνές νομοθετικό πλαίσιο

Το ευρωπαϊκό νομοθετικό πλαίσιο προστασίας προσωπικών δεδομένων αποτελεί μια κατακερματισμένη νομική περιοχή που εμπεριέχει πολλές νομικές πράξεις. Η νομοθετική κατοχύρωση της προστασίας προσωπικών δεδομένων και η εξασφάλιση της νόμιμης επεξεργασίας από το κράτος και τις επιχειρήσεις, ήταν λογικό επακόλουθο της εξέλιξης της κοινωνίας από μια βιομηχανική παραγωγική διάσταση σε μια μεταβιομηχανική οικονομία της πληροφορίας και της παροχής υπηρεσιών. Η προστασία των προσωπικών δεδομένων θα ήταν πολύ δύσκολη αν το θεσμικό πλαίσιο διέφερε ριζικά μεταξύ των κρατών. Αυτό οφείλεται στην ανταγωνιστικότητα των κανόνων δικαίου μεταξύ των διάφορων κρατών **(«θεσμικό αρμπιτράζ»)**.[79] Έστω ότι ανάμεσα σε δύο κράτη Α και Β, η νομοθεσία του κράτους Α δεν προβλέπει κανένα μέτρο προστασίας για τα δεδομένα των υποκειμένων, με αποτέλεσμα κάθε επιχείρηση να μπορεί, κατά τη διακριτική της ευχέρεια, να χρησιμοποιεί αυτά κατά το δοκούν. Εν αντιθέσει με το κράτος Α, το κράτος Β προβλέπει την προστασία δεδομένων μέσω της αυστηρής επιβολής μέτρων. Επομένως, μια επιχείρηση που σχεδιάζει μια νέα εγκατάσταση έχει σημαντικό κίνητρο να επιλέξει το πρώτο κράτος, γιατί το λειτουργικό κόστος θα είναι μικρότερο και θα δύναται να κερδοσκοπεί από την εκτεταμένη χρήση προσωπικών δεδομένων για άλλους σκοπούς πέραν της βασικής της δράσης. Συνεπώς, μια οικονομία που επιλέγει να προστατεύσει τους πολίτες της από την παράνομη επεξεργασία προσωπικών δεδομένων, καθίσταται λιγότερο ελκυστικός επενδυτικός προορισμός. Για να οδηγηθούμε σε λύση στο αδιέξοδο αυτό, αποτελεί αδήριτη ανάγκη η διεθνής καθιέρωση αντίστοιχων ή και ίδιων κανόνων δικαίου μεταξύ περισσότερων κρατών και οικονομιών.

Σημείο αφετηρίας στα σύγχρονα νομοθετήματα προστασίας των δεδομένων αποτελεί η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του Οργανισμού Ηνωμένων Εθνών (ΟΗΕ) και αφετέρου η Σύμβαση της Ρώμης, στην οποία βασίζονται κατά κύριο λόγο. Η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του 1948, αποτελεί το πρώτο διεθνές κείμενο με το οποίο κατοχυρώνεται ο σεβασμός της ιδιωτικής και οικογενειακής ζωής, στο πνεύμα της Γαλλικής Διακήρυξης των δικαιωμάτων του Ανθρώπου και του Πολίτη του 1789.[80] Αν και σήμερα όσα προβλέπονται από τη Διακήρυξη αποτελούν γενικώς αποδεκτές αξίες σε όλα τα δημοκρατικά καθεστώτα, τότε για πρώτη φορά έλαβε χώρα συλλογικά η «αναγνώριση της αξιοπρέπειας, που είναι σύμφυτη σε όλα τα μέλη της ανθρώπινης οικογένειας». Παράλληλα, εντοπίζεται στο εν λόγω κείμενο, η αναγνώριση ενός δικαιώματος στην πληροφορία και την πληροφορική αυτοδιάθεση, σύμφωνα με το άρθρο 19 που ορίζει πως «καθένας έχει ο δικαίωμα της ελευθερίας της γνώμης και της έκφρασης, που σημαίνει το δικαίωμα να μην υφίσταται δυσμενείς συνέπειες για τις γνώμες του και το δικαίωμα να αναζητεί, να λαμβάνει και να διαδίδει πληροφορίες και ιδέες, με οποιοδήποτε μέσο έκφρασης και από όλο τον κόσμο».[81] Παρά την πανηγυρική διακήρυξη των ανωτέρω, το κείμενο δεν είχε δεσμευτική ισχύ και δεν επέτρεπε στους πολίτες να διεκδικήσουν τα δικαιώματα που αναφέρονται σε αυτό. Αποτέλεσε, ωστόσο, έμπνευση

---

[79] Brian Kahin and Charles R Nesson, *Borders in Cyberspace*, 1st ed. (repr., Cambridge, Mass.: MIT Press, 1997), 205, 219-221.

[80] Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, *Προσωπικά Δεδομένα*, 1η εκδ. (Θεσσαλονίκη: Νομική Βιβλιοθήκη, 2016), 198.

[81] "Το κείμενο Της Διακήρυξης Είναι Διαθέσιμο Στην Ιστοσελίδα", Ohchr.Org, accessed 15 November 2021, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/grk.pdf.

για τους εθνικούς νομοθέτες και συνέβαλλε στην διασφάλιση ενός ελάχιστου βαθμού προστασίας σε συνδυασμό με τις ειδικότερες προβλέψεις των σύγχρονων συνταγμάτων.[82]

Πολύ σύντομα και συγκεκριμένα στις 4.11.1950, το Συμβούλιο της Ευρώπης υπέγραψε την Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ), για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών. Το κείμενο αυτό αποτελεί διεθνή συμφωνία (και όχι κείμενο αποκλειστικά της Ε.Ε.) και τέθηκε σε εφαρμογή το 1953. Σε αντίθεση με την προαναφερθείσα διακήρυξη του Ο.Η.Ε, το παρόν πρόκειται για νομικά δεσμευτικό κείμενο, με το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου να ερμηνεύει αυθεντικά την ΕΣΔΑ και να τιμωρεί τα κράτη επί παραβάσεων αυτής. Συγκεκριμένα, στο άρθρο 8 παρ. 1, ορίζει ότι καθένας έχει δικαίωμα στον σεβασμό της ιδιωτικής, οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας του, ενώ στην παρ. 2 του ίδιου άρθρου απαγορεύεται η επέμβαση οποιασδήποτε δημόσιας Αρχής στο δικαίωμα αυτό, εκτός αν κρίνεται αναγκαίο για τη δημόσια ασφάλεια και για την προάσπιση και προστασία των δικαιωμάτων και των ελευθεριών των άλλων.[83] Επίσης, προβλέπεται η απαγόρευση των βασανιστηρίων, της δουλείας και της καταναγκαστικής εργασίας, το δικαίωμα στην περιουσία αλλά και το δικαίωμα στη δίκαιη δίκη.

Την ΕΣΔΑ ακολούθησε το Διεθνές Σύμφωνο περί Ατομικών και Πολιτικών Δικαιωμάτων (16/12/1966), της Γενικής Συνέλευσης του ΟΗΕ, το οποίο στο άρθρο 17 ορίζει ότι «Κανείς δεν υπόκειται σε αυθαίρετες ή παράνομες παρενοχλήσεις της ιδιωτικής ζωής, της οικογένειας, της κατοικίας ή της αλληλογραφίας του, ούτε σε παράνομες προσβολές της τιμής και της υπόληψής του». Προς την ίδια κατεύθυνση κινήθηκε και η απόφαση 2450/19.12.1968 της Γενικής Συνέλευσης των Η.Ε., που κάνει αναφορά σε ζητήματα που αφορούν την καταπάτηση των ανθρωπίνων δικαιωμάτων χάρη στην χρήση των διαρκώς εξελισσόμενων τεχνολογιών και στην επιτακτική ανάγκη οριοθέτησης των τελευταίων.[84]

Οι πρώτες συζητήσεις ανάμεσα στους διεθνείς πολιτικούς ιθύνοντες για την ανάγκη της προστασίας των δεδομένων, μπορούν να τοποθετηθούν χρονικά προς το τέλος της δεκαετίας του 1960.Ήδη το 1968, το Συμβούλιο της Ευρώπης δημοσίευσε τη Σύσταση 509 σχετικά με τα προσωπικά δικαιώματα και τις τεχνολογικές εξελίξεις, ενώ στην πορεία έθεσε γενικές αρχές προστασίας δεδομένων σε τράπεζες δεδομένων στον δημόσιο και ιδιωτικό τομέα με τις υπ' αριθμόν 22/1973 και 29/1974 αποφάσεις του, με απώτερο στόχο να θέσει σε κίνηση τη νομοθέτηση σε εθνικό επίπεδο.[85] Στις αρχές της δεκαετίας του 1970, τόσο το Συμβούλιο της Ευρώπης όσο και ο Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη (**ΟΟΣΑ-OECD**), συμμετείχαν σε στοχευμένες προσπάθειες ώστε να αξιολογήσουν τα ζητήματα ιδιωτικότητας που σχετίζονταν με τις τράπεζες δεδομένων (***data banks***). Τελικά, αυτές οι προσπάθειες είχαν ως αποτέλεσμα την έκδοση των Κατευθυντήριων Αρχών για την «προστασία της ιδιωτικότητας και τη διασυνοριακή αποστολή προσωπικών δεδομένων» (***Guidelines on the Protection of Privacy and Transborder Flows of Personal Data***) καθώς και την υιοθέτηση της Σύμβασης υπ'αριθ. 108

---

[82] Ειρηνικός Πλατής, *Προσωπικά Δεδομένα-Προστασία GDPR*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Παπαδόπουλος, 2018), 23.
[83] Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, *Προσωπικά Δεδομένα*, 1η εκδ. (Θεσσαλονίκη: Νομική Βιβλιοθήκη, 2016), 198.
[84] Ibid., 199.
[85] Ειρηνικός Πλατής, *Προσωπικά Δεδομένα-Προστασία GDPR*, 1η εκδ.. (repr., Αθήνα: Εκδόσεις Παπαδόπουλος, 2018), 24.

του Συμβουλίου της Ευρώπης (**Σύμβαση 108/1981**) για την «προστασία των υποκειμένων από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα». Η Σύμβαση αναθεωρήθηκε στις 17-18.05.2018 και δημοσιεύθηκε ως Σύμβαση 108+, η οποία είναι σαφώς επηρεασμένη από τις εξελίξεις στην Ευρωπαϊκή Ένωση, με την ψήφιση του Γενικού Κανονισμού 2016/679, στον οποίο θα γίνει αναφορά σε επόμενη θέση.[86] Το κείμενο δεν τιτλοφορήθηκε ως «ευρωπαϊκή σύμβαση», διότι αποσκοπούσε στην υιοθέτηση των αρχών που εισήγαγε και από άλλες χώρες που δεν μετείχαν στο Συμβούλιο. Αποτέλεσε, ωστόσο, το πρώτο διεθνές κείμενο με δεσμευτική ισχύ για τις χώρες που το κύρωσαν. Ως συνέπεια αυτού του γεγονότος, απαιτούσε τη θέσπιση μέτρων προς την κατεύθυνση της παροχής προστασίας για τα ατομικά δικαιώματα των πολιτών αναφορικά με τα δεδομένα τους. Στις βασικές αρχές επαναλαμβάνεται η ανάγκη για επεξεργασία δεδομένων μόνο με τρόπο σύννομο και θεμιτό, η απαγόρευση της επεξεργασίας για σκοπούς διαφορετικούς από εκείνους για τους οποίους έχουν συλλεγεί και για πρώτη φορά σε διεθνές επίπεδο, προστατεύονται και ρητά τα ευαίσθητα δεδομένα.[87]

Ο Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη έδειξε από νωρίς ενδιαφέρον για την επεξεργασία πληροφοριών και την μηχανοργάνωση.[88] Από το 1960 και έπειτα, ο Οργανισμός θεωρούσε ότι οι πληροφορίες αποτελούσαν ένα σημαντικό οικονομικό κεφάλαιο. Όταν ήρθαν στο προσκήνιο οι πρώτες νομοθεσίες προστασίας δεδομένων, άρχισαν να εγείρονται προβληματισμοί για τον τρόπο με τον οποίο αυτές οι νομοθεσίες θα επηρέαζαν την διασυνοριακή ελεύθερη ροή των δεδομένων.[89] Οι διασυνοριακές ροές δεδομένων γενικότερα θεωρούνταν ως επωφελείς για την οικονομική και κοινωνική ανάπτυξη και κάθε περιορισμός τους θα μπορούσε να αποτελέσει τροχοπέδη στην συγκέντρωση των επωφελών αυτών αποτελεσμάτων. Ανάμεσα στα έτη 1968 και 1974, ο ΟΟΣΑ διεξήγαγε μια σειρά μελετών και διοργάνωσε πολλαπλά σεμινάρια που αφορούσαν τις τεχνολογικές, οικονομικές και νομικές επιπτώσεις της χρήσης των υπολογιστών. Το 1977, συστάθηκε μια διακυβερνητική ομάδα ειδημόνων για «τα διασυνοριακά εμπόδια των δεδομένων και την προστασία της ιδιωτικότητας» («**Transborder Data Barriers and Privacy Protection**»).Η αποστολή της ομάδας ήταν να αναπτύξει «κατευθυντήριες αρχές» για τους βασικούς κανόνες στους οποίους θα υπαγόταν η διασυνοριακή ροή δεδομένων και η προστασία των προσωπικών δεδομένων και της ιδιωτικότητας, διευκολύνοντας παράλληλα την εναρμόνιση. Επίσης, θα διερευνούσε τα νομικά και οικονομικά προβλήματα που σχετίζονταν με την διασυνοριακή ροή των μη προσωπικών δεδομένων.[90]Η ομάδα των ειδημόνων θα εκτελούσε τα καθήκοντά της σε στενή συνεργασία και μέσω διαβουλεύσεων με το Συμβούλιο της Ευρώπης και την Ευρωπαϊκή Κοινότητα. Το 1979, η ομάδα αυτή παρουσίασε το προσχέδιο των «κατευθυντήριων αρχών» μαζί με μια αιτιολογική έκθεση, στην Επιτροπή για την επιστημονική και τεχνολογική πολιτική.[91] Το Σεπτέμβριο του 1980, το Συμβούλιο του ΟΟΣΑ επίσημα εξέδωσε Σύσταση με σειρά «κατευθυντήριων γραμμών» που διέπουν την «προστασία της ιδιωτικής

---

[86] Ιωάννης Ιγγλεζάκης, *Δίκαιο Πληροφορικής*, 4η εκδ. (repr., Θεσσαλονίκη: Εκδόσεις Σάκκουλα, 2021), 326.
[87] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 161.
[88] Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and The United States*, 1st ed. (repr., Ithaca, N.Y.: Cornell University Press, 1992), 136.
[89] Michael D. Kirby, "Transborder Data Flows and The Basic Rules of Data Privacy", *Stanford Journal of International Studies* 16, no. 27 (1980), 42.
[90] Ibid., 43.
[91] Michael D. Kirby, "Transborder Data Flows and The Basic Rules of Data Privacy", *Stanford Journal of International Studies* 16, no. 27 (1980): 42.

σφαίρας του ανθρώπου και τις διασυνοριακές ροές προσωπικών δεδομένων».[92] Οι «κατευθυντήριες γραμμές» που εξέδωσε ο ΟΟΣΑ, χαρακτηρίζονταν από ελαστικότητα και η διατύπωσή τους ήταν ευρεία, με αποτέλεσμα να εξυπηρετείται η εισαγωγή τους σε εθνικές νομοθεσίες οι οποίες δεν διέθεταν μέχρι τότε σχετικές πρόνοιες, ενώ παράλληλα λειτουργούσαν ως σημείο αναφοράς και σύγκλισης των υπαρχουσών εθνικών νομοθεσιών.

Ο ΟΟΣΑ έθεσε μέσω των κατευθυντήριων γραμμών τα θεμέλια για το μέλλον των ρυθμιστικών νομοθετημάτων στην ψηφιακή εποχή. Οι κατευθυντήριες γραμμές αποτέλεσαν την πρώτη διεθνώς συμφωνηθείσα δήλωση των βασικών αρχών προστασίας της ιδιωτικότητας. Οι κατευθυντήριες γραμμές, ωστόσο, δεν αναπτύχθηκαν από μηδενική βάση. Οι συντάκτες τους «δεν ξεκίνησαν για να επανεφεύρουν τον τροχό ή να τροποποιήσουν χωρίς λόγο λογικές προσεγγίσεις που είχαν υιοθετηθεί από τους προκατόχους τους».[93] Ο πρόεδρος της ομάδας των ειδημόνων, Michael Kirby, επεσήμανε τη σημασία των πληροφοριών που ελήφθησαν από την ακαδημαϊκή συγγραφή αλλά και των κυβερνητικών αναφορών που ήταν διαθέσιμες εκείνη την εποχή, όπως αυτές που αναπτύχθηκαν στις Η.Π.Α, στο Ηνωμένο Βασίλειο και στην Γαλλία.[94] Επιπροσθέτως, ο Kirby επίσης επεσήμανε τη σημασία της συνεισφοράς του Frits Hondius, εκπροσώπου του Συμβουλίου της Ευρώπης, που συνέβαλε στον σχεδιασμό του έργου του Συμβουλίου, καθώς «μετέφραζαν την εργασία αυτή σε ένα διηπειρωτικό πλαίσιο».[95]

Στο σημείο αυτό, όσο η συλλογή των δεδομένων αυξανόταν εκθετικά, οι νομοθέτες άρχισαν να εφαρμόζουν περιορισμένα μέτρα προστασίας των δεδομένων, ειδικά στις Η.Π.Α, όπου οι προστασίες εφαρμόζονταν στο βαθμό που ήταν πραγματικά αναγκαίες.[96] Εάν οι Αρχές μπορούν να θεωρηθούν τα αρχικά σχέδια για τον ΓΚΠΔ, τότε η Οδηγία 95/46 μπορεί να θεωρηθεί το σχέδιο κάτοψης, αποκρυσταλλώνοντας πολλά από τα δικαιώματα των υποκειμένων των δεδομένων και παρέχοντας ευρεία πρωτεύουσα προστασία, σε αντίθεση με την τομεακή προσέγγιση των Η.Π.Α. Επιπροσθέτως, η Οδηγία προέβλεπε συγκεκριμένες απαιτήσεις για την διασυνοριακή μεταφορά δεδομένων, οδηγώντας έτσι στην συμφωνία-πλαίσιο ασφαλούς λιμένα ανάμεσα στην Ε.Ε. και τις Οι κατευθυντήριες γραμμές ορίστηκε ότι θα διέπουν την επεξεργασία δεδομένων τόσο στον ιδιωτικό αλλά και στον δημόσιο τομέα (παράγραφος 2). Αρχικά, δεν υπήρχε διάκριση σχετικά με την εφαρμογή τους στον κάθε τομέα. Οι κατευθυντήριες γραμμές, ωστόσο, αναγνώριζαν ότι μπορούσαν να γίνουν εξαιρέσεις εν ονόματι της εθνικής κυριαρχίας, της εθνικής ασφάλειας και της δημόσιας πολιτικής.[97] Οι κατευθυντήριες γραμμές εφαρμόζονταν μόνο για την επεξεργασία προσωπικών δεδομένων, που ορίζονταν ως «κάθε πληροφορία που σχετίζεται με ένα ταυτοποιημένο ή ταυτοποιήσιμο άτομο» (παράγραφος 1β). Επίσης, οι κατευθυντήριες γραμμές αρχικά εφαρμόζονταν τόσο στην αυτοματοποιημένη όσο και στην μη αυτοματοποιημένη επεξεργασία δεδομένων. Οι κατευθυντήριες γραμμές ήταν χωρισμένες σε τέσσερα ουσιαστικά

---

[92] Organisation for Economic Co-operation and Development (OECD), “Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data”, 23 September 1980.
[93] Michael Kirby, "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy", *International Data Privacy Law* 1, no. 1 (2010): 10, doi:10.1093/idpl/ipq002.
[94] Ibid.
[95] Ibid.
[96] Sanjay Sharma, *Data Privacy and GDPR Handbook*, 1st ed. (repr., Newark, United States: John Wiley & Sons, Incorporated, 2019), 27.
[97] Παρά το γεγονός ότι οι κατευθυντήριες γραμμές εκφράστηκαν ως μη δεσμευτική Σύσταση, οι υπεύθυνοι για την σύνταξη τους, θεώρησαν σημαντικό να ενσωματώσουν οδηγίες σχετικά με πιθανές εξαιρέσεις ή παρεκκλίσεις.(αιτιολογική έκθεση, παράγραφος 46).

μέρη: το πρώτο αφορούσε τις βασικές αρχές της εφαρμογής σε εθνικό επίπεδο, το δεύτερο τις βασικές αρχές εφαρμογής σε διεθνές επίπεδο, το τρίτο την εφαρμογή σε εθνικό επίπεδο και το τέταρτο την διεθνή συνεργασία. Συγκεκριμένα, οι κατευθυντήριες γραμμές ήταν οκτώ και προέβλεπαν τον περιορισμό της συλλογής των δεδομένων τα οποία πρέπει να αποκτηθούν με νόμιμο και θεμιτό τρόπο (για συγκεκριμένους σκοπούς)[98], την διασφάλιση της ποιότητας των δεδομένων[99], τον καθορισμό του σκοπού[100] και του χρόνου της συλλογής και διατήρησης[101] των δεδομένων[102], τον περιορισμό της χρήσης των δεδομένων με βάση τη συναίνεση του υποκειμένου, τη λήψη μέτρων ασφάλειας των δεδομένων[103], την ενημέρωση των υποκειμένων αναφορικά με τις πρακτικές και τις πολιτικές των οντοτήτων συλλογής των δεδομένων, την συμμετοχή των υποκειμένων ώστε να έχουν το δικαίωμα να προβούν σε διορθώσεις των προβλημάτων που προκύπτουν αναφορικά με τα δεδομένα τους και την λογοδοσία των υπευθύνων επεξεργασίας των δεδομένων, αλλά και την αρχή σύμφωνα με την οποία τα δεδομένα προσωπικού χαρακτήρα δεν πρέπει να διαβιβάζονται σε άλλες χώρες οι οποίες δεν παρέχουν επαρκές επίπεδο προστασίας των δικαιωμάτων του υποκειμένου[104].

2.1.1 Ο Νόμος για την προστασία των δεδομένων της Έσσης (1970)

Στην Ευρώπη, η πρώτη εθνική νομοθεσία για την προστασία των προσωπικών δεδομένων ήταν ο νόμος του γερμανικού κρατιδίου της Έσσης (Hessen) του 1970. Ακολουθώντας το «σχέδιο για την Έσση» του 1965, το γερμανικό Ομοσπονδιακό Κράτος της Έσσης, προέβη σε μια μεγάλης κλίμακας άσκηση συλλογής δεδομένων. Ο στόχος της άσκησης αυτής ήταν να συνδράμει την κυβέρνηση στην ανάπτυξη μακροχρόνιων πολιτικών σε οικονομικά και κοινωνικά ζητήματα, όπως η οικονομία και η κοινωνική ασφάλεια. Το 1969, η κυβέρνηση έθεσε σε εφαρμογή

---

[98]Εξειδίκευση αυτής της αρχής είναι ότι το πρόσωπο από το οποίο συλλέγονται τα δεδομένα δεν πρέπει να παραπλανηθεί και πρέπει να ενημερωθεί κατά τη στιγμή της συλλογής. Επίσης, πρέπει να δίνεται συγκατάθεση για τις περαιτέρω χρήσεις ή διαβιβάσεις. Ειδικά για την ηλεκτρονική συγκατάθεση βλ. Οδηγία της ΑΠΔΠΧ 2/2011, διαθέσιμη σε https://www.dpa.gr/sites/default/files/2020-01/2994_2_2011.PDF και αποφάσεις ΑΠΔΠΧ 83/2009 (**παράνομη συγκομιδή/harvesting**) και ΑΠΔΠΧ 59/2011 (**spam**). https://www.dpa.gr/sites/default/files/2019-09/DPA_ANNUAL_REPORT_2009.PDF

[99]Βλ. Γνωμοδότηση ΑΠΔΠΧ 1/2013 για την μεταγραφή ονομάτων στα διαβατήρια και τις αποφάσεις 26/2014,134/2014,175/2014,22/2015, για την «ακριβή» αναγραφή των ονομάτων με λατινικούς χαρακτήρες. Επίσης την ΑΠΔΠΧ 95/2014 για την «ακρίβεια» της αναγραφής των στοιχείων του καταγγέλλοντος. https://www.dpa.gr/sites/default/files/2020-12/ARXH%20PROSTASIAS_APOLOGISMOS%202013.PDF, https://www.dpa.gr/sites/default/files/2019-09/ANNUAL_2014_V2.0_WEB_VIEW.PDF

[100] Βλ. Γνωμοδότηση ΑΠΔΠΧ 1/2017 για το ηλεκτρονικό εισιτήριο ΟΑΣΑ και την σχετική απαγόρευση συλλογής αριθμών ΑΦΜ και ΑΜΚΑ, επειδή αντίκειται στην αρχή της ελαχιστοποίησης. Με τη γνωμοδότηση 4/2017 η Αρχή έκρινε ότι η νέα γνωστοποίηση του ΟΑΣΑ έχει εναρμονιστεί με τις προϋποθέσεις της γνωμοδότησης 1/2017. https://www.dpa.gr/sites/default/files/2020-12/OCT2017.PDF

[101] Βλ. αποφάσεις ΑΠΔΠΧ 24/2004,25/2004 για τον περιορισμό του χρόνου διατήρησης των δεδομένων των αρχείων της ΤΕΙΡΕΣΙΑΣ Α.Ε. https://www.dpa.gr/sites/default/files/2019-10/24-04-1_1.doc, https://www.dpa.gr/sites/default/files/2019-10/25-04-1_2.doc

[102]Βλ. απόφαση ΑΠΔΠΧ 185/2014 που έκρινε παράνομη την διεύρυνση του σκοπού της επεξεργασίας του συστήματος ελέγχου κινδύνου του Τειρεσία (**ΤΣΕΚ**) κυρίως λόγω της διεύρυνσης των αποδεκτών του αρχείου. https://www.dpa.gr/sites/default/files/2019-10/185_2014anonym.pdf.

[103]Βλ. την ΑΠΔΠΧ 98/2013 που επέβαλε πρόστιμο 150.000 ευρώ στην ΓΓΠΣ/Taxis λόγω διαρροής στοιχείων φορολογουμένων και έκρινε ότι το επίπεδο ασφαλείας πρέπει να είναι ανάλογο προς τους κινδύνους. https://eclass.uoa.gr/modules/document/file.php/LAW210/8%20%CE%91%CE%A0%CE%94%CE%A0%CE%A7%2098%202013.doc.

[104]Βλ. ΑΠΔΠΧ 13/2003 για την διαβίβαση στην Ελβετία αρχείων της εταιρείας «Αθήνα 2004 Α.Ε.». https://www.dpa.gr/sites/default/files/2020-12/DPA_ANNUAL_REPORT_2003.PDF.

νομοθεσία η οποία εξουσιοδοτούσε την δημιουργία ενός ενσωματωμένου συστήματος επεξεργασίας δεδομένων για τα κρατικά και κοινοτικά δεδομένα.[105] Χρησιμοποιώντας τεχνικές αυτόματης επεξεργασίας δεδομένων, οι υπεύθυνοι χάραξης πολιτικών θα είχαν τη δυνατότητα να αντικαταστήσουν τις πιο διαισθητικές πολιτικές αποφάσεις με ορθολογικά συμπεράσματα που θα βασίζονταν στη γνώση όλων των σχετικών δεδομένων. Προς το τέλος της δεκαετίας του 1960, ωστόσο, η ευφορία που οφειλόταν στα οφέλη της αυτοματοποίησης άρχισε να εξασθενεί, καθώς οι κριτικοί στοχασμοί που αφορούσαν τις επιπτώσεις των αυτοματοποιημένων συστημάτων άρχισαν να αυξάνονται. Οι ανησυχίες οφείλονταν στην πιθανή αποσταθεροποίηση της ισορροπίας των δυνάμεων ανάμεσα στην νομοθετική και εκτελεστική εξουσία **(«*Gewaltenteilung*»)** και στην απώλεια της ιδιωτικότητας που οφειλόταν στην δυνατότητα των τραπεζών δεδομένων να εκμεταλλεύονται τις πληροφορίες για διαφορετικούς σκοπούς **(«*Verlust jeglicher Privatheit*»)**.[106] Ο νόμος διαρρύθμιζε την χρήση των προσωπικών δεδομένων στο Κράτος και τέθηκε σε ισχύ για να αντισταθμίσει αυτό που θεωρούνταν ως η «εγγενής συγκεντρωτική ισχύς της μηχανής». Προτού σχεδιαστεί ο νόμος, συντελέστηκε μια αναλυτική μελέτη του συστήματος των Η.Π.Α, όπου οι τεχνολογικές εξελίξεις επέβαλλαν από νωρίς την ανάγκη νομοθετικής δράσης. Όντας το πρώτο νομοθέτημα του είδους του, ο «*Hessisches Datenschutzgesetz*», καθόριζε κάποια βασικά μοτίβα που αργότερα θα επέστρεφαν στην διεθνή νομοθεσία προστασίας δεδομένων. Ανάμεσα σε αυτά ήταν ο κανόνας που όριζε ότι η επεξεργασία των δεδομένων πάντα συνιστά μια παρεμβολή που απαιτεί νομιμοποίηση (***negative default rule***), οι κανόνες που καθόριζαν τα δικαιώματα των υποκειμένων και το γενικευμένο, αγνωστικιστικό ως προς τον τομέα νομοθετικό πλαίσιο (***omnibus approach***).[107] Θα πρέπει να σημειωθεί ότι το πεδίο εφαρμογής του νόμου περιοριζόταν στα δεδομένα που χειρίζονταν από (ή εκ μέρους) τους φορείς του δημόσιου τομέα του Κράτους της Έσσης. Επίσης ο νόμος εφαρμοζόταν σε όλες τις μορφές αυτοματοποιημένης επεξεργασίας, εφόσον τα αρχεία ή τα δεδομένα είχαν προετοιμαστεί για τους σκοπούς της αυτοματοποιημένης επεξεργασίας ή είχαν υποβληθεί σε τέτοια επεξεργασία. Τέλος, ο νόμος είχε τρεις σκοπούς: αρχικά στόχευε στην αποτροπή της μη εξουσιοδοτημένης παρέμβασης στα κυβερνητικά αρχεία δεδομένων, έπειτα αποσκοπούσε στην προστασία των ατόμων έναντι τους πιθανούς κινδύνους της αυτοματοποιημένης επεξεργασίας δεδομένων και τέλος στόχευε στην διασφάλιση της πρόσβασης της νομοθετικής εξουσίας σε πληροφορίες. Ο νόμος επίσης παρείχε τη δυνατότητα θεσμικού ελέγχου μέσω της δημιουργίας της υπηρεσίας του Επιτρόπου προστασίας δεδομένων, που θα αναλάμβανε την γενική εποπτεία.[108]

Ο νόμος της Έσσης χαρακτηρίστηκε ως νόμος «δοκιμής και σφάλματος», καθώς ένα σημαντικό κομμάτι του κειμένου του νόμου εστίαζε στη εγκαθίδρυση της υπηρεσίας του Επιτρόπου προστασίας δεδομένων, ο οποίος θα επέβλεπε την εφαρμογή του νόμου και θα αποκτούσε

---

[105] Ο εν λόγω νόμος, ήταν ο Νόμος της 16.12.1969, που εγκαθίδρυε το κέντρο επεξεργασίας δεδομένων του γερμανικού ομόσπονδου κράτους της Έσσης και αφορούσε επίσης τα κέντρα επεξεργασίας δεδομένων των τοπικών κοινοτήτων ["*Gesetz óber die Errichtungder Hessischen Zentrale fór Datenverarbeitung (HZD) und Kommunaler Gebietsrechenzentren (KGRZ)*"], *HE GVBI*, 22 December 1969, No. 32, Part I, p. 304–307. Όπως υποδεικνύει και ο τίτλος, ο νόμος παρείχε επίσης τη νομική βάση για την δημιουργία κέντρων επεξεργασίας δεδομένων στο επίπεδο των τοπικών κοινοτήτων, που θα είχαν την υποχρέωση να συνεργαστούν με το κρατικό κέντρο επεξεργασίας δεδομένων.

[106] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 162.

[107] Jef Ausloos, *The Right to Erasure in EU Data Protection Law*, 1st ed. (repr., Oxford: Oxford University Press, 2020), 40.

[108] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 166.

εμπειρία. Μέσω του καθορισμού του ρόλου του Επιτρόπου με τρόπο ευρύ, ο νόμος επέτρεπε την συνεχή τροποποίηση ώστε να συμβαδίζει με την συνεχώς αυξανόμενη αυτοματοποίηση της δημόσιας διοίκησης. Σε γενικές γραμμές, ο νόμος περιείχε στοιχεία που θα επηρέαζαν την νομοθεσία προστασίας δεδομένων κατά τις επόμενες δεκαετίες. Αρχικά, έθετε τον κανόνα της εμπιστευτικότητας για την επεξεργασία δεδομένων, σύμφωνα με τον οποίο όλα τα δεδομένα που υφίστανται αυτοματοποιημένη επεξεργασία θα πρέπει να διατηρούνται εμπιστευτικά, εκτός αν υπάρχει ρητή εξουσιοδότηση για την αποκάλυψή τους. Ο νόμος επίσης απέδιδε δικαιώματα στα υποκείμενα που δυνητικά μπορούσαν να επηρεαστούν από την επεξεργασία. Τα πιο αξιοσημείωτα από αυτά τα δικαιώματα είναι το δικαίωμα στη διόρθωση και το δικαίωμα κλειδώματος των δεδομένων. Ένα τρίτο στοιχείο επιρροής αποτελεί η εγκαθίδρυση θεσμικής επίβλεψης που προαναφέρθηκε. Ενώ οι εξουσίες των εποπτικών οργάνων θα διέφεραν από χώρα σε χώρα, η βασική ιδέα της απόδοσης της εξουσίας επίβλεψης των κανόνων προστασίας δεδομένων σε μια κυβερνητική οντότητα συναντάται ακόμα και σήμερα στους νόμους προστασίας δεδομένων σε όλη την Ευρώπη.[109] Αν και ο πρωτοποριακός νόμος της Έσσης δεν ορίζει επίσημα τον τρόπο με τον οποίο θα αναγνωρίζονταν οι αρμόδιες αρχές, κάποιοι από τους όρους που χρησιμοποιούνται στη διατύπωσή του, όπως «αυτοί που δικαιούνται να ασκούν τον έλεγχο» ή «τα κέντρα επεξεργασίας δεδομένων», εμφανίζουν ιδεολογική και γλωσσολογική ομοιότητα με τους όρους «υπεύθυνος επεξεργασίας» και «εκτελών την επεξεργασία», οι οποίοι υιοθετήθηκαν αργότερα μέσω της Οδηγίας 95/46 και του ΓΚΠΔ. Επιπροσθέτως, οι πρώτες ετήσιες αναφορές του Επιτρόπου προστασίας δεδομένων της Έσσης, αναγνώριζαν μια σειρά ζητημάτων που θα αποτελούσαν αργότερα θέμα συζήτησης, όπως η ανάγκη για επιπρόσθετα μέτρα όταν επιφορτίζονται με την επεξεργασία δεδομένων άλλες οντότητες που δεν υπάγονται άμεσα στο καθεστώς του νόμου.[110]

2.1.2 Ο Νόμος για τα δεδομένα της Σουηδίας (1973)

Σε σχέση με άλλες ευρωπαϊκές χώρες, στη Σουηδία επετεύχθη σχετικά νωρίς η ευρύτερη υιοθέτηση των υπολογιστών. Στις αρχές της δεκαετίας του 1960, η σουηδική κυβέρνηση άρχισε να επεκτείνει την χρήση της αυτοματοποιημένης επεξεργασίας δεδομένων (ADP) στον δημόσιο τομέα. Ανέπτυξε ένα ολοκληρωμένο σύστημα κεντρικών τραπεζών δεδομένων, που άρχισαν να καθίστανται λειτουργικές το 1963.[111] Αρχικά, αυτή η «υπολογιστικοποίηση» της δημόσιας διοίκησης έγινε αντιληπτή ως ορθολογική και θετική εξέλιξη.[112] Προς το τέλος της δεκαετίας του 1960, ωστόσο, η γενική αυτή αντίληψη κατέστη πιο αμφιλεγόμενη και οδήγησε σε μια πολιτική διαμάχη που κινήθηκε γύρω από δύο άξονες: τον άξονα της διαφάνειας και της ιδιωτικότητας. Πολλοί σχολιαστές αποδίδουν την πρώιμη υιοθέτηση της νομοθεσίας προσωπικών δεδομένων από τη Σουηδία στην μοναδική παράδοση της ανοιχτότητας και της διαφάνειας.[113] Για πάνω από δύο αιώνες η Σουηδία έχει αναγνωρίσει την γενική αρχή της ελεύθερης πρόσβασης σε όλα τα δημόσια έγγραφα. Με βάση αυτήν την αρχή, όλοι έχουν το δικαίωμα να μελετούν τα επίσημα

[109] Ibid., 173.
[110] Ibid., 174.
[111] Frits Willem Hondius, *Emerging Data Protection*, 1st ed. (repr., Amsterdam: North-Holland Publishing Company, 1975), 44.
[112] Lars Ilshammar, "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *Human IT* 9, no. 1 (2007): 9, https://lup.lub.lu.se/search/ws/files/2982893/3430823.
[113] Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and The United States*, 1st ed. (repr., Ithaca, N.Y.: Cornell University Press, 1992), 62.

δημόσια έγγραφα και να ζητούν αντίγραφα αυτών, ενώ κάθε εξαίρεση στην αρχή αυτή θα πρέπει να προβλέπεται από τη νομοθεσία. Όσο η χρήση των υπολογιστών διαδιδόταν ευρέως, εκφράστηκαν φόβοι ότι μπορεί η τάση αυτή να απειλήσει την ικανότητα του πληθυσμού να ασκήσει το δικαίωμά του στην πρόσβαση.[114] Συγκεκριμένα, διατυπώθηκαν επιφυλάξεις ότι οι πολίτες, οι οποίοι μπορούσαν να διαχειριστούν τα έντυπα έγγραφα, θα αντιμετώπιζαν δυσκολίες ενόψει της υιοθέτησης ενός ηλεκτρονικού αρχείου αναδίφησης εγγράφων.[115] Επιπροσθέτως, η ψηφιοποίηση των δημόσιων εγγράφων, σε συνδυασμό με την αρχή της δημοσιότητας, επέτρεπε σε ιδιωτικούς φορείς να αποκτήσουν πρόσβαση σε τεράστιες ποσότητες πληροφοριών που αφορούσαν τα υποκείμενα. Ανάμεσα σε αυτούς τους ιδιωτικούς φορείς υπήρχαν εμπορικές επιχειρήσεις αλλά και υπηρεσίες πιστοληπτικής αξιολόγησης και διαφήμισης.[116]Σε αυτήν την «Κοινωνία της Διαφάνειας», οι ιδιωτικές επιχειρήσεις μπορούσαν να αποκτήσουν πρόσβαση και να αντιγράψουν τα δεδομένα των πολιτών, να τα επεξεργαστούν και να τα εμπορευματοποιήσουν.[117] Επίσης, η ικανότητα διασύνδεσης των πληροφοριών με συγκεκριμένα υποκείμενα διευκολυνόταν σε σημαντικό βαθμό λόγω του γεγονότος ότι η σουηδική κυβέρνηση έκανε χρήση ενός ανεπτυγμένου συστήματος προσωπικών αριθμών αναγνώρισης.[118]

Η σουηδική κυβέρνηση εκλήθη τελικά να πραγματοποιήσει έρευνα που αφορούσε την ισορροπία ανάμεσα στην ανοιχτότητα και την ιδιωτικότητα. Στο πλαίσιο αυτό, τον Απρίλιο του 1969, συνέστησε την Επιτροπή για την νομοθεσία περί Δημοσιότητας και Μυστικότητας **(«*Off entlighets och Sekretesslagstifningskommiten*» – OSK)**.[119] Η Επιτροπή που απαρτιζόταν από ειδικούς εκλήθη να προχωρήσει σε διαβουλεύσεις για την θέσπιση νομοθεσίας που αφορούσε την δημοσιότητα και την μυστικότητα των δημοσίων εγγράφων, υπό το φως των τεχνικών ηλεκτρονικής επεξεργασίας.[120] Ενώ η Επιτροπή αρχικά εστίασε στο ζήτημα της δημοσιότητας, στον τρόπο δηλαδή μέσω του οποίου η αρχή της δημόσιας πρόσβασης θα μπορούσε να επεκταθεί στα υπολογιστικά μέσα, τα ζητήματα που αφορούσαν την ιδιωτικότητα ήρθαν στο προσκήνιο προς το τέλος του 1970.[121] Το 1972, έπειτα από τη διενέργεια πολλών ερευνών, διαβουλεύσεων και ακροάσεων, η Επιτροπή παρουσίασε την αναφορά της, που έφερε τον τίτλο «Δεδομένα και Ακεραιότητα» **(«*Data och integritet*»)**.[122] Σε σχέση με το ζήτημα της προστασίας της ιδιωτικότητας, η Επιτροπή πρότεινε ένα νέο νόμο για τα δεδομένα **(«*Data Act*»-*Datalag*)**, που ουσιαστικά θα υπέβαλλε την δημιουργία των μηχανογραφημένων αρχείων που περιείχαν

---

[114] Ibid., 63.
[115] Frits Willem Hondius, *Emerging Data Protection*, 1st ed. (repr., Amsterdam: North-Holland Publishing Company, 1975), 46.
[116] Lars Ilshammar, "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *Human IT* 9, no. 1 (2007): 22, https://lup.lub.lu.se/search/ws/files/2982893/3430823.
[117] Ibid.
[118] Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and The United States*, 1st ed. (repr., Ithaca, N.Y.: Cornell University Press, 1992), 62.
[119] Lars Ilshammar, "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *Human IT* 9, no. 1 (2007): 14,23, https://lup.lub.lu.se/search/ws/files/2982893/3430823.
[120] Robert Pagano, "Panorama of Personal Data Protection Laws", *Council of Europe, Legislation and Data Protection. Proceedings Of the Rome Conference on Problems Relating to The Development and Application of Legislation on Data Protection,* 1983, 306.
[121] Lars Ilshammar, "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *Human IT* 9, no. 1 (2007): 24, https://lup.lub.lu.se/search/ws/files/2982893/3430823.
[122] Robert Pagano, "Panorama of Personal Data Protection Laws", *Council of Europe, Legislation and Data Protection. Proceedings Of the Rome Conference on Problems Relating to The Development and Application of Legislation on Data Protection,* 1983, 306-307.

προσωπικές πληροφορίες σε προηγούμενη έγκριση. Η προτεινόμενη νομοθετική πράξη υιοθετήθηκε επίσημα στις 11 Μαΐου 1973 και τέθηκε σε ισχύ την 1η Ιουλίου 1973. Αποτελούσε την πρώτη νομοθεσία που θεσπίστηκε σε εθνικό επίπεδο και η οποία αφορούσε την προστασία των δεδομένων.[123] Ο νόμος ήταν εφαρμοστέος για την επεξεργασία δεδομένων στον δημόσιο αλλά και στον ιδιωτικό τομέα.[124]

Ο αρχικός στόχος της νομοθεσίας ήταν να αποτρέψει τις αδικαιολόγητες και αθέμιτες παραβιάσεις της προσωπικής ακεραιότητας των υποκειμένων και να αποκαταστήσει την εμπιστοσύνη ανάμεσα στο κράτος και τους πολίτες.[125] Πολλοί σχολιαστές έχουν περιγράψει τον σουηδικό νόμο περί προστασίας δεδομένων ως ένα «πείραμα» ή ως «μια στρατηγική για την απόκτηση εμπειρίας».[126]Τον καιρό εκείνο, ο εν λόγω νόμος αντιμετωπιζόταν ως κομμάτι της σταδιακής ανάπτυξης μιας νομοθεσίας που στόχευε στην επίλυση όλων των ζητημάτων που αφορούσαν την ιδιωτικότητα. Όπως ο νόμος της Έσσης που προηγήθηκε, ο σουηδικός νόμος έδινε έμφαση στο θεσμικό όργανο που θα αναλάμβανε την διασφάλιση της συμμόρφωσης. Στο πλαίσιο αυτό, η αποστολή του Συμβουλίου Επιθεώρησης δεδομένων («**Data Inspection Board**»), ήταν να διασφαλίσει ότι η αυτοματοποιημένη επεξεργασία δεδομένων δεν θα προκαλούσε αδικαιολόγητη παραβίαση της ιδιωτικότητας. Επιπροσθέτως, κάθε αυτοματοποιημένη επεξεργασία υποβαλλόταν σε προηγούμενη έγκριση από το Συμβούλιο. Ο νόμος βασιζόταν στην αρχή ότι «όλες οι πληροφορίες που αφορούν την κατάσταση των υποκειμένων μπορεί να αφορούν την ιδιωτικότητα».[127] Αυτό σήμαινε ότι κάθε μηχανογράφηση προσωπικών πληροφοριών απαιτούσε την προηγούμενη αδειοδότηση από το Συμβούλιο. Η μόνη εξαίρεση στον κανόνα αυτό ήταν τα προσωπικά μητρώα που εγκαθίδρυε ο Βασιλιάς του Κοινοβουλίου. Ακόμα και στις περιπτώσεις αυτές όμως, το Συμβούλιο διατύπωνε την γνώμη του και είχε την εξουσία να προτείνει κανονισμούς.[128]Μέσω της επίβλεψης της συμμόρφωσης από το Συμβούλιο, η σουηδική κυβέρνηση ήλπιζε να διατηρήσει την ευελιξία ενώ παράλληλα αποκτούσε εμπειρία για περαιτέρω μελλοντικές αποφάσεις που αφορούσαν πολιτικές σε αυτόν τον τομέα.[129]

Ο σουηδικός νόμος περί προστασίας δεδομένων θα αποτέλεσε επίσης πηγή έμπνευσης για τις επόμενες δεκαετίες. Σε πολλές από τις προβλέψεις του, μπορεί κανείς να εντοπίσει προπομπούς πολλών σημερινών αρχών προστασίας δεδομένων και υποχρεώσεων. Παραδείγματα αποτελούν οι περιορισμοί που αφορούν τα ευαίσθητα δεδομένα και τις διεθνείς μεταφορές, η χρήση σχημάτων προηγούμενης εξουσιοδότησης ως ρυθμιστικό εργαλείο, το καθήκον για διασφάλιση της ακρίβειας και της πληρότητας των πληροφοριών αλλά και η απόδοση δικαιωμάτων στα υποκείμενα των δεδομένων. Σε αντίθεση με τον νόμο της Έσσης, ο σουηδικός νόμος παρείχε γενικά κριτήρια για να καθοριστεί ποιος δρών ήταν υπεύθυνος για τη συμμόρφωση. Αυτά τα κριτήρια ήταν σχεδιασμένα για να αναθέτουν την ευθύνη στο μέρος που ουσιαστικά ήλεγχε το μητρώο, σε αντίθεση με όσους απλά παθητικά ακολουθούσαν τις οδηγίες. Μέσω αυτής της

---

[123] Ibid., 307.
[124] Jon Bing, "A Comparative Outline of Privacy Legislation", in *Comparative Law Yearbook 2*, 1st ed., 1978, 161.
[125] Gloria González Fuster, *The Emergence of Personal Data Protection as A Fundamental Right of the EU*, 1st ed. (repr., Cham: Springer, 2014), 58-59.
[126] Jon Bing, "A Comparative Outline of Privacy Legislation", in Comparative Law Yearbook 2, 1st ed., 1978, 150.
[127] Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and The United States*, 1st ed. (repr., Ithaca, N.Y.: Cornell University Press, 1992), 64.
[128] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 179.
[129] Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and The United States*, 1st ed. (repr., Ithaca, N.Y.: Cornell University Press, 1992), 169.

πρόβλεψης, ο νόμος απέκλειε ρητά, τις υπηρεσίες διαχείρισης (***service bureaus***) και άλλους συμβαλλόμενους που μπορεί να συμμετείχαν στην επεξεργασία των προσωπικών μητρώων αλλά στην ουσία δεν είχαν τον έλεγχό τους. Η κατάσταση αυτή δεν οδηγούσε ωστόσο σε εκτροχιασμό της εξουσίας της αρμόδιας αρχής που είχε την επίβλεψη, εφόσον ακόμα και στην περίπτωση της εξωτερικής ανάθεσης, η Επιτροπή θα είχε τη δυνατότητα να πραγματοποιήσει επιτόπια επιθεώρηση στις εγκαταστάσεις της εκάστοτε υπηρεσίας διαχείρισης, η οποία υποχρεούταν να συνεργαστεί. Τέλος, το ρίσκο της μη συμμόρφωσης αναλάμβανε ο υπεύθυνος για την κατοχή του μητρώου. Η έκθεση αυτή σε ευθύνη ρητά συμπεριλάμβανε την ευθύνη για βλάβες που προκαλούνταν από τη χρήση ανακριβών πληροφοριών αλλά και πρόστιμα που επιβάλλονταν λόγω της αποτυχίας για συμμόρφωση με τα καθήκοντα του υπεύθυνου κατόχου. Ο νόμος περιείχε επίσης διατάξεις κυρωτικού χαρακτήρα γενικότερης φύσεως, η εμβέλεια των οποίων δεν περιοριζόταν σε συγκεκριμένο τύπο δρώντων αλλά εκτεινόταν σε όλα τα υποκείμενα που δυνητικά μπορούσαν να αλληλεπιδράσουν με τις προσωπικές πληροφορίες που εμπεριέχονταν σε ένα μητρώο.[130]

2.1.3 Ο γαλλικός νόμος περί Πληροφορικής, Αρχείων και Ελευθεριών (1978)

Όπως συνέβη στην Έσση και στη Σουηδία, στη Γαλλία η δημόσια συζήτηση που αφορούσε την χρήση της αυτοματοποιημένης επεξεργασίας δεδομένων, ήρθε στο προσκήνιο χάρη στα σχέδια που προτάθηκαν για την επέκταση της χρήσης των υπολογιστών εντός του δημοσίου τομέα.[131] Το 1970, η γαλλική κυβέρνηση προώθησε δύο νομοσχέδια που υποδήλωναν τον αυξημένο διαμοιρασμό δεδομένων ανάμεσα στις δημόσιες διοικήσεις. Ο κοινοβουλευτικός διάλογος που συνόδευσε αυτές τις προτάσεις, λειτούργησε ως απόδειξη για την ανάγκη εξειδίκευσης των αρχών προστασίας δεδομένων. Παρά το γεγονός ότι κατά την ίδια χρονιά αναγνωρίστηκε μέσω του Αστικού Κώδικα το δικαίωμα στην ιδιωτικότητα, το ακριβές νόημα της νομοθετικής πρόβλεψης παρέμεινε ακαθόριστο.[132] Ο δημόσιος διάλογος που αφορούσε τους υπολογιστές, έφτασε στο αποκορύφωμά του το 1974 ως αποτέλεσμα του σχεδίου «Σαφάρι» (**«Systeme Automatise pour les Fichiers Administratifs et le Repertoire des Individus»**), μέσω του οποίου προτάθηκε η ελεύθερη πρόσβαση σε όλα τα αυτοματοποιημένα αρχεία του δημοσίου τομέα μέσω ενός μοναδικού αναγνωριστικού κωδικού.[133] Η Επιτροπή για την Πληροφορική και τις Ελευθερίες, επίσης ανέφερε ότι εκτός από το εν λόγω σχέδιο, η δημιουργία των τραπεζών δεδομένων αλλά και των υπολογιστικών δικτύων, ενέτεινε τις ανησυχίες του πληθυσμού.[134] Συνεπώς, η προώθηση ενός σχεδίου κεντρικής διαχείρισης των κυβερνητικών αρχείων, χαρακτηρίστηκε ως σοβαρή απειλή για την ατομική ελευθερία και την ισορροπία των δυνάμεων. Στην Επιτροπή ανατέθηκε η αποστολή της πρότασης μέτρων ώστε να διασφαλιστεί ότι η ανάπτυξη της επεξεργασίας των δεδομένων στον δημόσιο και στον ιδιωτικό τομέα θα λάβει χώρα στο πλαίσιο του σεβασμού για

---

[130] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 187.
[131] Frits Willem Hondius, *Emerging Data Protection*, 1st ed. (repr., Amsterdam: North-Holland Publishing Company, 1975), 32.
[132] Frits Willem Hondius, *Emerging Data Protection*, 1st ed. (repr., Amsterdam: North-Holland Publishing Company, 1975), 34.
[133] A. C. M. Nugter, *Transborder Flow of Personal Data Within The EC: A Comparative Analysis of The Privacy Statutes of The Federal Republic of Germany, France, The United Kingdom and The Netherlands and Their Impact on The Private Sector*, 1st ed. (repr., Deventer: Kluwer Law and Taxation Publishers, 1990), 77.
[134] Commission Informatique et Libertes, *Rapport de la Commission Informatique et libertes*, La Documentation Francaise, Paris, 1975, 7. https://www.cnil.fr/sites/default/files/atoms/files/rapport_tricot_1975_vd.pdf.

την ιδιωτική ζωή αλλά και τις ατομικές και τις δημόσιες ελευθερίες. Η Επιτροπή κατέληξε στο συμπέρασμα ότι παρά το γεγονός ότι η χρήση των υπολογιστικών τεχνολογιών δεν είχε έως τώρα οδηγήσει σε παραβιάσεις των ατομικών ελευθεριών, σημαντικοί κίνδυνοι υφίσταντο για το μέλλον.[135] Η αναφορά της Επιτροπής, η οποία δημοσιεύτηκε το 1975, συνοδεύτηκε από ένα προσχέδιο ενός νομοσχεδίου που είχε ως στόχο την διαρρύθμιση της επεξεργασίας των προσωπικών πληροφοριών. Το προσχέδιο αυτό λειτούργησε επίσης ως θεμέλιο για την μεταγενέστερη πρόταση που προωθήθηκε από την γαλλική κυβέρνηση το 1976.[136] Τέθηκε εν τέλει σε ισχύ στις 6 Ιανουαρίου 1978, ως Νόμος υπ'αριθ. 78-17, ως αφορών την Πληροφορική, τα Αρχεία και τις Ελευθερίες (LIFL).[137]

Ο Νόμος εφαρμοζόταν τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα, όσον αφορά την επεξεργασία δεδομένων (άρθρο 14). Συγκεκριμένα, ρύθμιζε την αυτοματοποιημένη, μη αυτοματοποιημένη και μηχανική επεξεργασία δεδομένων προσωπικού χαρακτήρα (άρθρο 5). Οι έννοιες «μη αυτοματοποιημένη» και «μηχανική» επεξεργασία προσωπικών δεδομένων, δεν εξειδικεύονταν περαιτέρω στο κείμενο του νόμου. Παρά το γεγονός ότι το μεγαλύτερο μέρος του νόμου επηρέαζε μόνο την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, πολλές από τις προβλέψεις του εφαρμόζονταν και στα μη αυτοματοποιημένα ή μηχανογραφημένα αρχεία (άρθρα 45, 25, 27, 29-33, τα οποία εφαρμόζονταν και στην μη αυτοματοποιημένη ή μηχανογραφική επεξεργασία προσωπικών δεδομένων εκτός αν αυτή η επεξεργασία αφορούσε αποκλειστικά προσωπική χρήση, «***dont l'usage releve strict exercice du droit a la vie privee***»).[138] Ο λόγος που συμπεριλήφθηκαν η μη-αυτοματοποιημένη και η μηχανογραφική επεξεργασία στο πεδίο εμβέλειας του νόμου, ήταν για να αποφευχθεί η προνομιακή αντιμετώπιση των μη αυτοματοποιημένων τεχνικών έναντι των αυτοματοποιημένων, αλλά και για να αποφευχθεί η παράκαμψη του νόμου.[139] Ο νόμος επίσης εφαρμοζόταν για την επεξεργασία των προσωπικών δεδομένων **(«*informations nominatives»)***, τα οποία ορίζονται στο άρθρο 4 ως «τα δεδομένα που επιτρέπουν, σε οποιαδήποτε μορφή, άμεσα ή εμμέσως, την αναγνώριση των φυσικών προσώπων με τα οποία σχετίζονται».[140][141] Η μη αυτοματοποιημένη και μηχανογραφημένη επεξεργασία προσωπικών δεδομένων εξαιρούνταν από το πεδίο εφαρμογής του νόμου, αν αυτή η επεξεργασία αφορούσε αποκλειστικά προσωπική χρήση (π.χ. καταχώριση διευθύνσεων σε προσωπικό ημερολόγιο). Επιπροσθέτως, το άρθρο 17 δημιούργησε την ευκαιρία για θέσπιση απλοποιημένων

---

[135] Ibid.

[136] Assemble Nationale, *Projet de loi relatif a l'informatique et aux libertes*, Enregistre a la Presidence de l'Assemblee national le 9 aout 1976, Annexe au proces-verbal de la seance du 2 Octobre 1976, Document Parl. no. 2516, 1–18. https://www.senat.fr/leg/pjl76-2516.pdf

[137] Law no. 78–17 of 6 January 1978 concerning informatics, files and liberties [«*Loi n° 78-17 du 6 Janvier 1978 relative a l'informatique, aux fichiers et aux libertes*»], Official Journal of the French Republic 7 January 1978, 227–231. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000886460

[138] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 190.

[139] Commission Informatique et Libertes, *Rapport de la Commission Informatique et libertes*, La Documentation Francaise, Paris, 1975, 21. https://www.cnil.fr/sites/default/files/atoms/files/rapport_tricot_1975_vd.pdf.

[140] A. C. M. Nugter, *Transborder Flow of Personal Data Within The EC: A Comparative Analysis of The Privacy Statutes of The Federal Republic of Germany, France, The United Kingdom and The Netherlands and Their Impact on The Private Sector*, 1st ed. (repr., Deventer: Kluwer Law and Taxation Publishers, 1990), 82.

[141] Ο νόμος δεν εφαρμοζόταν για την επεξεργασία δεδομένων που αφορούσαν νομικές οντότητες, παρά το γεγονός ότι αυτή ήταν η πρόθεση της κυβέρνησης κατά την σύνταξη του νομοσχεδίου. [Holleux, André. "La Loi Du 6 Janvier 1978 Sur l'informatique et Les Libertés -I-." *La Revue Administrative* 31, no. 181 (1978): 32. http://www.jstor.org/stable/40767795.

κανόνων για την επεξεργασία, που δεν εγκυμονούσαν κινδύνους για την ατομική ιδιωτικότητα ή τις θεμελιώδεις ελευθερίες.[142]

Ο νόμος στόχευε στην προστασία της ιδιωτικότητας και των ατομικών ελευθεριών μέσω της θέσης σε ισχύ διαδικασιών που προέβλεπαν την προηγούμενη διαβούλευση και γνωστοποίηση. Επιπροσθέτως, επέβαλε μια σειρά περιορισμών και υποχρεώσεων που σχετίζονταν με την επεξεργασία των προσωπικών δεδομένων. Παράλληλα, παρείχε στα υποκείμενα τα δεδομένα των οποίων υποβάλλονταν σε επεξεργασία, ορισμένα δικαιώματα και εγκαθίδρυε την Εθνική Επιτροπή για την Πληροφορική και τις Ελευθερίες, στην οποία χορηγήθηκαν εξουσίες επιβολής και ελέγχου.[143] Με βάση το άρθρο 15, η αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων από δημόσια ή ημικρατική οντότητα, απαιτούσε νομική ή ρυθμιστική βάση. Αυτός ο νόμος ή ρύθμιση μπορούσε να υιοθετηθεί έπειτα από τη λήψη αιτιολογημένης γνωμοδότησης της Επιτροπής. Σε περίπτωση αρνητικής γνωμοδότησης, η επεξεργασία μπορούσε να λάβει χώρα επί τη βάση διατάγματος που υιοθετούνταν σε συμφωνία με μια γνωμοδότηση που παρεχόταν από το Συμβούλιο της Επικρατείας (άρθρο 15).[144] Στον ιδιωτικό τομέα, η επεξεργασία των προσωπικών δεδομένων εκ μέρους των ιδιωτικών οντοτήτων δεν υποβαλλόταν σε προηγούμενη διαβούλευση, αλλά σε μια διαδικασία γνωστοποίησης (άρθρο 16). Κάθε ιδιωτική οντότητα που επεδίωκε να εκκινήσει την επεξεργασία των προσωπικών δεδομένων, έπρεπε αρχικά να υποβάλλει μια δήλωση γνωστοποίησης στην Επιτροπή. Έπειτα από την υποβολή, η Επιτροπή θα εξακρίβωνε εάν όλες οι απαιτούμενες πληροφορίες συμπεριλαμβάνονταν στη δήλωση. Εάν αυτό ίσχυε, εξέδιδε σχετική απόδειξη. Η απόδειξη αυτή επέτρεπε στον αιτούντα να εκκινήσει τη διαδικασία της επεξεργασίας (άρθρο 16).[145] Ο πρωταρχικός στόχος της διαδικασίας αυτής ήταν να διασφαλιστεί ότι η Επιτροπή θα συνέχιζε να συμβαδίζει με τις τεχνολογικές εξελίξεις εντός της κοινωνίας, αντί να δημιουργηθεί μια διαδικασία προηγούμενης έγκρισης.[146]

Παράλληλα με τις διαδικασίες της προηγούμενης διαβούλευσης και της γνωστοποίησης, ο νόμος περιλάμβανε επίσης μια σειρά επιπρόσθετων περιορισμών και υποχρεώσεων. Συγκεκριμένα, περιλάμβανε γενικές αρχές που αφορούσαν τη χρήση των τεχνολογιών της πληροφορικής, κανόνες που αφορούσαν τη συλλογή και την αποθήκευση προσωπικών δεδομένων, μια απαίτηση ασφαλείας της επεξεργασίας και περιορισμούς κατά τη χρήση των ευαίσθητων δεδομένων και των εθνικών αριθμών ταυτοποίησης. Το άρθρο 1 χαρακτηριστικά αναφέρει ότι: «η πληροφορική θα πρέπει να υπηρετεί κάθε πολίτη… δεν θα πρέπει να παραβιάζει ούτε την ανθρώπινη ταυτότητα

---

[142] A. C. M. Nugter, *Transborder Flow of Personal Data Within The EC: A Comparative Analysis of The Privacy Statutes of The Federal Republic of Germany, France, The United Kingdom and The Netherlands and Their Impact on The Private Sector*, 1st ed. (repr., Deventer: Kluwer Law and Taxation Publishers, 1990), 87.

[143] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 191.

[144] Εξαιτίας της απαίτησης για σύμφωνη γνώμη της Επιτροπής ή του Συμβουλίου της Επικρατείας, μπορούμε να ισχυριστούμε ότι η απαίτηση πρότερης διαβούλευσης αποτελούσε κατ'ουσίαν ένα σύστημα πρότερης εξουσιοδότησης ή αδειοδότησης. Ενώ η παρακράτηση της σύμφωνης γνώμης θα μπορούσε να έχει παρόμοιες επιπτώσεις σε πρακτικό επίπεδο, θα ήταν πιο ορθό να θεωρηθεί το γαλλικό σύστημα πρότερης διαβούλευσης ως μια διαδικασία για να διασφαλιστεί ότι λαμβάνονται υπόψιν οι πτυχές της ιδιωτικότητας και όχι ως μια επίσημη διαδικασία αδειοδότησης. [Jon Bing, "A Comparative Outline of Privacy Legislation", in *Comparative Law Yearbook 2*, 1st ed., 1978, 165.]

[145] A. C. M. Nugter, *Transborder Flow of Personal Data Within The EC: A Comparative Analysis of The Privacy Statutes of The Federal Republic of Germany, France, The United Kingdom and The Netherlands and Their Impact on The Private Sector*, 1st ed. (repr., Deventer: Kluwer Law and Taxation Publishers, 1990), 87.

[146] Commission Informatique et Libertes, *Rapport de la Commission Informatique et libertes*, La Documentation Francaise, Paris, 1975, 34. https://www.cnil.fr/sites/default/files/atoms/files/rapport_tricot_1975_vd.pdf.

ούτε τα δικαιώματα του ανθρώπου, ούτε την ιδιωτική ζωή αλλά ούτε και τις ατομικές ή δημόσιες ελευθερίες». Η ευρύτητα της διατύπωσης του άρθρου αυτού επανεπιβεβαιώνει ότι οι ανησυχίες αναφορικά με τη χρήση της πληροφορικής δεν περιορίζονταν στο ζήτημα της ιδιωτικότητας. Μια από τις βασικές λογικές βάσεις των συντακτών του νόμου ήταν ότι η τεχνολογία της πληροφορικής είχε τη δυνατότητα να επηρεάσει όλες τις πτυχές της κοινότητας και της κοινωνικής ζωής και όχι μόνο την ιδιωτική ζωή των ατόμων.[147] Αναφορικά με την συλλογή των δεδομένων, οι συντάκτες του νόμου επεδίωξαν να «τιθασεύσουν» την συλλογή και την καταγραφή των προσωπικών δεδομένων με ποικίλους τρόπους. Όπως προαναφέρθηκε, κάθε αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, έπρεπε αρχικά να συμπεριληφθεί σε ένα αίτημα για μια γνωμοδότηση ή μια διακήρυξη. Ως κομμάτι των καθηκόντων επίβλεψής της, η Επιτροπή θα ήλεγχε επίσης εάν τα δεδομένα αυτά ήταν πράγματι αναγκαία για να επιτευχθεί ο δηλωθείς σκοπός της επεξεργασίας. Εάν αυτό δεν συνέβαινε, η Επιτροπή προέβαινε στον περιορισμό κάθε συλλογής που κρινόταν πλεονάζουσα. Τέλος, το άρθρο 25 προέβλεπε ότι η συλλογή προσωπικών δεδομένων με κακόβουλα και απατηλά μέσα ήταν απαγορευμένη. Για παράδειγμα, θα ήταν παράνομο να συλλέγονται δεδομένα από αρχεία που δεν προορίζονταν για γνωστοποίηση σε τρίτα μέρη.[148]

Ο νόμος επίσης επέβαλλε επιπρόσθετους περιορισμούς για την επεξεργασία ορισμένων τύπων «ευαίσθητων» δεδομένων. Τα δεδομένα αυτά θεωρούνταν «ευαίσθητα» λόγω του διακριτικού χαρακτήρα τους ή γιατί μπορούσαν να λειτουργήσουν ως βάση για άδικες διακρίσεις.[149] Οι περιορισμοί αφορούσαν δεδομένα που είχαν σχέση με ποινικά αδικήματα, καταδίκες ή μέτρα ασφαλείας (άρθρο 30), καθώς και δεδομένα που αποκάλυπταν την εθνοτική καταγωγή, τις πολιτικές, φιλοσοφικές ή θρησκευτικές πεποιθήσεις, ή την συμμετοχή σε συνδικαλιστικές οργανώσεις (άρθρο 31). Η επεξεργασία των δεδομένων αυτών γενικώς απαγορευόταν. Τα δεδομένα που αφορούσαν τα ποινικά αδικήματα, τις καταδίκες ή τα μέτρα ασφαλείας, μπορούσαν αρχικά να αποτελέσουν αντικείμενο επεξεργασίας από «τις δικαιοδοτικές αρχές και τις δημόσιες αρχές που ενεργούσαν στο πλαίσιο της νομικής ισχύος τους και κατά τη σύμφωνη γνώμη της εθνικής επιτροπής και των εταιρειών που διαχειρίζονταν τις δημόσιες υπηρεσίες».[150] Τα δεδομένα που αφορούσαν την εθνοτική καταγωγή, τις πολιτικές, τις φιλοσοφικές και τις θρησκευτικές πεποιθήσεις ή την συμμετοχή σε συνδικαλιστικές οργανώσεις, μπορούσαν αρχικά να αποτελέσουν αντικείμενο επεξεργασίας μόνο έπειτα από ρητή συγκατάθεση του υποκειμένου το οποίο αφορούσαν.[151]Παράλληλα, ο νόμος παρείχε στα υποκείμενα των οποίων τα δεδομένα υφίσταντο επεξεργασία (**«*personnes concernees*»**), μια σειρά δικαιωμάτων. Σε αυτά συμπεριλαμβάνονταν

[147] A. C. M. Nugter, *Transborder Flow of Personal Data Within The EC: A Comparative Analysis of The Privacy Statutes of The Federal Republic of Germany, France, The United Kingdom and The Netherlands and Their Impact on The Private Sector*, 1st ed. (repr., Deventer: Kluwer Law and Taxation Publishers, 1990), 79.
[148] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 195.
[149] Commission Informatique et Libertes, *Rapport de la Commission Informatique et libertes*, La Documentation Francaise, Paris, 1975, 47. https://www.cnil.fr/sites/default/files/atoms/files/rapport_tricot_1975_vd.pdf.
[150] David H. Flaherty, *Protecting Privacy in Surveillance Societies*, 1st ed. (repr., United States: The University of North Carolina Press, 2014), 180.
[151] Εξαιρέσεις στον κανόνα της ρητής συγκατάθεσης ίσχυαν μόνο για θρησκευτικούς, φιλοσοφικούς ή πολιτικούς οργανισμούς που διατηρούσαν αυτοματοποιημένα αρχεία των μελών ή των ανταποκριτών τους (άρθρο 31). Εξαιρέσεις ίσχυαν και για λόγους δημοσίου συμφέροντος, έπειτα από πρόταση της Επιτροπής ή σύμφωνης γνώμης μέσω διατάγματος του Συμβουλίου της Επικρατείας (άρθρο 31).

το δικαίωμα ενημέρωσης, το δικαίωμα εναντίωσης, το δικαίωμα πρόσβασης, το δικαίωμα γνώσης και αμφισβήτησης και το δικαίωμα διόρθωσης (άρθρα 27, 26, 34, 35, 3, 36).

Αναφορικά με το ρόλο της Εθνικής Επιτροπής για την Πληροφορική και τις Ελευθερίες (***Commission Nationale Informatique et Liberte*– CNIL**), θα πρέπει να σημειωθεί ότι σκοπός της ίδρυσής της ήταν να εξασφαλίσει τη συμμόρφωση με τις νομοθετικές προβλέψεις του νόμου, μέσω της ενημέρωσης των υποκειμένων για τα δικαιώματα και τις υποχρεώσεις τους, διενεργώντας διαβουλεύσεις με αυτά και επιβλέποντας τη χρήση των τεχνολογιών της πληροφορικής κατά την επεξεργασία των προσωπικών δεδομένων.[152] Η αποστολή της Επιτροπής, επομένως, ήταν να ενημερώνει, να συμβουλεύει και να επιβλέπει τα άτομα που εμπλέκονταν (ή επηρεάζονταν) από την επεξεργασία των προσωπικών δεδομένων. Επιπροσθέτως, στα καθήκοντά της ενέπιπτε η διατήρηση μιας δημοσίως διαθέσιμης λίστας όλης της δημόσιας και ιδιωτικής επεξεργασίας δεδομένων (άρθρο 22). Η λίστα καθόριζε για κάθε σύστημα επεξεργασίας, τον νόμο ή την ρυθμιστική πράξη με βάση την οποία αποφασιζόταν η δημιουργία της επεξεργασίας, το όνομα και τον σκοπό της, την υπηρεσία με βάση την οποία κάποιος μπορούσε να ασκήσει το δικαίωμα πρόσβασής του και τους τύπους προσωπικών δεδομένων που είχαν καταχωρηθεί καθώς και τους παραλήπτες ή τις κατηγορίες των εξουσιοδοτημένων παραληπτών. Παράλληλα, στην Επιτροπή είχαν χορηγηθεί μέσω του νόμου ευρείες εποπτικές αρμοδιότητες. Ανάμεσα σε αυτές ήταν η διενέργεια ερευνών και επιθεωρήσεων, η ανάπτυξη προτάσεων και μοντέλων διαρρύθμισης που αφορούσαν την ασφάλεια της επεξεργασίας, η λήψη και η διαμεσολάβηση σε καταγγελίες, η έκδοση αποφάσεων σε συγκεκριμένες περιπτώσεις (π.χ. για να επιτρέψει εξαιρέσεις στην χορήγηση δικαιώματος πρόσβασης), η έκδοση προειδοποιήσεων και η ενημέρωση του δημόσιου κατηγόρου για πιθανές παραβάσεις για τις οποίες λάμβανε γνώση αλλά και η πρόταση νομοθετικών ή κανονιστικών μέτρων που έκρινε ότι ήταν απαραίτητα για την προστασία των ατομικών ελευθεριών υπό το φως των τεχνολογικών εξελίξεων.[153][154] Οι οντότητες που είχαν τον έλεγχο των ιδιωτικών ή δημοσίων οργανισμών, καθώς και οι οντότητες που είχαν στην κατοχή τους ή χρησιμοποιούσαν αρχεία που περιείχαν προσωπικά δεδομένα, ήταν υποχρεωμένες να συνεργάζονται με την Επιτροπή κατά την άσκηση των καθηκόντων της (άρθρο 21 *in fine*).

Ο γαλλικός νόμος περί Ελευθεριών, Πληροφορικής και Αρχείων, ακολούθησε το μονοπάτι που χάραξαν, ο γερμανικός και ο σουηδικός προκάτοχός του. Σε κάποιες πλευρές του παρουσίαζε ομοιότητα με τον γερμανικό νόμο προστασίας δεδομένων της Έσσης και τον νόμο της Ομοσπονδιακής Δημοκρατίας της Γερμανίας[155], ενώ σε άλλες πλευρές του έμοιαζε περισσότερο με τον σουηδικό νόμο περί δεδομένων.[156] Πολλές από τις βασικές διατάξεις του, όπως το δικαίωμα

---

[152] Commission Informatique et Libertes, *Rapport de la Commission Informatique et libertes*, La Documentation Francaise, Paris, 1975, 71. https://www.cnil.fr/sites/default/files/atoms/files/rapport_tricot_1975_vd.pdf.

[153] David H. Flaherty, *Protecting Privacy in Surveillance Societies*, 1st ed. (repr., United States: The University of North Carolina Press, 2014), 186-188.

[154] A. C. M. Nugter, *Transborder Flow of Personal Data Within The EC: A Comparative Analysis of The Privacy Statutes of The Federal Republic of Germany, France, The United Kingdom and The Netherlands and Their Impact on The Private Sector*, 1st ed. (repr., Deventer: Kluwer Law and Taxation Publishers, 1990), 97-101.

[155] Gesetz zum Schutz vor Miβbrauch personenbezogener Daten bei der Datenverarbeitung of 27 January 1977, *Bundesgesetblatt* 1 February 1977, I, No. 7, 201.
(γερμανικός ομοσπονδιακός νόμος για την προστασία του πολίτη από την αυτόματη επεξεργασία των προσωπικών πληροφοριών). http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl177007.pdf

[156] Αναφορικά με την εφαρμοστικότητά του στην επεξεργασία δεδομένων στον ιδιωτικό και δημόσιο τομέα και τα καθήκοντα του «υπεύθυνου κατόχου».

στην πρόσβαση, ο περιορισμός του χρόνου αποθήκευσης και το δικαίωμα στη γνώση, συναντώνται και στη σύγχρονη νομοθεσία περί προστασίας δεδομένων. Ο νόμος επίσης δεν όριζε επίσημα ποιοι φορείς (ή τύποι φορέων) θα ήταν υπεύθυνοι για τη συμμόρφωση με τις διατάξεις του. Αντίθετα έκανε χρήση πολλών διαφορετικών όρων για να αναφερθεί, από τη μια πλευρά στον φορέα που ήταν επιφορτισμένος με την κύρια ευθύνη της επεξεργασίας και από την άλλη πλευρά στους φορείς που μπορεί να εμπλέκονται στην επεξεργασία των προσωπικών δεδομένων εξ 'ονόματος άλλων. Η τελευταία ομάδα φορέων, δεν εξαιρούνταν ωστόσο από την συμμόρφωση καθώς πολλές από τις διατάξεις του νόμου ήταν άμεσα εφαρμοστέες στους φορείς που εκτελούσαν την επεξεργασία εξ 'ονόματος άλλων.[157][158]

2.1.4 Η νομοθεσία προσωπικών δεδομένων μετά το 1981

Μετά το 1981, τέθηκαν σε ισχύ δύο νόμοι που αφορούσαν την προστασία των δεδομένων. Ο πρώτος από αυτούς ήταν ο νόμος για την προστασία των δεδομένων του Ηνωμένου Βασιλείου (1984) και ο βελγικός νόμος προστασίας δεδομένων (1992). Η κυβέρνηση της Αγγλίας δημοσίευσε το 1982 μια λευκή βίβλο, επιβεβαιώνοντας με τον τρόπο αυτό την πρόθεσή της να νομοθετήσει. Στις 21 Δεκεμβρίου του 1982, η κυβέρνηση παρουσίασε το νομοσχέδιο για την προστασία των δεδομένων στο Κοινοβούλιο. Το νομοσχέδιο διέφερε από τις προτάσεις της Επιτροπής Lindop σε πολλά σημεία. Πιο σημαντική ήταν η μεταβολή της Αρχής Προστασίας Δεδομένων («Data Protection Authority») σε Γραμματεία Προστασίας Δεδομένων («Data Protection Registrar»), οι εξουσίες της οποίας ήταν πιο περιορισμένες. Σύμφωνα με σχολιαστές, ο μοναδικός στόχος του νόμου ήταν να επιτρέψει στο Η.Β να κυρώσει την Σύμβαση 108, την οποία το Η.Β είχε ήδη υπογράψει από το 1981. Έπειτα από μια σειρά τροποποιήσεων, ο αγγλικός νόμος περί προστασίας δεδομένων τέθηκε σε ισχύ στις 12 Ιουλίου 1984.[159] Σε γενικές γραμμές ο νόμος διατήρησε την ορολογία που είχε εισάγει η Επιτροπή Lindop. Ειδικότερα, έκανε χρήση του όρου «χρήστης δεδομένων» («***data user***») για να υποδηλώσει το κύριο υποκείμενο του κανονισμού. Ωστόσο, ένα άτομο θεωρούνταν χρήστης δεδομένων αν στην πραγματικότητα «κατείχε» τα δεδομένα υπό την έννοια του άρθρου 1 παρ. 5. Η «κατοχή» αυτή στοιχειοθετούνταν μόνο εφόσον το άτομο αυτό ήλεγχε τα περιεχόμενα και τη χρήση των δεδομένων. Η έννοια του ελέγχου επομένως βρισκόταν στον πυρήνα του ορισμού του «χρήστη» των δεδομένων. Αργότερα ο όρος εξειδικεύτηκε περαιτέρω από τη Γραμματεία προστασίας δεδομένων και ένα άτομο θεωρείτο ότι είχε τον έλεγχο των περιεχομένων της συλλογής δεδομένων εάν «βρίσκεται σε θέση να αποφασίζει ποιο στοιχείο και τύπος πληροφόρησης θα καταγραφεί ως δεδομένο».[160]

Ο αγγλικός νόμος για την προστασία των δεδομένων του 1984 περιλάμβανε οκτώ αρχές προστασίας που βασίζονταν στην αναφορά της Επιτροπής Younger και στη Σύμβαση 108 του Συμβουλίου της Ευρώπης. Λόγω της γενικής φύσης τους, οι αρχές δεν ήταν άμεσα εκτελεστές από τα δικαστήρια, αλλά μόνο έμμεσα μέσω της Γραμματείας. Οι πρώτες επτά αρχές

---

[157] Οι διατάξεις που είχαν κυρωτικό χαρακτήρα επίσης δεν διαχώριζαν ανάμεσα σε αυτούς που επεξεργάζονταν δεδομένα για δικό τους λογαριασμό και αυτούς που επεξεργάζονταν δεδομένα για λογαριασμό άλλων. Η αναφορά της Επιτροπής, ωστόσο, είχε υποδείξει μια επιθυμία να μην εισάγει διατάξεις για την καθ' υποκατάσταση ποινική ευθύνη. Ως αποτέλεσμα, μπορεί κάποιος να ισχυριστεί ότι όσοι δρουν εξ' ονόματος άλλων, μπορεί να μην θεωρούνται ποινικά υπεύθυνοι, εφόσον ενήργησαν σύμφωνα με τις οδηγίες που τους δόθηκαν.

[158] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 206.

[159] Ibid., 233-234.

[160] The Data Protection Registrar, "The Data Protection Act of 1984, https://www.legislation.gov.uk/ukpga/1984/35/enacted

εφαρμόζονταν στους χρήστες των δεδομένων. Η όγδοη αρχή εφαρμοζόταν τόσο στους χρήστες των δεδομένων όσο και στα άτομα που δραστηριοποιούνταν σε υπηρεσίες μηχανοργάνωσης (computer bureaux). Και οι δύο κατηγορίες προσώπων υποχρεούνταν να καταχωρίσουν την ταυτότητά τους στην Γραμματεία προστασίας δεδομένων. Οι χρήστες δεδομένων υποχρεούνταν να συμμορφωθούν με τις οκτώ αρχές που απαριθμούνται στο παράρτημα 1 του νόμου. Οι αρχές αυτές ήταν: η αρχή της δικαιοσύνης και της νομιμότητας, η αρχή του καθορισμού του σκοπού, η αρχή του περιορισμού της γνωστοποίησης και της χρήσης, η αναλογικότητα, η ακρίβεια, η αρχή του περιορισμού της διάρκειας αποθήκευσης, τα υποκείμενα των δεδομένων και η ασφάλεια.[161] Ο νόμος παρείχε επίσης στα υποκείμενα των δεδομένων τα δικαιώματα πρόσβασης, διόρθωσης και διαγραφής (τμήματα 21, 24). Παράλληλα κατοχύρωνε το δικαίωμα των υποκειμένων των δεδομένων να αξιώσουν αποζημίωση για βλάβη σε περίπτωση που η βλάβη αυτή οφειλόταν στην ανακρίβεια των δεδομένων (τμήμα 22) ή στην περίπτωση που η βλάβη επήλθε χάρη στην απώλεια, την μη εξουσιοδοτημένη γνωστοποίηση ή την πρόσβαση στα δεδομένα (τμήμα 23). Ενώ η αποζημίωση για την ανακρίβεια των δεδομένων μπορούσε να ληφθεί από τον χρήστη των δεδομένων, αποζημίωση για βλάβες σε περίπτωση παραβιάσεων ασφαλείας μπορούσε να ληφθεί και από την εκάστοτε υπηρεσία μηχανοργάνωσης.

Παρά την μακρά νομοθετική ιστορία, οι βασικές έννοιες που αποτελούν το θεμέλιο του νόμου προστασίας δεδομένων του 1984 παρέμειναν κατά κύριο λόγο αμετάβλητες. Από το ξεκίνημα, τόσο η Επιτροπή Younger όσο και η Επιτροπή Lindop, αναγνώρισαν τη διαφορά ανάμεσα στους «χρήστες», στους φορείς εκμετάλλευσης και στους ιδιοκτήτες των υπολογιστικών υπηρεσιών. Εν τέλει δύο διακριτοί ρόλοι αναγνωρίστηκαν: αυτός της υπηρεσίας μηχανοργάνωσης («computer bureau») και αυτός του χρήστη δεδομένων («data user»). Ο πρώτος θεωρήθηκε πρωτίστως ως πάροχος υπηρεσιών ενώ ο δεύτερος ως δικαιούχος του προϊόντος. Ένα ακόμα αξιοσημείωτο χαρακτηριστικό του νόμου ήταν η αναγνώριση του πλουραλιστικού ελέγχου, καθώς όχι μόνο αναγνώριζε ότι ο έλεγχος μπορεί να ασκηθεί από περισσότερα του ενός μέρη, αλλά αναγνώριζε επίσης δύο διαφορετικούς τρόπους με βάση τους οποίους ο έλεγχος μπορούσε να διαμοιραστεί (**«*jointly or in common*»**).

Η πρώτη κοινοβουλευτική πρόταση για την θέσπιση νομοθεσίας προστασίας δεδομένων στο Βέλγιο, υπεβλήθη το 1971.[162]Πολλές άλλες προτάσεις που εμφορούνταν από το ίδιο πνεύμα ακολούθησαν, χωρίς όμως κάποια να ψηφίζεται τελικά ως νόμος.[163]Καθ' όλη τη διάρκεια της δεκαετίας του 1970, η βελγική κυβέρνηση δεν επέδειξε μεγάλο ενδιαφέρον για τη νομοθέτηση της προστασίας των δεδομένων και περιορίστηκε στους υπάρχοντες νόμους που σύμφωνα με εκείνη προσέφεραν ικανοποιητική προστασία. Παράλληλα, ανέμενε το αποτέλεσμα των εν εξελίξει διεθνών πρωτοβουλιών και συγκεκριμένα αυτές που είχε αναλάβει το Συμβούλιο της Ευρώπης.[164]Στις αρχές της δεκαετίας του 1980, το Βέλγιο άρχισε να υιοθετεί νόμους οι οποίοι διαρρύθμιζαν τη χρήση ορισμένων κατηγοριών δεδομένων. Η εμβέλεια της εφαρμογής των νόμων

---

[161] Chris Edwards, Nigel Savage and Ian Walden, *Information Technology & The Law*, 2nd ed. (repr., London: Palgrave Macmillan, 1990), 72-74.

[162] Η νομοθετική πρόταση βασίστηκε σε μια ακαδημαϊκή δημοσίευση του C.Aronstein, «Defense de la vie privee. Essai pour contribuer a la survie de notre civilisation», [*Journal des Tribunaux* 1971,453–463].

[163] Robert Pagano, "Panorama of Personal Data Protection Laws", *Council of Europe, Legislation and Data Protection. Proceedings Of the Rome Conference on Problems Relating to The Development and Application of Legislation on Data Protection,* 1983, 243.

[164] Frits W. Hondius, *Emerging Data Protection in Europe*, 1st ed. (repr., American Elsevier Pub. Co, 1975), 27.

αυτών, ωστόσο, ήταν περιορισμένη σε συγκεκριμένους τομείς ή βάσεις δεδομένων. Οι πιο σημαντικοί ανάμεσα σε αυτούς ήταν ο Νόμος για το Εθνικό Μητρώο («Law on the National Register») και ο Νόμος για την εγκαθίδρυση της Τράπεζας Crossroads για την κοινωνική ασφάλιση («Crossroadsbank of Social Security»). Και οι δύο νόμοι επέβαλαν σημαντικούς περιορισμούς ως προς την διαθεσιμότητα ορισμένων πληροφοριών. Παράλληλα, επεδείκνυαν την θέληση νομιμοποίησης και διευκόλυνσης της αυτοματοποιημένης ανταλλαγής προσωπικών πληροφοριών. Το πρώτο σχέδιο για τον βελγικό νόμο προστασίας δεδομένων κατατέθηκε από την κυβέρνηση στις 16 Μαΐου 1991. Παρά τις εκκλήσεις για άμεση θέση σε ισχύ, υπεβλήθη σε πολλές τροποποιήσεις με αποτέλεσμα το τελικό κείμενο να ψηφιστεί στις 8 Δεκεμβρίου 1992.

Η ορολογία του βελγικού νόμου προστασίας δεδομένων παρουσίαζε πολλές ομοιότητες με την αντίστοιχη της Σύμβασης 108. Οι ορισμοί όμως δεν ήταν ίδιοι. Για παράδειγμα, ο βελγικός ορισμός για τον υπεύθυνο επεξεργασίας του αρχείου («***controller of file***») ήταν αρκετά πιο σύντομος σε σχέση με τον αντίστοιχο της Σύμβασης. Ο βελγικός νόμος επίσης αναγνώριζε επίσημα την έννοια του εκτελούντα την επεξεργασία («***processor***»).[165] Ο υπεύθυνος επεξεργασίας του αρχείου μπορούσε να είναι είτε φυσικό είτε νομικό πρόσωπο, ή ένας σύλλογος («***feitelijke vereniging»)***. Ο νόμος εφαρμοζόταν και στον ιδιωτικό και στον δημόσιο τομέα αλλά περιείχε εξαιρέσεις και παρεκκλίσεις για ορισμένες οντότητες του δημοσίου τομέα. Επίσης, προέβλεπε εξαίρεση για τα «δεδομένα που διατηρούνταν από φυσικά πρόσωπα, που προορίζονταν για ιδιωτική, οικογενειακή ή οικιακή χρήση και τα οποία διατηρούν αυτόν τον σκοπό» (άρθρο 3 παρ. 2). Ο υπεύθυνος επεξεργασίας του αρχείου ήταν το μέρος που ήταν «ικανό να αποφασίσει» σχετικά με την επεξεργασία. Αυτός ο ορισμός υιοθέτησε επομένως μια λειτουργική προσέγγιση, μεταθέτοντας την ευθύνη της συμμόρφωσης στο μέρος που μπορούσε να ασκήσει την εξουσία λήψης αποφάσεως σε σχέση με την επεξεργασία.[166] Στο άρθρο 7 παρ. 1 οριζόταν επίσης ο εκτελών την επεξεργασία ως «το φυσικό ή νομικό πρόσωπο ή ο σύλλογος που είναι επιφορτισμένο με την οργάνωση και την εκτέλεση της επεξεργασίας».

Από νομικής άποψης, ο βελγικός νόμος προστασίας δεδομένων του 1992, χαρακτηρίστηκε ως «προχειροδουλειά». Έπειτα από πολλά χρόνια συνεχιζόμενων αναβολών, η βελγική κυβέρνηση ξαφνικά αισθάνθηκε την ανάγκη να υιοθετήσει μια νομοθεσία προστασίας δεδομένων λόγω της εντεινόμενης διεθνούς πίεσης. Το αποτέλεσμα ήταν μια ημιτελής νομοθεσία, καθώς πολλές από τις διατάξεις της απαιτούσαν περαιτέρω εφαρμογή για να έχουν επίδραση.[167] Η θέσπιση νομοθετημάτων συνεχίστηκε στον τομέα αυτό κατά τη δεκαετία του 1980, με την εισαγωγή νομοθεσιών «δεύτερης γενεάς» σε χώρες όπως η Ιρλανδία, η Ολλανδία, η Ισπανία και η Πορτογαλία, αλλά και την αναθεώρηση παλαιότερων νομοθεσιών. Ακολούθως, η ψήφιση της κοινοτικής Οδηγίας 95/46/ΕΚ είχε ως συνέπεια να ακολουθήσει μια Τρίτη γενεά νομοθετημάτων κατά τη δεκαετία του 1990 και μετέπειτα.[168]

2.1.5 Η Οδηγία 95/46/Ε.Κ. της 24.10.1995

Η Οδηγία 95/46/Ε.Κ. του Ευρωπαϊκού Κοινοβουλίου της 24.10.1995 (L 281,31) «Για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων και για την

---

[165] Brendan Van Alsenoy, *Data Protection Law in the EU*, 1st ed. (repr., Cambridge: Intersentia, 2019), 253-254.
[166] Ibid., 255.
[167] Ibid., 260.
[168] Ιωάννης Ιγγλεζάκης, *Δίκαιο Πληροφορικής*, 4η εκδ. (repr., Θεσσαλονίκη: Εκδόσεις Σάκκουλα, 2021), 325.

ελεύθερη κυκλοφορία των δεδομένων αυτών», φιλοδοξούσε να συμφιλιώσει την προστασία των δεδομένων με την – απαραίτητη για την ολοκλήρωση της ευρωπαϊκής αγοράς- διασυνοριακή ροή πληροφοριών μεταξύ κρατών-μελών. Παράλληλα, αποσκοπεί στην εναρμόνιση των νομοθεσιών των κρατών-μελών της Ευρωπαϊκής Ένωσης ώστε να διασφαλίζεται η προστασία των προσώπων μέσω του καθορισμού των νόμιμων προϋποθέσεων για τη θεμιτή επεξεργασία των προσωπικών δεδομένων, με την ίδρυση υποχρεώσεων και την αναγνώριση δικαιωμάτων, τα οποία εξοπλίζονται με ένδικα μέσα και επιβολή κυρώσεων. Αντίστοιχα με τις προηγούμενες διεθνείς συνθήκες, είναι τεχνολογικά ουδέτερη ως προς τον τρόπο επεξεργασίας των δεδομένων.[169] Παράλληλα, προσδιορίζει τις υποχρεώσεις του υπευθύνου επεξεργασίας και προβλέπει ειδικές κυρώσεις για την παραβίαση αυτών. Ρυθμίζει επίσης τη διαβίβαση σε τρίτες χώρες (εκτός Ε.Ε) και ορίζει συγκεκριμένες προϋποθέσεις εγγυήσεων ασφαλείας που απαιτούνται για την εν λόγω διαβίβαση. Εξίσου σημαντικά, η Οδηγία προβλέπει την ίδρυση ανεξάρτητων εποπτικών αρχών για την προάσπιση των δικαιωμάτων των πολιτών. Η Οδηγία άφησε εκτός του πεδίου εφαρμογής της τις περιπτώσεις επεξεργασίας «στο πλαίσιο δραστηριοτήτων που δεν εμπίπτουν στο πεδίο εφαρμογής του κοινοτικού δικαίου,[…] και εν πάση περιπτώσει, στη επεξεργασία δεδομένων που αφορά τη δημόσια ασφάλεια, την εθνική άμυνα, την ασφάλεια του κράτους, […] και τις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου». Στις περιπτώσεις αυτές, ακολούθησε ειδική νομοθεσία όπως ο Κανονισμός 45/2001 σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων από τα όργανα και του οργανισμούς της κοινότητας.[170]

Ένα σημαντικό χαρακτηριστικό της Οδηγίας 95/46/Ε.Κ. ήταν η αναγνώριση του «επιμερισμένου» ή «κοινού» ελέγχου. Η νομοθεσία της Ε.Ε κυρίως προέβλεπε περιπτώσεις κατά τις οποίες μια σειρά μερών από κοινού αποφασίζουν τους σκοπούς και τα μέσα της επεξεργασίας εν συνόλω. Σύμφωνα με την Ομάδα Εργασίας του άρθρου 29, ωστόσο, ο πλήρης «κοινός» έλεγχος κατά τον οποίο όλοι οι υπεύθυνοι επεξεργασίας ισότιμα αποφασίζουν σχετικά με τους σκοπούς και τα μέσα επεξεργασίας, αποτελεί ένα από τα πολλά είδη «πλουραλιστικού ελέγχου».[171] Αντιμέτωπη με την αυξανόμενη πολυπλοκότητα της επεξεργασίας δεδομένων, η ομάδα του άρθρου 29 ανέλαβε το έργο της διαφοροποίησης ανάμεσα στις διαφορετικές μορφές που μπορεί να λάβει ο από κοινού έλεγχος. Αναμφίβολα, η ομάδα εργασίας έχει κατά καιρούς υπερβεί στην ερμηνεία της σχετικά με την έννοια του υπευθύνου επεξεργασίας, την αρχική έννοια που σχεδίαζαν οι συντάκτες της Οδηγίας 95/46/ΕΚ.[172]

Αναφορικά με την προσέγγιση του ΓΚΠΔ στο ζήτημα αυτό, η αυξανόμενη πολυπλοκότητα των σύγχρονων διαδικασιών επεξεργασίας δεδομένων, έχει οδηγήσει πολλούς σχολιαστές στην αμφισβήτηση της βιωσιμότητας των εννοιών του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία. Εν τέλει, ωστόσο, η νομοθεσία της Ε.Ε. ακολούθησε την άποψη της ομάδας εργασίας του άρθρου 29, σύμφωνα με την οποία οι ίδιες οι έννοιες παρέμεναν έγκυρες.[173] Οι

---

[169] Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, *Προσωπικά Δεδομένα*, 1η εκδ. (Θεσσαλονίκη: Νομική Βιβλιοθήκη, 2016), 207.

[170] Ειρηνικός Πλατής, *Προσωπικά Δεδομένα-Προστασία GDPR*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Παπαδόπουλος, 2018), 27-28.

[171]"Opinion 1/2010 On the Concepts of "Controller" and "Processor"", *ec.europa.eu*,2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

[172] Lokke Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, 1st ed. (repr., Oxford: Oxford University Press, 2012), 220-222.

[173]"Opinion 1/2010 On the Concepts of "Controller" and "Processor", *ec.europa.eu*,2010,33 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

νομοθετικές αλλαγές επίσης κωδικοποιούσαν τμήματα της καθοδήγησης που παρείχε η ομάδα 29 υπό το καθεστώς της Οδηγίας 95/46 και επιβεβαίωνε ορισμένες γενικές αρχές του δικαίου των αδικοπραξιών (π.χ. κανόνες για την εις ολόκληρον ευθύνη).

Παρά το γεγονός ότι δεν οριζόταν στην αρχική πρόταση της Επιτροπής, η τελική έκδοση της Οδηγίας 95/46 καθόριζε τον εκτελούντα την επεξεργασία ως ξεχωριστή οντότητα. Το κίνητρο πίσω από την ρύθμιση της «επεξεργασίας εκ μέρους του υπευθύνου επεξεργασίας» ήταν να αποφευχθούν περιπτώσεις στις οποίες η επεξεργασία από τρίτο μέρος εκ μέρους του υπευθύνου επεξεργασίας θα είχε επιπτώσεις ως προς τη μείωση του επιπέδου προστασίας που απολάμβανε το υποκείμενο των δεδομένων. Σύμφωνα με την ομάδα του άρθρου 29, η έννοια του εκτελούντος την επεξεργασία κατέληξε να υπηρετεί διπλό σκοπό εντός του νομοθετικού πλαισίου της Οδηγίας 95/46 και συγκεκριμένα: αναγνώριζε τις ευθύνες εκείνων των οντοτήτων που είναι στενά συνδεδεμένες κατά την επεξεργασία, αλλά πράττουν αυτό εκ μέρους ενός ή περισσότερων οντοτήτων (υπευθύνων επεξεργασίας) και χρησίμευε για να γίνεται διάκριση μεταξύ των εμπλεκόμενων που είναι υπεύθυνοι ως υπεύθυνοι επεξεργασίας και εκείνων που απλώς ενεργούν για λογαριασμό τους.[174] Στον πυρήνα της έννοιας του εκτελούντος την επεξεργασία έγκειται η δράση του εκτελούντος εκ μέρους του υπευθύνου επεξεργασίας. Η ομάδα του άρθρου 29 προσέγγισε την διατύπωση αυτή μέσω της νομικής έννοιας της εξουσιοδότησης, σύμφωνα με την οποία μια οντότητα ζητεί από μια άλλη οντότητα να αναλάβει την εκτέλεση ορισμένων καθηκόντων εκ μέρους της.[175] Η Οδηγία 95/46 αντιμετωπίζει τους εκτελούντες την επεξεργασία αποκλειστικά ως παθητικούς δρώντες, οι οποίοι απλά εκτελούν τις οδηγίες που έλαβαν από τον υπεύθυνο επεξεργασίας και δεν έχουν αποφασιστική επιρροή επί της επεξεργασίας. Το γεγονός αυτό εξηγεί γιατί η Οδηγία επιβάλει μόνο την περιορισμένη υποχρέωση της συμμόρφωσης με τις οδηγίες που έχει εκδώσει ο υπεύθυνος επεξεργασίας.

Υπό το καθεστώς της Οδηγίας 95/46, η ευθύνη για τη συμμόρφωση έγκειται αποκλειστικά στον υπεύθυνο επεξεργασίας. Οι εκτελούντες την επεξεργασία είναι καταρχήν μόνο έμμεσα υπεύθυνοι, δυνάμει μιας σύμβασης ή άλλης νομικής πράξης που τους συνδέει με τον υπεύθυνο επεξεργασίας. Τα πρώιμα σχέδια της Οδηγίας προέβλεπαν μια σειρά υποχρεώσεων που θα δέσμευαν τους εκτελούντες την επεξεργασία. Στην τελική έκδοση, ωστόσο, μόνο μια υποχρέωση παρέμεινε, αυτή του καθήκοντος να μην επεξεργάζονται προσωπικά δεδομένα εκτός αν συντρέχουν εντολές του υπευθύνου επεξεργασίας (άρθρο 16). Η Οδηγία επίσης δεν έδινε στα υποκείμενα των δεδομένων το δικαίωμα να στραφούν κατά των εκτελούντων την επεξεργασία, παρά το γεγονός ότι αντίστοιχο δικαίωμα προσφυγής μπορούσε να προβλεφθεί μέσω των εθνικών νομοθεσιών.

Ο βαθμός στον οποίο ο εκτελών την επεξεργασία συμμορφώνεται με τις κανονιστικές ρυθμίσεις της Οδηγίας, βασίζεται κατά κύριο λόγο στις συμβατικές δικλείδες ασφαλείας που τίθενται σε εφαρμογή. Το άρθρο 17 παρ. 3 της Οδηγίας, ορίζει ότι «η εκτέλεση επεξεργασίας μέσω άλλου προσώπου πρέπει να διέπεται από σύμβαση ή δικαιοπραξία που συνδέει τον εκτελούντα με τον υπεύθυνο της επεξεργασίας» και η οποία προβλέπει ότι «ο εκτελών την επεξεργασία ενεργεί μόνον κατ' εντολή του υπευθύνου επεξεργασίας» και θα πρέπει να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει την ασφάλεια της επεξεργασίας (άρθρο 17 παρ.

[174]"Opinion 1/2010 on the Concepts of "Controller" and "Processor", *ec.europa.eu*,2010,7 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.
[175] Ibid.

1).[176] Το άρθρο 17 παρ. 3 κάνει αναφορά μόνο στο ελάχιστο περιεχόμενο που πρέπει να συμπεριλαμβάνεται στην συμφωνία ανάμεσα στους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία, επομένως δεν αποκλείεται οι υπεύθυνοι επεξεργασίας να δεσμεύουν περαιτέρω τους εκτελούντες την επεξεργασία με επιπρόσθετες αρχές προστασίας δεδομένων ή δικλείδες ασφαλείας.

Η Οδηγία, ως εργαλείο της δευτερογενούς νομοθετικής πρωτοβουλίας της Ευρωπαϊκής Ένωσης, δεν παράγει αυτομάτως έννομα αποτελέσματα για τους πολίτες των κρατών-μελών, αλλά πρέπει να ενταχθεί στο εθνικό δίκαιο μέσα από την εθνική κοινοβουλευτική διαδικασία. Θέτει γενικές υποχρεώσεις για τα κράτη-μέλη, τις οποίες εκείνα πρέπει να προσαρμόσουν κατά το επιτρεπτό και να ενσωματώσουν κατά το δοκούν. Ως εκ τούτου, είναι αναμενόμενες ορισμένες διαφορές και αποκλίσεις μεταξύ των ειδικότερων σημείων μίας Οδηγίας. Χαρακτηριστικό παράδειγμα αυτού ήταν η απόκλιση στις εθνικές ρυθμίσεις με βάση τις οποίες απαγορευόταν, σε μεγαλύτερο ή μικρότερο βαθμό, η αποστολή προσωπικών δεδομένων σε τρίτες χώρες: η διαφοροποίηση αυτή μπορούσε να προκαλέσει σημαντικά προβλήματα και αυξημένα κόστη σε διεθνείς επιχειρήσεις, οι οποίες πρέπει να τηρούν διαφορετικό επίπεδο συμμόρφωσης με τις διάφορες έννομες τάξεις. Η διασπορά των ρυθμίσεων σε πλήθος νομοθετημάτων και το συλλογικό αίσθημα έλλειψης ομοιογενούς προστασίας των δεδομένων, ιδίως στον χώρο του διαδικτύου και στις ηλεκτρονικές συναλλαγές, αποτέλεσαν επίσης κίνητρο για την ανανέωση του θεσμικού πλαισίου.[177] Πολλοί επίσης θεωρούν ότι η Οδηγία δεν ανταποκρίθηκε στους στόχους της και απέτυχε να ευθυγραμμίσει το επίπεδο προστασίας δεδομένων εντός της Ε.Ε. Πολλές δραστηριότητες επεξεργασίας δεδομένων που επιτρέπονταν σε κάποια κράτη-μέλη, θεωρούνταν παράνομες σε άλλα σε σχέση με την συγκεκριμένη εκτέλεση της επεξεργασίας των δεδομένων. Στο πλαίσιο αυτό, και σύμφωνα με τον συρμό, η Οδηγία θεωρήθηκε πλέον ως απρόσφορο νομοθετικό εργαλείο, επειδή συνεπαγόταν κάποια διακριτική ευχέρεια των κρατών μελών στην προσαρμογή τους σε αυτήν. Για να αποκλείσει τη διαφορετική μεταχείριση των προσωπικών δεδομένων από χώρα σε χώρα, ο ενωσιακός νομοθέτης προέβη σε έκδοση του υπ'αριθ. 679/2016 «Γενικού Κανονισμού για την προστασία δεδομένων», ο οποίος ετέθη σε ισχύ από 25/5/2016, αλλά η εφαρμογή του ορίζεται αρχόμενη μετά την πάροδο διετούς περιόδου προσαρμογής, την 25/5/2018. Σε κάθε περίπτωση το καθ' ύλην πεδίο εφαρμογής της Οδηγίας περιορίζεται σε ζητήματα της εσωτερικής αγοράς, με αποτέλεσμα να μην εμπίπτουν στο πεδίο εφαρμογής της θέματα που αφορούν την αστυνομική και δικαστική συνεργασία σε ποινικές υποθέσεις. Στον τομέα αυτό η προστασία των δεδομένων διαρρυθμίζεται μέσω άλλων νομοθετημάτων του Συμβουλίου της Ευρώπης και της Ευρωπαϊκής Ένωσης (Σύμβαση 108/1981, Σύσταση R (87) 15 της επιτροπής Υπουργών του Συμβουλίου της Ευρώπης[178] της 17ης Σεπτεμβρίου 1987, Σύμβαση της

[176] "Οδηγία 95/46/ΕΚ Του Ευρωπαϊκού Κοινοβουλίου Και Του Συμβουλίου Της 24ης Οκτωβρίου 1995 Για Την Προστασία Των Φυσικών Προσώπων Έναντι Της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα Και Για Την Ελεύθερη Κυκλοφορία Των Δεδομένων Αυτών", Επίσημη Εφημερίδα αριθ. L 281 της 23/11/1995 σ. 0031 - 0050 § (1995). https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL.

[177] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)*, 1st ed. (repr., Cham: Springer International Publishing, 2017), 1-2.

[178] "Recommendation No. R (87) 15 Of The Committee Of Ministers To Member States Regulating The Use Of Personal Data In The Police Sector", Rm.Coe.Int, 2021, https://rm.coe.int/168062dfd4.

Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο του 2001 η οποία κυρώθηκε στον ελληνικό χώρο με τον νόμο 4411/2016[179]).

Ο κύριος στόχος της Οδηγίας 95/46/ΕΚ ήταν να εναρμονίσει τη νομοθεσία προστασίας δεδομένων στον ευρωπαϊκό χώρο. Στο μεγαλύτερο μέρος του, η Οδηγία βασίστηκε στο κεκτημένο της Σύμβασης 108, η οποία είχε ήδη κατοχυρώσει την βασική αρχιτεκτονική για τους εθνικούς νόμους προστασίας δεδομένων στην Ε.Ε. Παρ 'όλα αυτά, η Οδηγία 95/46 εισήγαγε μια σειρά νέων στοιχείων, σε σχέση με τον προκάτοχό της. Οι σημαντικές αλλαγές περιλάμβαναν κανόνες για το εφαρμοστέο δίκαιο, την εισαγωγή της έννοιας του εκτελούντος την επεξεργασία και η αναγνώριση του από κοινού ελέγχου. Εντός του ρυθμιστικού πλαισίου της Οδηγίας, ο υπεύθυνος επεξεργασίας ενέχει την πρωτεύουσα ευθύνη για την διασφάλιση της συμμόρφωσης. Κατά τη στιγμή της θέσπισής της, η ευρωπαϊκή νομοθεσία αναγνώριζε την πρακτική κατά την οποία ένας οργανισμός ζητά από κάποιον άλλο οργανισμό να εκτελέσει ορισμένες εργασίες επεξεργασίας εκ μέρους της. Εισάγοντας την έννοια του εκτελούντος την επεξεργασία, η ευρωπαϊκή νομοθεσία ήλπιζε να μπορέσει να αντιμετωπίσει την κατάσταση αυτή και να διασφαλίσει ένα συνεχές επίπεδο προστασίας. Συνεπώς, η Οδηγία αφιέρωσε πολλαπλές διατάξεις που αφορούν την σχέση ανάμεσα σε υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία (άρθρο 17 παρ. 1,2,3). Αντιθέτως, δεν περιλαμβάνει συγκεκριμένες απαιτήσεις που αποσκοπούν στην διαρρύθμιση της σχέσης ανάμεσα σε υπευθύνους επεξεργασίας. Στα 22 έτη λειτουργίας της, η Οδηγία έθεσε τις βασικές κατευθύνσεις για την εύρεση ισορροπίας μεταξύ πληροφοριακού αυτοπροσδιορισμού και ελεύθερης ροής δεδομένων. Προσπάθησε να εισαγάγει πρακτικές που στόχευαν στην ασφάλεια και την προστασία των δεδομένων και να λειτουργήσει παιδευτικά ως προς την δημιουργία ήθους προστασίας των προσωπικών δεδομένων. Σύντομα, όμως ξεπεράστηκε από τις τεχνολογικές εξελίξεις- ιδίως το Web 2.0 και τις διασυνοριακές ροές δεδομένων- και έδειξε τον δρόμο για τον επερχόμενο νέο Γενικό Κανονισμό Προστασίας Δεδομένων.

2.2 Το ελληνικό νομοθετικό πλαίσιο

Στην Ελλάδα η προστασία δεδομένων έχει σχετικά πρόσφατη ιστορία. Παρά την κύρωση της ΕΣΔΑ το 1953, το δικτατορικό καθεστώς του 1967 κατήγγειλε τη Σύμβαση. Μια από τις πρώτες ενέργειες της Μεταπολίτευσης ήταν η εκ νέου κύρωση της Σύμβασης το 1974. Στην πορεία, η Ελλάδα υπέγραψε τη Σύμβαση 108 του Συμβουλίου το 1983, αλλά την κύρωσε μόλις το 1992, αποκτώντας τότε, για πρώτη φορά, ένα δεσμευτικό κείμενο για την προστασία των προσωπικών δεδομένων. Λίγα χρόνια μετά ψηφίστηκε ο πρώτος ελληνικός νόμος 2472/1997, με αφορμή την ανάγκη εναρμόνισης με την κοινοτική Οδηγία 95/46/ΕΚ.[180]Μόλις το 2001 και με τη Ζ΄ Αναθεωρητική Βουλή ορίζεται ρητά πλέον στο Σύνταγμα, στο άρθρο 9^{A} ότι «καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει».

---

[179]"Νόμος 4411/ΦΕΚ Α' 142/3.8.2016", Dsanet.Gr, 2016, http://www.dsanet.gr/Epikairothta/Nomothesia/4411_2016.htm.

[180] Ειρηνικός Πλατής, *Προσωπικά Δεδομένα-Προστασία GDPR*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Παπαδόπουλος, 2018), 29.

Ειδικότερα, μέσω του νόμου 2472/1997, ρυθμίζονται οι προϋποθέσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, οι οποίες αποτείνουν στην προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής (άρθρο 1). Με το νόμο 2472/1997 θεσμοθετήθηκε ένα σαφές κανονιστικό πλαίσιο προστασίας των προσωπικών δεδομένων, το οποίο περιείχε κανόνες ουσιαστικούς, οργανωτικούς, διαδικαστικούς και κυρωτικούς. Οι κανόνες αυτοί αποσκοπούσαν στην οριοθέτηση της συνταγματικά ανεκτής επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κατά αυτόν τον τρόπο συνέβαλαν ουσιαστικά στην ρύθμιση της ροής και της κατανομής των πληροφοριών στο πλαίσιο του κράτους, της οικονομίας και της κοινωνίας. Ο νόμος προκάλεσε πλήθος αλλαγών στον ελληνικό χώρο, ενσωματώνοντας πρωτίστως τις αρχές που προέβλεπε η Οδηγία και οι διεθνείς συμβάσεις σχετικά με τη σύννομη και θεμιτή επεξεργασία προσωπικών δεδομένων, ενώ τίθενται σε εφαρμογή ειδικές ασφαλιστικές δικλείδες για την επεξεργασία ευαίσθητων δεδομένων.Το σύστημα του νόμου 2472/97 προϋποθέτει ότι η επεξεργασία επιτρέπεται μόνο όταν το υποκείμενο έχει δώσει τη συγκατάθεσή του[181] (άρθρα 2 στοιχ. ια΄ 5 παρ. 1,7). Η επεξεργασία χωρίς συγκατάθεση επιτρέπεται μόνο κατ' εξαίρεση για τις ακόλουθες νόμιμες βάσεις (άρθρο 5 παρ. 2 α-ε): α) για την εκτέλεση σύμβασης με συμβαλλόμενο το υποκείμενο ή για τη λήψη μέτρων κατά το προσυμβατικό στάδιο, β) για την εκπλήρωση υποχρέωσης του υπευθύνου επεξεργασίας που επιβάλλεται από το νόμο, γ) για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου εφόσον τελεί σε φυσική ή νομική αδυναμία να δώσει την συγκατάθεσή του, δ) για την εκτέλεση έργου δημοσίου συμφέροντος ή αυτού που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια Αρχή, ε) όταν είναι απολύτως απαραίτητη για την ικανοποίηση του εννόμου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας και υπό τον όρο ότι αυτό υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών.[182]

Για το ζήτημα των «ευαίσθητων» δεδομένων η γενική κατεύθυνση του νόμου είναι ότι η συλλογή και η επεξεργασία τους απαγορεύεται. Η συλλογή και επεξεργασία επιτρέπεται μόνο κατ' εξαίρεση και μόνο μετά από προηγούμενη άδεια της Αρχής[183] (άρθρο 7 παρ.2 α-ζ), εφόσον υπάρχει γραπτή συγκατάθεση του υποκειμένου, είναι αναγκαία για την διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, αφορά δεδομένα που δημοσιοποιεί το ίδιο το υποκείμενο ή είναι αναγκαία για την άσκηση, αναγνώριση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου ή πειθαρχικού οργάνου, αφορά θέματα υγείας[184], εκτελείται από δημόσια αρχή, πραγματοποιείται για επιστημονικούς ή ερευνητικούς σκοπούς, ή αφορά δεδομένα δημοσίων προσώπων, εφόσον αυτά συνδέονται με την άσκηση δημοσίου λειτουργήματος ή τη διαχείριση συμφερόντων τρίτων και πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος.[185][186]

---

[181]Βλ. Γνώμη 15/2011 της Ομάδας του άρθρου 29, σχετική με τον ορισμό της συγκατάθεσης, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_el.pdf

[182] Γεώργιος Γιαννόπουλος, *Εισαγωγή Στη Νομική Πληροφορική*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2018), 75.

[183] Μόνο στο πλαίσιο αυτό επιτρεπόταν ο προληπτικός έλεγχος νομιμότητας κάθε επιχειρηθησόμενης επεξεργασίας (**auditing**), ενώ στον ΓΚΠΔ προβλέπεται στο άρθρο 42.

[184] Για την χρήση τέτοιου είδους δεδομένων βλ. ΑΠΔΠΧ 74/2010. https://www.dpa.gr/sites/default/files/2020-12/ETHSIA%20EKTHESI%202010.PDF

[185] Βλ. ΑΠΔΠΧ 100/2000 που οδήγησε στην απόφαση ΣτΕ 3542/2002 και τις αποφάσεις ΑΠΔΠΧ 3/2009 και 8/2010.

[186] Γεώργιος Γιαννόπουλος, *Εισαγωγή Στη Νομική Πληροφορική*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2018), 76-77.

Προβλέπονται επίσης ρητά οι αρχές της νομιμότητας, της θεμιτής και νόμιμης επεξεργασίας, του σκοπού, της αναλογικότητας[187], της ορθότητας και της ακρίβειας[188] των δεδομένων, της πεπερασμένης διατήρησης[189], της διαφάνειας, της ασφάλειας και του ελέγχου. Επίσης προβλέπονται κυρώσεις σε περίπτωση παραβιάσεων, οι οποίες είναι διοικητικές[190] (άρθρο 21), ποινικές (άρθρο 22) που περιλαμβάνουν και επιβαρυντικές περιπτώσεις – σε βαθμό κακουργήματος- αν διαπιστωθεί προσπορισμός παράνομου περιουσιακού οφέλους ή προκληθεί κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, ενώ προβλέπεται και αστική ευθύνη (άρθρο 23) με δικαίωμα αποζημίωσης και χρηματική ικανοποίηση λόγω ηθικής βλάβης.

Η τήρηση των αρχών επεξεργασίας αποτελεί υποχρέωση του υπευθύνου επεξεργασίας και τα δεδομένα που έχουν συλλεχθεί, ή υφίστανται επεξεργασία κατά παράβαση των παραπάνω αρχών, καταστρέφονται με ευθύνη του υπευθύνου επεξεργασίας. Παράλληλα η Αρχή εάν εξακριβώσει παράβαση των αρχών επεξεργασίας επιβάλλει τη διακοπή της συλλογής ή της επεξεργασίας και την καταστροφή των προσωπικών δεδομένων που έχουν ήδη συλλεγεί ή έχουν τύχει επεξεργασίας. Στο πλαίσιο αυτό, η Αρχή διέταξε την καταστροφή αρχείου με ηλεκτρονικές διευθύνσεις των ενδιαφερομένων φυσικών ή νομικών προσώπων (άρθρο 11 νόμου 3471/2006), που είχαν παράνομα συλλεγεί και τηρούνταν από τον υπεύθυνο επεξεργασίας[191], την ολοσχερή καταστροφή του συνόλου του αρχείου που περιέχει προσωπικά δεδομένα που δεν ανήκουν στον ενοποιημένο και δημόσια προσβάσιμο κατάλογο του επικοινωνιακού παρόχου[192], αλλά και την καταστροφή αρχείου με παρανόμως τηρούμενα ευαίσθητα δεδομένα υγείας[193][194]. Ο νόμος 2472/97 ορίζει επίσης και την ίδρυση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ως αρμόδια εποπτική αρχή και παράλληλα θεσπίζει σύστημα γνωστοποίησης στη Αρχή με τις λεπτομέρειες για τα δεδομένα, τους σκοπούς της επεξεργασίας κ.λπ. που περιγράφονται στο άρθρο 6 παρ. 2 περ. α-η. Το σύστημα αυτό αποδείχτηκε εξαιρετικά

---

[187] Η αρχή αυτή προκύπτει από το άρθρο 4 παρ. 1β του νόμου 2472/1997, σύμφωνα με το οποίο τα προσωπικά δεδομένα, για να τύχουν νόμιμης επεξεργασίας, πρέπει να «είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών επεξεργασίας».

[188] Η αρχή αυτή προκύπτει από το άρθρο 4 παρ. 1γ του νόμου 2472/1997, σύμφωνα με το οποίο τα προσωπικά δεδομένα, για να τύχουν νόμιμης επεξεργασίας, πρέπει να «είναι ακριβή και εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση».

[189] Η αρχή αυτή προκύπτει από το άρθρο 4 παρ. 1δ του νόμου 2472/1997, σύμφωνα με το οποίο τα προσωπικά δεδομένα, για να τύχουν νόμιμης επεξεργασίας, πρέπει να «διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής, για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους». Η τήρηση της αρχής της καθορισμένης διάρκειας διατήρησης των δεδομένων ικανοποιεί το δικαίωμα του υποκειμένου να περιπίπτουν σε λήθη τα προσωπικά του δεδομένα, όταν παύουν να εξυπηρετούν το σκοπό της επεξεργασίας. [Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, *Προσωπικά Δεδομένα*, 1η εκδ. (Θεσσαλονίκη: Νομική Βιβλιοθήκη, 2016), 82.]

[190]α) Προειδοποίηση, β) πρόστιμο ποσού έως πενήντα εκατομμύρια (50.000.000 δρχ.= 146.734,94 ευρώ), γ) προσωρινή ανάκληση άδειας, δ) οριστική ανάκληση άδειας, ε) καταστροφή αρχείου ή διακοπή επεξεργασίας και καταστροφή, επιστροφή ή κλείδωμα (δέσμευση) των σχετικών δεδομένων.

[191]Βλ. αποφάσεις 83/2009, 38/2005 ΑΠΔΠΧ διαθέσιμες στα: https://www.dpa.gr/sites/default/files/2019-09/DPA_ANNUAL_REPORT_2009.PDF,https://www.dpa.gr/sites/default/files/202012/DPA_ANNUAL_REPORT_2005_0.PDF.

[192]Βλ. απόφαση ΑΠΔΠΧ 86/2013, διαθέσιμη στο: https://www.dpa.gr/sites/default/files/2020-12/ARXH%20PROSTASIAS_APOLOGISMOS%202013.PDF.

[193]Βλ. απόφαση ΑΠΔΠΧ 55/2010, διαθέσιμη στο: https://www.dpa.gr/sites/default/files/2020-12/ETHSIA%20EKTHESI%202010.PDF.

[194] Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, *Προσωπικά Δεδομένα*, 1η εκδ. (Θεσσαλονίκη: Νομική Βιβλιοθήκη, 2016), 85.

γραφειοκρατικό και αργότερα προστέθηκε το άρθρο 7^{A} που προβλέπει απαλλαγή από την υποχρέωση γνωστοποίησης για μεγάλες κατηγορίες υπευθύνων επεξεργασίας και δεδομένων όπως για παράδειγμα, για αυτά που δημιουργούνται από σχέση εργασίας ή έργου, τα δεδομένα πελατών ή προμηθευτών (όταν τα δεδομένα δεν διαβιβάζονται σε τρίτους), με εξαίρεση τις ασφαλιστικές, φαρμακευτικές εταιρείες, τράπεζες κ.λπ., τα δεδομένα σωματείων, εταιρειών κ.λπ. (απαιτείται συγκατάθεση), τα δεδομένα ιατρών και όσων παρέχουν υπηρεσίες υγείας, με εξαίρεση τα νομικά πρόσωπα, την τηλεϊατρική την παροχή συμβουλών μέσω δικτύου και τα δεδομένα δικηγόρων και συμβολαιογράφων.[195]

Ο νόμος αυτός, ο οποίος τροποποιήθηκε επανειλημμένα (από το άρθρο 8 του νόμου 2819/2000, το άρθρο 34 του νόμου 2915/2001, το άρθρο 26 παρ. 4 του νόμου 3156/2003, το άρθρο 10 του νόμου 3090/2002, το νόμο 3471/2006 και τελευταία το νόμο 3625/2007), αποτέλεσε τη γενική νομοθεσία για την προστασία των προσωπικών δεδομένων, ενώ ειδική νομοθεσία υφίσταται στον τομέα των τηλεπικοινωνιών (νόμος 3471/2006). Εξειδικευμένες ρυθμίσεις θεσπίζονται και με διατάξεις άλλων νομοθετημάτων (άρθρο 8 του νόμου 3144/2003, άρθρο 9 του νόμου 2737/1999, άρθρο 2 παρ. 12 Π.Δ. 61/1999, άρθρο 7 νόμου 3663/2008), που δεν εντάσσονται όμως σε ένα ειδικό πλαίσιο.

Θα πρέπει να σημειωθεί ότι ο Κανονισμός (άρθρο 94 παρ. 1) ορίζει ότι, από τη στιγμή που θα τεθεί σε εφαρμογή στις 25/5/2018, καταργεί την Οδηγία 95/46/ΕΚ, που έτσι φαίνεται ότι ήταν ισχύουσα μεταβατικώς και κατά τη διετή περίοδο προσαρμογής (25/5/2016-25/5/2018). Μετά από την πάροδο της διετίας αυτής, οι εθνικοί κανόνες του δικαίου προσωπικών δεδομένων δεν καταργήθηκαν στο σύνολό τους ρητώς, αλλά σιωπηρώς και εν μέρει, δηλαδή απλώς υποχώρησαν προ των αντιθέτων διατάξεων του ΓΚΠΔ ως μεταγενέστερου και τυπικώς υπέρτερου νομοθετήματος. Ως εκ τούτου, του ήδη σιωπηρώς καταργημένου νόμου 2472/1997, επιτασσόταν επιπλέον και η ρητή κατάργηση, ήτοι η πανηγυρική εξαγωγή του αντιενωσιακού νομοθετήματος από την έννομη τάξη.[196]

2.2.1 Η βασική διαφορά του ΓΚΠΔ με τον Ν. 2472/97

Η ευθύνη του υπευθύνου επεξεργασίας, υπό το πρίσμα καθαρά νομικών κριτηρίων, αποτελεί «νόθο αντικειμενική ευθύνη», δηλαδή πρόκειται για αντιστροφή του βάρους απόδειξης. Κατά την Οδηγία 95/46/ΕΚ η ευθύνη βάρυνε κυρίως τον υπεύθυνο επεξεργασίας και όχι τον εκτελούντα την επεξεργασία. Πλέον, με βάση τα δεδομένα που προκύπτουν από την ως τώρα εφαρμογή του ΓΚΠΔ, η ευθύνη επεκτείνεται και στους εκτελούντες, αφού «…κάθε πρόσωπο το οποίο υπέστη υλική ή μη ζημία ως αποτέλεσμα της παραβίασης του παρόντος κανονισμού δικαιούται αποζημίωση από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία για τη ζημιά που υπέστη..» (άρθρο 82 παρ. 1). Ωστόσο, η κύρια διαφορά του ΓΚΠΔ είναι ότι επιτείνει την ευθύνη εισάγοντας καθεστώς λογοδοσίας (**accountability**), αφού ο υπεύθυνος επεξεργασίας πρέπει ανά πάσα στιγμή να «εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ» (άρθρο 24 παρ. 1). Επίσης, ορίζεται ότι τα μέτρα αυτά, ως προς τον υπεύθυνο επεξεργασίας,

---

[195] Γεώργιος Γιαννόπουλος, *Εισαγωγή Στη Νομική Πληροφορική*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2018), 75.

[196] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 8.

περιλαμβάνουν και «κατάλληλες πολιτικές» (άρθρο 24 παρ. 2). Συνάγεται επομένως ότι η ευθύνη του υπευθύνου επεξεργασίας πλησιάζει κατ'ουσίαν την αντικειμενική ευθύνη και την ευθύνη από διακινδύνευση. Στο σύστημα που καθιερώνει ο ΓΚΠΔ, ο υπεύθυνος επεξεργασίας δεν αρκεί μόνο να αποδεικνύει ότι «δεν φταίει», αλλά πρέπει να αποδεικνύει ότι κινείται συνεχώς εντός των ορίων που χαράσσει η νέα νομοθεσία.

Ως προς τον εκτελούντα την επεξεργασία, όλες οι ενέργειές του τελούν σε άμεση συνάρτηση με τις εντολές του υπευθύνου της επεξεργασίας (άρθρο 82 παρ. 2 εδάφιο 2). Οφείλει επομένως να εφαρμόζει και αυτός τα κατάλληλα τεχνικά και οργανωτικά μέτρα ώστε η επεξεργασία να πληροί τις προϋποθέσεις του ΓΚΠΔ (άρθρο 28 παρ. 1) και να συνδράμει τον υπεύθυνο επεξεργασίας προκειμένου να συμμορφώνεται προς τις υποχρεώσεις που αποσκοπούν στην ασφάλεια των δεδομένων (άρθρο 28 παρ. 3 περ (στ')). Αυτές οι ειδικές υποχρεώσεις του εκτελούντος την επεξεργασία προβλέπονται σε κατάλογο που καταγράφει αναλυτικά το ελάχιστο περιεχόμενο της συμβάσεως ή άλλης νομικά δεσμευτικής πράξεως, με την οποία ο εκτελών την επεξεργασία δεσμεύεται ότι θα εκτελεί την επεξεργασία υπό συγκεκριμένες προϋποθέσεις (άρθρο 28 παρ. 3 περ. (α) έως (η)). Συνεπώς, η αντικειμενική ευθύνη του υπευθύνου επεξεργασίας, επιμερίζεται κατ' αναλογία και στον εκτελούντα την επεξεργασία. Παρεπόμενη υποχρέωση του εκτελούντος την επεξεργασία αποτελεί η αμελλητί ενημέρωση του υπευθύνου επεξεργασίας σε περίπτωση παραβιάσεων (άρθρο 33 παρ. 2). Επιπροσθέτως, ο ΓΚΠΔ περιλαμβάνει κανόνες (άρθρο 82 παρ. 4,5) για την ευθύνη εις ολόκληρον μεταξύ περισσοτέρων υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία, αλλά και για τυχόν αναγωγικές αξιώσεις από όποιον κατέβαλε αποζημίωση (ΑΚ 926,927). Τέλος, ο ΓΚΠΔ, εφαρμόζεται ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός τη Ένωσης (άρθρο 3 παρ. 1). Προϋπόθεση, για την χωρική επέκταση της ευθύνης στους εκτελούντες την επεξεργασία (άρθρο 3 παρ. 2 και αιτ. σκέψη 24) είναι να επεξεργάζονται προσωπικά δεδομένα υποκειμένων που διαμένουν στην Ε.Ε.[197]

2.3 Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων

Σήμερα, η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα διέπεται από τον Γενικό Κανονισμό για την Προστασία των Δεδομένων [Κανονισμός (ΕΕ) 2016/679 «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών…»], ο οποίος τέθηκε σε εφαρμογή στις 25 Μαΐου 2018 και αποβλέπει αφενός στην προσαρμογή της προστασίας στις τεχνολογικές εξελίξεις (ανάπτυξη της ψηφιακής οικονομίας, παγκόσμια διάσταση της επεξεργασίας, ανάπτυξη βιομετρικών και γενετικών δεδομένων κ.ο.κ.) και αφετέρου στην άρση των αναποτελεσματικών ρυθμίσεων του προισχύσαντος καθεστώτος. Μια από τις πιο σημαντικές αλλαγές που επέφερε ο ΓΚΠΔ αφορά την νομική του φύση. Έλαβαν χώρα στο παρελθόν πολλές συζητήσεις αναφορικά με τον αν το νέο αυτό θεσμικό και νομοθετικό εργαλείο θα πρέπει να λάβει τη μορφή Οδηγίας ή Κανονισμού.[198] Ο κανονισμός χαρακτηρίζεται από τη γενική του εφαρμογή (καθολική και απαρέγκλιτη) και είναι άμεσα εφαρμοστέος από την ημέρα θέσης του σε ισχύ, ενώ η Οδηγία

[197] Γεώργιος Γιαννόπουλος, "Η Εμπειρία Από Τη Συμμόρφωση Οργανισμών Και Επιχειρήσεων Με Τον Γενικό Κανονισμό Προστασίας Δεδομένων", σε *Δίκαιο Και Τεχνολογία*, 1η εκδ. (repr., Πειραιάς, Αθήνα: Εκδόσεις Σάκκουλα, 2019), 407-408.

[198] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 10.

δεσμεύει τα κράτη μέλη ως προς το επιδιωκόμενο αποτέλεσμα, αλλά αφήνει την επιλογή του τύπου και των μέσων στην αρμοδιότητα των εθνικών αρχών.[199]

Ένα από τα μεγαλύτερα παράπονα που διατυπώθηκαν για την Οδηγία 95/46/ΕΚ αφορούσε την έλλειψη εναρμόνισης που θα καθίσταντο δυνατή λόγω του χαρακτήρα της ως Οδηγία. Θεωρητικά, ο τύπος του νομικού μέσου που χρησιμοποιείται δεν είναι αφ' εαυτόν καθοριστικός σε σχέση με την εναρμόνιση. Για παράδειγμα, είναι δυνατό μια Οδηγία να αφήνει λίγα περιθώρια σε κάποιο κράτος-μέλος αναφορικά με την εφαρμογή της.[200] Ωστόσο, στην πράξη ένας Κανονισμός γενικότερα οδηγεί σε μεγαλύτερο βαθμό εναρμόνισης, εφόσον αμέσως καθίσταται τμήμα της εσωτερικής εθνικής νομικής τάξης, χωρίς να υφίσταται ανάγκη υιοθέτησής του μέσω ξεχωριστής εθνικής νομοθεσίας. Επίσης έχει νομική ισχύ ανεξάρτητη από το εθνικό δίκαιο και παρακάμπτει εθνικούς νόμους που έρχονται σε αντίθεση με αυτόν. Συνεπώς, ο ΓΚΠΔ είναι άμεσα εφαρμοστέος σε όλα τα κράτη μέλη της Ε.Ε. Αρχικά, τα κράτη μέλη δεν χρειάζεται να θεσπίσουν εθνική νομοθεσία ώστε να ενσωματώσουν τους νέους κανόνες στο εθνικό νομικό σύστημά τους. Αυτό σημαίνει ότι οι περισσότεροι εθνικοί νόμοι προστασίας δεδομένων είτε θα καταργηθούν ή θα περιοριστεί το πεδίο εφαρμογής τους (ώστε να διαρρυθμίσουν ζητήματα που ο ΓΚΠΔ δεν καλύπτει ή ρητά αφήνει προς ρύθμιση από το εθνικό δίκαιο). Παράλληλα, ο ΓΚΠΔ περιέχει πολλές «ρήτρες ευελιξίας» (**opening clauses**) που επιτρέπουν στα κράτη μέλη να εξειδικεύουν τους κανόνες του, συμπεριλαμβανομένων αυτών που αφορούν την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα και να προσδιορίζουν τις περιστάσεις ειδικών καταστάσεων επεξεργασίας, μεταξύ άλλων τον ακριβέστερο καθορισμό των προϋποθέσεων υπό τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σύννομη.[201][202] Πέραν της συνεκτικότητας της ρύθμισης της επεξεργασίας και προστασίας στα κράτη μέλη, η υιοθέτηση του μοντέλου του Κανονισμού αποσκοπούσε στην απλούστευση των διαδικασιών αλλά και στην μείωση του «κόστους συμμόρφωσης», ιδίως για εταιρείες που δραστηριοποιούνται σε περισσότερες χώρες της Ε.Ε.

Η επιλογή του Κανονισμού όμως συνάντησε εκτός από αποδοχή πολλές αντιδράσεις ή επιφυλάξεις. Συγκεκριμένα, προκάλεσε δικαιοπολιτικού τύπου ενστάσεις, καθώς ήδη η δεσμευτική ισχύς του ερχόταν σε αντίθεση με τις εθνικές αντιλήψεις και προτιμήσεις αναφορικά με το επίπεδο και τον επιβεβλημένο τρόπο προστασίας των προσωπικών δεδομένων. Στη Γερμανία το Ομοσπονδιακό Συμβούλιο (**Bundesrat**) αναφέρθηκε στον κίνδυνο του πλήρους αποκλεισμού των εθνικών ρυθμίσεων, ενώ στη Γαλλία η Αρχή για την Πληροφορική και τις Ελευθερίες (**CNIL**-Αρχή προστασίας προσωπικών δεδομένων), αντιτάχθηκε επίσης στην προοπτική της ρύθμισης μέσω ενός Κανονισμού. Σε θεωρητικό επίπεδο παρατηρήθηκαν επίσης επικρίσεις καθώς θεωρήθηκε ότι η ρύθμιση μέσω Κανονισμού βασίζεται σε μια αντίληψη «συγκεντρωτικής και μονοπωλιακής νομοθέτησης» και είναι αντίθετη στην επικουρικότητα, μια βασική συνιστώσα του ενωσιακού δικαίου, καθώς εισάγει δεσμευτικό δίκαιο σε ευρύ πεδίο τομέων και αφήνει στενά περιθώρια για μελλοντικές εναλλακτικές επιλογές προστασίας που θα

---

[199] Χριστιανός Β, Περάκης Ε. *Νομοθεσία Της Ευρωπαϊκής Ένωσης Μετά Τη Συνθήκη Της Λισαβόνας*. 1η εκδ. (Αθήνα, Νομική Βιβλιοθήκη 2010), 258.

[200] Παράδειγμα αποτελεί η Οδηγία για τα δικαιώματα των καταναλωτών (Οδηγία 2011/83/ΕΕ διαθέσιμη στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32011L0083&from=EN)

[201] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 11.

[202] Βλ. αιτ. σκέψεις 10,19 του Προοιμίου ΓΚΠΔ.

μπορούσαν να αναπτυχθούν σε διάφορες χώρες της Ε.Ε. Επίσης, οι αντιδράσεις αφορούσαν το γεγονός ότι η πρόταση του Κανονισμού έδινε στην Ευρωπαϊκή Επιτροπή ευρύτατη κανονιστική αρμοδιότητα, ώστε να προσδιορίζει το ειδικότερο περιεχόμενο των ρυθμίσεων και των υποχρεώσεων. Οι αντιδράσεις αυτές επικεντρώθηκαν στην αρμοδιότητα της Επιτροπής να υιοθετεί πράξεις κατ' εξουσιοδότηση (**delegated acts**) και εκτελεστικές πράξεις (**implementing acts**), μια αρμοδιότητα που θεωρείται κρίσιμη, ειδικά στις περιπτώσεις που το ρυθμιζόμενο και συνάμα διακυβευόμενο αγαθό είναι ένα θεμελιώδες δικαίωμα. Πέραν των επιφυλάξεων για την ενίσχυση της κανονιστικής εξουσίας της Επιτροπής, μια ουσιαστική επιφύλαξη αφορούσε την δυνατότητα της τελευταίας να επεμβαίνει ακόμα και σε μεμονωμένες περιπτώσεις, με αποτέλεσμα να καταστρατηγεί τον ρόλο των εθνικών ανεξάρτητων αρχών.[203]

Τον Ιανουάριο του 2012, η Ευρωπαϊκή Επιτροπή υπέβαλε την πρότασή της για την ριζική αναθεώρηση της Οδηγίας 95/46/ΕΚ, προκειμένου να ενισχυθούν η προστασία των δεδομένων στο διαδίκτυο και οι ηλεκτρονικές συναλλαγές. Ο Ευρωπαίος Επόπτης Προσωπικών Δεδομένων και η Ομάδα Εργασίας στη συνέχεια σχολίασαν την εν λόγω πρόταση, προχώρησαν σε αλλαγές και τροποποιήσεις και στις 12 Μαρτίου 2014 το Ευρωπαϊκό Κοινοβούλιο υιοθέτησε κατά συντριπτική πλειοψηφία την πρόταση του Κανονισμού. Ακολούθησαν διαβουλεύσεις και συστάσεις ανάμεσα στις αρμόδιες αρχές, το Ευρωπαϊκό Κοινοβούλιο, την Επιτροπή και το Συμβούλιο της Ε.Ε. και τελικά διαμορφώθηκε το τελικό κείμενο του Κανονισμού. Ο Κανονισμός τέθηκε σε ισχύ στις 24 Μαΐου 2016, όρισε όμως ότι η υποχρέωση συμμόρφωσης με τις διατάξεις του ξεκινά στις 25 Μαΐου 2018, παρέχοντας έτσι μια προθεσμία δύο ετών στους οργανισμούς που υπόκεινται στο πεδίο εφαρμογής του να προσαρμοστούν στην νέα πραγματικότητα.[204]

Εικόνα 1. Χρονοδιάγραμμα ΓΚΠΔ

[203] Λίλιαν Μήτρου, *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Σάκκουλα, 2017), 33-36.
[204] Ειρηνικός Πλατής, *Προσωπικά Δεδομένα-Προστασία GDPR*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Παπαδόπουλος, 2018), 32.

Ο Κανονισμός επιτυγχάνει τους στόχους του, από τη μια πλευρά, ενισχύοντας τις ήδη εδραιωμένες αρχές προστασίας δεδομένων οι οποίες ορίζονταν ήδη στην Οδηγία 95/46/ΕΚ, όπως η συγκατάθεση και ο περιορισμός του σκοπού, ενώ από την άλλη πλευρά, προβλέπει νέες αρχές όπως το δικαίωμα στη φορητότητα των δεδομένων, την υποχρέωση για διενέργεια εκτιμήσεων αντικτύπου σχετικών με την προστασία των δεδομένων και την προστασία της ιδιωτικότητας ήδη από το σχεδιασμό, ανάμεσα σε άλλες. Ήδη από το πρώτο σχέδιο του Κανονισμού το 2012, έχουν λάβει χώρα πολλές συζητήσεις στους νομικούς και ακαδημαϊκούς κύκλους σχετικά με τις θεμελιώδεις αλλαγές που εισάγει. Δύο αρχές του Κανονισμού, ωστόσο, τάραξαν τα νερά του νομικού, ακαδημαϊκού και επιχειρηματικού κόσμου : η επανεισαχθείσα έννοια της συγκατάθεσης μαζί με την ανάκλησή της αλλά και το νεοεισαχθέν δικαίωμα στη λήθη. Και οι δύο δημιούργησαν αντιπαραθέσεις χάρη στις δραστικές επιπτώσεις της επιβολής αυτών των νέων απαιτήσεων στην εποχή των μεγάλων δεδομένων, των αποκεντρωμένων υπηρεσιών και του Διαδικτύου των Πραγμάτων (**Internet of Things-IoT**).[205]

Παρά την ενωσιακή ταυτότητα του Κανονισμού, η εφαρμογή του δεν περιορίζεται εντός των ορίων της Ε.Ε. Δεδομένης της παγκόσμιας οικονομίας με τις πολυεθνικές ομάδες και τις διασυνοριακές μεταφορές δεδομένων, οι διεθνείς πτυχές έχουν ληφθεί υπόψιν κατά την δημιουργία του ΓΚΠΔ. Η εναρμονισμένη διεθνική εφαρμογή δύναται να παρέχει τα εχέγγυα της πλήρους ιδιωτικότητας των ατόμων και τις δίκαιες συνθήκες ανταγωνισμού στην ευρωπαϊκή εσωτερική ενιαία αγορά. Επίσης, αποτρέπεται το φαινόμενο της πρακτικής της αναζήτησης της ευνοϊκότερης δικαιοδοσίας («***forum shopping***») καθώς υπό το παλαιότερο καθεστώς τα διαφορετικά πρότυπα προστασίας δεδομένων εντός των κρατών μελών, έδιναν στις εταιρείες τη δυνατότητα να επιλέξουν την κύρια εγκατάστασή τους σύμφωνα με τα λιγότερο αυστηρά εθνικά πρότυπα προστασίας των δεδομένων. Επομένως, η ευρωπαϊκή νομοθεσία προδιαγράφει ένα αρκετά ευρύ εδαφικό πεδίο εφαρμογής. Υπό το πρίσμα της εδαφικής εφαρμογής, ο Κανονισμός δεν κάνει διάκριση ανάμεσα σε υπεύθυνο επεξεργασίας και εφαρμόζεται σε κάθε υπεύθυνο επεξεργασίας ή εκτελούντα που διενεργεί επεξεργασία δεδομένων στο πλαίσιο των δραστηριοτήτων του και έχει εγκατάσταση εντός της Ε.Ε. Επίσης, εφαρμόζεται σε κάθε υπεύθυνο επεξεργασίας ή εκτελούντα ανεξαρτήτως της έδρας ή του τόπου εγκατάστασης εφόσον οι δραστηριότητες επεξεργασίας σχετίζονται με την παροχή αγαθών ή υπηρεσιών σε πρόσωπα που είναι εγκατεστημένα στην Ε.Ε ή αφορούν την παρακολούθηση της συμπεριφοράς των εν λόγω προσώπων στο βαθμό που η συμπεριφορά τους λαμβάνει χώρα εντός της Ε.Ε. (άρθρο 3 παρ. 2 ΓΚΠΔ).[206]

Με τον τρόπο αυτό διευρύνθηκε σε μεγάλο βαθμό το πεδίο εφαρμογής της νομοθεσίας προστασίας προσωπικών δεδομένων σε ευρωπαϊκό επίπεδο, καθώς έπαψε να αφορά μόνο τους υπεύθυνους επεξεργασίας που έχουν την έδρα τους ή την κρίσιμη εγκατάστασή τους στο έδαφος της Ε.Ε.[207] Αποτελεί παράλληλα και σημαντική διαφορά σε σχέση με την Οδηγία 95/46/ΕΚ,

---

[205] Eugenia Politou et al., *Privacy and Data Protection Challenges in The Distributed Era*, 1st ed. (repr., Cham: Springer International Publishing AG, 2021), 14.

[206] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)*, 1st ed. (repr., Cham: Springer International Publishing, 2017), 22.

[207] Βλ. απόφαση 1/2019 της Εθνικής Επιτροπής Πληροφορικής και Ελευθεριών της Γαλλίας (CNIL), με βάση την οποία ερμηνεύεται στενά ο όρος «κύρια εγκατάσταση» (άρθρο 4 αρ. 16 ΓΚΠΔ), κρίνοντας ότι οι επιχειρήσεις, ο τόπος της κεντρικής διοίκησης των οποίων δε βρίσκεται στην Ε.Ε., λαμβάνουν τις αποφάσεις τους σχετικά με την επεξεργασία των δεδομένων στον εκτός της Ένωσης ευρισκόμενο τόπο της κεντρικής διοίκησής τους και επομένως

καθώς εκεί ο νομοθέτης προτίμησε το κριτήριο της «εδαφικότητας», το οποίο ορίζει ότι οι κανόνες που προβλέπονται από την Οδηγία, εφαρμόζονται σε υπευθύνους επεξεργασίας που είχαν την έδρα ή τουλάχιστον μια «σχετική/κρίσιμη» εγκατάστασή τους[208] στο έδαφος της Κοινότητας ή σε υπευθύνους επεξεργασίας που ακόμα και αν δεν συνέτρεχε η ύπαρξη έδρας ή «σχετικής» ή «κρίσιμης» εγκατάστασης, προσέφευγαν σε μέσα, είτε αυτοματοποιημένα είτε όχι, που βρίσκονταν στο έδαφος της Κοινότητας. Με την θέσπιση του Κανονισμού, ο ενωσιακός νομοθέτης υιοθέτησε το «δόγμα των επιπτώσεων» (***effects doctrine***), το οποίο ακολουθεί και ο εθνικός μας νομοθέτης, μέσω του άρθρου 3 του εφαρμοστικού νόμου 4624/2019, το οποίο προβλέπει ότι οι διατάξεις του εφαρμόζονται, πέραν της περίπτωσης κατά την οποία ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία επεξεργάζονται δεδομένα εντός της ελληνικής Επικράτειας (άρθρο 3 περ. α') ή στην περίπτωση κατά την οποία η επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία εντός της ελληνικής Επικράτειας (άρθρο 3 περ. β') και σε υπευθύνους επεξεργασίας, οι οποίοι αν και δεν έχουν εγκατάσταση σε κράτος μέλος της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Οικονομικού Χώρου, εντούτοις καταλαμβάνονται από το πεδίο εφαρμογής του Κανονισμού (άρθρο 3 περ. γ').

2.3.1 Το πεδίο εφαρμογής του δικαίου των προσωπικών δεδομένων

Οι προϋποθέσεις εφαρμογής του ΓΚΠΔ είναι αυστηρότερες σε σχέση με τις αντίστοιχες του άρθρου 9^{A} του Συντάγματος, πολύ δε περισσότερο από τα όρια του θεσμού του πληροφοριακού αυτοκαθορισμού ή -πολλώ μάλλον- της ιδιωτικής σφαίρας. Θα πρέπει να πρόκειται για επεξεργασία προσωπικών μόνο δεδομένων με σκοπό όχι αποκλειστικά οικιακό ή «προσωπικό» και ειδικά κατά τέτοιο τρόπο, ώστε αυτά να περιλαμβάνονται ή να πρόκειται να περιληφθούν σε «σύστημα αρχειοθέτησης». Επομένως, το πεδίο εφαρμογής του ΓΚΠΔ προσδιορίζεται διττώς, αρχικά καθ' ύλην (**ratione materiae**) και καθ' υποκείμενο (**ratione personae**). Σύμφωνα με το άρθρο 4 στοιχεία 1 και 2, στην έννοια των «δεδομένων προσωπικού χαρακτήρα» υπάγεται «κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο» (υποκείμενο των δεδομένων). Τέτοιες προσωπικές πληροφορίες μπορεί να είναι ο αριθμός δελτίου ταυτότητας, ο ΑΜΚΑ, οι εργασιακές συνθήκες ή οι ασχολίες[209], τα δεδομένα που αφορούν το εισόδημα ή τη φορολόγηση[210], οι λεπτομέρειες διαβατηρίου[211], τα δακτυλικά αποτυπώματα[212], τα έγγραφα εξετάσεων και τα

δεν θα πρέπει να απολαμβάνουν της πρόνοιας του άρθρου 56 του ΓΚΠΔ, περί καθορισμού μιας κύριας εποπτικής αρχής στη δικαιοδοσία της οποίας θα υπάγονται και η οποία μόνο αυτή θα μπορεί να επιβάλλει κυρώσεις, αλλά υπόκεινται στον έλεγχο και την επιβολή κυρώσεων από κάθε εποπτική αρχή κάθε κράτους μέλους στο οποίο αναπτύσσουν δραστηριότητα.

[208]Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN.

[209] Case C-101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* para. 37. ECLI:EU:C: 2003:596. https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:62001CJ0101.

[210] Joined Cases C- 465/ 00, C- 138/ 01 and C- 139/ 01, *Österreichischer Rundfunk*, para. 64; Case C- 73/ 07, *Satamedia*, para. 35; Case C- 201/ 14, *Smaranda Bara*, para. 29.

[211] Case C- 524/ 06, *Heinz Huber v Bundesrepublik Deutschland*, paras. 31 and 43. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62006CJ0524.

[212] Case C- 291/ 12, *Michael Schwarz κατά Stadt Bochum*, para. 27 (αναφέρεται επίσης στις παραγράφους 68 and 84 της απόφασης του Ευρωπαϊκού Δικαστηρίου των ανθρωπίνων δικαιωμάτων στην υπόθεση *Marper*). https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:62012CJ0291.

σχόλια των εξεταστών στα έγγραφα αυτά[213], ο τηλεφωνικός αριθμός, η ηλεκτρονική διεύθυνση, η διεύθυνση IP ενός Η/Υ[214], μηχανικές απεικονίσεις όπως φωτογραφίες, βίντεο[215], ακτινογραφίες, οι καταγεγραμμένες ομιλίες, τα δεδομένα γενετικής ταυτότητας κ.α.[216]

Ο ορισμός των «προσωπικών δεδομένων» έχει καθοριστική σημασία για να αποφασιστεί εάν εφαρμόζεται ή όχι ο ΓΚΠΔ. Τα προσωπικά δεδομένα (ή ισότιμοι όροι όπως «προσωπικές πληροφορίες»), αποτελούν όρο-κλειδί για την εφαρμογή του νόμου προσωπικών δεδομένων γενικότερα, καθώς αν τα δεδομένα που αποτελούν αντικείμενο επεξεργασίας δεν είναι προσωπικά δεδομένα, η επεξεργασία τους δεν υπόκειται σε τέτοιου είδους νομοθεσία. Τα δεδομένα που δεν είναι προσωπικά, συχνά αναφέρονται ως «ανώνυμα δεδομένα» και η διαδικασία μέσω της οποίας τα προσωπικά δεδομένα καθίστανται απρόσωπα τυπικά ονομάζεται «ανωνυμοποίηση». Για να αποκλεισθεί πάντως η υπαγωγή στο πεδίο εφαρμογής του νόμου για τα προσωπικά δεδομένα, θα πρέπει όχι απλώς να μην συνδέονται οι πληροφορίες προς κάποιο πρόσωπο, αλλά και να μην είναι δυνατή η σύνδεσή τους αυτή, δηλαδή να μην υφίσταται ούτε δυνατότητα (επαν)ονομαστικοποίησής τους. Κατά τούτο διαφέρουν τα ανώνυμα από τα ψευδώνυμα (ή ψευδωνυμοποιημένα) δεδομένα, κατά το ότι δεν φέρονται να συνδέονται προς κάποιο υπαρκτό πρόσωπο, αλλά μπορούν να συνδεθούν, εφόσον μπορεί να εξακριβωθεί ποιος υποδηλώνεται με το συγκεκριμένο ψευδώνυμο. Επομένως, τα ψευδώνυμα δεδομένα υπάγονται στο πεδίο εφαρμογής του νόμου, εφόσον υπάρχει δυνατότητα να εξακριβωθεί η αληθινή ταυτότητα του ψευδονοματιζόμενου υποκειμένου.[217] Ο προσωπικός χαρακτήρας των δεδομένων δεν ενυπάρχει ωστόσο πάντοτε εξ 'ορισμού σε αυτά τα ίδια, αλλά προστίθεται σε αυτά από στοιχεία επιπρόσθετα προς αυτά («συγκείμενα»), κατ'ουσίαν μέσω του σκοπού της επεξεργασίας, με χαρακτηριστικό παράδειγμα τα στοιχεία επικοινωνίας των αντικειμένων στο διαδίκτυο των πραγμάτων. Επίσης δεν μπορεί να αποκλειστεί η εκ των υστέρων επανονομαστικοποίηση των ανωνυμοποιημένων δεδομένων, εάν λάβουμε υπόψιν την ραγδαία ανάπτυξη των τεχνολογιών της πληροφορικής και των επικοινωνιών, καθώς μάλιστα τα πρωτογενώς συλλεγόμενα δεδομένα θα είναι αρχικά ανώνυμα. Πρόκειται για το ζήτημα της *πρόσθετης πληροφόρησης,* την οποία μπορεί να έχει κάποιος, ώστε να μπορέσει να συνδέσει τα εκ πρώτης όψεως ανώνυμα δεδομένα προς συγκεκριμένο πρόσωπο.[218]Παράδειγμα αποτελούν οι αναδιασταυρούμενες πολλαπλές φωτογραφήσεις των graffities επί φορτηγών αυτοκινήτων που θα μπορούσαν να οδηγήσουν σε εντοπισμό των περιθωριακών ζωγράφων.[219]

---

[213] Case C- 434/ 16, *Peter Nowak v Data Protection Commissioner.*, para. 36. ECLI identifier: ECLI:EU:C:2017:994. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62016CJ0434&from=en

[214] Joined Cases C-293/ 12 and C- 594/ 12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.*, para. 26; Case C- 582/ 14, *Patrick Breyer*, para. 49. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN, https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62014CJ0582&from=el

[215] Case C- 212/ 13, *František Ryneš v Úřad pro ochranu osobních údajů.*, para. 22; Case C- 345/ 17, *Sergejs Buivids*, para. 32. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62013CJ0212&from=EN , https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62017CJ0345&from=en.

[216] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 23.

[217] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 27.

[218] Ibid., 28.

[219] Ομάδα άρθρου 29, Γνώμη 4/2007 σχετικά με την έννοια του όρου «δεδομένα προσωπικού χαρακτήρα», σελ.21. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_el.pdf.

Παράδειγμα απρόσωπων δεδομένων αποτελούν τα «συγκεντρωτικά στατιστικά στοιχεία», τα οποία δεν υπάγονται στο πεδίο εφαρμογής του ΓΚΠΔ και μόνο με την επίκληση του γενικού δικαιώματος του «πληροφοριακού αυτοκαθορισμού», θα μπορούσε να προστατευθεί εκείνος από τον οποίο προέρχονται τα «ανωνυμοποιημένα δεδομένα». Επίσης τα δεδομένα αυτά υπάγονται στο προστατευτικό καθεστώς άλλων νομικών εργαλείων της Ε.Ε., όπως του Κανονισμού Ε.Ε 2018/1807 που αφορά το πλαίσιο ελεύθερης ροής των δεδομένων μη προσωπικού χαρακτήρα στην Ε.Ε και περιορίζει τη δυνατότητα των κρατών μελών να εισάγουν ή να διατηρούν συγκεκριμένες απαιτήσεις, οι οποίες δυσχεραίνουν την επεξεργασία δεδομένων εκτός συγκεκριμένης γεωγραφικής περιοχής ή επικράτειας στην Ένωση (άρθρο 4 παρ. 1).[220] Θα πρέπει επίσης να σημειωθεί ότι τα προσωπικά δεδομένα αποτελούν πληροφορίες που αναφέρονται σε φυσικά πρόσωπα που βρίσκονται εν ζωή, καθώς η προστασία των δεδομένων των φυσικών προσώπων που δεν βρίσκονται στη ζωή εκφεύγει των κανονιστικών αρμοδιοτήτων της ΑΠΔΠΧ.[221] Η εστίαση της νομοθεσίας προστασίας δεδομένων στα προσωπικά δεδομένα, αντανακλά τον βασικό της στόχο που είναι η διαφύλαξη της ιδιωτικότητας και των σχετικών συμφερόντων των φυσικών προσώπων, ειδικά εντός της πληροφοριακής σφαίρας. Στην Ευρώπη η διαφύλαξη τέτοιων συμφερόντων θεωρείται ζήτημα προστασίας των θεμελιωδών ανθρωπίνων δικαιωμάτων και ελευθεριών, όπως μπορεί κανείς να διαπιστώσει και μέσω της μελέτης των άρθρων 7 και 8 του Χάρτη Θεμελιωδών δικαιωμάτων, του άρθρου 8 της Ευρωπαϊκής Σύμβασης για τα δικαιώματα του ανθρώπου και της νομολογίας του ΔΕΕ που παραπέμπει στις εν λόγω διατάξεις. Επομένως, η νομοθεσία για την προστασία των προσωπικών δεδομένων, συμπεριλαμβανομένου του Κανονισμού, τείνει να υιοθετεί μια ευρεία έννοια των προσωπικών δεδομένων, ώστε να παρέχει ένα υψηλό επίπεδο προστασίας που υπερασπίζει παράλληλα τα θεμελιώδη δικαιώματα. Θα πρέπει να σημειωθεί ότι κατά την νομοθετική διαδικασία του ΓΚΠΔ, η Επιτροπή αρχικά πρότεινε την ενσωμάτωση του ορισμού των «προσωπικών δεδομένων» εντός του ορισμού του «υποκειμένου των δεδομένων (άρθρο 4 παρ. 1 πρότασης ΓΚΠΔ). Ωστόσο, η πρόταση αυτή δεν αντιμετωπίστηκε ευνοϊκά από το Κοινοβούλιο και το Συμβούλιο και τελικά απορρίφθηκε.[222]

Με βάση το έργο της Ομάδας του άρθρου 29[223], ο ορισμός των «προσωπικών δεδομένων» συχνά αναλύεται με βάση τα τέσσερα βασικά στοιχεία του: α) «κάθε πληροφορία», β) «που αφορά», γ) «ταυτοποιημένο ή ταυτοποιήσιμο», δ) «φυσικό πρόσωπο». Αναφορικά με τα πρώτα από αυτά τα στοιχεία, το ΔΕΕ στην υπόθεση *Nowak,* ανέφερε σχετικά: «η χρήση της έκφρασης κάθε πληροφορία στο ορισμό της έννοιας «προσωπικά δεδομένα»… αντανακλά τον στόχο της ευρωπαϊκής νομοθεσίας να αποδώσει ένα ευρύ πεδίο στην έννοια αυτή, που δεν περιορίζεται σε πληροφορίες που είναι ευαίσθητες ή ιδιωτικές, αλλά δυνητικά περιλαμβάνει κάθε είδους πληροφοριών, όχι μόνο αντικειμενική αλλά και υποκειμενική, υπό τη μορφή γνώμης ή εκτιμήσεως, υπό την προϋπόθεση ότι οι πληροφορίες «αφορούν» το ενδιαφερόμενο

---

[220] Κανονισμός (ΕΕ) 2018/1807 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Νοεμβρίου 2018, σχετικά με ένα πλαίσιο για την ελεύθερη ροή των δεδομένων μη προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση.
[221] Απόφαση 38/2010 ΑΠΔΠΧ, https://www.dpa.gr/sites/default/files/2019-10/38_2010_anonym_2.doc και αιτιολογική σκέψη 27 ΓΚΠΔ.
[222] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 106.
[223] Opinion 4/2007 on the concept of personal data, https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf

πρόσωπο».[224][225] Επιπροσθέτως, οι προτάσεις του Γενικού Εισαγγελέα Sharpston στην υπόθεση *YS,* κρίνονται ιδιαίτερα καθοδηγητικές στο πλαίσιο αυτό. Συγκεκριμένα αναφέρει: «Το ουσιαστικό περιεχόμενο των πληροφοριών αυτών δεν ασκεί επιρροή εφόσον αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί. Το εν λόγω περιεχόμενο συνδέεται με στοιχεία που αφορούν την ιδιωτική ζωή και, ενδεχομένως, την επαγγελματική ζωή του προσώπου (η οποία δύναται να περιλαμβάνει μια δημόσια πτυχή της ιδιωτικής ζωής). Το εν λόγω περιεχόμενο μπορεί να εμφανίζεται είτε σε γραπτή μορφή είτε ως περιεχόμενο, για παράδειγμα, ήχου ή εικόνας».

Αναφορικά με το δεύτερο στοιχείο του ορισμού («που αναφέρεται»), το ΔΕΕ και πάλι υιοθέτησε μια ευρεία προοπτική. Στην υπόθεση *Nowak,* δήλωσε ότι η προϋπόθεση αυτή πληρούται «όταν, λόγω του περιεχομένου της, του σκοπού της ή του αποτελέσματός της, η πληροφορία συνδέεται με συγκεκριμένο πρόσωπο».[226]Αυτό προσθέτει ένα ακόμα κενό στα λιγοστά όρια της έννοιας των προσωπικών δεδομένων, παρά το γεγονός ότι η αναφορά σε «συγκεκριμένο πρόσωπο» δείχνει να αποκλείει ότι τα δεδομένα που σχετίζονται με ένα σύνολο ανθρώπων, είναι προσωπικά δεδομένα, ανεξαρτήτως του μεγέθους αυτού του συνόλου. Παρά το γεγονός αυτό, σε μια προηγούμενη υπόθεση που αφορούσε την πρόσβαση στα δεδομένα του φακέλου για έναν αιτούντα άσυλο, το ΔΕΕ έκρινε ότι η νομική ανάλυση σε έναν τέτοιο φάκελο δεν συνιστά προσωπικό δεδομένο.[227] Το Δικαστήριο ακολούθησε τη γραμμή αυτή όχι μόνο σε σχέση με την ανάλυση που συμπεριλαμβάνει την αφαιρετική ερμηνεία του δικαίου, αλλά και σε σχέση με «τον νομικό χαρακτηρισμό των στοιχείων που συνδέονται με πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί (ή γεγονός που αφορά το εν λόγω πρόσωπο) και τις εκτιμήσεις ως προς το εφαρμοστέο δίκαιο».[228] Ενώ το Δικαστήριο δεν είχε καμία αμφιβολία ότι «ότι τα σχετικά με τον αιτούντα άδεια διαμονής στοιχεία που περιλαμβάνονται στο πρακτικό, όπως το όνομα, η ημερομηνία γεννήσεως, η υπηκοότητα, το φύλο, η εθνότητα, η θρησκεία και η γλώσσα, αποτελούν πληροφορίες που αναφέρονται στο εν λόγω φυσικό πρόσωπο, του οποίου η ταυτότητα μπορεί να εξακριβωθεί στο πρακτικό αυτό, ιδίως διά του ονόματός του, και ότι, ως εκ τούτου, οι πληροφορίες αυτές πρέπει να χαρακτηριστούν ως «δεδομένα προσωπικού χαρακτήρα»[229], ωστόσο έκρινε διαφορετικά σε σχέση με την νομική ανάλυση στο ίδιο πρακτικό: «όσον αφορά, αντιθέτως, τη νομική ανάλυση.. εφόσον δεν περιορίζεται σε μια αποκλειστικά αφηρημένη ερμηνεία της νομοθεσίας,… πληροφορία που αφορά την ερμηνεία και εφαρμογή, από την αρμόδια αρχή, της εν λόγω νομοθεσίας στην περίπτωση του αιτούντος, του οποίου η προσωπική κατάσταση διαπιστώνεται βάσει των σχετικών με το πρόσωπο αυτό δεδομένων προσωπικού χαρακτήρα που

---

[224] Joined Cases C-141/12 and C-372/12. Opinion of Advocate General Sharpston delivered on 12 December 2013. https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:62012CC0141&from=EN

[225] Case C- 434/ 16, *Peter Nowak v Data Protection Commissioner.*, para. 34. ECLI identifier: ECLI:EU:C:2017:994. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62016CJ0434&from=en

[226] Ibid., para. 35. Εδώ το ΔΕΕ φαίνεται να αποδέχεται την θέση που υιοθέτησε η ομάδα του άρθρου 29, WP29 2007, σελ. 9-12.

[227] Joined Cases C-141/12 and C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S,* par. 48, ECLI:EU:C:2014:208, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0141&from=en.

[228] Joined Cases C-141/ 12 and C-372/ 12, *YS* (Προτάσεις ΓΕ), para. 54. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62012CC0141&from=en.

[229] Joined Cases C-141/12 and C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S,* para 38, ECLI:EU:C:2014:208, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0141&from=en.

έχει στη διάθεσή της η εν λόγω αρμόδια αρχή».[230] Αυτή είναι μια σπάνια περίπτωση κατά την οποία το Δικαστήριο ερμήνευσε την έννοια των «προσωπικών δεδομένων» περιοριστικά. Παρ 'όλα αυτά, η τρέχουσα κατάσταση του αποτελέσματος στην υπόθεση *YS* κρίνεται αβέβαιη, αν λάβουμε υπόψιν την διευρυμένη γραμμή που ακολούθησε το ΔΕΕ στην υπόθεση *Nowak*.

Αναφορικά με το τρίτο στοιχείο της ταυτοποίησης, το Δικαστήριο εξέτασε την έννοια των προσωπικών δεδομένων περιοριστικά. Αυτό υποδεικνύει και η διατύπωση του άρθρου 4 (1) και η διατύπωση της αιτιολογικής σκέψης 26 και ειδικά οι αναφορές στον όρο «διαχωρισμό», στους όρους «άμεση» ή «έμμεση», και στην φράση «είτε από τον υπεύθυνο επεξεργασίας είτε από τρίτο πρόσωπο». Επομένως, τα δεδομένα δύνανται να είναι προσωπικά ακόμα και αν ο υπεύθυνος επεξεργασίας δεν μπορεί να τα συνδέσει σε συγκεκριμένο πρόσωπο χωρίς την βοήθεια από άλλες πηγές. Όπως ανέφερε το ΔΕΕ στην υπόθεση *Breyer*, «δεν απαιτείται όλες οι πληροφορίες που καθιστούν δυνατή την εξακρίβωση του εμπλεκόμενου προσώπου να βρίσκονται στη διάθεση ενός μόνον προσώπου».[231] Ωστόσο, όπως αναφέρει η αιτιολογική σκέψη 26, «θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν» κατά τη διαδικασία της εξακρίβωσης της ταυτότητας. Σύμφωνα με το ΔΕΕ, το κριτήριο αυτό δεν θα πληρούνταν, «εάν η εξακρίβωση της ταυτότητας του οικείου προσώπου απαγορεύεται από τον νόμο ή είναι ανέφικτη στην πράξη, παραδείγματος χάρη λόγω του ότι συνεπάγεται δυσανάλογη προσπάθεια από άποψη χρόνου, οικονομικών και ανθρώπινων πόρων, οπότε ο κίνδυνος εξακριβώσεως της ταυτότητας είναι στην πραγματικότητα αμελητέος».[232]

Τέλος, αναφορικά με το τέταρτο στοιχείο («φυσικό πρόσωπο»), υποδεικνύει ότι τα δεδομένα που αφορούν εταιρείες, εταιρικές σχέσεις και άλλα νομικά πρόσωπα δεν προστατεύονται από τον Κανονισμό. Το ΔΕΕ έχει αποφασίσει ωστόσο ότι «στο μέτρο που η επωνυμία του νομικού προσώπου προσδιορίζει ένα ή περισσότερα φυσικά πρόσωπα», τα νομικά πρόσωπα μπορούν να επικαλούνται την προστασία των δεδομένων που συνδέονται με αυτά, βάσει των άρθρων 7 και 8 του ΧΘΔ.[233] Επίσης, τα διοικητικά στελέχη αλλά και οι εκπρόσωποί τους, εντάσσονται στο προστατευτικό πεδίο των διατάξεων του ΓΚΠΔ και του εθνικού νόμου 4624/2019.[234] Σε μια υπόθεση που αφορούσε την πρόσβαση σε δεδομένα σχετικά με τις φορολογικές υποθέσεις μιας εταιρείας, το ΔΕΕ διατήρησε τον θεμελιώδη διαχωρισμό ανάμεσα σε δεδομένα που σχετίζονται με νομικό πρόσωπο και σε αυτά που σχετίζονται με φυσικά πρόσωπα.[235] Το ΔΕΕ επέμεινε στη θέση του ότι μόνο τα δεδομένα που σχετίζονται με φυσικά πρόσωπα απολαμβάνουν προστασία με βάση τον Κανονισμό αλλά και ως θεμελιώδες δικαίωμα του δικαίου της Ε.Ε.[236] Ακολούθησε επομένως την προσέγγιση του ΓΕ *Bobek*, ο οποίος δήλωσε: «Πράγματι, στην υπό κρίση υπόθεση, η πρόσβαση σε πληροφορίες ζητείται όσον αφορά τα φορολογικά στοιχεία ενός νομικού

---

[230] Ibid., para. 39-40.
[231] Case C-582/ 14, *Patrick Breyer κατά Bundesrepublik Deutschland.*, para. 43. ECLI:EU:C:2016:779. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0582&from=el .
[232] Ibid., para. 46.
[233] Joined Cases C-92/ 09 and 93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, para. 53. ECLI:EU:C:2010:662. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62009CJ0092&from=en. Βλ. επίσης υπόθεση C-419/14, *WebMindLicenses kft v Nemzeti Adó- és Vámhivatal Kiemelt Adó-és Vám Főigazgatóság,* παρ. 79. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62014CJ0419&from=en
[234] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1st ed. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 25.
[235] Case C-620/19, *Land Nordrhein-Westfalen v D.-H. T. as liquidator of J & S Service UG.* ECLI:EU:C: 2020:1011. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62019CJ0620&from=en.
[236] Ibid., para.46.

προσώπου. Τούτο προφανώς δεν αποτελεί απλή λεπτομέρεια: η εξισορρόπηση που προβλέπει το άρθρο 23, παράγραφος 1 δεν μπορεί να γίνεται με τον ίδιο τρόπο όσον αφορά τα δεδομένα που ανήκουν σε νομικό πρόσωπο, επί του οποίου ο κανονισμός 2016/679 δεν έχει καν εφαρμογή, και ως εκ τούτου δεν πραγματοποιούνται εκτιμήσεις εξισορροπητικού ή νομοθετικού χαρακτήρα όσον αφορά την εν λόγω κατάσταση. Το συμφέρον φυσικού προσώπου για την προστασία της ιδιωτικής και οικογενειακής ζωής του ουδόλως δύναται να συγκριθεί με το συμφέρον ενός νομικού προσώπου το οποίο, ενδεχομένως, να πρέπει να προστατεύσει δεδομένα τα οποία αφορούν, επί παραδείγματι, την επιχειρηματική του δραστηριότητα, την οργάνωση ή τη φορολογική του κατάσταση».[237] Από τη στιγμή που τα δεδομένα στην υπό κρίση υπόθεση ήταν δεδομένα που αφορούσαν φορολογικές υποθέσεις μιας εταιρείας και όχι φυσικού προσώπου, το ΔΕΕ έκρινε ότι ήταν αναρμόδιο να εξετάσει τα ζητήματα που παραπέμφθηκαν σε αυτό από το γερμανικό δικαστήριο – ζητήματα που προϋπέθεταν ότι ο ΓΚΠΔ είχε επιπτώσεις αναφορικά με τη χρήση των δεδομένων αυτών με βάση το γερμανικό δίκαιο.[238]

Επιπροσθέτως, γεννώνται σοβαρές αμφιβολίες γύρω από το εάν στο πεδίο εφαρμογής των ειδικών ρυθμίσεων που αφορούν τα προσωπικά δεδομένα θα μπορούσε να εμπέσει κάθε γενική αξιολογική κρίση, ακόμα και αν λόγω της γενικότητάς τους δεν πληροφορούν για κάτι συγκεκριμένο και αποτελούν έκφραση της προσωπικότητας του αξιολογούντος, δηλαδή αποτελούν δικά του προσωπικά δεδομένα τα οποία είναι ανεπίδεκτα πρόσβασης εκ μέρους του υποκειμένου το οποίο αφορούν. Σε τέτοιες περιπτώσεις ο θιγόμενος δύναται να αναζητήσει προστασία μέσω του δικαίου της προσωπικότητας, δυνάμει της διάταξης ΑΚ 57 σε συνδυασμό με την διάταξη ΠΚ 361 που αποδοκιμάζει την εξύβριση από την έννομη τάξη. Στις περιπτώσεις όμως της αξιολόγησης μπορεί να εμπεριέχονται και αξιολογικές κρίσεις. Υπό τέτοιες περιπτώσεις αξιολογήσεων, υπονοούνται και οι αντίστοιχες προς αυτές οντολογικές κρίσεις. Η διάκριση κρίνεται δύσκολη στην πράξη και η ασάφεια μπορεί να λυθεί με τελολογικά κριτήρια, δηλαδή εν αμφιβολία υπέρ του υποκειμένου. Για το λόγο αυτό γίνεται δεκτό ότι δεν συνιστούν δεδομένα οι τόσο γενικές αξιολογικές κρίσεις οι οποίες δεν μπορούν να υποδηλώνουν συγκεκριμένα πραγματικά περιστατικά.[239]

Στις περιπτώσεις όμως αξιολογήσεων υπηρεσιακής ή πιστοληπτικής ικανότητας (**listing ή scoring**), συντρέχουν κατηγοριοποιήσεις που συνιστούν υπαινιγμούς περί της συνδρομής συγκεκριμένων περιστατικών, τα οποία συνδέονται αντικειμενικώς πλέον με το υποκείμενο, την κοινωνική ή εργασιακή του θέση, ανεξαρτήτως αν είναι βάσιμα ή ακριβή ή όχι, αφού προορίζονται να συνοδεύουν εσαεί τον φάκελό του όπου αυτός εργάζεται. Επομένως, πρόκειται για πληροφορίες που οδηγούν σε αξιολόγηση του υποκειμένου από συγκεκριμένα πρόσωπα, δηλαδή αποτελούν ένα είδος «μετα-κρίσεων» με οντολογικό χαρακτήρα. Αποτελούν εν τέλει προσωπικά δεδομένα τόσο του κρινόμενου προσώπου, όσο και του κρίνοντος. Δεδομένα αποτελούν επίσης και οι ανακριβείς πληροφορίες, ανεξαρτήτως του δόλου του πληροφορούντος (υπευθύνου της επεξεργασίας, δεδομένου ότι και αυτές αφορούν και δύνανται να οδηγήσουν σε στιγματισμό του υποκειμένου. Ως δεδομένα νοούνται ακόμη και οι πληροφορίες που αναφέρονται χωρίς βεβαιότητα από την πλευρά του πληροφορούντος, οι ενδοιαστικές, ασαφείς, πιθανοτικές, όπως

---

[237] Case C-620/19, *Land Nordrhein-Westfalen v D.-H. T. as liquidator of J & S Service UG (AG Opinion), para 88.* ECLI:EU:C:2020:649. https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:62019CC0620&from=en.

[238] Christopher Kuner et al., "The EU General Data Protection Regulation: A Commentary/Update of Selected Articles", *SSRN Electronic Journal*, 2021, 25, doi:10.2139/ssrn.3839645.

[239] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 24.

υπόνοιες, ερωτήματα ή και απλοί συνειρμοί. Οι συνειρμοί αυτοί, αν και ολότελα απίθανοι, δεν θα πρέπει να λογίζονται ως νομικά κρίσιμοι και ως εκ τούτου δεν είναι αναγκαίο να υφίσταται βαθμός βεβαιότητας ή πιθανότητας μεγαλύτερος του 50%, εφόσον η σκιά τους συνεχίζει να ακολουθεί και να πλανάται πάνω από το υποκείμενο, αφού δύναται να επηρεάσουν τη συμπεριφορά άλλων ατόμων προς το υποκείμενο. Η ΑΠΔΠΧ, λόγω της πιθανότητας να αληθεύει η πληροφορία, αρκέστηκε στην ιατρική άποψη που δέχεται τον κίνδυνο της εξακριβωσιμότητας των γενετικών ασθενειών από την ανάλυση μιας αναφερόμενης στην καταγωγή περιοχής του ανθρώπινου DNA, παρά το γεγονός ότι η άποψη αυτή μειοψηφεί στην επιστημονική κοινότητα.[240][241]

Για να εμπίπτουν στο προστατευτικό πεδίο του Κανονισμού, τα δεδομένα θα πρέπει να είναι προσωπικά, δηλαδή να συνδέονται με ορισμένο πρόσωπο ή έστω εξατομικεύσιμο πρόσωπο, πρόσωπο δηλαδή του οποίου η ταυτότητα μπορεί να εξακριβωθεί σύμφωνα με το άρθρο 4 παρ. 2 του ΓΚΠΔ. Σύμφωνα με τα προαναφερθέντα λοιπόν, προσωπικά δεδομένα αποτελούν και οι μονές φωτογραφίες ή απεικονίσεις, ακόμα και στις περιπτώσεις που δεν συνοδεύονται από λεζάντα που υποδεικνύει το όνομα του εικονιζόμενου. Αυτό συμβαίνει αρχικά επειδή το πρόσωπο δεν θα πρέπει να ταυτίζεται προς το όνομά του, που αποτελεί έναν μόνο από τους συντελεστές της προσωπικότητας και της ταυτότητάς του, η οποία αντιθέτως «προσδιορίζεται από επί μέρους στοιχεία που χαρακτηρίζουν την υπόστασή του από βιολογική, οικονομική, ψυχολογική, πολιτιστική ή κοινωνική άποψη», σύμφωνα με το άρθρο 4, αρ.1,2 του ΓΚΠΔ. Επιπροσθέτως, το άτομο δεν θα πρέπει να ταυτίζεται και με συντελεστές της προσωπικότητας όπως π.χ. τα εξωτερικά του χαρακτηριστικά. Άλλωστε, είναι δυνατόν κάποιος μέσω ορισμένων χαρακτηριστικών να εξακριβώσει ή να πιθανολογήσει την ταυτότητά του. Ως αποτέλεσμα, γίνεται συχνά λόγος για ευρεία σύλληψη της έννοιας του προσώπου.[242] Για αυτόν ακριβώς το λόγο δεν κρίνεται ως πειστική και η άποψη[243] σύμφωνα με την οποία δεν αποτελεί επεξεργασία προσωπικών δεδομένων η πανοραμική παρακολούθηση μέσω βίντεο όπου παρά την μεγέθυνση της εικόνας δεν είναι ταυτοποιήσιμα τα πρόσωπα που βιντεοσκοπούνται.

2.3.2 Οι διακρίσεις των δεδομένων στον Γενικό Κανονισμό

Στο άρθρο 9 του Κανονισμού ορίζονται και αριθμούνται τα «δεδομένα ειδικών κατηγοριών» ως «τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση,… στην υγεία ή τη σεξουαλική ζωή και το γενετήσιο προσανατολισμό». Λαμβάνοντας μια επιπρόσθετη αξιολογική φόρτιση, τα δεδομένα αυτά χαρακτηρίζονται ως «ευαίσθητα».[244] Το άρθρο 9 προσθέτει νέες κατηγορίες δεδομένων που θεωρούνται «ευαίσθητα» και δεν προβλέπονταν από την Οδηγία 95/46/ΕΚ (π.χ. βιομετρικά και γενετικά δεδομένα)[245], νέες επιτρεπόμενες

---

[240] Ibid., 25-26.

[241] Ολ. ΑΠΔ 29/2012, 44/2009. Διαθέσιμες στις: http://www.dsanet.gr/Epikairothta/Nomologia/apd29_12.htm, https://www.dpa.gr/sites/default/files/2019-10/44_09anonym1.doc

[242] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 26.

[243] "Working Document on The Processing of Personal Data by Means of Video Surveillance", Article 29 Data Protection Working Party, *ec.Europa.eu*, 2002, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp67_en.pdf.

[244] Βλ. και αιτιολογικές σκέψεις 10,51,52,53,54,55,56 του ΓΚΠΔ, άρθρα 10,11,19,24,27,29 Οδηγίας (ΕΕ) 2016/680, άρθρα 2 (γ), 5, 9 και αιτιολογικές σκέψεις 25,35 Οδηγίας 2002/58/ΕΚ.

[245] Άρθρα 4(14) και 4(13) ΓΚΠΔ.

δραστηριότητες επεξεργασίας (δικαστήρια που εκτελούν τα δικαιοδοτικά τους καθήκοντα[246], εργασία και κοινωνική περίθαλψη[247] και δημόσιο συμφέρον στον τομέα της δημόσιας υγείας, όπως οι σοβαρές διασυνοριακές απειλές για την υγεία[248]), δικλείδες ασφαλείας στο πλαίσιο του ουσιαστικού δημοσίου συμφέροντος[249], και πολλαπλές «ρήτρες ευελιξίας» που επιτρέπουν την επεξεργασία όταν αυτό προβλέπεται από το ενωσιακό δίκαιο ή το δίκαιο του εκάστοτε κράτους μέλους.[250]

Η ιστορία της Ευρώπης στον 20ο αιώνα έχει δείξει ότι η κατάχρηση των ευαίσθητων δεδομένων μπορεί να διευκολύνει την παραβίαση των ανθρωπίνων δικαιωμάτων σε μεγάλη κλίμακα. Η κατάχρηση των ευαίσθητων δεδομένων μπορεί επίσης να προκαλέσει σοβαρές συνέπειες για τα υποκείμενα, όπως δυσμενείς διακρίσεις.[251] Όπως αναφέρει η αιτιολογική σκέψη 51 του ΓΚΠΔ, ένα υψηλό επίπεδο προστασίας θεωρείται απαραίτητο καθώς «είναι εκ φύσεως ιδιαίτερα ευαίσθητα σε σχέση με θεμελιώδη δικαιώματα και ελευθερίες και χρήζουν ειδικής προστασίας καθότι το πλαίσιο της επεξεργασίας τους θα μπορούσε να δημιουργήσει σημαντικούς κινδύνους για τα θεμελιώδη δικαιώματα και τις ελευθερίες». Επίσης, ως ratio της αυστηρότερης προστασίας τους προβάλλεται η προληπτική συμμόρφωση στην κατά ΧΘΔ 21 απαγόρευση των διακρίσεων, στις οποίες θα μπορούσε να οδηγήσει η λήψη υπόψιν των προαναφερθέντων κατηγοριών δεδομένων.[252]Κάποια «ευαίσθητα δεδομένα» (π.χ. κάποιοι τύποι βιομετρικών δεδομένων), «μεταβάλλουν αμετάκλητα την σχέση ανάμεσα στο σώμα και την ταυτότητα, καθώς καθιστούν τα χαρακτηριστικά του ανθρώπινου σώματος «μηχανικά αναγνώσιμα» και υποκείμενα σε περαιτέρω χρήση.. δια παντός».[253] Η επεξεργασία ευαίσθητων δεδομένων επίσης έχει τη δυνατότητα να επηρεάσει άλλα θεμελιώδη δικαιώματα[254] κατά τρόπο που αντίκειται προς το κοινό συμφέρον και φέρει μεγάλο βαθμό ρίσκου για τα υποκείμενα.[255]Παράλληλα, η επεξεργασία των ευαίσθητων δεδομένων μπορεί να έχει οφέλη (π.χ. η επεξεργασία των δεδομένων υγείας στην ιατρική έρευνα μπορεί να οδηγήσει στην δημιουργία νέων τύπων θεραπείας). Η ραγδαία ανάπτυξη της τεχνολογίας θέτει επομένως ρίσκα για την επεξεργασία των ευαίσθητων δεδομένων, αλλά δημιουργεί και νέες ευκαιρίες για τέτοιου είδους επεξεργασίες που ωφελούν τόσο τα άτομα όσο και την κοινωνία εν γένει.

Η παροχή ειδικής προστασίας, ωστόσο, για συγκεκριμένες κατηγορίες δεδομένων έχει δεχθεί έντονη κριτική τόσο de lege ferenda (για υπερβολές, ασάφειες), όσο και de lege lata (για αντίθεση

---

[246] Άρθρο 9 (2) στοιχ. στ', ΓΚΠΔ.
[247] Άρθρο 9 (2) στοιχ. η', ΓΚΠΔ.
[248] Άρθρο 9 (2) στοιχ. θ', ΓΚΠΔ.
[249] Άρθρο 9 (2) στοιχ. ζ', ΓΚΠΔ. (ρήτρα ευελιξίας για λήψη περαιτέρω μέτρων εφαρμογής ΓΚΠΔ).
[250] Άρθρο 9 (2)-(4), ΓΚΠΔ.
[251] Άρθρο 6(2) επικαιροποιημένη Σύμβαση 108.
[252] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 32.
[253] Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (OJ 2005 C 181 p.20). https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=OJ:C:2005:181:TOC.
[254] Για παράδειγμα, η επεξεργασία προσωπικών δεδομένων που αποκαλύπτουν τις θρησκευτικές πεποιθήσεις μπορούν να επηρεάσουν την ελευθερία στην θρησκεία (άρθρο 10 ΧΘΔ) και η επεξεργασία προσωπικών δεδομένων που αποκαλύπτουν τη συμμετοχή σε συνδικαλιστική οργάνωση μπορεί να επηρεάσει την ελευθερία της συμμετοχής σε τέτοιου είδους οργανώσεις (άρθρο 12 ΧΘΔ).
[255] Article 29 Working Party, 'Advice Paper on Special Categories of Data' (4 April 2011), available at https:// ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_ artwp_ mme_ le_ bail_ directive_ 9546ec_ annex1_ en.pdf.

στο ενωσιακό δίκαιο και το Σύνταγμα), με αποτέλεσμα η διάκριση ανάμεσα σε ευαίσθητα και απλά δεδομένα να έχει σχετική μόνο αξία. [256] Επομένως, έχει υποστηριχθεί ότι «ο διαχωρισμός σχετικά καθορισμένων υποσυνόλων προσωπικών δεδομένων τα οποία υπάγονται σε ειδική προστασία, οοδηγεί σε ρήξη με τον κατά τα άλλα κοινότοπο ισχυρισμό στον τομέα αυτό ότι η ευαισθησία των δεδομένων είναι κατ' ουσία εξαρτώμενη από το εκάστοτε πλαίσιο».[257] Επιπλέον προστατευτικά μέτρα για τα ευαίσθητα δεδομένα ελήφθησαν μέσω της Σύμβασης 108 το 1980, τα οποία άσκησαν μεγάλη επιρροή στα κράτη μέλη ώστε αυτά να θεσπίσουν παρόμοιες διατάξεις στους νόμους τους και να υιοθετήσουν το άρθρο 8 της Οδηγίας 95/46/ΕΚ.[258] Η προσέγγιση και οι κανόνες της Οδηγίας τελικά διατηρήθηκαν μέσω της διάταξης 9 του Κανονισμού, παρά την τροποποιημένη και ανανεωμένη μορφή τους. Ο Κανονισμός 45/2001 επίσης περιλάμβανε μια διάταξη που αφορούσε τα ευαίσθητα δεδομένα (άρθρο 10), η οποία ήταν παρόμοια με το άρθρο 8 της Οδηγίας. Ο Κανονισμός (ΕΕ) 2018/1725 επίσης περιέχει διατάξεις για τα ευαίσθητα δεδομένα, οι οποίες ακολουθούν αυτές του Κανονισμού και δομούνται με τον ίδιο τρόπο (αιτιολογική σκέψη 5 Κανονισμού 2018/1725). Η ομάδα εργασίας του άρθρου 29 επίσης δημοσίευσε μια σειρά γνωμών και άρθρων που αντιμετωπίζουν την επεξεργασία των ευαίσθητων δεδομένων. Σε αυτά συμπεριλαμβάνεται ένα άρθρο για τα γενικά ζητήματα των ευαίσθητων δεδομένων[259], καθώς και άρθρα που εξετάζουν συγκεκριμένα θέματα, όπως τα βιομετρικά δεδομένα[260] και τα γενετικά δεδομένα.[261]

2.3.2.1 Τα ευαίσθητα δεδομένα στον Γενικό Κανονισμό Προστασίας Δεδομένων

Η λίστα των ευαίσθητων δεδομένων που περιέχεται στο άρθρο 9 του ΓΚΠΔ είναι εξαντλητική, και εισάγει έναν «κλειστό αριθμό» ευαίσθητων δεδομένων, ώστε δεν υπάρχει δυνατότητα να προστεθούν περαιτέρω κατηγορίες σε αυτά. Η λίστα περιλαμβάνει όχι απλά σαφείς και άμεσες ενδείξεις των ευαίσθητων δεδομένων, αλλά επίσης πληροφορίες που μπορούν να χρησιμοποιηθούν ώστε να τα υποδείξουν εμμέσως, όπως αποδεικνύεται και από την χρήση της λέξης «αποκαλύπτουν» στο άρθρο 9 (1) του ΓΚΠΔ.[262] Για παράδειγμα, στην έκθεσή της για το

---

[256] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 370.

[257] Lee Andrew Bygrave, *Data Privacy Law*, 1st ed. (repr., New York: Oxford University Press, 2013), 165.

[258] Spiros Simitis, 'Revisiting Sensitive Data', Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) (Strasbourg, 24– 26 November 1999),1. https://rm.coe.int/09000016806845af.

[259] Article 29 Working Party, 'Advice Paper on Special Categories of Data' (4 April 2011), available at https:// ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_ artwp_ mme_ le_ bail_ directive_ 9546ec_ annex1_ en.pdf.

[260] Article 29 Working Party, 'Working Document on Biometrics' (WP 80, 1 August 2003), 'Opinion No. 7/ 2004 on the Inclusion of Biometric Elements in Residence Permits and Visas Taking Account of the Establishment of the European Information System on visas (VIS)' (WP 96, 11 August 2004), 'Opinion 3/ 2005 on Implementing Council Resolution (EC) No. 2252/ 2004 of 13 December 2004 on Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States' (WP 112, 30 September 2005), 'Opinion 3/ 2012 on Developments in Biometric Technologies' (WP 193, 27 April 2012). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec7

[261] Article 29 Working Party, 'Working Document on Genetic Data' (WP 91, 17 March 2004). https://www.statewatch.org/media/documents/news/2004/mar/wp91.pdf.

[262] Article 29 Working Party, 'Advice Paper on Special Categories of Data' (4 April 2011),6, available at https:// ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_ artwp_ mme_ le_ bail_ directive_ 9546ec_ annex1_ en.pdf., το οποίο κάνει αναφορά σε σχέση με το άρθρο 8 της Οδηγίας 95/46, υποδεικνύοντας ότι δεν καλύπτονται από τη διάταξη μόνο τα δεδομένα που από τη φύση τους περιέχουν ευαίσθητες πληροφορίες, αλλά και αυτά από τα οποία μπορούν να εξαχθούν ευαίσθητες πληροφορίες για ένα άτομο.

σκάνδαλο της Cambridge Analytica, η Υπηρεσία Επιτρόπου Πληροφοριών (ICO) του Η.Β. δήλωσε ότι η εταιρεία επεξεργάστηκε προσωπικά δεδομένα τα οποία ελήφθησαν από τους χρήστες του Facebook, ώστε να κάνει προβλέψεις για τις πολιτικές προτιμήσεις τους και απόψεις και ότι τέτοιου είδους δεδομένα θα πρέπει επομένως να θεωρηθούν ότι αποτελούν ευαίσθητα δεδομένα στο πλαίσιο εκείνο.[263] Επίσης δεν κρίνεται απαραίτητο να αποδεικνύεται ότι η επεξεργασία έχει ως αποτέλεσμα βλάβη ή ζημιά για να εφαρμοστούν οι προστατευτικές διατάξεις του άρθρου 9.[264] Ταυτοχρόνως, ο ευρύς ορισμός των ευαίσθητων δεδομένων μπορεί να δημιουργήσει ζητήματα ερμηνείας. Για παράδειγμα, οι φωτογραφίες ή οι πίνακες μπορεί να επιδεικνύουν την φυλετική καταγωγή του υποκειμένου (βάσει του χρώματος του δέρματός του) ή την θρησκεία του (εάν φορούν θρησκευτικό ένδυμα), αλλά η υπαγωγή όλων των εικόνων των ατόμων σε φωτογραφίες ή καλλιτεχνικές αναπαραστάσεις στο προστατευτικό πεδίο του άρθρου 9 θα ήταν υπερβολικό[265] και θα προσέκρουε με άλλα δικαιώματα. Η αιτιολογική σκέψη του Κανονισμού επομένως υποδεικνύει ότι οι φωτογραφίες θα πρέπει να θεωρούνται ευαίσθητα δεδομένα μόνο όταν εμπίπτουν στον ορισμό των βιομετρικών δεδομένων.Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων έχει δηλώσει ότι «το υλικό βιντεοσκόπησης που δείχνει το υποκείμενο των δεδομένων να φοράει γυαλιά ή να χρησιμοποιεί αναπηρικό αμαξίδιο δεν θεωρούνται ειδικές κατηγορίες προσωπικών δεδομένων».[266] Ωστόσο, εάν το υλικό βιντεοσκόπησης υφίσταται επεξεργασία ώστε να αφαιρεθούν τα ευαίσθητα δεδομένα από αυτό, τότε εφαρμόζεται το άρθρο 9.[267] Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων παρέχει τα παρακάτω παραδείγματα: «οι πολιτικές γνώμες θα μπορούσαν να συναχθούν από εικόνες που δείχνουν ταυτοποιήσιμα υποκείμενα δεδομένων να συμμετέχουν σε εκδηλώσεις, απεργίες κ.λπ. Αυτό εμπίπτει στο άρθρο 9, όπως και η περίπτωση του «νοσοκομείου που εγκαθιστά σύστημα βιντεοεπιτήρησης για να παρακολουθεί την κατάσταση της υγείας ενός ασθενούς θα μπορούσε να θεωρηθεί επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων».[268] Τέλος, έχει υποστηριχθεί στην ακαδημαϊκή βιβλιογραφία ότι οι πληροφορίες που αφορούν ένα άτομο και λαμβάνονται σε καθημερινές καταστάσεις, δεν θα πρέπει να θεωρείται ότι περιέχουν ευαίσθητα δεδομένα, εκτός αν υπάρχει πρόθεση να χρησιμοποιηθούν με βάση κάποιο από τα συγκεκριμένα στοιχεία ευαισθησίας που απαριθμούνται στον νόμο.[269]

Τρεις από τις κατηγορίες ευαίσθητων δεδομένων που αναγράφονται στο άρθρο 9 (1) του ΓΚΠΔ ορίζονται στο άρθρο 4 (γενετικά δεδομένα, βιομετρικά δεδομένα, δεδομένα που αφορούν την υγεία). Δεν παρέχονται ορισμοί στον Κανονισμό για τις άλλες πέντε κατηγορίες ευαίσθητων

---

[263] Information Commissioner's Office, 'Investigation into the use of Data Analytics in Political Campaigns (6 November 2018), 36. https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

[264] Βλ. υπόθεση ΔΕΕ Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk. παρ. 75. ECLI:EU:C:2003:294. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62000CJ0465&from=en

[265] Article 29 Working Party, 'Advice Paper on Special Categories of Data' (4 April 2011),8, available at https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_ artwp_ mme_ le_ bail_ directive_ 9546ec_ annex1_ en.pdf., που κάνει αναφορά στην ταξινόμηση των φωτογραφιών και των εικόνων ως ευαίσθητων υπό το άρθρο 8 της Οδηγίας ως «ιδιαίτερα προβληματική».

[266] European Data Protection Board, 'Guidelines 3/ 2019 on the processing of personal data through video devices (version for public consultation)' (10 July 2019),14.
https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

[267] Ibid.

[268] Ibid.

[269] Peter Gola et al., *Bundesdatenschutzgesetz*, 1st ed. (repr., München: C.H. Beck, 2010), 53.

δεδομένων που αναγράφονται στο άρθρο 9, δηλαδή τα δεδομένα που αποκαλύπτουν την τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση και τα δεδομένα που αφορούν την σεξουαλική ζωή των φυσικών προσώπων ή τον σεξουαλικό προσανατολισμό. Η κατηγορία της φυλετικής ή εθνοτικής καταγωγής προκύπτει από το άρθρο 21 (1) του ΧΘΔ, που με τη σειρά του πηγάζει από το άρθρο 19 ΣΛΕΕ και 14 της ΕΣΔΑ. Στην αιτιολογική σκέψη 51 του Κανονισμού, επίσης αναφέρεται ότι «η χρήση του όρου φυλετική καταγωγή στον παρόντα Κανονισμό δεν συνεπάγεται ότι η Ένωση αποδέχεται θεωρίες που υποστηρίζουν την ύπαρξη χωριστών ανθρώπινων φυλών». Τα πολιτικά φρονήματα βασίζονται στην ελευθερία της έκφρασης όπως αυτή προστατεύεται από το άρθρο 11 του ΧΘΔ και το άρθρο 10 της ΕΣΔΑ. Η έκφραση των πολιτικών φρονημάτων περιλαμβάνει τη συμμετοχή σε πολιτικό κόμμα, σε διαμαρτυρίες και στην έκφραση πολιτικών δηλώσεων ή την έκδοση πολιτικών κειμένων. Η ελευθερία της θρησκείας προστατεύεται, στη συνέχεια, μέσω του άρθρου 10 ΧΘΔ και του άρθρου 9 της ΕΣΔΑ, όπως προστατεύεται και η εξάλειψη διακρίσεων και η θρησκευτική ποικιλομορφία βάσει του άρθρου 21 (1) ΧΘΔ και 14 της ΕΣΔΑ. Αναφορικά με τη συμμετοχή σε συνδικαλιστικές οργανώσεις, το άρθρο 28 ΧΘΔ και 11 ΕΣΔΑ προστατεύουν τα συλλογικά δικαιώματα διαπραγμάτευσης. Εδώ εντάσσονται και τα δεδομένα που αφορούν την πιστοποίηση της ιδιότητας του μέλους στην εκάστοτε συνδικαλιστική οργάνωση. Αναφορικά με την σεξουαλική ζωή ή τον προσανατολισμό ενός φυσικού προσώπου, θα πρέπει να σημειωθεί ότι η προστασία τους αποτελεί μέρος της προστασίας της ιδιωτικής και οικογενειακής ζωής βάσει των άρθρων 7 ΧΘΔ και 8 της ΕΣΔΑ.

Η παράγραφος 1 του άρθρου 9 απαγορεύει την επεξεργασία των ευαίσθητων δεδομένων, ενώ η παράγραφος 2 θέτει εξαιρέσεις/νομικές βάσεις σε αυτήν την απαγόρευση σε ορισμένες περιπτώσεις. Η λίστα των εξαιρέσεων/νομικών βάσεων είναι εξαντλητική και όλες θα πρέπει να ερμηνεύονται περιοριστικά. Η επεξεργασία των ευαίσθητων δεδομένων πάντα απαιτεί συμμόρφωση με άλλες διατάξεις του Κανονισμού, πέρα από αυτές του άρθρου 9.[270] Αυτό εγείρει το ερώτημα εάν το άρθρο 9 αποτελεί μια ξεχωριστή νομική βάση για την επεξεργασία των δεδομένων ή αν απλά συμπληρώνει το άρθρο 6 του Κανονισμού και επομένως θα πρέπει επίσης να υποστηριχθεί από μια νομική βάση που προβλέπεται στο άρθρο 6. Η Επιτροπή έχει δηλώσει ότι η επεξεργασία των ευαίσθητων δεδομένων πάντα πρέπει να υποστηρίζεται από μια νομική βάση που προβλέπεται στο άρθρο 6 ΓΚΠΔ, σε συνδυασμό με την συμμόρφωση με τις περιπτώσεις που καλύπτονται στο άρθρο 9 (2) ΓΚΠΔ.[271] Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων επίσης έχει δηλώσει ότι «αν το σύστημα βιντεοεπιτήρησης χρησιμοποιείται για να γίνει επεξεργασία ειδικών κατηγοριών δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει να προσδιορίσει τόσο την εξαίρεση που αφορά την επεξεργασία ειδικών κατηγοριών δεδομένων σύμφωνα με το άρθρο 9 (π.χ. εξαίρεση από τον γενικό κανόνα ότι δεν θα πρέπει κανένας να επεξεργάζεται ειδικές κατηγορίες δεδομένων), όσο και τη νομική βάση σύμφωνα με το άρθρο 6».[272] Σε ένα αίτημα προδικαστικής παραπομπής που υπεβλήθη εκ μέρους του γαλλικού Συμβουλίου της Επικρατείας

---

[270] Βλ. αιτιολογική σκέψη 51 ΓΚΠΔ, που δηλώνει εν μέρει σε σχέση με την επεξεργασία των ευαίσθητων δεδομένων: «εκτός από τις ειδικές απαιτήσεις στις οποίες υπάγεται η εν λόγω επεξεργασία, θα πρέπει να εφαρμόζονται οι γενικές αρχές και οι λοιποί κανόνες του παρόντος κανονισμού, ιδίως σε ότι αφορά τους όρους νόμιμης επεξεργασίας.»

[271] Commission expert group on the Regulation (EU) 2016/ 679 and Directive (EU) 2016/ 680, 'Minutes of the Second Meeting', 2. https://ec.europa.eu/transparency/expert-groups-register/core/api/front/document/9290/download.

[272]Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών,19.https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_el.pdf.

και το οποίο αφορούσε την εφαρμογή του δικαιώματος της αφαίρεσης από τα αποτελέσματα αναζήτησης που παράγονται μέσω της λειτουργίας μιας μηχανής αναζήτησης, ο ΓΕ Szpunar πρότεινε ότι «ο φορέας εκμετάλλευσης μηχανής αναζήτησης υποχρεούται να κάνει δεκτές συστηματικά τις αιτήσεις διαγραφής συνδέσμων προς ιστοσελίδες οι οποίες περιέχουν ευαίσθητα δεδομένα».[273] Όταν ο υπεύθυνος επεξεργασίας έχει μια νομική βάση για την επεξεργασία, αυτή μπορεί να καλύπτει και τον εκτελούντα την επεξεργασία που ενεργεί εκ μέρους του, εφόσον οι σχετικές νομικές απαιτήσεις που προβλέπονται για τους εκτελούντες την επεξεργασία (όπως αυτές του άρθρου 28), πληρούνται. Οι εξαιρέσεις που προβλέπονται στο άρθρο 9 (2) θα πρέπει να ερμηνεύονται συσταλτικά με κριτήριο την πρόθεση του νομοθέτη να προστατεύσει τα υποκείμενα από πιθανές καταχρήσεις των ευαίσθητων δεδομένων τους, που μπορεί να έχουν αντίκτυπο στα ανθρώπινα δικαιώματά τους.

Επομένως, η επεξεργασία των ευαίσθητων δεδομένων επιτρέπεται αρχικά όταν το υποκείμενο δεδομένων έχει παράσχει τη ρητή συγκατάθεσή του (άρθρο 9 (2) α'). Εδώ καθιερώνεται ένα υψηλότερο όριο σε σχέση με το άρθρο 6 (1) α', που αναφέρει τη συγκατάθεση ως νομική βάση για την επεξεργασία δεδομένων χωρίς να απαιτεί αυτή να είναι ρητή. Ρητή συγκατάθεση απαιτείται και στην περίπτωση της μεταφοράς προσωπικών δεδομένων εκτός Ε.Ε.(άρθρο 49 (1) α'). Η έννοια της ρητής συγκατάθεσης υποδηλώνει ότι η συγκατάθεση δεν μπορεί να είναι σιωπηρή και απαιτεί μεγαλύτερο βαθμό ακρίβειας και σαφήνειας κατά την δήλωση της συγκατάθεσης, καθώς και ακριβή περιγραφή των σκοπών της επεξεργασίας. Η δεύτερη εξαίρεση[274] αφορά τις περιπτώσεις που η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας. Η εξαίρεση αυτή καλύπτει περιπτώσεις στις οποίες οι εργοδότες πρέπει να επεξεργαστούν τα ευαίσθητα δεδομένα των εργαζόμενων για να επιτευχθεί ο σκοπός της συμμόρφωσης με τις υποχρεώσεις τους που προκύπτουν από το εργατικό δίκαιο, το δίκαιο κοινωνικής ασφάλειας και το δίκαιο κοινωνικής προστασίας. Ένα παράδειγμα τέτοιας κατάστασης αποτελεί η ανάγκη ενός εργοδότη στη Γερμανία να συλλέξει δεδομένα που αφορούν την θρησκεία του εργαζόμενου για να αφαιρέσει τον εκκλησιαστικό φόρο. Μια άλλη περίπτωση είναι αυτή της συλλογής βιομετρικών δεδομένων για χρήση από συστήματα πρόσβασης στην εργασία. Η εξαίρεση αυτή περιορίζεται στην επεξεργασία δεδομένων από εργοδότες που ενεργούν ως υπεύθυνοι επεξεργασίας. Η τρίτη εξαίρεση[275] αφορά την επεξεργασία που είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου ή άλλου φυσικού προσώπου τα οποία άπτονται της ζωής και της σωματικής του ακεραιότητας εφόσον το υποκείμενο είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί και η επεξεργασία δεν προσκρούει στην υποθετική βούληση αυτού. Απαιτεί μια αξιολόγηση των συμφερόντων προστασίας δεδομένων των υποκειμένων, της ευαλωτότητάς τους και άλλων σημαντικών συμφερόντων και καλύπτει τόσο τα υποκείμενα των δεδομένων όσο και άλλα φυσικά πρόσωπα. Η αιτιολογική σκέψη 46 αναφέρει ότι αυτό περιλαμβάνει την επεξεργασία «που είναι απαραίτητη για να προστατευθεί ένα συμφέρον που είναι ουσιώδες για τη ζωή του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου».

---

[273]Υπόθεση C-136/17, *G.C., A.F., B.H., E.D* (Προτάσεις ΓΕ), 23. ECLI:EU:C: 2019:14. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62017CC0136&from=el.

[274] Άρθρο 9 (2) β'.

[275] Άρθρο 9 (2) γ'.

Στη αιτιολογική σκέψη 112 που αφορά τις μεταφορές δεδομένων, κάνει αναφορά σε «ζωτικά συμφέροντα» όπως η «σωματική ακεραιότητα ή η ζωή», υποδεικνύοντας ότι η περίπτωση θα πρέπει να συμπεριλαμβάνει την υγεία και την ασφάλεια των ατόμων. Μια περίπτωση που μπορεί να γίνει επίκληση της εξαίρεσης αφορά την ανάγκη επεξεργασίας ευαίσθητων δεδομένων για ιατρική περίθαλψη ή για επείγοντες περιπτώσεις ανθρωπιστικού χαρακτήρα. Για να χρήζει εφαρμογής, πρέπει το υποκείμενο να αδυνατεί να παράσχει τη συγκατάθεσή του είτε σωματικά είτε νομικά (π.χ. γιατί είναι ανήλικος, υπό πίεση, ή δεν αναμένεται από αυτό κατανόηση των επιπτώσεων της απόφασης).[276]

Περαιτέρω, η επεξεργασία μπορεί να διενεργείται, υπό καθεστώς κατάλληλων εγγυήσεων, στο πλαίσιο των νόμιμων δραστηριοτήτων μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο, και υπό την προϋπόθεση ότι η επεξεργασία αφορά αποκλειστικά τα μέλη του ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του.[277] Η εξαίρεση αυτή καλύπτει μη κερδοσκοπικούς οργανισμούς όπως πολιτικά κόμματα, ομάδες νέων, μη κερδοσκοπικά ιδρύματα και παρόμοιες ομάδες που έχουν «έναν πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο» και η αιτιολογική σκέψη 51 αναφέρει ότι πρέπει να έχουν ως σκοπό να επιτρέπεται η «άσκηση των θεμελιωδών ελευθεριών». Επομένως, δεν καλύπτεται από την εξαίρεση αυτή κάθε ΜΚΟ ή μη κερδοσκοπικός οργανισμός. Θα πρέπει ο οργανισμός να έχει οργανωθεί με μια μη κερδοσκοπική βάση, αν και αυτό δεν τον περιορίζει από το να συμμετέχει σε διοργανώσεις εράνου περιστασιακά. Η εξαίρεση εφαρμόζεται μόνο στην επεξεργασία δεδομένων που διενεργείται σε σύνδεση με τους σκοπούς της οργάνωσης (π.χ. η επεξεργασία δεδομένων από μια θρησκευτική οργάνωση για τον σκοπό της διαφήμισης δεν θα καλυπτόταν από την εξαίρεση). Επίσης, η εξαίρεση καλύπτει την εσωτερική επεξεργασία δεδομένων του οργανισμού και όχι την μεταφορά δεδομένων σε τρίτα μέρη. Οποιαδήποτε αποκάλυψη ευαίσθητων δεδομένων εκτός του οργανισμού σε άλλον υπεύθυνο επεξεργασίας απαιτεί τη συγκατάθεση του υποκειμένου των δεδομένων.[278]

Η επεξεργασία επίσης επιτρέπεται όταν αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν δημοσιοποιηθεί προδήλως από το υποκείμενο.[279] Στο πλαίσιο αυτό η «δημοσιοποίηση» θα πρέπει να διαμορφώνεται ώστε να συμπεριλαμβάνει την δημοσίευση των δεδομένων στα μέσα μαζικής ενημέρωσης, την διάθεσή τους στα μέσα κοινωνικής δικτύωσης ή παρόμοιες δράσεις. Απαιτείται μια θετική δράση του υποκειμένου των δεδομένων και να έχει συνειδητοποιήσει ότι αυτό θα είναι το αποτέλεσμα. Το ΕΣΠΔ έχει δηλώσει ότι «οι υπεύθυνοι επεξεργασίας που επεξεργάζονται τα δεδομένα αυτά στο πλαίσιο της βιντεοπαρακολούθησης δεν μπορούν να βασιστούν στο άρθρο 9 (2) ε', που επιτρέπει την επεξεργασία που σχετίζεται με τα προσωπικά δεδομένα που προδήλως δημοσιοποιούνται από το υποκείμενο των δεδομένων. Το απλό γεγονός ότι το υποκείμενο των δεδομένων εμπίπτει στην εμβέλεια της κάμερας δεν συνεπάγεται πρόθεσή του να δημοσιοποιήσει

[276] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 377.
[277] Άρθρο 9 (2) δ'.
[278] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 378.
[279] Άρθρο 9 (2) ε'.

ειδικές κατηγορίες δεδομένων που το αφορούν.[280] Η επεξεργασία δεδομένων δεν εμπίπτει στην εξαίρεση αυτήν εάν τα δεδομένα έχουν δημοσιοποιηθεί παρανόμως.

Η επεξεργασία επιτρέπεται επίσης όταν είναι απαραίτητη για τη δικαστική και εξωδικαστική θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων, κατόπιν στάθμισης συμφερόντων μεταξύ αφενός του δικαιώματος του υπευθύνου επεξεργασίας για δικαστική προστασία και αφετέρου του υποκειμένου των δεδομένων για προστασία των δεδομένων του. Η εξαίρεση αυτή είναι σχεδιασμένη για να προστατεύει το δικαίωμα σε αποτελεσματικό ένδικο βοήθημα και στο δικαίωμα σε δίκαιη δίκη όπως προβλέπεται στο άρθρο 47 ΧΘΔ και στο άρθρο 6 της ΕΣΔΑ και επομένως εφαρμόζεται σε δικαστικές διαδικασίες, είτε για ενάγοντες είτε για εναγόμενους, καθώς και ενώπιον διοικητικών και ιδιωτικών ακροαματικών διαδικασιών (όπως διαιτητικά δικαστήρια).[281] Η έννοια των νομικών αξιώσεων θα πρέπει να ερμηνευτεί διασταλτικά για να συμπεριλάβει αυτές που εμπίπτουν στο δημόσιο και ιδιωτικό δίκαιο, για την διεκδίκηση των οποίων οι υπεύθυνοι επεξεργασίας μπορούν να θεωρηθούν ότι έχουν έννομο συμφέρον υπό το πρίσμα της διάταξης 6 (1) στ' ΓΚΠΔ. Η εξαίρεση δεν εφαρμόζεται όταν τα ευαίσθητα δεδομένα υφίστανται επεξεργασία υπό την προσδοκία μιας ενδεχόμενης διαφοράς χωρίς να έχει ασκηθεί ή κατατεθεί επίσημη αξίωση ή χωρίς να υπάρχει ένδειξη ότι επίκειται η άσκηση επίσημης αξίωσης.[282]

Περαιτέρω, η επεξεργασία μπορεί να επιβάλλεται για λόγους ουσιαστικού δημοσίου συμφέροντος και διενεργείται επί τη βάσει κανόνα ευρωπαϊκής ή εθνικής προέλευσης, πάντα εντός των ορίων της αρχής της αναλογικότητας και υπό το φως του επιδιωκόμενου σκοπού. Αυτές οι δικλείδες ασφαλείας ανταποκρίνονται σε μια κριτική της ομάδας του άρθρου 29, που είχε συμπεράνει ότι το άρθρο 8 (4) της Οδηγίας 95/46/ΕΚ που αφορούσε με το ουσιαστικό δημόσιο συμφέρον, δεν ήταν διατυπωμένη με αρκετή ακρίβεια.[283] Η ανεύρεση του ουσιαστικού δημοσίου συμφέροντος απαιτεί την εξισορρόπηση ανάμεσα στο δημόσιο συμφέρον και στα ρίσκα για τα υποκείμενα των δεδομένων. Για να υφίσταται επεξεργασία ευαίσθητων δεδομένων το δημόσιο συμφέρον θα πρέπει να είναι «ουσιαστικό», σε αντίθεση με τις προϋποθέσεις για την επεξεργασία προσωπικών δεδομένων με βάση μια εργασία που εκτελείται για το δημόσιο συμφέρον υπό το πρίσμα της διάταξης 6 (1) ε', σύμφωνα με την οποία δεν υπάρχει απαίτηση το δημόσιο συμφέρον να είναι «ουσιαστικό». Η αιτιολογική σκέψη 46 αναφέρει ως παραδείγματα επεξεργασίας δεδομένων που υπηρετούν σημαντικούς λόγους δημοσίου συμφέροντος, τους ανθρωπιστικούς σκοπούς, συμπεριλαμβανομένης της παρακολούθησης επιδημιών ή την εξάπλωσή τους ή τις περιπτώσεις φυσικών ή ανθρωπογενών καταστροφών. Τα δεδομένα ψηφοφόρων μπορούν να τύχουν επεξεργασίας βάσει δημοσίου συμφέροντος όταν αυτό απαιτείται από τη λειτουργία του

[280]Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών, 20 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_el.pdf.

[281] Βλ. αιτιολογική σκέψη 52.

[282] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 379.

[283] Article 29 Working Party, 'Advice Paper on Special Categories of Data' (4 April 2011), p.11, available at https:// ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_ artwp_ mme_ le_ bail_ directive_ 9546ec_ annex1_ en.pdf.

δημοκρατικού συστήματος σε κάποιο κράτος μέλος, εφόσον έχουν εγκαθιδρυθεί οι απαραίτητες δικλείδες ασφαλείας.[284]

Η επεξεργασία επίσης επιτρέπεται όταν είναι απαραίτητη για σκοπούς υγειονομικής περίθαλψης (προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας για εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας, ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών) και λαμβάνει χώρα σύμφωνα με όσα ορίζονται στο ευρωπαϊκό ή εθνικό δίκαιο, ή σε σύμβαση με επαγγελματία του τομέα υγείας.[285] Η επεξεργασία δεδομένων για σκοπούς ιατρικής έρευνας δεν καλύπτεται από την διάταξη αυτή αλλά από τα άρθρα 9 (2) θ' και 9 (2) ι'. Η διάταξη αυτή καλύπτει όλους τους τύπους ιατρικής και κοινωνικής πρόνοιας, συμπεριλαμβανομένης της διάγνωσης, της περίθαλψης και της πρόληψης. Επιπροσθέτως, για να εφαρμοστεί η εξαίρεση, θα πρέπει να πληρούνται οι απαιτήσεις της διάταξης 9 (3), που απαιτεί τα ευαίσθητα δεδομένα να υφίστανται επεξεργασία «από ή υπό την ευθύνη επαγγελματία που υπόκειται στην υποχρέωση τήρησης του επαγγελματικού απορρήτου», όπως ιατρούς, οδοντιάτρους, ψυχολόγους, νοσοκομεία και ασφαλιστικές εταιρείες. Μπορεί επίσης να συμπεριλαμβάνεται η επεξεργασία δεδομένων που εκτελείται μέσω της χρήσης ιατρικών συσκευών ή εφαρμογών, εφόσον χρησιμοποιούνται υπό το καθεστώς ευθύνης κάποιου ανάλογου επαγγελματία. Πέρα από την ιατρική πρόνοια, η εξαίρεση καλύπτει σχετικούς σκοπούς, όπως την αξιολόγηση εάν ένας εργαζόμενος είναι ιατρικά ικανός για εργασία. Επίσης, καλύπτει την επεξεργασία ευαίσθητων δεδομένων υπό το πρίσμα της διαχείρισης υγειονομικών ή κοινωνικών συστημάτων. Η διάταξη επίσης καλύπτει υπηρεσίες που εκτελούνται βάσει σύμβασης, αν και δεν απαιτείται η ύπαρξη αυτής. Ο όρος «κοινωνική πρόνοια» θα πρέπει να ερμηνεύεται διασταλτικά για να συμπεριλαμβάνει όλα τα είδη συνδρομής που παρέχεται από τις αρχές κοινωνικής ασφάλειας.[286]

Όταν η επεξεργασία είναι απαραίτητη για την προάσπιση της δημόσιας υγείας, θα πρέπει να εξετάσουμε το άρθρο 9 (2) θ' για να κρίνουμε το θεμιτό της επεξεργασίας αυτής. Σύμφωνα με την αιτιολογική σκέψη 54, η «δημόσια υγεία» θα πρέπει να κατανοηθεί υπό το πρίσμα του Κανονισμού 1338/2008/ΕΚ (άρθρο 3 γ'), δηλαδή ως «το σύνολο των στοιχείων που συνδέονται με την υγεία, συγκεκριμένα η κατάσταση της υγείας, περιλαμβανομένων της νοσηρότητας και της αναπηρίας, οι καθοριστικοί παράγοντες που επιδρούν στην κατάσταση της υγείας, οι ανάγκες υγειονομικής περίθαλψης, οι πόροι που διατίθενται για την υγειονομική περίθαλψη, η παροχή υγειονομικής περίθαλψης και η πρόσβαση από όλους σε αυτήν , καθώς και οι δαπάνες και η χρηματοδότηση της υγειονομικής περίθαλψης και οι αιτίες θνησιμότητας». Το άρθρο 9 (2) ι' επίσης ορίζει ότι εφαρμόζεται συγκεκριμένα σε περιπτώσεις «σοβαρών διασυνοριακών απειλών, ή τη διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων». Απαγορεύεται επομένως η επεξεργασία των δεδομένων αυτών για άλλους σκοπούς από τρίτα μέρη. Υπό το φως της διάταξης 17(3) γ' του

[284] Βλ. αιτιολογική σκέψη 56.
[285] Άρθρο 9 (2) η'.
[286] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 380.

Κανονισμού, το δικαίωμα διαγραφής δεν εφαρμόζεται σε δεδομένα που υφίστανται επεξεργασία υπό την εξαίρεση αυτή.

Τέλος, η επεξεργασία διενεργείται όταν είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, εφόσον λαμβάνονται τεχνικά και οργανωτικά μέτρα για την ελαχιστοποίηση των δεδομένων (π.χ. ψευδωνυμοποίηση). Θα πρέπει να σημειωθεί ότι η νομοθετική ιστορία υποδεικνύει ότι μόνο οι σκοποί αρχειοθέτησης θα πρέπει να ανταποκρίνονται στην απαίτηση του «δημοσίου συμφέροντος» (οι επιστημονικοί, οι στατιστικοί και οι σκοποί ιστορικής έρευνας δεν απαιτείται να είναι προς το «δημόσιο συμφέρον»). Δευτερευόντως, οι σκοποί θα πρέπει να βασίζονται και να συμμορφώνονται με το ενωσιακό ή εθνικό δίκαιο, όπως οι νόμοι των κρατών μελών που αφορούν την αρχειοθέτηση ή την επιστημονική έρευνα. Η αναλογικότητα επίσης στο πλαίσιο αυτό απαιτεί η επεξεργασία των δεδομένων να διενεργείται όταν αυτό κρίνεται απολύτως απαραίτητο. Το γεγονός ότι ο νομοθέτης θεώρησε απαραίτητη την ρητή αναφορά στο σημείο αυτό, με στόχο τον σεβασμό στην ουσία του δικαιώματος στην προστασία των δεδομένων, δείχνει τη βαρύτητα που έχει ο σεβασμός αυτός στην προστασία των δικαιωμάτων των δεδομένων στο πλαίσιο της αρχειοθέτησης και της έρευνας. Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα πρέπει να σχεδιάζουν μέτρα ασφαλείας που βασίζονται στις αρχές της αναλογικότητας, της ελαχιστοποίησης των δεδομένων και της ασφάλειας αυτών. Αυτό μπορεί να συμπεριλαμβάνει μια σειρά μέτρων που βασίζονται στους σκοπούς της επεξεργασίας και στην ευαισθησία των δεδομένων, όπως η κρυπτογράφηση, η ελαχιστοποίηση των ευαίσθητων δεδομένων που υφίστανται επεξεργασία, η εκπαίδευση του προσωπικού που χειρίζεται τα προσωπικά δεδομένα και η θέση του προσωπικού αυτού υπό καθεστώς εμπιστευτικότητας.[287]

2.3.3 Οι «αρχές» της επεξεργασίας στον Γενικό Κανονισμό

Από τη στιγμή που ξεκινάει η επεξεργασία προσωπικών δεδομένων, αυτή διέπεται από ένα πλέγμα πρωτευόντων κανόνων, που είναι γνωστοί και ως «αρχές» και αποτελούν γενικές ρυθμίσεις που διέπουν οποιαδήποτε επεξεργασία, ανεξάρτητα από τον παράνομο ή μη χαρακτήρα της. Μέσω της καθιέρωσης των αρχών αυτών, ο νομοθέτης του δικαίου των προσωπικών δεδομένων δεν στοχεύει στην απαγόρευση της επεξεργασίας, αλλά στην υποβολή της σε εντονότερα διαφανείς και δημοσίου χαρακτήρα εγγυήσεις. Το άρθρο 5 του Κανονισμού ορίζει τις βασικές αρχές που αποτελούν τη βάση για την προστασία των προσωπικών δεδομένων. Αυτές είναι οι αρχές της νομιμότητας, της αντικειμενικότητας και της διαφάνειας (άρθρο 5 (1) α'), η αρχή του περιορισμού του σκοπού (άρθρο 5 (1) β'), η αρχή της ελαχιστοποίησης των δεδομένων (άρθρο 5 (1) γ'), η αρχή της ακριβείας (άρθρο 5 (1) δ'), η αρχή του περιορισμού της περιόδου αποθήκευσης (άρθρο 5 (1) ε'), η αρχή της ακεραιότητας και της εμπιστευτικότητας (άρθρο 5 (1) στ') και η αρχή της λογοδοσίας (άρθρο 5 (2)). Ορισμένες αρχές αναπτύσσονται περαιτέρω σε άλλα τμήματα του Κανονισμού. Αυτό συμβαίνει στην περίπτωση της αρχής της διαφάνειας έναντι του υποκειμένου που λαμβάνει την μορφή καθήκοντος ενημέρωσης των υποκειμένων (άρθρα 12-15), καθώς και στην περίπτωση της αρχής ακεραιότητας και της εμπιστευτικότητας (άρθρα 5 (1) στ' που εξειδικεύεται στα άρθρα 32 επ.), αλλά και στην περίπτωση της αρχής της λογοδοσίας (άρθρο 5

[287] Article 29 Working Party, 'Advice Paper on Special Categories of Data' (4 April 2011), p.11, available at https:// ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_ artwp_ mme_ le_ bail_ directive_ 9546ec_ annex1_ en.pdf.

(2)) που εξειδικεύεται μεταξύ άλλων στα άρθρα 24 και 25.[288]Ο ΓΚΠΔ εισάγει την καινοτομία της υποχρέωσης εξασφάλισης της «προστασίας των δεδομένων κατά το σχεδιασμό και εξ 'ορισμού (άρθρο 25), μέσω της επιβολής μέτρων εκ μέρους των οργανισμών, όπως της ελαχιστοποίησης των δεδομένων, ως συνήθη προσέγγιση στην συλλογή και χρήση των δεδομένων. Παρά την μακρά ιστορία της ενσωμάτωσης των αρχών της προστασίας κατά το σχεδιασμό σε συστήματα που χαρακτηρίζονται από ιδιωτικότητα, η ιδιωτικότητα κατά τον σχεδιασμό συνετέθη σε συγκεκριμένες εφαρμοστέες αρχές σχεδιασμού από την Cavoukian το 2011.[289] Συνήθως γίνεται δεκτό[290] ότι οι εν λόγω αρχές αποτελούν αναγκαστικό δίκαιο και διατυπώνονται ρητώς, ώστε να παράγουν αμέσως έννομα αποτελέσματα και η παραβίασή τους κατά την εκδίκαση των σχετικών υποθέσεων να στοιχειοθετεί τον πρώτο αναιρετικό λόγο του άρθρου 559 ΚΠολΔ από μόνη της και όχι σε συνδυασμό προς κάποιαν άλλη εφαρμοστέα διάταξη, όπως θα δεχόταν η σήμερα κρατούσα νομολογία[291], αν επρόκειτο απλώς για την προβλεπόμενη στο άρθρο 25 παρ. 1 γ' του Συντάγματος αρχή της αναλογικότητας.

2.3.3.1 Η αρχή της νομιμότητας, αντικειμενικότητας, και διαφάνειας της επεξεργασίας

Η πρώτη βασική αρχή που αφορά την προστασία των δεδομένων ορίζει ότι τα προσωπικά δεδομένα «υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο και σε σχέση το υποκείμενο των δεδομένων». Όπως ίσχυε και υπό το καθεστώς της Οδηγίας 95/46/ΕΚ, η απαίτηση ότι η επεξεργασία των δεδομένων θα πρέπει να είναι σύννομη ουσιαστικά σημαίνει ότι σέβεται όλες τις εφαρμοστέες νομικές απαιτήσεις (π.χ. την υποχρέωση τήρησης της επαγγελματικής εχεμύθειας, αν είναι εφαρμοστέα). Το άρθρο 6 (1) του ΓΚΠΔ ορίζει ότι η επεξεργασία είναι σύννομη μόνο εφόσον και στο βαθμό που μια τουλάχιστον από τις προϋποθέσεις που προβλέπει ισχύει. Με τον ίδιο τρόπο η Οδηγία (ΕΕ) 680/2016 στο άρθρο 8 ορίζει τις προϋποθέσεις που απαιτούνται για να είναι σύννομη η επεξεργασία στο πεδίο αυτό. Με βάση το σχόλιο του Οργανισμού Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και του Συμβουλίου της Ευρώπης, η αρχή της νομιμότητας της επεξεργασίας θα πρέπει να κατανοηθεί σε άμεση συνάρτηση με τις προϋποθέσεις για τους σύννομους περιορισμούς του δικαιώματος στην προστασία των δεδομένων ή του δικαιώματος για το δικαίωμα στην ιδιωτική ζωή, υπό το φως του άρθρου 52 (1) του ΧΘΔ και του άρθρου 8 (2) της ΕΣΔΑ. Παράλληλα, για να θεωρείται σύννομη, η επεξεργασία των προσωπικών δεδομένων θα πρέπει να είναι σύμφωνη με το νόμο, να επιδιώκει έναν νόμιμο σκοπό και να είναι απαραίτητη και ανάλογη σε μια δημοκρατική κοινωνία ώστε να επιτύχει το σκοπό αυτό. Η έννοια της θεμιτής επεξεργασίας υποδηλώνει ότι τα δεδομένα δεν έχουν αποκτηθεί ή υποστεί επεξεργασία μέσω αθέμιτων μέσων, μέσω παραπλάνησης ή χωρίς το υποκείμενο να έχει σχετική γνώση της επεξεργασίας.[292] Η αρχή της διαφάνειας αναλύεται στην αιτιολογική σκέψη 39, που αρχικά προσδιορίζει ότι «θα πρέπει να είναι σαφές για τα φυσικά

---

[288] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 380.

[289] Ann Cavoukian, "Privacy By Design The 7 Foundational Principles Implementation And Mapping Of Fair Information Practices", Privacy.Ucsc.Edu, 2011, https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf.

[290]Βλ. απόφαση ΑΠΔΠΧ 52/2003, 101. Διαθέσιμη σε : https://www.dpa.gr/sites/default/files/2020-12/DPA_ANNUAL_REPORT_2003.PDF.

[291] ΟλΑΠ 6/2009, ΝοΒ 2009, 568-569. ΑΠ 163/2007, 634/2007, 769/2007, 1255/2007.

[292] Σχετική με την αθέμιτη επεξεργασία είναι η υπόθεση του ΕΔΔΑ, *K.H. and Others v. Slovakia,* No. 32881/04, 28 April 2009.

πρόσωπα ότι δεδομένα προσωπικού χαρακτήρα που τα αφορούν συλλέγονται, χρησιμοποιούνται, λαμβάνονται υπόψη ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία». Επίσης γίνεται αναφορά στην ποιότητα των πληροφοριών που παρέχονται στα υποκείμενα, οι οποίες θα πρέπει να είναι εύκολα προσβάσιμες και κατανοητές. Για να επιτευχθεί αυτό, θα πρέπει να χρησιμοποιείται σαφής και απλή γλώσσα. Ειδικά στο πλαίσιο της δημόσιας διοίκησης, η αρχή της νομιμότητας νοείται και με τη θετική της σημασία: ό,τι δεν προβλέπεται ρητώς, απαγορεύεται. Αυτό ισχύει ειδικά στην περίπτωση που η επεξεργασία στηρίζεται σε κανονιστική διοικητική πράξη χωρίς την αναγκαία κατά Σ 43 παρ. 2, 5 σε συνδυασμό με 72 παρ. 1 ειδική νομοθετική εξουσιοδότηση. Θα πρέπει να σημειωθεί ότι η συγκατάθεση του υποκειμένου εν τοιαύτη περιπτώσει αποτελεί ρητώς προβλεπόμενο λόγο άρσεως του αδίκου χαρακτήρα της επεξεργασίας των δεδομένων.[293]

2.3.3.2 Η αρχή του περιορισμού του σκοπού της επεξεργασίας

Η αρχή του περιορισμού του σκοπού θεωρείται από καιρό ως ο ακρογωνιαίος λίθος της προστασίας των δεδομένων αλλά και ως προαπαιτούμενο για τις άλλες θεμελιώδεις απαιτήσεις. Η αρχή απαιτεί τα δεδομένα να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς (διάσταση του «καθορισμού του σκοπού»[294]) και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς (διάσταση της «συμβατής χρήσης»[295]). Οι σκοποί της επεξεργασίας προσωπικών δεδομένων θα πρέπει να καθορίζονται εξ 'αρχής , κατά τον χρόνο συλλογής των προσωπικών δεδομένων. Η επεξεργασία προσωπικών δεδομένων για ακαθόριστους ή απεριόριστους σκοπούς είναι αθέμιτη, εφόσον δεν επιτρέπει την οριοθέτηση της εμβέλειας της επεξεργασίας. Οι σκοποί της επεξεργασίας των δεδομένων θα πρέπει να είναι επίσης αδιαμφισβήτητοι και σαφώς διατυπωμένοι αντί να παραμένουν κρυφοί.[296] Τέλος, οι σκοποί θα πρέπει να είναι νόμιμοι, που σημαίνει ότι δεν συνεπάγονται δυσανάλογη παρέμβαση στα δικαιώματα, τις ελευθερίες και τα συμφέροντα που διακυβεύονται, στο όνομα των συμφερόντων του υπευθύνου της επεξεργασίας.[297][298] Σε κάθε περίπτωση, η επεξεργασία δεδομένων που υπηρετεί αθέμιτους σκοπούς δεν μπορεί να θεωρηθεί ότι βασίζεται σε νόμιμο σκοπό. Η δεύτερη διάσταση της αρχής του περιορισμού του σκοπού υποδηλώνει ότι ο υπεύθυνος επεξεργασίας μπορεί να εκτελεί επί των δεδομένων αυτών όλες τις δραστηριότητες που μπορούν να θεωρηθούν συμβατές με τους αρχικούς σκοπούς. Αυτή η έννοια της «συμβατής» επεξεργασίας των δεδομένων έχει εγείρει αρκετά ζητήματα κατά την πρακτική εφαρμογή της. Το άρθρο 6 παρ. 4 παρέχει μια σειρά κριτηρίων για να καθοριστεί εάν η επεξεργασία για σκοπό διαφορετικό από αυτόν για τον οποίο συνελέγησαν τα δεδομένα μπορεί να θεωρηθεί ως συμβατή με τον αρχικό αυτό σκοπό.[299] Θα πρέπει να καταγραφεί η πιθανή σύνδεση ανάμεσα στους δύο σκοπούς, το πλαίσιο εντός του

---

[293] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 110.
[294]Article 29 Working Party, "Opinion 03/2013 On Purpose Limitation", Ec.Europa.Eu, 2013, 11-12. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[295] Ibid.,12-13.
[296] Ibid., 39.
[297] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 380.
[298] Βλ. και Council of Europe, 'Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data' (10 October 2018), 8 , available at https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.
[299] Η λίστα βασίζεται σε αυτήν που διαμορφώθηκε από την ομάδα του άρθρου 29, "Opinion 03/2013 On Purpose Limitation", 40.

οποίου τα προσωπικά δεδομένα έχουν συλλεχθεί (ειδικά σε συνάρτηση με τη σχέση ανάμεσα στα υποκείμενα των δεδομένων και τον υπεύθυνο επεξεργασίας), η φύση των προσωπικών δεδομένων (απλά ή ευαίσθητα), οι πιθανές συνέπειες της περαιτέρω σκοπούμενης επεξεργασίας για τα υποκείμενα των δεδομένων, και η ύπαρξη κατάλληλων μέτρων ασφαλείας.[300]

Τέλος, ορισμένες επαναχρήσεις των δεδομένων θεωρούνται a priori συμβατές εφόσον πληρούνται ορισμένες προϋποθέσεις[301], όπως επιτρεπόταν και υπό το προηγούμενο καθεστώς της Οδηγίας 95/46/ΕΚ. Αυτές αφορούν «την περαιτέρω επεξεργασία των δεδομένων για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς».[302] Αυτές οι κατηγορίες για περαιτέρω επεξεργασία είναι ελαφρώς πιο περιοριστικές σε σχέση με πριν εφόσον ο «ιστορικός σκοπός» έχει δώσει τη θέση του στον «σκοπό αρχειοθέτησης» - και μόνο για λόγους δημοσίου συμφέροντος- και για σκοπούς ιστορικής έρευνας. Ο «επιστημονικός σκοπός» έχει επίσης απομειωθεί σε «σκοπούς επιστημονικής έρευνας». Το Συμβούλιο της Ευρώπης, μέσω της πρότασής του, έχει επιχειρήσει να διασαφήσει τους όρους αυτούς, δηλώνοντας ότι η επεξεργασία των δεδομένων για σκοπούς επιστημονικής έρευνας στοχεύει στην παροχή πληροφοριών στους ερευνητές, που συμβάλλουν στην κατανόηση των φαινομένων σε διάφορα επιστημονικά πεδία (επιδημιολογία, ψυχολογία, οικονομικά, κοινωνιολογία, γλωσσολογία, πολιτικές επιστήμες, εγκληματολογία κ.α.), με απώτερο στόχο την εγκαθίδρυση σταθερών αρχών, νόμων συμπεριφοράς ή μοτίβων αιτιότητας που υπερβαίνουν τα άτομα στα οποία εφαρμόζονται.[303] Η κατηγορία της επεξεργασίας των δεδομένων για στατιστικούς σκοπούς παραμένει ως έχει. Ο «στατιστικός σκοπός» αναφέρεται στην εκπόνηση στατιστικών ερευνών ή στην παραγωγή στατιστικών, συγκεντρωτικών αποτελεσμάτων.[304] Τα στατιστικά στοχεύουν στην ανάλυση και τον χαρακτηρισμό των μαζικών ή συλλογικών φαινομένων σε έναν συγκεκριμένο υπό εξέταση πληθυσμό.[305]

2.3.3.3 Η αρχή της ελαχιστοποίησης των δεδομένων

Όπως ίσχυε και υπό το νομοθετικό καθεστώς της Οδηγίας 95/46/ΕΚ, τα προσωπικά δεδομένα που υποβάλλονται σε επεξεργασία πρέπει να είναι επαρκή, σχετικά και περιορισμένα σε αυτό που απαιτείται σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία. Ωστόσο, υπό τον Κανονισμό, τα προσωπικά δεδομένα πρέπει να «περιορίζονται στο αναγκαίο» και όχι να μην είναι «υπερβολικά», όπως ίσχυε στην Οδηγία (άρθρο 6 παρ. 1 γ'). Η Οδηγία 680/2016 έχει ωστόσο διατηρήσει τη διατύπωση αυτή και στο άρθρο 4 παρ. 1 γ' αναφέρει ότι τα δεδομένα δεν πρέπει να είναι «υπερβολικά». Η διαφορά αυτή ως προς τη διατύπωση, ωστόσο, δεν επιφέρει ουσιαστικές συνέπειες ως προς την εμβέλεια της εφαρμογής της αρχής της ελαχιστοποίησης των δεδομένων. Στην αιτιολογική σκέψη 39, ο Κανονισμός προσδιορίζει ότι απαιτείται, συγκεκριμένα,

---

[300] Άρθρο 6 παρ. 4 και αιτ. σκέψη 50 ΓΚΠΔ.
[301] Οι προϋποθέσεις αυτές αναπτύσσονται στο άρθρο 89 παρ. 1 ΓΚΠΔ.
[302] Ibid., άρθρο 5 παρ. 1 β' ΓΚΠΔ.
[303] Council of Europe, 'Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data' (10 October 2018), 3 , available at https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.
[304] Committee of Ministers of the Council of Europe, 'Recommendation Concerning the Protection of Personal Data Collected and Processed for Statistical Purposes' (Rec (1997)18, 30 September 1997), Appendix, σημείο 1.
[305] Council of Europe, 'Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data' (10 October 2018), 8 , available at https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

τα προσωπικά δεδομένα να «υποβάλλονται σε επεξεργασία μόνο εάν ο σκοπός της επεξεργασίας δεν μπορεί να επιτευχθεί με άλλα μέσα». Επιπροσθέτως, η απαίτηση αυτή αναφέρεται όχι μόνο στην ποσότητα, αλλά και στην ποιότητα των δεδομένων. Καθίσταται επομένως σαφές ότι κάποιος δεν μπορεί να επεξεργαστεί έναν μεγάλο όγκο προσωπικών δεδομένων (π.χ. η περίπτωση που ζητείται από τον εργαζόμενο να παραδώσει τον συνολικό ιατρικό του φάκελο για να αξιολογηθεί η ικανότητά του για εργασία). Αλλά είναι δυνατόν κάποιος να επεξεργαστεί ένα μοναδικό δεδομένο ακόμα και αν αυτό συνεπάγεται μια δυσανάλογη παρέμβαση στα δικαιώματα και τα συμφέροντα του υποκειμένου (π.χ. στην περίπτωση της συλλογής πληροφοριών αναφορικά με την κατανάλωση ναρκωτικών ουσιών από αιτούντα εργασία).[306] Το κριτήριο του «περιορισμού στο αναγκαίο» απαιτεί επίσης «την διασφάλιση ότι η περίοδος για την οποία τα δεδομένα αποθηκεύονται είναι περιορισμένη στο ελάχιστο». Για να κρίνουμε επομένως εάν μια επεξεργασία είναι συμβατή με την αρχή της ελαχιστοποίησης των δεδομένων, θα πρέπει να ακολουθείται η «δοκιμασία των δύο σταδίων» ***(«two steps test» / «epreuve de deux etapes»***), κατά την οποία ελέγχεται αρχικά η συνάφεια και η καταλληλόλητα των προσωπικών δεδομένων με τον επιδιωκόμενο σκοπό και αν αυτή η συνθήκη ικανοποιείται, προχωράμε ακολούθως στον έλεγχο του ποσοτικού κριτηρίου για να εξασφαλίσουμε ότι η επεξεργασία είναι σύμφωνη με την αρχή της αναλογικότητας.[307]

2.3.3.4 Η αρχή της ακρίβειας

Η απαίτηση σύμφωνα με την οποία τα δεδομένα πρέπει να είναι ακριβή και όπου κρίνεται απαραίτητο να διατηρούνται ενημερωμένα, ήταν ήδη παρούσα στην Οδηγία 95/46 και στη Σύμβαση 108 και έχει διατηρηθεί στον ΓΚΠΔ. Στο ελληνικό δίκαιο η αρχή προκύπτει από το άρθρο 4 παρ. 1 γ' του νόμου 2472/1997, σύμφωνα με το οποίο τα προσωπικά δεδομένα, για να τύχουν νόμιμης επεξεργασίας, πρέπει «να είναι ακριβή και εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση». Όλα τα ανακριβή δεδομένα θα πρέπει να διορθώνονται ή να διαγράφονται. Ο υπεύθυνος επεξεργασίας θα πρέπει να λαμβάνει όλα τα απαραίτητα μέτρα για να διασφαλίζει ότι τηρείται η αρχή της ακρίβειας. Ο ΓΚΔΠ διευκρινίζει ότι αυτή η παρέμβαση θα πρέπει να διενεργείται χωρίς καθυστέρηση. Περαιτέρω στο άρθρο 7 παρ. 2 της Οδηγίας (ΕΕ) 680/2016, γίνεται αναφορά στον τομέα της αστυνομικής δραστηριότητας: «Σε κάθε διαβίβαση δεδομένων προσωπικού χαρακτήρα επισυνάπτονται, στο μέτρο του δυνατού, οι αναγκαίες πληροφορίες που επιτρέπουν στην αρμόδια αρχή που παραλαμβάνει τα δεδομένα να αξιολογήσει την ακρίβεια, την πληρότητα, την αξιοπιστία των δεδομένων προσωπικού χαρακτήρα, καθώς και τον βαθμό επικαιροποίησής τους». Η ακρίβεια και η ενημέρωση των στοιχείων βαρύνει, κατ' αρχήν[308], τον υπεύθυνο της επεξεργασίας. Όταν η Τειρεσίας Α.Ε επεξεργάζεται δεδομένα οικονομικής φύσεως, η διαγραφή των δυσμενών δεδομένων, που συνιστά προϋπόθεση για την τήρηση της ακρίβειας του σχετικού αρχείου, αποτελεί υποχρέωση του υπευθύνου επεξεργασίας όταν τα γεγονότα που

---

[306] Ibid., 9, αναφορικά με τον προσδιορισμό της έννοιας «υπερβολικά» δεδομένα.

[307] Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, *Προσωπικά Δεδομένα*, 1η εκδ. (Θεσσαλονίκη: Νομική Βιβλιοθήκη, 2016), 73.

[308] Βλ. υπ'αριθ. 109/31.3.2009 απόφαση της ΑΠΔΠΧ. Ο κανόνας ωστόσο δεν είναι ανεξαίρετος, όπως στις περιπτώσεις που ο υπεύθυνος επεξεργασίας δεν έχει πρόσβαση σε νεότερα στοιχεία, τα οποία τροποποιούν δεδομένα του αρχείου που τηρεί.

δικαιολογούν τη διαγραφή αποκτούν δημοσιότητα (π.χ. άρση προσημειώσεων/υποθηκών).[309] Εάν τα δικαιολογητικά της διαγραφής δεν αποκτούν δημοσιότητα, τα σχετικά στοιχεία προσκομίζονται από τα ενδιαφερόμενα υποκείμενα.[310]

2.3.3.5 Η αρχή του περιορισμού της περιόδου αποθήκευσης

Η διάταξη[311] που αφορά την αρχή της καθορισμένης χρονικής διάρκειας διατήρησης των προσωπικών δεδομένων δεν διαφοροποιείται από την αντίστοιχη διάταξη της Οδηγίας 95/46 που απαγορεύει την διατήρηση των προσωπικών δεδομένων σε μορφή που επιτρέπει την αναγνώριση των υποκειμένων των δεδομένων για διάστημα μεγαλύτερο από αυτό που απαιτείται για να επιτευχθούν οι σκοποί της επεξεργασίας (άρθρο 6 παρ. 1 ε'). Ωστόσο, υπάρχει ένα νέο στοιχείο στην αιτιολογική σκέψη 39 του Κανονισμού, που καλεί τους υπευθύνους επεξεργασίας να ορίσουν προθεσμίες για την διαγραφή ή την περιοδική επανεξέταση των δεδομένων. Κατά αυτόν τον τρόπο θα διασφαλιστεί ότι τα προσωπικά δεδομένα δεν διατηρούνται για περισσότερο χρόνο από όσο απαιτείται. Το άρθρο 4 παρ. 1 ε' της Οδηγίας 680/2016 προβλέπει την ίδια απαγόρευση και το άρθρο 5 επιβάλλει την θέσπιση προθεσμιών για την διαγραφή των δεδομένων ή για την περιοδική επανεξέταση της ανάγκης αποθήκευσης των δεδομένων. Το κείμενο απαιτεί την υιοθέτηση διαδικαστικών μέτρων ώστε να διασφαλιστεί ότι τηρούνται οι χρονικές προθεσμίες. Στο σημείο αυτό θα πρέπει επίσης να ληφθούν υπόψη τα άρθρα 25 του Κανονισμού και 20 της Οδηγίας 680/2016, εφόσον επιβάλλουν την λήψη και εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων από τον υπεύθυνο επεξεργασίας, ώστε να διασφαλιστεί ότι, εξ' ορισμού, η νόμιμη περίοδος αποθήκευσης των προσωπικών δεδομένων τηρείται. Επιπροσθέτως, η αρχή του περιορισμού της περιόδου αποθήκευσης επιτρέπει την αποθήκευση προσωπικών δεδομένων για μεγαλύτερες χρονικές περιόδους, εάν πρόκειται για την επίτευξη σκοπών αρχειοθέτησης προς το δημόσιο συμφέρον ή την επίτευξη επιστημονικών ή ιστορικών σκοπών έρευνας ή στατιστικών σκοπών και υπόκειται στην εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων ώστε να διασφαλιστούν τα δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων.[312]

2.3.3.6 Η αρχή της εμπιστευτικότητας και της ακεραιότητας

Υπό τον τίτλο «ακεραιότητα και εμπιστευτικότητα» ανευρίσκει κανείς την κρίσιμη απαίτηση ασφαλείας που τώρα συμπεριλαμβάνεται στη λίστα των θεμελιωδών αρχών της προστασίας των δεδομένων. Τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε επεξεργασία με τρόπο που διασφαλίζει την ενδεδειγμένη ασφάλεια των δεδομένων «συμπεριλαμβανομένης της προστασίας τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων».[313] Η αρχή αυτή αντανακλά κατά προσέγγιση τους όρους του άρθρου 17 της Οδηγίας 95/46/ΕΚ. Ως πρωτεύοντες κανόνες οι εν λόγω αρχές συνάγονται και από τους δευτερεύοντες κανόνες που καθιδρύουν

---

[309] Έχει κριθεί ότι τα δεδομένα που αφορούν εγγυητές πρέπει να διαγράφονται χωρίς να έχει υποβληθεί σχετικό αίτημα από το υποκείμενο, από τη στιγμή που η απαίτηση εξοφλήθηκε και γνωστοποιήθηκε η εξόφληση στον υπεύθυνο επεξεργασίας (απόφαση 26/2002 ΑΠΔΠΧ, KNoB 51 (2003) 736).

[310] Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, *Προσωπικά Δεδομένα*, 1η εκδ. (Θεσσαλονίκη: Νομική Βιβλιοθήκη, 2016), 81.

[311] Άρθρο 5 παρ. 1 ε' ΓΚΠΔ.

[312] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 318.

[313] Άρθρο 5 παρ.1 στ' ΓΚΠΔ.

υποχρεώσεις του υπευθύνου επεξεργασίας προς πληροφόρηση και λήψη μέτρων ασφαλείας των δεδομένων (άρθρα 12-15 και 25, 32 επ.). Τα καθήκοντα αυτά συμπεριλαμβάνουν και την νέα απαίτηση για γνωστοποίηση σχετικά με τις παραβιάσεις των προσωπικών δεδομένων στην αρμόδια εποπτική Αρχή και σε ορισμένες περιπτώσεις και στα ίδια τα υποκείμενα των δεδομένων. Στο πλαίσιο της ασφάλειας των δεδομένων εντάσσεται και η μέριμνα για την ασφαλή καταστροφή τους. Συγκεκριμένα, η Αρχή έχει εκδώσει την υπ'αριθμ. 1/2005 Οδηγία που εμπεριέχει κανόνες ασφαλούς καταστροφής των αρχείων που διατηρούνται τόσο σε φυσική όσο και σε ηλεκτρονική μορφή, ενώ μέσω μιας σειράς αποφάσεων που έχει εκδώσει[314], έχει επιβάλλει πρόστιμα σε υπευθύνους επεξεργασίας οι οποίοι αφού ολοκληρώθηκε η επεξεργασία αμέλησαν να διατηρήσουν ασφαλή αρχεία προσωπικών δεδομένων, αφήνοντας αυτά εκτεθειμένα σε δημόσιο χώρο.

2.3.3.7 Η αρχή της λογοδοσίας

Από την αρχή της διαφάνειας απορρέει και η αρχή της λογοδοσίας (**accountability**)[315]. Ένα νέο στοιχείο προστίθεται στον Κανονισμό σε σχέση με την Οδηγία 95/46/ΕΚ, καθώς ο υπεύθυνος επεξεργασίας πρέπει πλέον να μπορεί να αποδεικνύει τη συμμόρφωση της επεξεργασίας με τους νομικούς κανόνες και δη (όχι μόνο απέναντι στο υποκείμενο, αλλά και) στην εποπτική αρχή.[316]Η απαίτηση αυτή όχι μόνο για τη διασφάλιση αλλά και για την ικανότητα απόδειξης της συμμόρφωσης, αναπτύσσεται στο άρθρο 24 του ΓΚΠΔ που επικεντρώνεται στην ευθύνη του υπευθύνου της επεξεργασίας. Συνεπώς, προκειμένου για τις πιο επικίνδυνες μορφές επεξεργασίας, κυρίως των ευαίσθητων δεδομένων και των επεξεργασιών μεγάλης κλίμακας (**large – scale processing**), επιτάσσεται η λήψη πρόσθετων μέτρων λογοδοσίας: κατάρτισης και διατήρησης αρχείου δραστηριοτήτων επεξεργασίας (άρθρο 30 ΓΚΠΔ), υποβολής μελέτης αντικτύπου (της επεξεργασίας, **DPIA**), στην ΑΠΔΠΧ (άρθρο 35 ΓΚΠΔ) και ορισμού υπευθύνου προστασίας (άρθρο 37 ΓΚΠΔ, **DPO**).[317]

---

[314]ΑΠΔΠΧ 73/2012,76/2012, 55/2007, 46/2007,12/2016, 15/2016, 16/2016. Διαθέσιμες στην ιστοσελίδα www.dpa.gr.

[315] Συναντάται και υπό άλλες εννοιολογικές παραλλαγές π.χ. ανταποκρισιμότητα (**responsiveness**), απαντησιμότητα (**answerability**).

[316] Article 29 Working Party, "Opinion 03/2010 On the Principle Of Accountability", Ec.Europa.Eu, 2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

[317] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 110.

ΜΕΡΟΣ Β'

ΤΡΙΤΟ ΚΕΦΑΛΑΙΟ
Η ΕΝΝΟΜΗ ΣΧΕΣΗ ΑΝΑΜΕΣΑ ΣΕ ΤΡΑΠΕΖΙΚΑ ΙΔΡΥΜΑΤΑ ΚΑΙ ΠΕΛΑΤΕΣ

3.1 Εισαγωγικές παρατηρήσεις

Οι επαφές των πελατών με τα τραπεζικά ιδρύματα συνήθως δεν εξαντλούνται σε κάποια συγκεκριμένη στιγμιαία συναλλαγή, αλλά εντάσσονται σε μια σχέση διαρκείας (όπως π.χ. συμβαίνει στην περίπτωση του ανοίγματος ενός τραπεζικού λογαριασμού), από την οποία είναι δυνατόν να απορρέουν σημαντικές παρεπόμενες υποχρεώσεις, για την πλευρά του αντισυμβαλλόμενου τραπεζικού ιδρύματος, σε μεγαλύτερο βαθμό απ' ότι συμβαίνει σε άλλες συμβατικές μορφές. Και στις περιπτώσεις όμως των στιγμιαίων συναλλακτικών επαφών των τραπεζών με τους πελάτες τους, οι ευθύνες των τραπεζών από τις διαπραγματεύσεις είναι αυξημένες σε σύγκριση με άλλες συμβατικές σχέσεις. Επιπροσθέτως, αυξημένες υποχρεώσεις μπορεί να υπέχει το τραπεζικό ίδρυμα ακόμα και μετά τη λήξη της συμβατικής ή συναλλακτικής του σχέσης με τον εκάστοτε πελάτη. Όλες αυτές οι υποχρεώσεις που στοιχειοθετούνται στο πλαίσιο της παροχής υπηρεσιών από τα τραπεζικά ιδρύματα, αποσκοπούν στην παροχή αυξημένης προστασίας στους πελάτες, καθώς επιβάλλουν στα τραπεζικά ιδρύματα την τήρηση ορισμένης συμπεριφοράς, ανεξαρτήτως εάν ο πελάτης θεωρείται ή όχι καταναλωτής με βάση την έννοια του Ν. 2251/1994 και τυγχάνει της προστασίας του σχετικού νομοθετικού πλαισίου που αφορά την προστασία των καταναλωτών.

Αυτό συμβαίνει γιατί η τράπεζα είναι επαγγελματίας και γνώστης της αγοράς χρήματος, με αποτέλεσμα να κατέχει ευρύτατη πληροφόρηση στο πλαίσιο του χρηματοπιστωτικού τομέα, γεγονός που μπορεί να οδηγήσει στη γένεση της υποχρεώσεώς της να παράσχει στον πελάτη της πληροφορίες και συμβουλές. Επιπροσθέτως, η οικονομική υπόσταση των πελατών, συχνά εξαρτάται από τη συμπεριφορά της τράπεζας, όπως συμβαίνει για παράδειγμα στις περιπτώσεις που αυτή αποφασίζει να συνεχίσει ή να διακόψει τη χρηματοδότηση προς τον πελάτη, ή να ενημερώσει αυτόν σχετικά με σημαντικές για την εκάστοτε συναλλαγή πληροφορίες. Επίσης, οι σχέσεις ανάμεσα στο τραπεζικό ίδρυμα και τους πελάτες του εντάσσονται σε ένα πλαίσιο προστασίας της εμπιστοσύνης και των προσωπικών πληροφοριών των τελευταίων, καθώς η τράπεζα, εξαιτίας της συναλλακτικής της επαφής με τους πελάτες γνωρίζει και έχει στην κατοχή της πλήθος προσωπικών και απόρρητων στοιχείων τους. Κατανοούμε επομένως, ότι η σχέση ανάμεσα στις τράπεζες και τους πελάτες τους είναι πολυδιάστατη και στο πλαίσιο αυτής γεννώνται για την τράπεζα αυξημένες παρεπόμενες υποχρεώσεις προστασίας των εννόμων συμφερόντων των πελατών της.[318]

[318] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 8-9.

3.2 Η σύμβαση ως θεμέλιο των εννόμων σχέσεων τράπεζας-πελάτη

Χαρακτηριστικό όλων των τραπεζικών συναλλαγών αποτελεί ο δικαιοπρακτικός, και ειδικά ο συμβατικός χαρακτήρας τους, είτε πρόκειται για παθητικές, είτε για ενεργητικές εργασίες, είτε για παροχή υπηρεσιών. Πολλά είδη μονομερών δικαιοπραξιών, όπως η παροχή πληρεξουσιότητας, αποτελούν παρακολουθήματα άλλων, κύριων συμβατικών σχέσεων όπως στην περίπτωση που ο πελάτης χορηγεί πληρεξουσιότητα στην τράπεζα ώστε αυτή να διενεργήσει στο όνομά του συγκεκριμένη εργασία (π.χ. αγορά χρεογράφων ή επενδυτικών προϊόντων), την οποία της έχει αναθέσει μέσω σύμβασης που έχει καταρτιστεί μεταξύ τους ή για την διενέργεια δικαιοπραξίας που συνίσταται και προς το συμφέρον της τράπεζας , όπως πώληση ενεχυρασμένων σε αυτήν αξιογράφων, οπότε μπορεί να θεωρηθεί και ανέκκλητη (ΑΚ 218 εδάφιο 2). Υπάρχει όμως και η περίπτωση δημιουργίας εξωδικαιοπρακτικών ενοχών, ειδικά σε περίπτωση που η τράπεζα προξενήσει ζημία στον πελάτη χάρη σε αδικαιοπρακτική της συμπεριφορά ή αντιστρόφως. Επίσης, η τράπεζα μπορεί να προβεί σε πράξεις που συνιστούν γνήσια διοίκηση αλλοτρίων, όπως συμβαίνει όταν η τράπεζα εκποιεί χρεόγραφα που ανήκουν σε απουσιάζοντα πελάτη της, χωρίς να έχει εντολή προς τούτο. Ωστόσο, η διαχείριση υποθέσεων των πελατών, χωρίς ειδική εντολή ή εξουσιοδότησή τους, συνιστά κατά τη συνηθισμένη πρακτική άσκηση εξουσίας ή εκπλήρωση υποχρεώσεως, που πηγάζει από μια ευρύτερη σχέση ανάμεσα σε πελάτη και τράπεζα.

Στο πλαίσιο αυτό, εντάσσεται και η διαχείριση χαρτοφυλακίων των πελατών, που αποτελεί μέρος της σύγχρονης «ιδιωτικής τραπεζικής» (**«private banking»**). Η τράπεζα κατά την διενέργεια των δραστηριοτήτων αυτών έχει εξουσία λήψεως αποφάσεων και διενέργειας συναλλαγών ερήμην του πελάτη της, ο οποίος ενημερώνεται εκ των υστέρων. Ακόμα και οι ενέργειες αυτές όμως προβλέπονται σε συμβάσεις και δεν μπορεί να θεωρηθεί ότι εκτελούνται «χωρίς εντολή» από τον πελάτη. Συνέπεια αυτού του γεγονότος αποτελεί και η τυχόν ευθύνη της τράπεζας, η οποία θα είναι δικαιοπρακτική, πράγμα που έχει σημασία για το βάρος αποδείξεως του πταίσματος της τράπεζας. Οι τράπεζες στην πράξη πάντως, περιορίζουν ή αποκλείουν την ευθύνη αυτή μέσω της διατύπωσης απαλλακτικών ρητρών στους γενικούς όρους συναλλαγών τους. Σε κάθε περίπτωση, χρήζει εφαρμογής και η ειδική νομοθεσία για τις αγορές χρηματοπιστωτικών μέσων και τις επενδυτικές συμβουλές (νόμος 4514/2018, που ενσωματώνει την Οδηγία 2014/65/ΕΕ, γνωστή και ως MiFID II και Κανονισμός (ΕΕ) 600/2014, γνωστός και ως MiFIR).[319]

Περαιτέρω, το τραπεζικό ίδρυμα δύναται στο πλαίσιο άσκησης της οικονομικής του ελευθερίας, να μην ασκεί σε όλες τις επιτρεπτές σε αυτό δραστηριότητες ή να περιορίζει αυτές με γενικά κριτήρια (π.χ. παροχή επενδυτικών υπηρεσιών μόνο σε καταθέσεις πάνω από ορισμένο ύψος). Επίσης, πολλές τράπεζες έχουν διαμορφώσει την εσωτερική τους οργάνωση ώστε να περιορίζουν ακόμα και απλούστερες συναλλαγές, όπως την σύμβαση καταθέσεως, με αποτέλεσμα να μην δέχονται σε ευρεία κλίμακα καταθέσεις, καθώς στην περίπτωση πολλαπλών καταθέσεων μικρών ποσών, η τράπεζα μπορεί να ζημιωθεί ως προς την διαχείρισή τους ή να έχει ελάχιστα κέρδη.[320] Κρίσιμη θεωρείται και η συνδρομή ή μη των λεγόμενων «τραπεζικών κριτηρίων», δηλαδή αυτών που καθορίζουν την σώφρονα και σύμφωνα με τους κανόνες της χρηστής διαχειρίσεως διενέργειας των συναλλαγών της τράπεζας, τα οποία κατά κύριο λόγο προσδιορίζονται από

[319] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 58-59.
[320] Νικόλαος Κ. Ρόκας et al., *Στοιχεία Τραπεζικού Δικαίου*, 3η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2016), 470-471.

κανονιστικές πράξεις της Τράπεζας της Ελλάδος. Εάν η τράπεζα κρίνει ότι αυτά δεν συντρέχουν, δεν μπορεί να γίνει λόγος για αδικαιολόγητη άρνηση παροχής υπηρεσιών ή κατάχρησης της συμβατικής της ελευθερίας, που θα έθετε ζητήματα αναγκαστικής συμβάσεως. Δικαιολογημένα αρνείται επομένως, την σύναψη συμβάσεως με πρόσωπα που κρίνονται ύποπτα για νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες.

Η κατάσταση κρίνεται διαφορετική όταν καθίσταται υποχρεωτική η χρήση του τραπεζικού συστήματος για νομικώς αναγκαία για τον αιτούμενο συναλλαγή. Τέτοια υποχρέωση καθιερώνεται μέσω ειδικών διατάξεων που προβλέπουν την χρήση τραπεζικών μέσων πληρωμής ή τραπεζικού λογαριασμού για την καταβολή οφειλών προς το Δημόσιο ή την είσπραξη από αυτό[321] ή την υποχρεωτική εγκατάσταση τερματικών αποδοχής πιστωτικών καρτών (point of sale-POS) σε καταστήματα και επαγγελματικούς χώρους.[322] Στις περιπτώσεις αυτές υπάρχει η δυνατότητα θεμελίωσης υποχρέωσης της τράπεζας προς σύμπραξη στην κατάρτιση της σχετικής συμβάσεως και στην παροχή της αντίστοιχης υπηρεσίας, έναντι της προβλεπόμενης αμοιβής. Η διάγνωση της υποχρεώσεως αυτής, υπόκειται σε κριτήρια που αφορούν το κατά πόσον η συγκεκριμένη συναλλαγή εμφανίζει κινδύνους ή όχι για την τράπεζα και κατά πόσο μπορεί η υπηρεσία να παρασχεθεί (εκουσίως) από άλλη τράπεζα, χωρίς να χειροτερεύσει η θέση του επίδοξου πελάτη.[323]

3.2.1 μορφή των τραπεζικών συμβάσεων

Για την πλειοψηφία των τραπεζικών εργασιών, ο νόμος δεν προβλέπει την τήρηση συγκεκριμένου τύπου. Επομένως, αυτές επιτρέπεται να συναφθούν αρχικά ατύπως (ΑΚ 158). Στην τραπεζική πρακτική ωστόσο, συνηθίζεται να τηρείται ο (εκούσιος) τύπος του ιδιωτικού εγγράφου, τουλάχιστον για αποδεικτικούς σκοπούς. Ακόμα και όταν χρησιμοποιούνται μέσα τηλεπικοινωνιών για τη σύναψη συμβάσεων, όπως συμβαίνει στην περίπτωση των τηλεφωνικών εντολών (**phone banking**), στο μέτρο που το μήνυμα μέσω αυτών δεν μπορεί να θεωρηθεί έγγραφο, αυτό θα προβλέπεται σε έγγραφη σύμβαση πλαίσιο που αφορά τέτοιου είδους συναλλαγές, ενώ για να επιτευχθεί ο σκοπός της απόδειξης θα τηρούνται κατόπιν συμφωνίας των μερών οι σχετικές καταγραφές. Σε περίπτωση πάντως που δεν έχει συμφωνηθεί διαφορετικά (π.χ. ότι θα τηρείται ο συστατικός τύπος για συγκεκριμένες συναλλαγές), η παράλειψη τήρησης του έγγραφου τύπου για συναλλαγή για την οποία ο νόμος δεν προβλέπει αυτό, ακόμα και αν ο τύπος αυτός έχει τηρηθεί σε άλλες ομοειδείς συμβάσεις ή προγενέστερες συναλλαγές, δεν θα επιδρά στο κύρος της εν λόγω συναλλαγής.

Οι τραπεζικές συμβάσεις είναι κατά κύριο λόγο τυποποιημένες και καταρτίζονται κυρίως με βάση τους Γενικούς Όρους Συναλλαγών. Πέρα από τους Γενικούς Όρους Συναλλαγών που διέπουν την σχέση τραπεζικού ιδρύματος και πελάτη, οι επί μέρους συμβάσεις επίσης είναι κατά κύριο λόγο

---

[321] Σύμφωνα με την ΠΟΛ 1156/11.5.2010 απόφαση του ΥΠΟΙΚ οφειλές προς το Δημόσιο που υπερβαίνουν τα 250 ευρώ ημερησίως για τους ασκούντες επιχείρηση και τα 500 ευρώ για τα λοιπά πρόσωπα, εξοφλούνται υποχρεωτικά με επιταγές.

[322] Σύμφωνα με το άρθρο 65 του νόμου **4446/2016**, «Οι δικαιούχοι πληρωμής, στο πλαίσιο των συναλλαγών τους με πληρωτές οι οποίοι ενεργούν για λόγους που δεν εμπίπτουν στην εμπορική, επιχειρηματική ή επαγγελματική τους δραστηριότητα, υποχρεούνται… να αποδέχονται μέσα πληρωμής με κάρτα για την ολοκλήρωση των πράξεων πληρωμής».

[323] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 62.

τυποποιημένες, ειδικά ως προς τους προβλεπόμενους όρους. Οι όροι αυτοί μπορεί να λαμβάνουν είτε πάγιο είτε μεταβλητό χαρακτήρα (ύψος παροχής, επιτόκιο, εξασφαλίσεις κ.α.). Στις τραπεζικές συμβάσεις περιλαμβάνονται κυρίως ρητές δηλώσεις βουλήσεως των μερών. Συχνά συμφωνείται όμως ότι έχει δικαιοπρακτικό χαρακτήρα και συγκεκριμένη συμπεριφορά των μερών (λ.χ. όταν συμφωνείται ότι η πίστωση ή η χρέωση λογαριασμού πελάτη από την τράπεζα συνιστά αποδοχή αιτήματος για διενέργεια συγκεκριμένης συναλλαγής) ή ακόμα και η απλή αδράνειά τους (λ.χ. η σιωπή του πελάτη για ορισμένο χρονικό διάστημα μετά την αποστολή υπολοίπου του λογαριασμού συνιστά αποδοχή του).[324]

Για να πραγματοποιηθεί η κατάρτιση των συμβάσεων αυτών συμβάλλονται εκ μέρους της τράπεζας υποκατάστατοι (άρθρα 67 εδάφιο 2 και 70 ΑΚ και 87 του νόμου 4548/2018), εφόσον έχει παρασχεθεί από το διοικητικό συμβούλιο η σχετική εξουσία, είτε μέσω αντιπροσώπων, δυνάμει της σχετικής πληρεξουσιότητας. Με απώτερο στόχο την προστασία του καλόπιστου πελάτη της τράπεζας, η προαναφερθείσα πληρεξουσιότητα μπορεί να θεωρηθεί ότι υπάρχει, ακόμα και αν έχει παύσει ή ουδέποτε χορηγηθεί. Αρκεί το πρόσωπο που εμφανίζεται ως πληρεξούσιος, να δημιουργεί ευλόγως την εντύπωση ότι έχει πληρεξουσιότητα, η δε τράπεζα από τη μεριά της να γνώριζε ή να όφειλε, μέσω της επίδειξης της προσήκουσας επιμέλειας, να γνωρίζει την δραστηριοποίηση του υπαλλήλου επ'ονόματί της.[325]

Η σύναψη των τραπεζικών συμβάσεων προϋποθέτει την συνδρομή όλων των προϋποθέσεων για την έγκυρη κατάρτιση συμβάσεως σύμφωνα με το αστικό δίκαιο. Εάν ελλείπει κάποια από τις προϋποθέσεις αυτές η σύμβαση καθίσταται άκυρη ή ακυρώσιμη. Ειδικότερα, εάν για τη συνδρομή ενός λόγου ακυρότητας ή ακυρωσίας απαιτείται η συνδρομή υποκειμενικών στοιχείων, στο πρόσωπο αμφοτέρων των δικαιοπρακτούντων, το στοιχείο αυτό θα πρέπει να συντρέχει και από τη μεριά της τράπεζας. Για να χαρακτηριστεί μια τραπεζική σύμβαση εικονική, απαιτείται η πρόθεση να μην επέλθουν οι έννομες συνέπειες να συντρέχει σε αμφοτέρους τους συμβαλλομένους. Αντιστοίχως για να κριθεί ως ανήθικη μια τραπεζική σύμβαση, σε περίπτωση που η ανηθικότητα προσδίδεται από το κίνητρο ή τον σκοπό του δικαιοπρακτούντος, απαιτείται γνώση των στοιχείων αυτών και από την τράπεζα. Η γνώση αυτή εκ μέρους της τράπεζας, θα πρέπει να συντρέχει στο πρόσωπο που συνάπτει την σχετική σύμβαση. Αυτό το πρόσωπο μπορεί να έχει την ιδιότητα του αντιπροσώπου, του οργάνου ή του υποκατάστατου. Σε κάθε περίπτωση θα τυγχάνει εφαρμογής το άρθρο 214 ΑΚ, το οποίο ορίζει ότι «Τα ελαττώματα της βούλησης, η γνώση ή η υπαίτια άγνοια ορισμένων περιστατικών, καθώς και η επίδρασή τους στη δικαιοπραξία κρίνονται από το πρόσωπο του αντιπροσώπου».[326]

3.3 Η γενική σχέση ανάμεσα σε τράπεζα και πελάτη

Κατά μια άποψη, η ύπαρξη μιας γενικής σχέσης ανάμεσα σε τράπεζα και πελάτη διακρίνεται από τις ειδικές σχέσεις-πλαίσια, όπως αυτές που αφορούν τις συμβάσεις διαχείρισης χαρτοφυλακίου των πελατών. Οι πελάτες συνήθως συμβάλλονται με τα τραπεζικά ιδρύματα για να

[324] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 62-63.
[325]ΑΠ 939/2004 ΔΕΕ 2005, 605 (αφορά συναλλαγή που διενεργήθηκε από διευθυντή τράπεζας που είχε τεθεί σε διαθεσιμότητα).
[326] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 66.

πραγματοποιήσουν το σύνολο ή το μέγιστο μέρος των τραπεζικών τους συναλλαγών, συνήθως μέσω ενός συγκεκριμένου καταστήματος. Η συνεχής αυτή ροή ομοειδών ή ετεροειδών συναλλαγών δημιουργεί μια στενή σχέση ανάμεσα σε τράπεζα και πελάτη, ακόμα και στις περιπτώσεις που ο πελάτης είναι νομικό πρόσωπο. Θα πρέπει επομένως να εξεταστεί εάν από τις ειδικότερες έννομες σχέσεις που διαμορφώνονται ανάμεσα σε πελάτη και τράπεζα προκύπτει μια γενικότερη έννομη σχέση από την οποία απορρέουν ειδικές έννομες συνέπειες.

Σύμφωνα με τους υποστηρικτές της θεωρίας αυτής, η σχέση αυτή ιδρύεται μέσω της σύναψης μιας «γενικής τραπεζικής συμβάσεως» (**allgemeiner Bankvertrag**), η οποία καταρτίζεται σιωπηρώς. Κατά μια άποψη, η σύμβαση αυτή καταρτίζεται μέσω προπαρασκευαστικών ενεργειών για την σύναψη ορισμένης συμβάσεως, είτε με την υπογραφή των Γενικών Όρων Συναλλαγών της τράπεζας εκ μέρους του πελάτη, είτε μέσω κατάρτισης συγκεκριμένης συμβάσεως, κυρίως μέσω του ανοίγματος λογαριασμού. Από αυτήν δεν παράγονται πρωτογενείς υποχρεώσεις προς κύρια παροχή εκ μέρους της τράπεζας και δεν αναγνωρίζεται υποχρέωση της τράπεζας να συμπράξει σε κατάρτιση μελλοντικών, επί μέρους, συμβάσεων με τον πελάτη.[327] Η τραπεζική σύμβαση που καταρτίζεται είναι κατά κανόνα ενοχική, υποσχετική, αμφοτεροβαρής, συχνά διαρκής, μεικτή και σύμβαση πλαίσιο, που καταρτίζεται από τον πελάτη και τους αρμόδιους υπαλλήλους ενός καταστήματος μιας τράπεζας. Πάντοτε αποτελεί σύμβαση προσχωρήσεως, αφού χάριν της βέλτιστης εξασφάλισης των συμφερόντων της τράπεζας και της ταχύτητας των συναλλαγών είναι πάντοτε προδιατυπωμένη, ώστε ο πελάτης να την δέχεται ως έχει ή να αρνείται την αποδοχή της, στερούμενος της ευχέρειας διαπραγμάτευσης του περιεχομένου της. Το οποιοδήποτε, πάντως περιεχόμενο της σύμβασης διευρύνει η καλή πίστη, με την δημιουργούμενη σχέση εμπιστοσύνης. Πέραν των καθαρών συμβατικών υποχρεώσεων γεννώνται, δηλαδή, και άλλες παρεπόμενες υποχρεώσεις των μερών, που έχουν ως έρεισμα την καλή πίστη (ΑΚ 288), ώστε η μη εκπλήρωσή τους να συνιστά πλημμελή εκπλήρωση της παροχής και, κατά τις περιστάσεις, σωρευτικά, προσβολή της προσωπικότητας και αδικοπραξία.[328]

Αντικείμενο της «γενικής σχέσεως» ανάμεσα σε τράπεζα και πελάτη αποτελούν αποκλειστικά οι υποχρεώσεις προστασίας και πίστεως, κυριότατα εις βάρος της τράπεζας. Συνεπώς, η τράπεζα θα πρέπει, για παράδειγμα, να απέχει από την κήρυξη ενός δανείου ως ληξιπρόθεσμου και απαιτητού, εάν ο πελάτης καθυστέρησε για λίγες ημέρες την καταβολή των τόκων μιας εξαμηνιαίας. Αντίστοιχα, ο πελάτης δεν θα πρέπει να αναμένει ότι η τράπεζα δεν θα προβεί σε χορήγηση δανείου σε ανταγωνιστή του. Ακόμα και αν υπήρχε ρητή συμφωνία ως προς κάτι τέτοιο, αυτή θα ήταν ανίσχυρη ως αντιβαίνουσα και περιοριστική του ελεύθερου ανταγωνισμού. Επίσης, η τράπεζα δεν θα πρέπει να προσδοκά ότι ο πελάτης της δεν θα απευθυνθεί σε ανταγωνίστριά της για την χορήγηση δανείου με στόχο την χρηματοδότηση των εργασιών του. Επομένως, η συναγωγή μιας γενικής έννομης σχέσης ανάμεσα σε τράπεζα και πελάτη δεν είναι δυνατόν να θεμελιωθεί στη ρητή βούληση των μερών, αφού δεν καταρτίζεται σε κανένα σημείο σύμβαση με αντικείμενο την τηρητέα εν γένει στο μέλλον συμπεριφορά μεταξύ τράπεζας και πελάτη. Εάν όμως η έννομη σχέση δεν θεμελιωθεί στην βούληση των μερών αλλά απ' ευθείας στον νόμο, θα πρέπει να εφαρμοστούν οι γενικές ρήτρες και ιδίως το άρθρο 288 ΑΚ (αρχή της καλής πίστης). Με βάση την ερμηνεία της διατάξεως αυτής, γίνεται δεκτό ότι μπορεί να θεμελιωθεί σε αυτήν και

---

[327] Ibid., 68.

[328] Σπυρίδων Δ. Ψυχομάνης, *Εγχειρίδιο Τραπεζικού Δικαίου*, 2η εκδ. (repr., Αθήνα, Θεσσαλονίκη: Εκδόσεις Σάκκουλα, 2016), 114.

η γένεση ενοχών.[329] Εφόσον πρόκειται για υποχρεώσεις που γεννώνται κυρίως εις βάρος της τράπεζας, μπορεί να γίνει αποδεκτή η άποψη ότι οι γενικές υποχρεώσεις πίστεως και προνοίας της τράπεζας έναντι των πελατών της πηγάζουν από την διάταξη ΑΚ 288 και επομένως υφίσταται μια γενική, αλλά ετεροβαρής ως προς την τράπεζα, έννομη σχέση μεταξύ των δύο.

Κατά μια δεύτερη άποψη, η ύπαρξη γενικής τραπεζικής συμβάσεως απορρίπτεται και η δέσμη υποχρεώσεων της τράπεζας βασίζεται στην αρχή της καλής πίστης (ΑΚ 281 και 288), από τη σχέση εμπιστοσύνης που δημιουργείται ανάμεσα σε τράπεζα και πελάτη, είτε απορρέει από την ευθύνη από διαπραγματεύσεις (ΑΚ 197). Σε κάθε περίπτωση εκτιμώνται τα αμοιβαία δικαιώματα και οι υποχρεώσεις στην εξέλιξη των επιμέρους εννόμων σχέσεων μεταξύ τράπεζας και πελάτη.[330]Σύμφωνα με την άποψη αυτή, για να εδραιωθεί η έννομη σχέση μεταξύ πελάτη και τράπεζας δεν απαιτείται η σύναψη σύμβασης, αλλά αρκεί μια αρχική «δικαιοπρακτική επαφή». Η πρόκριση μιας τέτοιας ad hoc αντιμετώπισης μπορεί να θεωρηθεί πιο ευέλικτη και να οδηγήσει σε λύσεις πιο εξατομικευμένες, λαμβάνοντας υπόψιν τις ιδιοτυπίες κάθε ξεχωριστής περίπτωσης. Αντιθέτως, η προσφυγή σε μια a priori γενικής έννομης σχέσεως με εκ τω προτέρων προσδιορισμένο περιεχόμενο, μπορεί να οδηγήσει σε προκρούστειες λύσεις.[331] Μια τρίτη άποψη υποστηρίζει ότι οι υποχρεώσεις των τραπεζικών ιδρυμάτων έναντι των πελατών-καταναλωτών τους, μπορούν να θεμελιωθούν στο άρθρο 8 του νόμου 2251/1994, που θεμελιώνει αυτοτελή λόγο ευθύνης ασχέτως αν υφίσταται σύμβαση ή αδικοπρακτική ενοχή.[332]

Σε γενικές γραμμές, κρίνεται ασφαλέστερη η θεμελίωση των υποχρεώσεων πίστεως και προνοίας της τράπεζας να θεμελιώνονται στην επιμέρους έννομη σχέση που την συνδέει με τους πελάτες της και σε όλες τις παρεπόμενες περιστάσεις, όπως η μακροχρόνια συνεργασία ανάμεσα στα μέρη και η ομαλότητα της ανελίξεώς της. Οι προαναφερθείσες διατάξεις (ΑΚ 288, ΑΚ 197-198, ΑΚ 914), σε συνδυασμό με τις ειδικές διατάξεις της τραπεζικής νομοθεσίας, μπορούν να διαμορφώσουν το κατάλληλο νομοθετικό πλαίσιο για την αντιμετώπιση κάθε περιπτώσεως.

3.4 Οι υποχρεώσεις πρόνοιας των τραπεζικών ιδρυμάτων έναντι των πελατών τους

Την σχέση ανάμεσα σε τράπεζα και πελάτη διαπνέει μια αμοιβαία εμπιστοσύνη, ότι κάθε μέρος θα πράξει ή θα αποφύγει να πράξει οτιδήποτε μπορεί να βλάψει τα συμφέροντα του άλλου μέρους. Η τράπεζα, λόγω της θέσης που κατέχει, είναι το μέρος που προσφέρει εμπιστοσύνη, προσελκύοντας τον πελάτη, υποσχόμενη, σιωπηρά, ότι θα προασπίσει με τον βέλτιστο τρόπο και ανυστερόβουλα, τα ατομικά, οικονομικά του συμφέροντα. Αυτός είναι και ο λόγος για τον οποίο οι τράπεζες έχουν χαρακτηριστεί και ως δημόσιες υπηρεσίες (**public service**). Η σχέση αυτή εμπιστοσύνης εδράζεται στην αρχή της καλής πίστεως, η οποία κατά τον νόμο (ΑΚ 197,198,288),

---

[329] Μιχαήλ Σταθόπουλος, *Γενικό Ενοχικό Δίκαιο*, 4η εκδ. (repr., Αθήνα-Κομοτηνή: Εκδόσεις Σάκκουλα, 2004), 91-92, 95.

[330] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 9.

[331] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 70.

[332] Βλ. ΑΠ 589/2001, σύμφωνα με την οποία έγινε δεκτή η ευθύνη τραπεζικού ιδρύματος κατά την παροχή υπηρεσιών και κατά τη διατύπωση καταχρηστικών ΓΟΣ. Η απόφαση είναι καθοριστική για την ευθύνη εκ του νόμου της Τράπεζας ως προμηθευτή υπηρεσιών. Επίσης, βλ. ΕφΑθ 9460/1999, ΤΝΠ ΝΟΜΟΣ και ΠΠρΘεσ 19932/09 που αφορούσε το ζήτημα των αγωγών αποζημίωσης επενδυτών κατά πιστωτικών ιδρυμάτων λόγω παροχής ακατάλληλων επενδυτικών συμβουλών.

πρέπει να υπαγορεύει και να διαπνέει την συμπεριφορά των συναλλασσομένων μερών ήδη από το προσυμβατικό ή διαπραγματευτικό στάδιο των σχέσεων τους, συνεχίζοντας κατά το κύριο συμβατικό στάδιο και φθάνοντας μέχρι και το μετασυμβατικό στάδιο. Οι συναλλασσόμενοι παράγοντες αναλαμβάνουν έτσι να εκπληρώσουν ορισμένες υποχρεώσεις έναντι αλλήλων, οι οποίες υπαγορεύονται από την ευθύτητα και την εντιμότητα, που πρέπει να διακρίνουν τις συναλλαγές τους. Το άρθρο 8 του π.δ. 10/1.3.2017 («Κώδικας καταναλωτικής δεοντολογίας») κάνει ιδιαίτερη μνεία σχετικά με την παραγόμενη σχέση εμπιστοσύνης και τις υποχρεώσεις που αναλαμβάνει τόσο η τράπεζα όσο και οι πελάτες-καταναλωτές στην μεταξύ τους σχέση.

Κατά το προσυμβατικό ή διαπραγματευτικό στάδιο της σχέσης ανάμεσα σε τράπεζα και πελάτη, το οποίο αρχίζει με την διερευνητική προσέγγιση του πελάτη σε κάποιο τραπεζικό υποκατάστημα ή μέσω των τραπεζικών διαφημίσεων, που αποτελούν πρόσκληση προς τον υποψήφιο πελάτη να απευθύνει πρόταση στην τράπεζα για την κατάρτιση κάποιας τραπεζικής σύμβασης, η τράπεζα έχει τις γενικές, κατά κύριο λόγο, υποχρεώσεις της πλήρους και ειλικρινούς διαφώτισης και ενημέρωσης του πελάτη, σχετικά με τη σύμβαση που εκείνος επιθυμεί να καταρτίσει και της λήψης των αναγκαίων μέτρων για την προστασία των απολύτων εννόμων αγαθών και της περιουσίας του (ΑΚ 197). Εν συνεχεία, κατά το συμβατικό στάδιο, πέρα από τις λοιπές υποχρεώσεις συμβατικής φύσεως, η τράπεζα βαρύνεται επιπλέον με την γενική υποχρέωση διαφυλάξεως των συμφερόντων του πελάτη, η οποία αναλύεται στις ειδικότερες υποχρεώσεις τήρησης του απορρήτου, της επιμελούς ακροάσεως και εκτιμήσεως των συμφερόντων του πελάτη, της συμβουλευτικής καθοδήγησής του και της προειδοποίησής του ενόψει κινδύνων, που δύνανται να απειλήσουν τα συμφέροντά του, και της παροχής πληροφοριών (ΑΚ 288). Αναφορικά με την υποχρέωση τήρησης του απορρήτου, θα πρέπει να σημειωθεί ότι ως υποχρέωση βαρύνει την τράπεζα ακόμα και μετά τη λήξη της συμβατικής σχέσεως (ΑΚ 288). Εάν η τράπεζα παραβιάσει τις υποχρεώσεις αυτές, θα υποχρεωθεί σε αποζημίωση του πελάτη ή ακόμα και σε ικανοποίηση της ηθικής του βλάβης. Το τραπεζικό απόρρητο, ειδικότερα, επιβάλλεται τόσο από την σχέση εμπιστοσύνης της τράπεζας και του πελάτη, όσο και από ένα πλέγμα διατάξεων (άρθρα 5 Σ, 57 ΑΚ και 371 ή 252 ΠΚ) και συνίσταται στην υποχρέωση της τράπεζας να σιωπά για τις προσωπικές και οικονομικές υποθέσεις του πελάτη. Θα πρέπει, ωστόσο, να ληφθεί υπόψη και η ίδια η βούληση του πελάτη αναφορικά με τα πραγματικά περιστατικά που ο ίδιος επιθυμεί να κρατηθούν μυστικά. Αν η βούληση του αυτή δεν έχει εκφρασθεί ή δεν είναι ευχερώς διαγνώσιμη, η τράπεζα υποχρεώνεται να σιωπά για οτιδήποτε περιέρχεται σε γνώση της και αφορά τον πελάτη της, έναντι πάντων.[333]

Αναφορικά με τις υποχρεώσεις πρόνοιας της τράπεζας προς τους πελάτες της, θα πρέπει να σημειωθεί ότι η νομολογία συνάγει αυτές αφενός μεν λόγω της αυξημένης δυνατότητας επεμβάσεως της τράπεζας στην περιουσιακή σφαίρα του πελάτη[334], αφετέρου δε λόγω της

---

[333]Σπυρίδων Δ. Ψυχομάνης, *Εγχειρίδιο Τραπεζικού Δικαίου*, 2η εκδ. (repr., Αθήνα, Θεσσαλονίκη: Εκδόσεις Σάκκουλα, 2016), 356-357.

[334] Πρβλ. ΑΠ 1352/2011: «*Ειδικότερα οι Τράπεζες, ως χρηματοδοτικοί οργανισμοί που ασκούν αποφασιστική επίδραση στην ανάπτυξη και στη λειτουργία των χρηματοδοτούμενων απ' αυτές επιχειρήσεων, έχουν αυξημένη ευθύνη κατά την άσκηση του χρηματοδοτικού τους έργου και οφείλουν να μεριμνούν για τα συμφέροντα των επιχειρήσεων που χρηματοδοτούν, αφού από τη φύση της η πιστωτική σχέση, ως διαρκής έννομη σχέση ιδιαίτερης εμπιστοσύνης μεταξύ των συμβαλλομένων, επιβάλλει την υποχρέωση πίστης και προστασίας από την πλευρά των τραπεζών των συμφερόντων των πελατών τους, ώστε να αποφεύγονται υπέρμετρα επαχθείς γι' αυτούς συνέπειες*». Αντιστοίχως και ΕφΑθ 1403/2015, ΤΝΠ ΝΟΜΟΣ, ΕφΛαμ 27/2013 ΤΝΠ ΝΟΜΟΣ.

γενικότερης θέσης των τραπεζών στο χρηματοοικονομικό σύστημα.[335] Παράλληλα, η αναγνώριση τω υποχρεώσεων προνοίας και προστασίας εκ μέρους των τραπεζικών ιδρυμάτων για τον πελάτη έχει ως αφετηρία τη διαπίστωση ότι η καλή πίστη επιβάλλει σε κάθε συμβαλλόμενο να λαμβάνει υπόψιν, κατά την εξέλιξη της συμβατικής σχέσεως, τα εύλογα συμφέροντα του αντισυμβαλλόμενού του, ενώ φροντίζει για την εξυπηρέτηση των δικών του συμφερόντων. Η θέση αυτή δεν οδηγεί όμως στο συμπέρασμα ότι η τράπεζα θα πρέπει να προτάσσει το συμφέρον του πελάτη της εφόσον αυτό μπορεί να οδηγήσει σε ζημία των δικών της συμφερόντων. Συνεπώς, η τράπεζα μπορεί να επιλέξει να μην εισέλθει σε συναλλακτική σχέση με κάποιον πελάτη που παρουσιάζει μειωμένη αφερεγγυότητα[336] ή να αποφασίσει να χρηματοδοτήσει συγκεκριμένους τομείς της οικονομίας ή να χρηματοδοτήσει επενδύσεις που λαμβάνουν χώρα σε συγκεκριμένες γεωγραφικές περιοχές.[337] Παράλληλα, η ανάληψη συγκεκριμένων υποχρεώσεων από τις τράπεζες έναντι των πελατών τους, δεν συνεπάγεται συμφωνία ανάληψης μέρους του επιχειρηματικού και εν γένει οικονομικού κινδύνου από την δράση των τελευταίων. Η έμμεση μετάθεση του εν λόγω κινδύνου χάρη στην ευρεία θεμελίωση υποχρεώσεων προνοίας έναντι του πελάτη, μπορεί να οδηγήσει σε αλλοίωση της συμβατικής τους σχέσης αλλά και στη μομφή της άνισης μεταχειρίσεως μεταξύ των πελατών, εφόσον αλλοιώνονται ή αδρανούν οι αξιώσεις της τράπεζας έναντι ορισμένων μόνον εξ 'αυτών με βάση το κριτήριο της οικονομικής δυσχέρειάς τους.[338] Η αρχή της καλής πίστης και τα χρηστά ήθη μπορούν ωστόσο, να επιβάλλου επιμέρους υποχρεώσεις προστασίας, που θεωρείται ότι εντάσσονται στην υποχρέωση προνοίας. Μια από αυτές αφορά την επιβολή σύναψης συναλλακτικών σχέσεων με κάποιον πελάτη ή τη μη διακοπή υφιστάμενων, όταν έχει προκληθεί εμπιστοσύνη ως προς την συνέχιση της χρηματοδοτήσεως ή ως προς την ρύθμιση των οφειλών του.[339] Στην περίπτωση αυτή, για να υποχρεώνεται η τράπεζα σε ανοχή, θα πρέπει να λαμβάνονται υπόψιν ιδιαίτερες περιστάσεις, όπως η ένταση και η διάρκεια της σχέσεως εμπιστοσύνης που συνδέει τον οφειλέτη με την τράπεζα, το ύψος της επαπειλούμενης ζημίας του οφειλέτη που μπορεί να προέλθει από την διακοπή της χρηματοδότησης, το μέγεθος της

---

[335] Πρβλ. ΑΠ 1717/2012: «*Ακόμη οι τράπεζες εν γένει, αφού η δραστηριότητα τους αντανακλά ευθέως στην εθνική οικονομία, έχουν απέναντι στους πελάτες τους υποχρέωση να προστατεύουν τα περιουσιακά αγαθά τους όπως απαιτεί η καλή πίστη και τα συναλλακτικά ήθη σύμφωνα με το άρθρο 288 ΑΚ*». Αντιστοίχως και ΕφΘεσ 76/2009 Αρμ. 2009, 868, ΠΠρΑθ 437/2012 ΤΝΠ ΝΟΜΟΣ.

[336] Αυτό προκύπτει και από την Οδηγία 2008/48/ΕΚ περί υπεύθυνου δανεισμού σε συμβάσεις καταναλωτικής πίστης, η οποία ενσωματώθηκε στο ελληνικό δίκαιο με την ΚΥΑ αριθ. Ζ1-699/2010, η οποία στο άρθρο 8 προβλέπει ότι: «*Πριν από τη σύναψη της σύμβασης πίστωσης, ο πιστωτικός φορέας, ερευνά και αξιολογεί την πιστοληπτική ικανότητα και φερεγγυότητα του καταναλωτή, βάσει επαρκών στοιχείων που λαμβάνονται κατά περίπτωση από τον καταναλωτή κατά το προσυμβατικό στάδιο αλλά και εκείνων που έχει παράσχει κατά τη διάρκεια μακροχρόνιας συναλλακτικής σχέσης, και κατόπιν έρευνας στην κατάλληλη βάση δεδομένων, σύμφωνα με τις ειδικότερες διατάξεις για την εποπτεία των πιστωτικών και χρηματοδοτικών ιδρυμάτων*».

[337] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 11.

[338] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 73.

[339]Πρβλ. ΑΠ 1352/2011: «Έτσι σε περίπτωση δυσχέρειας του πιστούχου της Τράπεζας να ανταποκριθεί στις υποχρεώσεις του από την πιστωτική σύμβαση λόγω πρόσκαιρης οικονομικής αδυναμίας του, που όμως υπερβαίνει τα όρια της αντοχής του, η καλόπιστη από την πλευρά της Τράπεζας συμπεριφορά επιβάλλει σ' αυτή την υποχρέωση να ανεχθεί μια εύλογη καθυστέρηση στην εκπλήρωση της παροχής του οφειλέτη, ιδίως όταν η επιδίωξη της άμεσης εκπλήρωσης της παροχής του πρόκειται να οδηγήσει σε πλήρη οικονομική καταστροφή του, χωρίς ουσιαστικό κέρδος για την ίδια. Κατά την έννοια αυτή η Τράπεζα θα πρέπει, σε περίπτωση πρόσκαιρης οικονομικής αδυναμίας του πελάτη της, να αποφύγει την εσπευσμένη καταγγελία της μεταξύ τους πιστωτικής σύμβασης και το κλείσιμο του αλληλόχρεου λογαριασμού τους, προπάντων όταν οι απαιτήσεις της είναι ασφαλισμένες με εμπράγματες ή προσωπικές ασφάλειες, ο δε πελάτης της βρίσκεται σε άμεση οικονομική εξάρτηση απ' αυτή και δεν οφείλει σε τρίτους, αφού τότε οι παραπάνω ενέργειές της προσλαμβάνουν καταχρηστικό χαρακτήρα».

επιβάρυνσης της τράπεζας σε περίπτωση που ληφθεί απόφαση να συνεχιστεί η χρηματοδότηση, η ύπαρξη επαρκών ασφαλειών κ.α. Επομένως, πρόκειται για συνεκτίμηση ανά περίπτωση των εύλογων συμφερόντων του οφειλέτη, και όχι για καθιέρωση γενικής υποχρέωσης προς διάσωσή του. [340] Τέλος, δεν μπορεί να γίνει δεκτή υποχρέωση της τράπεζας προς χορήγηση πιστώσεως προς κάθε ενδιαφερόμενο, καθώς αυτό θα οδηγούσε σε σύναψη αναγκαστικής συμβάσεως και θα περιοριζόταν η οικονομική ελευθερία των πιστωτικών ιδρυμάτων.

Περαιτέρω, θα πρέπει να εξεταστεί πως μεταφέρεται η αρχή της ισότητας και της ίσης μεταχειρίσεως στο πλαίσιο των τραπεζικών συναλλαγών και με ποιο τρόπο επηρεάζει τη συμβατική σχέση ανάμεσα σε τράπεζες και τους πελάτες-καταναλωτές. Είναι κοινώς αποδεκτό ότι η συνταγματικά κατοχυρωμένη αρχή της ισότητας επιδρά και στις σχέσεις ιδιωτικού δικαίου. Συγκεκριμένα, σύμφωνα με το άρθρο 25 παρ. 1 εδ. γ' του Συντάγματος, τα θεμελιώδη δικαιώματα «ισχύουν και στις σχέσεις μεταξύ ιδιωτών στις οποίες προσιδιάζουν». Επομένως, είτε πρόκειται για άμεση ισχύ των συνταγματικών διατάξεων, είτε για τριτενέργεια στις ιδιωτικές έννομες σχέσεις, η ερμηνεία των διατάξεων του ιδιωτικού δικαίου ανάγεται και στις συνταγματικές αξιολογήσεις. Το ζήτημα της ίσης μεταχειρίσεως των πελατών μιας τράπεζας προκύπτει όταν συντρέχει περίπτωση σύμφωνα με την οποία η τράπεζα αρνείται να συνάψει σύμβαση, την οποία έχει ήδη προσφέρει στο κοινό και έχει ήδη συνάψει με άλλους πελάτες της. Επιπροσθέτως, το ζήτημα δύναται να ανακύψει και στην περίπτωση που η τράπεζα αρνηθεί να αναδιαρθρώσει τον δανεισμό οφειλέτη της, ενώ το έχει πράξει για άμεσους ανταγωνιστές του. Αυτό που ενδιαφέρει σε αμφότερες τις περιπτώσεις είναι η θεμελίωση της ευθύνης της τράπεζας έναντι του μελλοντικού ή υφιστάμενου πελάτη, με έρεισμα το χαρακτηρισμό της άνισης αυτής μεταχειρίσεως ως παράνομης ή ως παραβιάζουσας παρεπόμενη υποχρέωση που προκύπτει από την ισχύουσα σύμβαση συμπεριφοράς.[341]

Το εύρος των εργασιών που αναλαμβάνει μια τράπεζα αλλά και η πληθώρα πελατών που παρουσιάζουν ιδιαίτερα χαρακτηριστικά ως προς τις συναλλαγές τους με αυτήν, καθιστούν δύσκολη και περίπλοκη την εφαρμογή της αρχής της ίσης μεταχειρίσεως. Η διαφορετικότητα ανάμεσα στους πελάτες είναι τόσο καταλυτική που μπορεί να γίνει λόγος για ίση μεταχείριση μόνο μεταξύ καταστάσεων τόσο «συγγενών» ώστε η ίση αυτή μεταχείριση να επιβάλλεται από τη φύση του πράγματος, δηλαδή από την προαναφερθείσα «συγγένεια». Η απόλυτη ταύτιση όμως είναι πρακτικά αδύνατη καθώς η βιοτική και συναλλακτική πραγματικότητα αποκλείουν την εν λόγω ταυτότητα. Η εφαρμογή της αρχής θα ήταν εύκολη αν αντιμετωπίζαμε την υποθετική περίπτωση δύο οφειλετών που είχαν συνάψει το ίδιο είδος συμβάσεως, ίδιου ποσού, ίδιου επιτοκίου, ίδιας διάρκειας, ίδιων εξασφαλίσεων κ.λπ. Στην περίπτωση αυτή, θα έπρεπε αναγκαστικά να γίνει εφαρμογή της αρχής της ίσης μεταχειρίσεως. Σε κάθε περίπτωση, εάν η διαφοροποίηση αφορά σε ιδιότητες και χαρακτηριστικά που κρίνονται ως άσχετα με την υπό εξέταση συναλλαγή, τότε δεν μπορούμε να θεωρήσουμε ότι υπάρχει διαφοροποίηση ανάμεσα στις δύο.[342] Σε περιπτώσεις όμως που η τράπεζα θα πρέπει να σταθμίσει οικονομικά συμφέροντα και

---

[340] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 74.
[341] Ibid., 75.
[342] Αυτό αποτελεί και ρητή νομοθετική επιταγή, σύμφωνα με το άρθρο 3 παρ. 2 του νόμου 4443/2016 (Ενσωμάτωση της Οδηγίας 2000/43/ΕΚ περί εφαρμογής της αρχής της ίσης μεταχείρισης προσώπων ασχέτως φυλετικής ή εθνοτικής τους καταγωγής), που προβλέπει ότι: *«η αρχή της ίσης μεταχείρισης ανεξαρτήτως φυλής, χρώματος, εθνικής ή εθνοτικής καταγωγής, γενεαλογικών καταβολών, θρησκευτικών*

κοινωνικά κριτήρια, όπως συμβαίνει όταν η τράπεζα καλείται να αποφασίσει εάν θα διασώσει μια επιχείρηση που απασχολεί πέντε εργαζομένους ή την ανταγωνίστριά της που απασχολεί εκατό ή όταν ένας πελάτης υπέπεσε για πρώτη φορά σε παράβαση των συμβατικών του υποχρεώσεων ενώ ο άλλος σε περισσότερες, η τελική απάντηση θα πρέπει να δοθεί από τον δικαστή. Η κρίση του τελευταίου θα πρέπει να είναι ειδικά αιτιολογημένη και να αναφέρεται στα ειδικά περιστατικά της υπό κρίση περιπτώσεως ενώ παράλληλα δεν θα πρέπει να περιορίζεται σε μια γενική αναφορά στην προς εφαρμογή διάταξη. Ακόμα και αν οι υπό κρίση περιπτώσεις παρουσιάζουν επαρκή ομοιότητα, αν τίθεται ζήτημα προγνώσεως που αφορά την βιωσιμότητα μιας επιχείρησης, θα πρέπει να δίνεται διακριτική ευχέρεια στην τράπεζα ώστε να προβεί σε διαφοροποίηση των πελατών της εφόσον αυτή δεν αντιβαίνει στα χρηστά ήθη ή έχει παράνομο χαρακτήρα. Θα πρέπει σε κάθε περίπτωση να ληφθεί υπόψη ότι οι τράπεζες στοχεύουν πάντοτε στη μεγιστοποίηση του κέρδους τους και στην αποτροπή ή τον περιορισμό της ζημίας τους και επομένως το ζήτημα που αφορά την ίση μεταχείριση των πελατών θα πρέπει να εξετάζεται με βάση τα δεδομένα αυτά.

3.4.1 Οι υποχρεώσεις ενημερώσεως και πληροφορήσεως των τραπεζικών ιδρυμάτων έναντι των πελατών τους

Τα τραπεζικά ιδρύματα, στο πλαίσιο των συναλλακτικών τους σχέσεων με τους πελάτες τους, αναλαμβάνουν επίσης την υποχρέωση για προσήκουσα ενημέρωση και διαφώτισή τους, καθώς και για την παροχή πληροφοριών και συμβουλών που σχετίζονται με τις επιμέρους συναλλαγές τους μαζί τους. Οι υποχρεώσεις αυτές αποτελούν συνήθως απόρροια της πληροφοριακής και γνωστικής ασυμμετρίας που χαρακτηρίζει την σχέση τράπεζας και πελάτη. Η ασυμμετρία αυτή παρουσιάζει διαφοροποιήσεις ανάλογα με το είδος της συναλλαγής, των χαρακτηριστικών του κάθε πελάτη και άλλων ειδικών περιστάσεων. Επομένως, δεν μπορεί να καθιερωθεί μια γενική υποχρέωση των τραπεζών προς διαφώτιση των πελατών τους, αλλά η γέννηση και η έκταση της εν λόγω υποχρέωσης θα πρέπει να εξετάζεται κατά περίπτωση.[343]

Με βάση την ανωτέρω υποχρέωση, η τράπεζα αναλαμβάνει να ενημερώνει και να πληροφορεί τον πελάτη της για σημαντικά περιστατικά που αξιολογεί ως κρίσιμα για την λήψη αποφάσεων εκ μέρους του, ώστε να εξελίσσεται ομαλά και με βάση τα συμφέροντα του πελάτη η μεταξύ τους σχέση. Ωστόσο, η υποχρέωση αυτή οριοθετείται από την ανάγκη επιδιώξεως των συμφερόντων της τράπεζας, τα οποία δεν μπορεί να αξιωθεί να θυσιάσει προς όφελος των πελατών της. Επίσης, η τράπεζα καλείται να διαφυλάξει και τα συμφέροντα των υπολοίπων πελατών της, τα οποία μπορεί να συγκρούονται με τα συμφέροντα του υπό εξέταση εκάστοτε πελάτη. Κατά κανόνα η διοχέτευση (δυσμενών) πληροφοριών που η τράπεζα γνωρίζει για ορισμένους πελάτες, μπορεί να προσκρούει στην υποχρέωση εχεμύθειας που αυτή υπέχει απέναντί τους και στο γενικό τραπεζικό απόρρητο.[344] Συνάγεται επομένως το συμπέρασμα ότι η το πρόβλημα δεν είναι η θεμελίωση των υποχρεώσεων ενημερώσεως και πληροφορήσεως των πελατών εκ μέρους της τράπεζας, αλλά η

ή άλλων πεποιθήσεων, αναπηρίας ή χρόνιας πάθησης, ηλικίας, οικογενειακής ή κοινωνικής κατάστασης, σεξουαλικού προσανατολισμού, ταυτότητας ή χαρακτηριστικών φύλου στον τομέα της εργασίας και της απασχόλησης, εφαρμόζεται σε όλα τα πρόσωπα, στο δημόσιο και τον ιδιωτικό τομέα».

[343] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 99.

[344] Ωστόσο γίνεται αποδεκτή η υποχρέωση της τράπεζας να πληροφορήσει τον πελάτη της ότι ο λήπτης εμβάσματος έχει περιέλθει σε κατάσταση παύσεως πληρωμών [Νικόλαος Κ. Ρόκας et al., *Στοιχεία Τραπεζικού Δικαίου*, 3η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2016), 480-481.]

οριοθέτησή τους, ενόψει της σύγκρουσης συμφερόντων της τράπεζας, του πελάτη και των τρίτων. Επιπροσθέτως, η υποχρέωση ενημέρωσης, πληροφόρησης και παροχής συμβουλών δεν συνιστούν πάντα αντικείμενο παρεπόμενης υποχρέωσης της τράπεζας που συνάγεται από την καλή πίστη. Πολλές φορές αποτελούν πρωτογενή συμβατική υποχρέωση της τράπεζας που πηγάζει από συναφή σύμβαση, ή αποτελούν υποχρεώσεις που επιβάλλονται στην τράπεζα και πηγάζουν από ειδικές νομοθετικές ή κανονιστικές διατάξεις ή από την καλή πίστη.

Παράδειγμα περίπτωσης που η παροχή πληροφοριών ή συμβουλών προβλέπεται ως πρωτογενής ή κύρια υποχρέωση της τράπεζας, αποτελεί η παροχή συμβουλών και πληροφοριών που προβλέπεται στο άρθρο 11 παρ. 1 του νόμου 4261/2014[345]. Ειδικότερα, η περίπτωση θ' αναφέρει ως τραπεζική εργασία την «παροχή συμβουλών σε επιχειρήσεις όσον αφορά τη διάρθρωση του κεφαλαίου, τη βιομηχανική στρατηγική και συναφή θέματα παροχής συμβουλών, καθώς και υπηρεσιών στον τομέα της συγχώνευσης και της εξαγοράς επιχειρήσεων», η περίπτωση ια' την «διαχείριση χαρτοφυλακίου ή παροχή συμβουλών για τη διαχείριση χαρτοφυλακίου» και η περίπτωση ιγ' την «συλλογή και επεξεργασία εμπορικών πληροφοριών, περιλαμβανομένων και των υπηρεσιών αξιολόγησης πιστοληπτικής ικανότητας πελατών». Στις περιπτώσεις αυτές, οι εν λόγω πληροφορίες ή συμβουλές δεν θα σχετίζονται, ως παρεπόμενο στοιχείο, με συγκεκριμένη συναλλαγή που ο πελάτης επιδιώκει να συνάψει με την τράπεζα, αλλά θα αποτελούν αυτοτελές «οικονομικό αγαθό», το οποίο ο εκάστοτε πελάτης επιδιώκει να αποκτήσει από την τράπεζα.

Στη σύμβαση αυτή θα προβλέπεται λεπτομερώς, το περιεχόμενο, η έκταση και ο τρόπος με τον οποίο θα εκπληρωθεί η παροχή, δηλαδή θα προβλέπεται η παροχή συγκεκριμένων πληροφοριών και συμβουλών, μέσω της τήρησης ειδικής διαδικασίας.[346] Η μη εκπλήρωση ή η πλημμελής εκπλήρωση των υποχρεώσεων που προβλέπονται στους συμβατικούς όρους, συνιστά αθέτηση πρωτογενούς υποχρεώσεως της τράπεζας και συνεπάγεται αξίωση προς εκπλήρωση, σε αντίθεση με την αθέτηση παρεπόμενων υποχρεώσεων που στοιχειοθετούν υποχρέωση προς αποζημίωση εφόσον παραβιασθούν.[347] Σε περίπτωση που η τράπεζα δεν παράσχει τις αιτούμενες πληροφορίες, θα μπορεί να εξαναγκασθεί ως προς αυτό, εάν το επιθυμεί ο πελάτης. Ο πελάτης με τη σειρά του θα έχει τη δυνατότητα να προβάλλει την ένσταση μη εκπληρωθέντος συναλλάγματος (ΑΚ 374), και θα διατηρεί και τα δικαιώματά του από την ανώμαλη εξέλιξη της αμφοτεροβαρούς συμβάσεως με την τράπεζα (ΑΚ 380), που θα εκτείνονται μέχρι την καταγγελία της συμβάσεως παροχής πληροφοριών ή συμβουλών.[348]

Η υποχρέωση πληροφορήσεως και ενημερώσεως του πελάτη ανακύπτει κυρίως σε περιπτώσεις που παρατηρείται πληροφοριακή ασυμμετρία ανάμεσα σε τράπεζα και πελάτη, δηλαδή σε περιπτώσεις που υπάρχει ανισότητα πληροφορήσεως ανάμεσα σε τράπεζα και πελάτη που οφείλεται σε έλλειψη εξειδικευμένων γνώσεων. Η ίδια υποχρέωση υπάρχει και όταν η τράπεζα

---

[345]Νόμος 4261/2014, Πρόσβαση στη δραστηριότητα των πιστωτικών ιδρυμάτων και προληπτική εποπτεία πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων (ενσωμάτωση της Οδηγίας 2013/36/ΕΕ), κατάργηση του ν. 3601/2007 και άλλες διατάξεις. Διαθέσιμος στην ιστοσελίδα: https://www.bankofgreece.gr/RelatedDocuments/N.%204261_2014%20CRD%20IV.pdf

[346] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 101.

[347] Μιχαήλ Σταθόπουλος, *Γενικό Ενοχικό Δίκαιο*, 4η εκδ. (repr., Αθήνα-Κομοτηνή: Εκδόσεις Σάκκουλα, 2004), 39,42.

[348] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 101.

γνωρίζει ότι το πρόσωπο υπέρ του οποίου δίνει εντολή πληρωμής ο πελάτης βρίσκεται σε κατάσταση πτώχευσης.[349]Η ανάγκη ενημερώσεως του πελάτη κρίνεται ανάλογα με τις ιδιαιτερότητες κάθε περίπτωσης, ενώ η νομολογία στον ελληνικό χώρο δέχεται ότι υφίσταται υποχρέωση ενημερώσεως λόγω συνδρομής περιστάσεων που είναι γνωστές στην τράπεζα, τις οποίες όμως ο πελάτης δεν είναι ευλόγως δυνατό να γνωρίζει.[350] Κριτήρια για την οριοθέτηση της υποχρέωσης καθοδήγησης και διαφώτισης των πελατών αποτελούν: α) το πρόσωπο του αντισυμβαλλομένου (επίπεδο γνώσεων, ηλικία, επάγγελμα, οικογενειακή, οικονομική, περιουσιακή κατάσταση), β) η συμπεριφορά του αν μέσω αυτής έχει υποδηλώσει ότι διαθέτει την εμπειρία και τις γνώσεις για την εκάστοτε συναλλαγή (π.χ. έμπορος με πολυετή δραστηριότητα), γ) το αντικείμενο της συναλλαγής ειδικά αν πρόκειται για συναλλαγές που ενέχουν κίνδυνο για τον πελάτη[351] (πιστωτικές συναλλαγές και παροχές επενδυτικών συμβουλών), δ) η διάρκεια και η ένταση στη σχέση ανάμεσα στον πελάτη και την τράπεζα, ε) η στάθμιση συμφερόντων του πελάτη με τα αντίστοιχα της τράπεζας, ειδικά σε περιπτώσεις που παρατηρείται σύγκρουση της υποχρεώσεως της τράπεζας προς ενημέρωση και διαφώτιση με υποχρεώσεις της προς άλλους πελάτες (υποχρέωση εχεμύθειας[352]). Στην περίπτωση αυτή θα πρέπει να δίνεται προτεραιότητα στο εννόμως προστατευόμενο συμφέρον του πελάτη προς τήρηση εχεμύθειας.[353]

3.4.1.1 Οι υποχρεώσεις ενημερώσεως και πληροφορήσεως των τραπεζικών ιδρυμάτων βάσει της ΠΔΤΕ 2501/2002

Η Πράξη του Διοικητή της Τράπεζας της Ελλάδος 2501/31.10.2002 (ΦΕΚ Α΄ 277/18.11.2002, «Ενημέρωση των συναλλασσομένων με τα πιστωτικά ιδρύματα[354] για τους όρους που διέπουν τις συναλλαγές τους»), όπως ισχύει έπειτα από την τροποποίησή της[355], αποτελεί το νομοθέτημα μέσω του οποίου θεσπίζεται το γενικό πλαίσιο της ενημέρωσης των αντισυμβαλλομένων των τραπεζών σε σχέση με τις συναλλαγές τους. Μέσω της πράξης ρυθμίζεται τόσο το αντικείμενο της αναγκαίας ενημερώσεως, ανάλογα με τον τύπο της συναλλαγής που αφορά, όσο και ο τρόπος εκπλήρωσης των σχετικών υποχρεώσεων ενημερώσεως και πληροφορήσεως. Στο πρώτο κεφάλαιο της πράξεως καθορίζονται οι γενικές αρχές που διέπουν την υποχρέωση ενημερώσεως εκ μέρους των πιστωτικών ιδρυμάτων. Συγκεκριμένα, ορίζεται ότι

---

[349] Βλ. απόφ. Εφετείου Κολωνίας της 24.03.04, WM 2005, 557.

[350] Πρβλ. ΠΠρΑθ 2087/2004 ΕΕμΔ 2005, 777 (αφορά την παράλειψη τράπεζας να καθοδηγήσει τον πελάτη της για τον τρόπο μέσω του οποίου θα μπορούσε να εξαρτήσει την πληρωμή εμβάσματος στην αλλοδαπή από την προσκόμιση εγγυητικής επιστολής), ΕφΑθ 1403/2015 ΤΝΠ ΝΟΜΟΣ (ύπαρξη ασφαλιστικής κάλυψης για το χρεωστικό υπόλοιπο πιστωτικών καρτών σε περίπτωση θανάτου του δικαιούχου).

[351] Σε αυτού του είδους τις κινδυνώδεις συναλλαγές στόχος της ενημέρωσης είναι η συνειδητοποίηση του κινδύνου που αναλαμβάνει ο πελάτης μέσω της διενέργειας της συναλλαγής. Πρβλ. ΑΠ 244/2016 ΤΝΠ ΝΟΜΟΣ και 1738/2013 ΤΝΠ ΝΟΜΟΣ.

[352] Πρβλ. ΑΠ 1727/2008, ΕΕμπΔ 2009, 620 (Στην περίπτωση αυτή η τράπεζα όφειλε να ενημερώσει τον πελάτη Α ότι δεν είναι δυνατή η επέμβαση της σε λογαριασμό του πελάτη Β προς εξόφληση του Α), ΑΠ 820/2002 ΔΕΕ 2002, 1262 (Στοιχειοθετεί υποχρέωση της πληρώτριας τράπεζας να ενημερώσει τον κομιστή επιταγής, την οποία εμφανίζει προκειμένου να διαπιστώσει αν μπορεί να πληρωθεί, ότι η επιταγή έχει αποτελέσει αντικείμενο κλοπής, σύμφωνα με πληροφόρηση του εκδότη προς την τράπεζα).

[353] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 110-111.

[354] Σύμφωνα με τη διάταξη του κεφαλαίου IV της ΠΔ/ΤΕ 2622/2009, οι υποχρεώσεις που καθορίζονται στην ΠΔ/ΤΕ 2501/2002, ισχύουν αναλόγως και για τις εταιρείες χρηματοδοτικής μισθώσεως, για τις Α.Ε παροχής πιστώσεων και για τις εταιρείες πρακτορείας επιχειρηματικών απαιτήσεων.

[355] Υπ' αριθμ. 234/11.12.2006 απόφαση της ΕΤΠΘ «Τροποποίηση και συμπλήρωση της ΠΔ/ΤΕ 2501/31.10.2002 και της απόφασης ΕΤΠΘ 178/3/19.07.2004», http://www.bankofgreece.gr/Pages/el/Bank/LegalF/Acts.aspx

τα πιστωτικά ιδρύματα πρέπει να ενημερώνουν τους συναλλασσομένους σχετικά με τη φύση και τα χαρακτηριστικά των προσφερόμενων υπηρεσιών αλλά και για τους όρους και τις προϋποθέσεις που διέπουν τις τραπεζικές συναλλαγές. Καθορίζεται επίσης η διάθεση ειδικής υπηρεσιακής μονάδας για την εξέταση παραπόνων ή καταγγελιών των πελατών και καθιερώνεται η υποχρέωση των τραπεζικών ιδρυμάτων να ανταποκρίνονται εντός ευλόγου χρονικού διαστήματος στα αιτήματα των συναλλασσομένων.

Στο δεύτερο κεφάλαιο προβλέπεται το κατά νόμον αναγκαίο περιεχόμενο της προσυμβατικής ενημερώσεως, ανάλογα με την κατηγορία των συναλλαγών. Πρόκειται για στοιχεία και πληροφορίες που τα πιστωτικά ιδρύματα οφείλουν να παρέχουν στους πελάτες[356], ώστε να σχηματίζουν πριν τη σύναψη των συμβάσεων σαφή εικόνα σχετικά με τις παρεχόμενες υπηρεσίες και τα προϊόντα. Η συγκεκριμένη προσυμβατική ενημέρωση διαρθρώνεται ανά τύπο σκοπούμενης συναλλαγής (καταθέσεις, χορηγήσεις, λοιπές εργασίες, πιστωτικές κάρτες, παράγωγα προϊόντα). Αναφορικά με τη διαδικασία ή τη μορφή παροχής των πληροφοριών δεν προβλέπεται συγκεκριμένη διαδικασία. Η ρύθμιση πάντως κρίνεται λεπτομερής, καθώς στην Πράξη περιλαμβάνονται εκτενής κατάλογοι με τις κατηγορίες των πληροφοριών που πρέπει να παρέχονται. Ειδικότερα, αναφέρεται εν προκειμένω ότι οι πληροφορίες για τις καταθέσεις περιλαμβάνουν, το ύψος του επιτοκίου ή των επιτοκίων που εφαρμόζονται ανάλογα με τη διάρκεια ή το ποσό κατάθεσης, το χρόνο έναρξης ή λήξης της τοκοφορίας, την χρονική βάση υπολογισμού των τόκων, τις ημερομηνίες λογισμού των τόκων κ.ο.κ. Αναφορικά με τα παράγωγα προϊόντα «Τα πιστωτικά ιδρύματα ενημερώνουν για τα βασικά χαρακτηριστικά των παραγώγων προϊόντων που διαθέτουν για ίδιο λογαριασμό ή για λογαριασμό τρίτων, θέτοντας στη διάθεση των συναλλασσομένων την αναγκαία πληροφόρηση για την κατανόηση του οφέλους και των κινδύνων που αναλαμβάνουν και των πιθανών ζημιογόνων επιπτώσεων από την αιφνίδια μεταβολή της αξίας τους, είτε ως μεμονωμένων πράξεων είτε σε συνδυασμό με άλλες (π.χ. χορήγηση συμπληρωματικής πίστωσης για την εκπλήρωση αναληφθεισών υποχρεώσεων)».

Το τρίτο κεφάλαιο της ΠΔ/ΤΕ ρυθμίζει τον τρόπο ενημέρωσης των πελατών, ενώ ειδική ρύθμιση προβλέπεται για την δέουσα πληροφόρηση για συναλλαγές που διενεργούνται μέσω διαδικτύου. Αρχικά (Γ,1), προβλέπεται γενική ενημέρωση όλων των συναλλασσομένων για την φύση και τα χαρακτηριστικά των προσφερόμενων προϊόντων και υπηρεσιών και για τους όρους που διέπουν τις αντίστοιχες συναλλαγές (βασικά επιτόκια, προμήθειες, αμοιβές, εφάπαξ δαπάνες). Η ενημέρωση αυτή συντελείται μέσω ενημερωτικών φυλλαδίων ή μέσω γνωστοποίησης δια του τύπου, αλλά κυρίως με την ανάρτηση στους χώρους συναλλαγών πινάκων. Κατά την εξέλιξη της συμβατικής σχέσεως, η ΠΔ/ΤΕ επιβάλλει για τις καταθέσεις και τις χορηγήσεις δύο τύπους υποχρεώσεων ενημερώσεως. Αρχικά το πιστωτικό ίδρυμα υπόκειται σε υποχρέωση περιοδικής (τουλάχιστον ανά τρίμηνο) ενημερώσεως[357], χωρίς να έχει προηγηθεί υποβολή σχετικού αιτήματος από τον πελάτη, για συγκεκριμένα προβλεπόμενα στην πράξη στοιχεία (Γ,2,α-β), όπως στοιχεία που αφορούν το ύψος των επιτοκίων και τις τυχόν επιβαρύνσεις για τις καταθέσεις, την εξέλιξη των ληξιπρόθεσμων οφειλών, των τόκων και λοιπών επιβαρύνσεων, καθώς και στοιχεία

[356] Πρβλ. ΕφΠειρ 329/2021, (οι ενάγοντες δεν ενημερώθηκαν σχετικά από υπαλλήλους της τράπεζας ότι με τις συμβάσεις στεγαστικών δανείων σε ελβετικό φράγκο, αναλάμβαναν εκτός από τον κίνδυνο του κυμαινόμενου επιτοκίου και τον κίνδυνο διακύμανσης της συναλλαγματικής ισοτιμίας). http://www.efeteio-peir.gr/wordpress/?p=7549.

[357] Βλ. διευκρίνιση αποφ. ΕΤΠΘ 178/3/2004 παρ. 4.

που αφορούν κάθε μεταβολή του επιτοκίου για τις χορηγήσεις. Επιπροσθέτως, το πιστωτικό ίδρυμα υποχρεούται να χορηγεί, κατόπιν αιτήματος των πελατών (Γ,3,α), «πληροφορίες που ενδεχομένως δεν καλύπτονται από την περιοδική τους ενημέρωση σύμφωνα με τις διατάξεις της παρούσας εντός ευλόγου χρονικού διαστήματος, ανάλογα με τον απαιτούμενο βαθμό έρευνας για την παροχή των πληροφοριών».

3.4.1.2 Οι υποχρεώσεις ενημερώσεως και πληροφορήσεως των τραπεζικών ιδρυμάτων βάσει διατάξεων για συγκεκριμένες κατηγορίες συναλλαγών

Πέρα από τις υποχρεώσεις που επιβάλλονται μέσω της γενικής ρυθμίσεως της ΠΔ/ΤΕ 2501/2002, ειδικότερες διατάξεις, που κατά κανόνα ενσωματώνουν κανόνες ενωσιακής προελεύσεως, θεσπίζουν επί μέρους υποχρεώσεις ενημερώσεως και πληροφορήσεως για συγκεκριμένες κατηγορίες συναλλαγών. Αρχικά θα πρέπει να γίνει αναφορά στην ΚΥΑ Ζ1-669/23.6.2010 (ΦΕΚ 917/Β/23-6-2010**)**, που διέπει τις συμβάσεις καταναλωτικής πίστεως και ενσωματώνει στο ελληνικό δίκαιο την Οδηγία 2008/48/ΕΚ.[358] Στο δεύτερο κεφάλαιο (άρθρο 4 επ.), προβλέπονται τυποποιημένες πληροφορίες που πρέπει να περιλαμβάνονται στις διαφημίσεις αλλά και στοιχεία που πρέπει να παρέχονται από το πιστωτικό ίδρυμα στον πελάτη του πριν από τη σύναψη της συμβάσεως[359], ενώ στο τέταρτο κεφάλαιο (άρθρα 10 επ.) της ΚΥΑ θεσπίζονται υποχρεώσεις παροχής πληροφοριών κατά τη σύναψη και την λειτουργία της συμβατικής σχέσεως.

Θα πρέπει επίσης να γίνει αναφορά στον νόμο 4438/2016[360], ο οποίος ενσωμάτωσε στο ελληνικό δίκαιο την Οδηγία 2014/17/ΕΕ και διέπει τις συμβάσεις πιστώσεως για καταναλωτές και για ακίνητα που προορίζονται για κατοικία. Στο τέταρτο κεφάλαιο (άρθρα 9 επ.), του νόμου γίνεται και πάλι αναφορά σε τυποποιημένες πληροφορίες που πρέπει να περιλαμβάνονται στις διαφημίσεις, καθώς και πληροφορίες που πρέπει να παρέχονται κατά το προσυμβατικό στάδιο. Προβλέπονται επίσης υποχρεώσεις ενημερώσεως κατά τη λειτουργία της συμβάσεως ως προς διάφορα επιμέρους θέματα (π.χ. μεταβολή των επιτοκίων, μεταβολή της ισοτιμίας επί δανείου χορηγηθέντος σε ξένο νόμισμα κ.ο.κ).

Κρίσιμες θεωρούνται και οι διατάξεις του νόμου 2251/1994[361] (άρθρο 4θ[362]) που συνιστά ενσωμάτωση της Οδηγίας 2002/65/ΕΚ και αφορά στην από απόσταση εμπορία χρηματοοικονομικών υπηρεσιών (τραπεζικών, πιστωτικών, ασφαλιστικών, επενδυτικών κ.ο.κ). Η παράγραφος 3 του υπό εξέταση άρθρου ρυθμίζει την πληροφόρηση στην οποία δικαιούται ο καταναλωτής στο προσυμβατικό στάδιο από απόσταση, ενώ προβλέπεται ότι τυχόν πρόσθετες απαιτήσεις πληροφορήσεως θεσπιζόμενες με ειδικές διατάξεις, εξακολουθούν να ισχύουν. Ο νόμος 4538/2018, για τις υπηρεσίες πληρωμών, ενσωματώνει στην ελληνική νομοθεσία την Οδηγία 2015/2366/ΕΕ, προβλέπει στον τίτλο ΙΙΙ (άρθρα 38 επ.) εκτεταμένη υποχρέωση ενημερώσεως των παρόχων υπηρεσιών πληρωμών προς τους χρήστες. Στις υπό εξέταση διατάξεις προβλέπεται ενημέρωση τόσο σε προσυμβατικό στάδιο όσο και μετά την εκτέλεση της πληρωμής

---

[358]Διαθέσιμη στην ιστοσελίδα: https://www.lawspot.gr/nomikes-plirofories/nomothesia/koini-ypoyrgiki-apofasi-z1699-2010.

[359]Ανθή Πελλένη-Παπαγεωργίου, *Ζητήματα Από Τις Νέες Ρυθμίσεις Για Τις Συμβάσεις Καταναλωτικής Πίστης*, 1η εκδ. (repr., Αθήνα: Αντ. Ν. Σάκκουλα, 2012), 191.

[360] Διαθέσιμος στην ιστοσελίδα: https://www.taxheaven.gr/law/4438/2016.

[361]Διαθέσιμος στην ιστοσελίδα: https://www.taxheaven.gr/law/4537/2018.

[362]Όπως τροποποιήθηκε με την παρ. 12 του άρθρου 102 του ν. 4512/2018. https://www.kodiko.gr/nomothesia/document/217614/nomos-2251-1994.

και περιλαμβάνεται ρύθμιση όχι μόνο για το είδος, αλλά και για τον τρόπο και την μορφή της παροχής συγκεκριμένων πληροφοριών. Τέλος, ο νόμος 4514/2018[363] («Αγορές χρηματοπιστωτικών μέσων και άλλες διατάξεις») ενσωματώνει στο ελληνικό δίκαιο την Οδηγία 2014/65/ΕΕ (**MiFID II**) και προβλέπει σχετικά στο άρθρο 24 παρ. 4 ρύθμιση για την επαρκή πληροφόρηση των επενδυτών.

Σε περίπτωση που τα τραπεζικά ιδρύματα παραβιάσουν τις υποχρεώσεις τους σχετικά με την διαφώτιση και την καθοδήγηση των πελατών κατά το στάδιο των διαπραγματεύσεων προς κατάρτιση τραπεζικής συναλλαγής, θα τύχουν εφαρμογής τα άρθρα 197-198 ΑΚ. Με βάση δηλαδή τα άρθρα αυτά θα θεμελιωθεί η κακόπιστη συμπεριφορά της τράπεζας κατά τις διαπραγματεύσεις και θα υποχρεωθεί η τράπεζα να ανορθώσει τη ζημία που υπέστη ο πελάτης λόγω της συμπεριφοράς της αυτής. Πρόκειται για περιπτώσεις στις οποίες οφείλεται αρνητικό διαφέρον, δηλαδή ο πελάτης θα πρέπει να περιέλθει στην κατάσταση στην οποία θα ευρισκόταν αν δεν είχε μεσολαβήσει η αθέτηση των υποχρεώσεων της τράπεζας. Επομένως, στην περίπτωση αυτή διακρίνονται δύο ενδεχόμενα. Στην πρώτη περίπτωση, ο πελάτης δύναται να ζητήσει να περιέλθει στην κατάσταση που θα βρισκόταν εάν δεν είχε προχωρήσει στην κατάρτιση της συμβάσεως, αφού συνυπολογισθούν τυχόν οφέλη, κατά τους γενικούς κανόνες.[364] Στην δεύτερη περίπτωση, ο πελάτης θα έχει δικαίωμα να ζητήσει να περιέλθει στην κατάσταση στην οποία θα βρισκόταν, εάν είχε καταρτίσει τη σύμβαση με άλλους όρους, έπειτα από την προσήκουσα ενημέρωσή του (π.χ. εάν είχε επιλέξει διαφορετικό επιτόκιο ή διαφορετική διάρκεια επί δανειακής σύμβασης). Θα βαρύνεται όμως να αποδείξει ότι και η τράπεζα θα αποδεχόταν να συνάψει την εν λόγω σύμβαση με τους ευμενέστερους για εκείνον όρους.[365]

Εάν η τράπεζα, στο πλαίσιο υφιστάμενης συμβατικής σχέσεως, παραβιάσει τις υποχρεώσεις της προς ενημέρωση, διαφώτιση ή καθοδήγηση του πελάτη της, θα οφείλει να τον αποζημιώσει λόγω πλημμελούς εκπλήρωσης της συμβάσεως. Η αποζημίωση θα υπολογισθεί βάσει της συγκρίσεως της περιουσιακής κατάστασης του πελάτη με την υποθετική περιουσιακή κατάστασή του εάν η τράπεζα είχε εκπληρώσει με προσήκοντα τρόπο τις υποχρεώσεις της. Επιπροσθέτως, εάν η αθέτηση των υποχρεώσεων αυτών έχει επιδράσει με ουσιώδη τρόπο στην συμβατική σχέση του πελάτη με την τράπεζα ή έχει οδηγήσει σε ισχυρό κλονισμό της εμπιστοσύνης του προς αυτήν, ο πελάτης θα έχει επίσης τη δυνατότητα να υπαναχωρήσει ή να καταγγείλει τη σύμβαση.

Σύμφωνα με πάγια νομολογία, η παραβίαση των υποχρεώσεων περί ενημερώσεως και διαφώτισης του πελάτη εκ μέρους της τράπεζας, αποτελεί ενέργεια παράνομη που πληροί το πραγματικό του άρθρου 914 ΑΚ. Σύμφωνα με την απόφαση υπ'αριθ. *1422/2021* του Μονομελούς Πρωτοδικείου Αθηνών, οι τράπεζες οφείλουν να χορηγούν ορθές και σαφείς συμβουλές στους πελάτες τους, ιδίως στην περίπτωση των περίπλοκων και επικίνδυνων επενδυτικών προϊόντων, όπως είναι τα ομόλογα ατελεύτητης διάρκειας («**perpetual bonds**»). Επιπροσθέτως, η υποχρέωση των τραπεζών να πληροφορούν τους πελάτες τους για τα διάφορα επενδυτικά προϊόντα, αλλά και για την απόδοση αυτών και την τυχόν διακινδύνευση του κεφαλαίου που εισφέρεται, συνεκτιμώντας παράγοντες ως προς την παροχή εξειδικευμένων συμβουλών ανά πελάτη, ειδικά αν είναι επαγγελματίας επενδυτής ή μη, γεννούν υποχρέωση αποζημίωσης εις βάρος των τραπεζικών

---

[363] Διαθέσιμος στην ιστοσελίδα: https://www.taxheaven.gr/law/4514/2018.
[364] Καράσης Μαριάνος, "Άρθρα 197-198", σε *Αστικός Κώδικας, Ερμηνεία Κατ' Άρθρον, Τόμος Ιβ, Γενικές Αρχές / Άρθρα 127-286*, 2η εκδ. (repr., Αθήνα: Π.Ν Σάκκουλας, 2016), αρ. 43.
[365] Ibid., αρ. 44.

ιδρυμάτων. Συνεπώς, γεννάται η αδικοπρακτική ευθύνη από την παροχή των επενδυτικών υπηρεσιών. Στο πλαίσιο της συναλλακτικής δραστηριότητας, θα πρέπει να μην παραβιάζεται η γενική υποχρέωση ασφάλειας και ο πάροχος επενδυτικών υπηρεσιών (τράπεζα) οφείλει να προστατεύει τα συμφέροντα των επενδυτών-επενδυτών και να ενημερώνει αυτούς προσηκόντως. Η παράλειψη αυτής της υποχρεώσεως ενημερώσεως, όταν αυτή κρίνεται αναγκαία, συνιστά παράλειψη οφειλόμενης σύμφωνα με την καλή πίστη ενέργειας και ανάγεται σε αδικοπραξία του άρθρου 914 ΑΚ και παράγει υποχρέωση αποζημιώσεως. Επίσης, υφίσταται ευθύνη της τράπεζας βάσει του άρθρου 919 ΑΚ από παροχή επενδυτικών υπηρεσιών, όταν υπάρχει αντίθεση συμπεριφοράς στα χρηστά ήθη και πρόθεση επαγωγής ζημίας, αρκούντος και του ενδεχόμενου δόλου. [366][367]

Μέσω της κατασκευής αυτής, η νομολογία παρακάμπτει το πρόβλημα ότι με την αθέτηση των υποχρεώσεων αυτών προσβάλλεται η περιουσία των πελατών, η οποία δεν έχει αναχθεί σε αντικείμενο προστασίας με τις διατάξεις των αδικοπραξιών.[368] Υπάρχει όμως και το ενδεχόμενο η οφειλόμενη από την τράπεζα αποζημίωση να αποκλεισθεί ή να μειωθεί λόγω συνυπαιτιότητας του πελάτη (ΑΚ 300). Αυτό συμβαίνει διότι η αξιολόγηση της συμπεριφοράς και των ατομικών ιδιοτήτων του κάθε πελάτη ενδιαφέρει σε τρία στάδια. Αρχικά, ως προς τις πληροφορίες που ο πελάτης κατέχει ή οφείλει να κατέχει, δεν γεννάται υποχρέωση διαφωτίσεως από την τράπεζα («αρχή της αυτοευθύνης»). Με βάση την αρχή αυτή κάθε κοινωνός του δικαίου οφείλει να αναλάβει τις συνέπειες για τις πράξεις ή τις παραλήψεις του. Επίσης, οι πελάτες των τραπεζών συχνά προσκομίζουν ελλιπή ή εσφαλμένα προσωπικά στοιχεία. Περαιτέρω, η συμπεριφορά του πελάτη μπορεί να συμβάλει στην γένεση της ζημίας του, όταν προχωράει στη σύναψη συμβάσεως ή αποφασίζει να εκτελέσει μια συναλλαγή, ενώ γνωρίζει ότι δεν έχει κατανοήσει πλήρως τις παραμέτρους αυτής ή δεν είναι επαρκώς ενημερωμένος ως προς αυτήν. Η συνδρομή οικείου πταίσματος μπορεί επίσης να στοιχειοθετηθεί όταν ο πελάτης βασίζεται αποκλειστικά στις πληροφορίες που του παρέχει η τράπεζα και παραλείπει συνειδητά να εξετάσει τα ειδικότερα περιστατικά, αν και του παρέχεται αυτή η δυνατότητα.[369] Τέλος, ο πελάτης ενδέχεται να συμβάλλει στην γένεση ή την έκταση της ζημίας του όταν παραλείπει να περιορίσει τις ζημιογόνες συνέπειες του επιζήμιου αρχικού γεγονότος.[370]

3.5 Οι υποχρεώσεις ελέγχου της προέλευσης των χρημάτων και λοιπών περιουσιακών στοιχείων

Οι αρχές για την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για την νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες («**money laundering**») και τη χρηματοδότηση της τρομοκρατίας καθορίζονται, από το 2006, στην απόφαση 231/4/13.10.2006 της Επιτροπής Τραπεζικών και Πιστωτικών Θεμάτων της Τράπεζας της Ελλάδος[371], η οποία

---

[366] Σουζάνα Κλημεντίδη, "Η Αδικοπρακτική Ευθύνη Των Τραπεζών Από Την Παροχή Επενδυτικών Υπηρεσιών Και Η Υποχρέωση Χρηματικής Αποζημίωσης - ΕΕΑ", ΕΕΑ, 2021, https://www.eea.gr/arthra-eea/i-adikopraktiki-eythyni-ton-trapezon-apo-tin-parochi-ependytikon-ypiresion-kai-i-ypochreosi-chrimatikis-apozimiosis/.
[367] Ενδεικτικά ΑΠ 244/2016, 2212/2014 ΤΝΠ ΝΟΜΟΣ, ΑΠ 1350/2018.
[368] Γεώργιος Γεωργιάδης, "Οι Υποχρεώσεις Της Τράπεζας Για Ενημέρωση, Διαφώτιση Και Παροχή Συμβουλών Στον Πελάτη", in *Τιμητικός Τόμος Γεωργίου Δ. Καλλιμόπουλου*, 1η εκδ. (repr., Αθήνα: Αντ. Ν. Σάκκουλας, 2010), 57.
[369] Ibid., 62-63.
[370] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 113.
[371] Απόφαση ΕΤΠΘ 231/4/13.10.2006, ΦΕΚ Β 1626.

συμπληρώνει, ως Παράρτημα 4, την ΠΔ/ΤΕ 2577/9.3.2006[372], αναφορικά με το πλαίσιο αρχών λειτουργίας και κριτηρίων αξιολόγησης της οργάνωσης και των Συστημάτων Εσωτερικού Ελέγχου των πιστωτικών και χρηματοδοτικών ιδρυμάτων και σχετικές αρμοδιότητες των διοικητικών τους οργάνων. Περαιτέρω, τόσο σε διεθνές όσο και σε ευρωπαϊκό επίπεδο συναντώνται ειδικές νομικές πράξεις, μέσω των οποίων επιβάλλεται στα πιστωτικά ιδρύματα η θέσπιση κατάλληλων και επαρκών μέτρων ώστε να αποτραπεί η νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες και η χρηματοδότηση της τρομοκρατίας.[373][374]

Οι ρυθμίσεις που καθιερώθηκαν με την απόφαση 231/4/13.10.2006 μπορούν να ενταχθούν συστηματικά σε δύο κατηγορίες. Η πρώτη αφορά τις ρυθμίσεις που καθορίζουν τις βασικές αρχές και τα κριτήρια προσέγγισης του ξεπλύματος χρήματος και της χρηματοδότησης της τρομοκρατίας με βάση τον κίνδυνο[375], ενώ η δεύτερη περιλαμβάνει ρυθμίσεις που αναφέρονται στην υλοποίηση επαρκών πληροφοριακών συστημάτων για τη διαρκή παρακολούθηση και αντιμετώπιση του κινδύνου και τις αρμοδιότητες της μονάδας κανονιστικής συμμόρφωσης.[376]

Ο κύριος φορέας από τον οποίο εκπορεύονται οι κανόνες του διεθνούς δικαίου για την καταπολέμηση της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες είναι η Ομάδα Χρηματοοικονομικής Δράσης (**Financial Action Task Force**, «FATF»). Ο φορέας αυτός, ο οποίος δεν έχει την υπόσταση διεθνούς οργανισμού, υποστηρίζεται γραμματειακά από τον ΟΟΣΑ και συστάθηκε το 1989, έπειτα από πρωτοβουλία των αρχηγών κρατών-μελών του G-7 κατά τη διάρκεια της ετήσιας συνόδου στο Παρίσι. Η Ομάδα απαρτίζεται από 39 κράτη[377], ανάμεσα στα οποία βρίσκεται και η Ελλάδα. Στόχος της Ομάδας είναι η καθιέρωση διεθνών προτύπων, τα οποία κατά τα πρώτα χρόνια λειτουργίας της αφορούσαν αποκλειστικά την καταπολέμηση της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες, ενώ πλέον αφορούν και την καταστολή της χρηματοδότησης της τρομοκρατίας. Στο πλαίσιο των εργασιών της, εξέδωσε το 1990 40 Συστάσεις («**Forty Recommendations on Money Laundering**»), οι οποίες ισχύουν σήμερα όπως διαμορφώθηκαν μετά την τροποποίησή τους το 1996, το 2003 και το 2012. Επίσης, εξέδωσε το 2001[378] 9 Ειδικές Συστάσεις («**Nine Special Recommendations on Terrorist Financing**»), οι οποίες ισχύουν σήμερα όπως τροποποιήθηκαν και συμπληρώθηκαν το 2004.[379]

Περαιτέρω, σε διεθνές επίπεδο, η Επιτροπή της Βασιλείας για την Τραπεζική Εποπτεία, έχει διατυπώσει κατά καιρούς τις θέσεις της σε θέματα πρόληψης της χρησιμοποίησης του τραπεζικού

---

[372] ΠΔ/ΤΕ 2577/9.3.2006, ΦΕΚ Α 59.

[373]Νόμος 4557/2018 (ενσωμάτωση Οδηγίας 2015/849/ΕΕ), Νόμος 3691/2008, Οδηγία 2005/60/ΕΚ, Οδηγία 2006/70/ΕΚ, Οδηγία (ΕΕ) 2015/849, Κανονισμός (ΕΕ) 847/2015, Απόφαση ΕΤΠΘ 281/5/17.3.2009 (Επιτροπής Τραπεζικών και Πιστωτικών Θεμάτων (ΕΤΠΘ) για την πρόληψη της χρησιμοποίησης των εποπτευομένων από την Τράπεζα της Ελλάδος πιστωτικών ιδρυμάτων και χρηματοπιστωτικών οργανισμών για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας.

[374] Ελληνική Ένωση Τραπεζών, "Πρόληψη Της Χρησιμοποίησης Του Χρηματοπιστωτικού Συστήματος Για Τη Νομιμοποίηση Εσόδων Από Εγκληματικές Δραστηριότητες Και Την Καταπολέμηση Της Τρομοκρατίας" (repr., Αθήνα: Ελληνική Ένωση Τραπεζών, 2006), 11. https://www.hba.gr/5Ekdosis/UplPDFs/deltia/4_2006/4-41.pdf.

[375] Απόφαση 231/4/13.10.2006, κεφάλαια 1,2,3 και 5, παρ. 5.1.

[376] Ibid., κεφάλαια 2, παρ. 2.3, και 4 έως 9.

[377] https://www.fatf-gafi.org/countries/

[378]https://www.fatfgafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf

[379] Ελληνική Ένωση Τραπεζών, "Πρόληψη Της Χρησιμοποίησης Του Χρηματοπιστωτικού Συστήματος Για Τη Νομιμοποίηση Εσόδων Από Εγκληματικές Δραστηριότητες Και Την Καταπολέμηση Της Τρομοκρατίας" (repr., Αθήνα: Ελληνική Ένωση Τραπεζών, 2006), 13-14. https://www.hba.gr/5Ekdosis/UplPDFs/deltia/4_2006/4-41.pdf.

συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και καταστολής της χρηματοδότησης της τρομοκρατίας, με στόχο την προώθηση της ομοιόμορφης ερμηνείας και αντιμετώπισης από τις εθνικές εποπτικές αρχές-μέλη των βασικών ζητημάτων που ανακύπτουν. Για το λόγο αυτό , εκδόθηκε, μεταγενέστερα της Εγκυκλίου Διοίκησης 16/2.8.2004, η έκθεση με τίτλο «*Consolidated KYC (Know Your Customer) Risk Management*»[380], η οποία περιέχει διεξοδικές αρχές αναφορικά με την διαχείριση του κινδύνου στο πλαίσιο της ακολουθούμενης διαδικασίας αναγνώρισης και πιστοποίησης της ταυτότητας των πελατών. Τέλος, με την Απόφαση-πλαίσιο του Συμβουλίου 2001/500/ΔΕΥ τα κράτη μέλη εκλήθησαν να λάβουν τα απαραίτητα μέτρα προκειμένου να μην διατυπώνουν ούτε να διατηρούν επιφυλάξεις όσον αφορά τα άρθρα 2 και 6 της Σύμβασης του Στρασβούργου (μέτρα δήμευσης και αδικήματα σχετικά με τη νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες, αντίστοιχα).[381] Καθιερώθηκαν επίσης διατάξεις σε σχέση με τις επιβαλλόμενες από τα κράτη μέλη κυρώσεις επί των εγκλημάτων της παρ. 1 του άρθρου 6 της εν λόγω Σύμβασης, της δήμευσης περιουσιακών στοιχείων αξίας αντίστοιχης προς εκείνη των προϊόντων του εγκλήματος, καθώς και τον τρόπο αντιμετώπισης των αιτήσεων αμοιβαίας συνδρομής.[382][383]

Στο πλαίσιο της αντιμετώπισης του φαινομένου της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες, η ΑΠΔΠΧ εξέδωσε την απόφαση 116/2014, με την οποία κρίθηκε ότι αποτελεί νόμιμη επεξεργασία ο έλεγχος λογαριασμών πελάτη τράπεζας, ο οποίος κατηγορείται για συμμετοχή σε εγκληματικές ενέργειες. Με την απόφαση 91/2014, η ΑΠΔΠΧ έκρινε επίσης ότι ο έλεγχος λογαριασμών, προς ικανοποίηση των υποχρεώσεων της τράπεζας στο πλαίσιο της πρόληψης και καταστολής των εσόδων από εγκληματικές δραστηριότητες, συνιστά επίσης νόμιμη επεξεργασία. Αντιθέτως, με την απόφαση 109/2013 της Αρχής, κρίθηκε ότι η τράπεζα θα πρέπει να καταστρέψει παρανόμως αποκτηθείσες λίστες δεδομένων προσωπικού χαρακτήρα, τις οποίες είχε αγοράσει με σκοπό την προώθηση προϊόντων και υπηρεσιών.

---

[380] https://www.bis.org/publ/bcbs101.htm

[381] Απόφαση-πλαίσιο του Συμβουλίου 2001/500/ΔΕΥ, άρθρο 1. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32001F0500&from=EL.

[382] Ibid., άρθρα 2-4.

[383] Ελληνική Ένωση Τραπεζών, "Πρόληψη Της Χρησιμοποίησης Του Χρηματοπιστωτικού Συστήματος Για Τη Νομιμοποίηση Εσόδων Από Εγκληματικές Δραστηριότητες Και Την Καταπολέμηση Της Τρομοκρατίας" (repr., Αθήνα: Ελληνική Ένωση Τραπεζών, 2006), 15-16. https://www.hba.gr/5Ekdosis/UplPDFs/deltia/4_2006/4-41.pdf.

ΤΕΤΑΡΤΟ ΚΕΦΑΛΑΙΟ
ΟΙ ΥΠΟΧΡΕΩΣΕΙΣ ΤΩΝ ΠΙΣΤΩΤΙΚΩΝ ΙΔΡΥΜΑΤΩΝ ΠΕΡΙ ΤΑ ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

4.1 Εισαγωγικές παρατηρήσεις

Οι τεχνολογικές καινοτομίες έχουν ενισχύσει σημαντικά την δυνατότητα των παρόχων οικονομικών υπηρεσιών και των τραπεζικών ιδρυμάτων να συλλέγουν, να αποθηκεύουν, να συνδυάζουν και να αναλύουν μια ευρεία ποικιλία δεδομένων, που αφορούν την οικονομική τους κατάσταση, τις προτιμήσεις τους, τις συνήθειες τους αλλά και την φυσική τους τοποθεσία. Αυτές οι τάσεις μπορούν να παρέχουν σημαντικά οφέλη για τους καταναλωτές, αλλά φέρνουν στο προσκήνιο και νέους κινδύνους που αφορούν αποκλειστικά τον τομέα παροχής οικονομικών υπηρεσιών και απαιτούν την εφαρμογή ρυθμίσεων που καθορίζουν τις νόμιμες προϋποθέσεις της νόμιμης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα αλλά και την αναγνώριση δικαιωμάτων στα υποκείμενα των δεδομένων, ώστε να δύνανται να ελέγξουν την κυκλοφορία των δεδομένων τους. Στο σύγχρονο επιγραμμικό περιβάλλον, παρατηρείται επίταση των κινδύνων αυτών, καθώς οι καταναλωτές έρχονται αντιμέτωποι με την περιθωριοποίησή τους, ως αποτέλεσμα των αδιαφανών και πιθανότατα άδικων πρακτικών εξόρυξης δεδομένων (**data mining**), ή βρίσκονται έκθετοι σε πιθανές απάτες και σε κυβερνοεγκλήματα. Σύμφωνα με την SQN Banking Systems, οι μεγαλύτερες απειλές κυβερνοασφάλειας για τα συστήματα των τραπεζικών ιδρυμάτων προέρχονται από τα μη κρυπτογραφημένα δεδομένα, τα κακόβουλα λογισμικά (**malware**), τα μη ασφαλή συστήματα τρίτων φορέων, τα χειραγωγημένα δεδομένα (**manipulated data**) αλλά και την παραπλάνηση μέσω της χρησιμοποίησης των στοιχείων ταυτοποίησης των προσώπων για δόλιους σκοπούς (**spoofing**).[384]

Υπό το φως των πρόσφατων παραβιάσεων δεδομένων (Morgan Stanley, Equifax Breach[385], Capital One, PayPay, SolarWinds[386]), η ανάγκη προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας των πελατών έχει καταστεί πιο επιτακτική από ποτέ και έχει λάβει κεντρική θέση στον κόσμο των ρυθμιστικών συστημάτων. Αυτό ισχύει και στην περίπτωση της βιομηχανίας των οικονομικών υπηρεσιών, εάν ληφθούν υπόψιν οι τεράστιες ποσότητες δεδομένων που υφίστανται επεξεργασία από τις τράπεζες και τους χρηματοπιστωτικούς οργανισμούς αλλά και από τους τρίτους φορείς παροχής υπηρεσιών πληροφορικής με τους οποίους αυτοί συμβάλλονται. Ειδικότερα, η διαδικασία σύναψης συμβάσεως ανάμεσα στον πελάτη και το εκάστοτε πιστωτικό ίδρυμα, συνεπάγεται την ανάγκη συλλογής πληροφοριών προσωπικής ταυτοποίησης και αυτό μπορεί να εκτείνεται από τον διαμοιρασμό δεδομένων που δεν έχουν οικονομική φύση, όπως ονοματεπωνύμων, διευθύνσεων, διευθύνσεων ηλεκτρονικού ταχυδρομείου, αριθμών κοινωνικής ασφάλισης κ.λπ. έως τον διαμοιρασμό οικονομικών δεδομένων που έχουν τη μορφή καταθέσεων, αποταμιεύσεων, λογαριασμών δανείων αλλά και αριθμών χρεωστικών ή πιστωτικών καρτών.

Οι τράπεζες, επομένως , για να διεκπεραιώνουν επιτυχώς τις τραπεζικές συναλλαγές, πρέπει να έχουν πρόσβαση σε πλήθος – κυρίως, αλλά όχι μόνο οικονομικής φύσεως- πληροφορίες που αφορούν τους πελάτες της. Εάν στη συναλλακτική σχέση συμμετέχουν και τρίτα πρόσωπα, όπως

---

[384] https://sqnbankingsystems.com/blog/the-5-biggest-threats-to-a-banks-cyber-security/.
[385] https://krebsonsecurity.com/2017/09/the-equifax-breach-what-you-should-know/.
[386] https://www.upguard.com/blog/biggest-data-breaches.

εγγυητές ή τρίτοι που παρέχουν εμπράγματη ασφάλεια, απαιτείται και η γνώση των δικών τους πληροφοριών. Οι παραπάνω πληροφορίες θα πρέπει επίσης να επικαιροποιούνται ή να συνδυάζονται με λοιπές πληροφορίες που κατέχει η τράπεζα ή πιθανότατα και τρίτα μέρη (π.χ. να ελέγχεται η συνολική δανειακή έκθεση του πελάτη σε άλλες ή και όλες τις τράπεζες). Τρίτα ως προς την τράπεζα πρόσωπα μπορεί να είναι οι εποπτεύουσες ή άλλες δημόσιες αρχές (π.χ. φορολογικές), άλλα πιστωτικά ιδρύματα, φορείς αξιολογήσεως της πιστοληπτικής ικανότητας ή διαχείρισης ληξιπρόθεσμων απαιτήσεων, καθώς και άλλοι πελάτες της τράπεζας, στους οποίους η τράπεζα υποχρεούται να παρέχει πληροφόρηση. Η υποχρέωση αυτή μπορεί να προκύπτει από συναφθείσα σύμβαση ή από την αρχή της καλής πίστης.

4.2 Η συλλογή και επεξεργασία δεδομένων οικονομικής συμπεριφοράς από τα πιστωτικά ιδρύματα

Με στόχο να εκπληρώσουν τις νόμιμες και θεμιτές δραστηριότητές τους, οι οποίες προσδιορίζονται από νομοθετικές και κανονιστικές διατάξεις[387][388], τα πιστωτικά ιδρύματα συλλέγουν από τους ενδεχόμενους πελάτες τους ποικίλα στοιχεία ταυτοποίησης και προχωρούν σε επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τους αφορούν. Οι δραστηριότητες που διεξάγουν καθημερινά οι τράπεζες είναι πολυπληθείς και εκτείνονται από τις βασικές δραστηριότητες του ανοίγματος λογαριασμών και της δανειοδότησης (λιανικές τραπεζικές υπηρεσίες-**retail banking**), έως τις πιο εξειδικευμένες δραστηριότητες της χρηματοδότησης εταιρειών (επενδυτικές τραπεζικές υπηρεσίες-**investment banking**). Επίσης, οι τράπεζες προσφέρουν μια ευρεία γκάμα εμπορικών τραπεζικών υπηρεσιών, στις οποίες εντάσσονται οι υπηρεσίες χρηματοδοτικής μίσθωσης (**leasing**) και οι υπηρεσίες πρακτορείας επιχειρηματικών απαιτήσεων (**factoring**). Τέλος, τα τραπεζικά ιδρύματα προσφέρουν εξατομικευμένες υπηρεσίες

---

[387] Το άρθρο 11 του νόμου **4261/2014** προσδιορίζει τις δραστηριότητες των πιστωτικών ιδρυμάτων. Αυτές είναι: « α) η αποδοχή καταθέσεων και άλλων επιστρεπτέων κεφαλαίων, β) η χορήγηση δανείων ή λοιπών πιστώσεων, στις οποίες συμπεριλαμβάνεται μεταξύ άλλων: η καταναλωτική πίστη, συμβάσεις πίστωσης εν σχέσει με ακίνητα, οι πράξεις αναδόχου εισπράξεως απαιτήσεων (factoring) με ή χωρίς δικαίωμα αναγωγής και η χρηματοδότηση εμπορικών συναλλαγών συμπεριλαμβανομένου του forfeiting),γ) η χρηματοδοτική μίσθωση (leasing), δ) οι υπηρεσίες πληρωμών του Παραρτήματος Ι της Οδηγίας 2015/2366/ΕΕ (ΕΕ L 337), ε) η έκδοση και διαχείριση άλλων μέσων πληρωμών (π.χ. ταξιδιωτικών και τραπεζικών επιταγών) στο βαθμό που η δραστηριότητα αυτή δεν καλύπτεται από την προηγούμενη περίπτωση, στ) εγγυήσεις και αναλήψεις υποχρεώσεων, ζ) οι συναλλαγές για λογαριασμό του ιδίου του ιδρύματος ή της πελατείας του σε οποιαδήποτε από τις ακόλουθες περιπτώσεις: αα) μέσα της χρηματαγοράς (αξιόγραφα, πιστοποιητικά καταθέσεων κ.λπ.), ββ) συνάλλαγμα, γγ) προθεσμιακά συμβόλαια χρηματοπιστωτικών τίτλων ή χρηματοπιστωτικά δικαιώματα, δδ) συμβάσεις ανταλλαγής επιτοκίων και συναλλάγματος, εε) κινητές αξίες, η) οι συμμετοχές σε εκδόσεις τίτλων και παροχή συναφών υπηρεσιών περιλαμβανομένων ειδικότερα και των υπηρεσιών αναδόχου εκδόσεως τίτλων, θ) η παροχή συμβουλών σε επιχειρήσεις όσον αφορά τη διάρθρωση του κεφαλαίου, τη βιομηχανική στρατηγική και συναφή θέματα παροχής συμβουλών, καθώς και υπηρεσιών στον τομέα της συγχώνευσης και της εξαγοράς επιχειρήσεων, ι) η διαμεσολάβηση στις διατραπεζικές αγορές, ια) η διαχείριση χαρτοφυλακίου ή παροχή συμβουλών για τη διαχείριση χαρτοφυλακίου, ιβ) η φύλαξη και διαχείριση κινητών αξιών, ιγ) η συλλογή και επεξεργασία εμπορικών πληροφοριών, περιλαμβανομένων και των υπηρεσιών αξιολόγησης πιστοληπτικής ικανότητας πελατών, ιδ) η εκμίσθωση θυρίδων, ιε) η έκδοση ηλεκτρονικού χρήματος, ιστ) οι επενδυτικές υπηρεσίες και δραστηριότητες της παρ. 1 του άρθρου 4 του ν. 3606/2007 και οι παρεπόμενες υπηρεσίες της παραγράφου 2 του ίδιου άρθρου οι οποίες αφορούν χρηματοπιστωτικά μέσα κατά την έννοια του άρθρου 5 του ν. 3606/2007.

[388] Περαιτέρω, η λειτουργία των πιστωτικών ιδρυμάτων διέπεται από: α) το νομοθετικό διάταγμα **1059/1971** που αφορά την προστασία του τραπεζικού απορρήτου, β) το νόμο **4557/2018** που θεσπίζει το νομοθετικό και κανονιστικό πλαίσιο για την αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και την χρηματοδότηση της τρομοκρατίας, γ) την **ΠΔ/ΤΕ 2501/2002** και τέλος υπό δ) την **ΠΕΕ 42/1014**.

διαχείρισης περιουσιακών στοιχείων (**private wealth management**), με στόχο την βελτιστοποίηση των κεφαλαίων των πελατών τους. [389]

Το οικονομικό σύστημα είναι διασυνδεδεμένο σε μεγάλο βαθμό σε όλα τα επίπεδα και για αυτό το λόγο είναι σημαντικό το κανονιστικό πλαίσιο διαρρύθμισής του να είναι εναρμονισμένο και συντονισμένο σε όλα τα επίπεδα. Η κανονιστική ρύθμιση και εποπτεία των τραπεζών αφορά κανόνες με τους οποίους οι τράπεζες θα πρέπει να συμμορφώνονται, ενώ η επίβλεψή τους αφορά τις διαδικασίες παρακολούθησης που ακολουθούνται από τις ρυθμιστικές και εποπτικές αρχές (Τράπεζα της Ελλάδος, Ευρωπαϊκή Αρχή Τραπεζών, Ευρωπαϊκή Κεντρική Τράπεζα)[390]. Στο κανονιστικό και νομοθετικό αυτό πλαίσιο, εντάσσεται και η συλλογή και επεξεργασία προσωπικών δεδομένων των πελατών των τραπεζών, η οποία θα πρέπει να πραγματοποιείται σύμφωνα με τις ειδικότερες νομοθετικές διατάξεις και να αποσκοπεί στην ορθή εκτέλεση των τραπεζικών συναλλαγών και συμβάσεων αλλά και στην εξυπηρέτηση των επιχειρηματικών συμφερόντων τους.[391]

Ως προσωπικά δεδομένα οικονομικής συμπεριφοράς, λογίζονται τα δεδομένα που αφορούν στην οικονομική ζωή του υποκειμένου, όπως αυτή εκφράζεται μέσα από την γενικότερη κοινωνική του δραστηριότητα, η οποία αποτελεί μια επιπρόσθετη έκφανση του δικαιώματος της πληροφοριακής του αυτοδιάθεσης. Σύμφωνα με την Αρχή, τα δεδομένα που σχετίζονται με την οικονομική κατάσταση του υποκειμένου είναι: τα έσοδα, τα περιουσιακά στοιχεία, οι επενδύσεις, ο απολογισμός εξόδων, τα δάνεια, οι υποθήκες, οι πιστώσεις, τα επιδόματα, τα εργασιακά προνόμια, οι επιχορηγήσεις, τα δεδομένα ασφάλισης, τα δεδομένα σύνταξης γήρατος, τα αγαθά και οι υπηρεσίες που προσφέρονται στο υποκείμενο των δεδομένων, καθώς και τα αγαθά ή οι υπηρεσίες που προσφέρει το άτομο, οι τραπεζικοί λογαριασμοί, οι πιστωτικές κάρτες, η κληρονομιά, οι αποζημιώσεις και γενικότερα οτιδήποτε αποτελεί στοιχείο της οικονομικής κατάστασης του ατόμου. Παρά το γεγονός ότι τα δεδομένα αυτά θεωρούνται κατά κύριο λόγο ως ευαίσθητα, ανήκουν στην κατηγορία των απλών προσωπικών δεδομένων. Αυτό συνάγεται εξ 'αντιδιαστολής από το γεγονός ότι τόσο στο κείμενο του νόμου 2472/1997 όσο και στην Οδηγία 95/46/ΕΚ, τα δεδομένα αυτά δεν συμπεριλήφθηκαν στην κατηγορία των ευαίσθητων δεδομένων.[392]

---

[389] Matthias Haentjens and Pierre De Gioia-Carabellese, *European Banking and Financial Law*, 2nd ed. (repr., London: Routledge, 2020), 111.

[390] Βλ. Γνωμοδότηση 5/2013 ΑΠΔΠΧ σχετικά με την ανάγκη λήψης μέτρων για την ορθή χρήση του Συστήματος Μητρώων Τραπεζικών Λογαριασμών και Λογαριασμών Πληρωμών (στο οποίο εντάσσονται δημόσιες αρχές και υπηρεσίες που ασκούν ελεγκτικό και διωκτικό έργο και στις οποίες παρέχεται η δυνατότητα αυτοματοποιημένης πρόσβασης σε στοιχεία τραπεζικών λογαριασμών και λογαριασμών πληρωμών που τηρούν τα πιστωτικά ιδρύματα και τα ιδρύματα πληρωμών για φυσικά και νομικά πρόσωπα [άρθρο 62 Ν.4170/2013], στην οποία η ΑΠΔΠΧ επεσήμανε ότι «στο βαθμό που η προβλεπόμενη επεξεργασία συνιστά περιορισμό του ατομικού δικαιώματος του πληροφοριακού αυτοκαθορισμού, θα πρέπει να ορίζεται γενικώς και αντικειμενικώς με τυπικό νόμο ή κατόπιν ειδικής νομοθετικής εξουσιοδότησης με διάταγμα, να δικαιολογείται από αποχρώντες λόγους δημοσίου συμφέροντος, να τελεί σε πρόδηλη λογική συνάφεια με τον επιδιωκόμενο σκοπό, να είναι πρόσφορη, κατάλληλη και αναγκαία για την επίτευξη του σκοπού αυτού, να μην θίγει τον πυρήνα του δικαιώματος και να μην απονέμει στη Διοίκηση ευρεία διακριτική ευχέρεια. Κατά συνέπεια είναι απαραίτητο η σκοπούμενη επεξεργασία να προβλέπεται σε νομοθετική διάταξη, η οποία θα αναφέρει τα βασικά χαρακτηριστικά της επεξεργασίας, δηλαδή τον υπεύθυνο επεξεργασίας, το σκοπό αυτής, τα δεδομένα τα οποία θα τύχουν επεξεργασίας και το χρόνο τήρησης αυτών καθώς και τους αποδέκτες των δεδομένων».

[391] Anu Arora, *Banking Law*, 1st ed. (repr., London, UK: Pearson Education Limited, 2014), 169.

[392] Μαρία Μυλώση και Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, "Προσωπικά Δεδομένα Οικονομικής Συμπεριφοράς Και Ηλεκτρονική Επεξεργασία Τους Από Την ΤΕΙΡΕΣΙΑΣ Α.Ε.", *Δίκαιο Μέσων Μαζικής Ενημέρωσης*, no. 45 (1/2015): 26.

Υποστηρίζεται[393] ότι το δικαιολογητικό έρεισμα για την μη συμπερίληψη των δεδομένων αυτών στον κατάλογο των ευαίσθητων δεδομένων βρίσκεται στην ανάγκη εξασφάλισης διαφάνειας και περιορισμού του «βρώμικου χρήματος», που πιθανότατα δεν θα επιτυγχάνονταν εάν στα δεδομένα αυτά αναγνωριζόταν ένα ειδικό καθεστώς προστασίας. Εάν τα δεδομένα αυτά όμως συνδέονται με περιπτώσεις υποκειμένων που χρήζουν κοινωνικής πρόνοιας, όπως συμβαίνει κατά την ανάρτηση από δημόσιες υπηρεσίες ονομαστικών λιστών δικαιούχων κοινωνικών επιδομάτων, τότε πρόκειται για περιπτώσεις επεξεργασίας που πρέπει να γίνεται βάσει της αυξημένης νομικής προστασίας για τα ευαίσθητα προσωπικά δεδομένα.

Ειδικότερα, στο πλαίσιο των συναλλακτικών τους σχέσεων με τους πελάτες τους, οι τράπεζες συλλέγουν δεδομένα ταυτοποίησής τους, όπως ονοματεπώνυμο, πατρώνυμο, μητρώνυμο, στοιχεία δελτίου ταυτότητας ή διαβατηρίου, αριθμό φορολογικού μητρώου, ΑΜΚΑ, ημερομηνία και τόπο γέννησης, φύλο, υπηκοότητα, δεδομένα υπογραφής κλπ. Επιπροσθέτως, οι πελάτες θα πρέπει να παρέχουν τα δεδομένα που επιτρέπουν την επικοινωνία της τράπεζας με αυτούς, όπως την ταχυδρομική διεύθυνσή τους, τα στοιχεία της ηλεκτρονικής διεύθυνσής τους αλλά και τους αριθμούς κινητού και σταθερού τηλεφώνου τους. Περαιτέρω, στο πλαίσιο της σύναψης κατ' ιδίαν συμβάσεων με τους πελάτες, τα τραπεζικά ιδρύματα δύνανται να προχωρήσουν σε επεξεργασία επιπρόσθετων στοιχείων, όπως αυτών που αφορούν την οικονομική φερεγγυότητα των πελατών (ακάλυπτες επιταγές, διαταγές πληρωμής, αιτήσεις και αποφάσεις υπαγωγής σε διαδικασίες προπτωχευτικές, πτωχευτικές, εξυγιαντικές κλπ.), τα δεδομένα πιστοληπτικής ικανότητας (πιστώσεις, εγγυητικές επιστολές κ.λπ.), τα δεδομένα πιστοληπτικής βαθμολόγησης (**credit profiling-scoring**), ισολογισμούς, στοιχεία εργοδοτών, δεδομένα ηλεκτρονικής ταυτοποίησης και σύνδεσης με υπηρεσίες ηλεκτρονικής τραπεζικής (λ.χ. **e-banking, mobile banking, v-banking**), δεδομένα εικόνας από τα συστήματα βιντεοσκόπησης των χώρων της Τράπεζας, δεδομένα που αφορούν τις επενδυτικές συναλλαγές, δεδομένα ασφαλιστικών προϊόντων, δεδομένα απαντήσεων σε έρευνες κ.λπ.[394][395]

Σύμφωνα με το ενημερωτικό δελτίο της ΑΠΔΠΧ, οι πελάτες υποχρεούνται κατ' ελάχιστο να προσκομίζουν τα ανωτέρω στοιχεία που αφορούν την πιστοποίηση της ταυτότητας τους στα τραπεζικά ιδρύματα.[396] Περαιτέρω, ορίζεται ότι με βάση τις Πράξεις 281/17.3.2009 και 94/15.11.2013 της ΕΤΠΘ της ΤτΕ, τα χρηματοπιστωτικά ιδρύματα και άλλα υπόχρεα πρόσωπα οφείλουν να πραγματοποιούν εξακρίβωση και έλεγχο των πελατών τους και να ζητούν την προσκόμιση εγγράφων που οδηγούν σε πιστοποίηση της ταυτότητάς του. Τέλος, τα πιστωτικά ιδρύματα δύνανται με βάση το προαναφερθέν κανονιστικό πλαίσιο, να ζητούν την προσκόμιση κάθε στοιχείου που κρίνεται συναφές με το αντικείμενο και την φύση της εκάστοτε συναλλαγής

[393] Ιωάννης Ιγγλεζάκης, *Ευαίσθητα Προσωπικά Δεδομένα*, 1η εκδ. (repr., Θεσσαλονίκη: Εκδόσεις Σάκκουλα, 2003), 94.
[394] https://www.eurobank.gr/el/gdpr-prosopika-dedomena/.
[395] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 64.
[396] "Ενημερωτικό Δελτίο ΑΠΔΠΧ - Τεύχος 12 Ιούλιος 2015", σελ. 3, (2015). Διαθέσιμο στην ιστοσελίδα: https://www.dpa.gr/sites/default/files/2020-12/JULY2015.PDF.

καθώς και να επαληθεύουν αυτά υπό το πρίσμα των νομοθετικών διατάξεων (νόμος 3691/2008, άρθρο 13 παρ. 1 στοιχ. γ'[397]), μέσω εκκαθαριστικού σημειώματος φορολογίας εισοδήματος.[398]

Σύμφωνα με την αρχή του περιορισμού του σκοπού, τα τραπεζικά ιδρύματα θα πρέπει να συλλέγουν τα προσωπικά δεδομένα των πελατών τους μόνο για καθορισμένους ρητούς και νόμιμους σκοπούς και να μην υποβάλλουν αυτά σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς.[399] Η αρχή αυτή έχει δύο σκέλη: σύμφωνα με το πρώτο σκέλος, επιβάλλεται στον υπεύθυνο επεξεργασίας (τράπεζα) η υποχρέωση να γνωστοποιήσει τους σκοπούς για τους οποίους συλλέγονται τα δεδομένα. Περαιτέρω, τέτοια γνωστοποίηση θα πρέπει να είναι ρητή και οι σκοποί της επεξεργασίας να είναι νόμιμοι. Σύμφωνα με το δεύτερο σκέλος της διάταξης, τα προσωπικά δεδομένα δεν θα πρέπει να υφίστανται επεξεργασία με τρόπο ασύμβατο προς τον σκοπό για τον οποίο συνελέγησαν. Από τη στιγμή που ένας διαφορετικός σκοπός δεν θα ήταν απαραίτητα ένας ασύμβατος σκοπός, η αρχή δεν απαγορεύει απαραίτητα την επεξεργασία για σκοπό διαφορετικό από αυτόν που έχει αρχικά καθοριστεί. Τον Απρίλιο του 2013 η Ομάδα εργασίας του άρθρου 29, μέσω της Γνωμοδότησης που δημοσίευσε[400], παρείχε εκτεταμένη καθοδήγηση στους υπευθύνους επεξεργασίας σχετικά με την αρχή περιορισμού του σκοπού. Συγκεκριμένα, στο κείμενο της Γνωμοδότησης αναφέρεται ότι όλες οι σχετικές περιστάσεις θα πρέπει να ληφθούν υπόψιν όταν διενεργείται μια αξιολόγηση σχετικά με το αν η περαιτέρω επεξεργασία είναι συμβατή με τον αρχικό σκοπό.[401] Κατά την αξιολόγηση αυτή, τέσσερις κρίσιμοι παράγοντες θα πρέπει να ληφθούν υπόψιν. Ο πρώτος αφορά τη σχέση ανάμεσα στους δύο σκοπούς για τους οποίος έχουν συλλεχθεί τα δεδομένα και τους σκοπούς της περαιτέρω επεξεργασίας. Ο δεύτερος αφορά το πλαίσιο εντός του οποίου έχουν συλλεχθεί τα δεδομένα καθώς και τις εύλογες προσδοκίες των υποκειμένων των δεδομένων αναφορικά με την περαιτέρω χρήση τους. Επιπλέον, θα πρέπει να ληφθεί υπόψιν η φύση των προσωπικών δεδομένων καθώς και οι επιπτώσεις της περαιτέρω επεξεργασίας επί των υποκειμένων των δεδομένων. Τέλος, θα πρέπει να ληφθούν υπόψιν τα μέτρα ασφαλείας που έχουν ληφθεί από τους υπευθύνους επεξεργασίας ώστε να διασφαλιστεί η σύννομη επεξεργασίας και να αποφευχθεί οποιοδήποτε ανεπιθύμητο αντίκτυπο για τα υποκείμενα των δεδομένων.

Ο ΓΚΠΔ αναφέρει επίσης κάποιους τύπους επεξεργασίας που δεν θεωρούνται ασύμβατοι με τους σκοπούς που καθορίζονται από την υπό εξέταση αρχή. Οι σκοποί αυτοί είναι: η αρχειοθέτηση προς το δημόσιο συμφέρον ή για σκοπούς επιστημονικής ή ιστορικής έρευνας αλλά και για στατιστικούς σκοπούς.[402] Ωστόσο, ο νόμος 4624/2019 στο άρθρο 25 ορίζει αρχικά ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα από ιδιωτικούς φορείς επιτρέπεται για σκοπό διαφορετικό από αυτόν για τον οποίο έχουν συλλεγεί, εφόσον είναι απαραίτητη για την αποτροπή απειλών κατά της εθνικής ή της δημόσιας ασφάλειας κατόπιν αιτήματος δημόσιου φορέα. Επίσης, επιτρέπεται για τη δίωξη ποινικών αδικημάτων ή για τη θεμελίωση, την άσκηση ή την υποστήριξη

---

[397] Όπως τροποποιήθηκε από το νόμο 4174/2013, άρθρο 68 παρ. 7 και την υπ'αριθμ. 2652/2012 ΠΔ/ΤΕ.

[398] "Ενημερωτικό Δελτίο ΑΠΔΠΧ - Τεύχος 12 Ιούλιος 2015", σελ. 3, (2015). Διαθέσιμο στην ιστοσελίδα: https://www.dpa.gr/sites/default/files/2020-12/JULY2015.PDF.

[399] Βλ. άρθρο 5 παρ. 1 στοιχείο β' ΓΚΠΔ.

[400] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (2 April 2013), available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[401] Βλ. και άρθρο 6 παρ. 4, που επιτρέπει υπό προϋποθέσεις, επεξεργασία για άλλο σκοπό, «συμβατό» όμως με αυτόν για τον οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα.

[402] Peter Carey, *Data Protection - A Practical Guide to UK Law*, 5th ed. (repr., Oxford, UK: Oxford University Press, 2018), 34-35.

νομικών αξιώσεων, εκτός εάν υπερτερεί το συμφέρον του υποκειμένου των δεδομένων να μην τεθούν υπό επεξεργασία τα δεδομένα αυτά.[403]

4.3 Οι προϋποθέσεις για την θεμιτή επεξεργασία των δεδομένων των πελατών των τραπεζών

Στο πεδίο των τραπεζικών συναλλαγών, το τραπεζικό ίδρυμα θα πρέπει να περιορίζει την επεξεργασία μόνο σε όσα δεδομένα παρουσιάζουν άμεση συνάφεια προς τον σκοπό που αυτή επιδιώκει με την επεξεργασία. Για παράδειγμα, εάν η τράπεζα σκοπεύει να αξιολογήσει την πιστοληπτική ικανότητα ενός υποκειμένου, για το άνοιγμα πιστώσεως με αλληλόχρεο λογαριασμό που θα εξυπηρετεί την επιχειρηματική του δραστηριότητα, έχει το δικαίωμα να ζητήσει σχετικό επιχειρηματικό σχέδιο από τον πελάτη, στο οποίο θα συμπεριλαμβάνονται πληροφορίες που αφορούν τόσο εκείνον όσο και την επιχείρησή του. Σε αντίθετη περίπτωση, εάν στο ίδιο πρόσωπο πρόκειται να χορηγήσει καταναλωτικό δάνειο μικρού ύψους, δεν δικαιούται να ζητήσει και να επεξεργαστεί επιχειρηματικό σχέδιο, διότι υπερβαίνει το αναγκαίο για τον σκοπό επεξεργασίας μέτρο, ανεξάρτητα από το αν ο ενδιαφερόμενος παρείχε τη συγκατάθεσή του στην χορήγησή του.[404] Το ίδιο ισχύει και σε περίπτωση διαβίβασης στοιχείων του πελάτη σε τρίτους, καθώς στην περίπτωση αυτή θα πρέπει να διαβιβάζονται μόνο τα απολύτως αναγκαία στοιχεία του πελάτη, για την εξυπηρέτηση του προκαθορισμένου εκάστοτε σκοπού. Επί παραδείγματι, εάν μεταβιβασθεί σε τρίτο μέρος απαίτηση της τράπεζας από πίστωση, δεν είναι νόμιμη η πληροφόρηση του εκδοχέα αναφορικά με άλλες συναλλακτικές σχέσεις του πελάτη με την τράπεζα.[405]

Τα άρθρα 5 και 6 του Κανονισμού οριοθετούν το πλαίσιο δράσεως κάθε επεξεργαζόμενου τα προσωπικά δεδομένα. Επομένως, οι αρχές και οι βάσεις νομιμότητας που προβλέπονται στα εν λόγω άρθρα είναι απολύτως δεσμευτικές για τα πιστωτικά ιδρύματα και η επεξεργασία που πραγματοποιείται από αυτά είναι νόμιμη εφόσον ερείδεται σε κάποια από τις βάσεις νομιμότητας που προβλέπονται στο άρθρο 6 του Κανονισμού ενώ παράλληλα θα πρέπει να είναι σύμφωνη με τις αρχές που προβλέπονται στο άρθρο 5 του Κανονισμού. Με βάση αυτές τις αρχές και τις νόμιμες βάσεις θα πρέπει να λειτουργούν και όλοι οι εντασσόμενοι στις οργανωτικές δομές παράγοντες των πιστωτικών ιδρυμάτων που συμμετέχουν στην επεξεργασία των προσωπικών δεδομένων.

Περαιτέρω, σύμφωνα με το άρθρο 13 του ΓΚΠΔ, τα υποκείμενα των δεδομένων θα πρέπει να ενημερώνονται από τα πιστωτικά ιδρύματα σχετικά με τις λεπτομέρειες της δραστηριότητας της επεξεργασίας κατά το χρόνο που αυτά ως υπεύθυνοι επεξεργασίας συλλέγουν τα προσωπικά δεδομένα απευθείας από τους ίδιους τους πελάτες. Εάν τα προσωπικά δεδομένα των πελατών συλλέγονται από τρίτα μέρη, τότε χρήζει εφαρμογής το άρθρο 14 του Κανονισμού, που προβλέπει στην παράγραφο 3 συγκεκριμένο χρονικό διάστημα, εντός του οποίου θα πρέπει να ενημερώνονται τα υποκείμενα των δεδομένων.

---

[403] Βλ. άρθρο 25, Νόμος υπ'αριθμ. 4624/2019 (ΦΕΚ 137/Α/29-8-2019). www.et.gr.
[404] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 122.
[405] Ibid.

4.3.1 Η επεξεργασία των δεδομένων των πελατών με βάση την αρχή της διαφάνειας

Μια από τις αρχές της επεξεργασίας δεδομένων είναι η αρχή της διαφάνειας, η οποία συνδέεται στενά με τις αρχές της νομιμότητας και της αντικειμενικότητας, όπως αυτές προβλέπονται στο άρθρο 5 παρ. 1 στοιχείο α'. Η ενημέρωση των υποκειμένων των δεδομένων αναφορικά με τις λεπτομέρειες της δραστηριότητας της επεξεργασίας μπορεί να θεωρηθεί ως απαραίτητη προϋπόθεση για την σύννομη επεξεργασία και σίγουρα αποτελεί απαραίτητη προϋπόθεση για την εξασφάλιση της διαφάνειας της επεξεργασίας. Ενώ η διαφάνεια μπορεί να επιτευχθεί με πολλούς διαφορετικούς τρόπους, το βασικό δομικό στοιχείο της αποτελούν οι πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων κατά την έναρξη της δραστηριότητας της επεξεργασία ή πριν λάβει χώρα αυτή («**data protection notice**»/ «**privacy notice**») και οι οποίες έπειτα θα πρέπει να είναι εύκολα προσβάσιμες κατά τη διάρκεια των πράξεων της επεξεργασίας.

Η πληρότητα και η ακρίβεια των πληροφοριών που παρέχονται στο υποκείμενο των δεδομένων σχετικά με την δραστηριότητα της επεξεργασίας είναι επίσης ύψιστης σημασίας για την λήψη έγκυρης συναινέσεως σύμφωνα με τις διατάξεις του Κανονισμού[406], τόσο στην περίπτωση που τα δεδομένα λαμβάνονται απευθείας από τα υποκείμενα των δεδομένων αλλά και στην περίπτωση που λαμβάνονται από άλλη πηγή. Θα πρέπει να σημειωθεί, ωστόσο, ότι η υποχρέωση παροχής λεπτομερών πληροφοριών στο υποκείμενο των δεδομένων, ισχύει εξίσου για όλες τις πράξεις επεξεργασίας, ανεξαρτήτως από την νομική βάση της επεξεργασίας στην οποία βασίζονται. Για παράδειγμα, ακόμα και όταν η επεξεργασία βασίζεται στην υποχρέωση εκπληρώσεως συμβατικής υποχρέωσης, ή στην διαφύλαξη των νόμιμων συμφερόντων του υπευθύνου επεξεργασίας ή τρίτων, οι υπεύθυνοι επεξεργασίας υπόκεινται ακόμα στην υποχρέωση να παρέχουν ενημέρωση σύμφωνα με την διάταξη του άρθρου 13 του Κανονισμού.[407]Για παράδειγμα, εάν το τραπεζικό ίδρυμα διαβιβάζει τις κινήσεις λογαριασμών πελατών της στην ΤτΕ ή στις αρμόδιες φορολογικές αρχές, προς εκπλήρωση υποχρέωσής της που πηγάζει από τον νόμο, οφείλει σε κάθε περίπτωση να ενημερώνει σχετικά τους πελάτες της, ακόμα και στην περίπτωση που για την διαβίβαση δεν απαιτείται η συγκατάθεσή τους. Η αθέτηση της αυτοτελούς υποχρεώσεως προς ενημέρωση των υποκειμένων των δεδομένων συνεπάγεται εποπτική και αστική ευθύνη της τράπεζας, ανεξαρτήτως εάν κατά τα λοιπά η επεξεργασία είναι σύννομη.[408]Για την επιβολή διοικητικής κυρώσεως δεν απαιτείται επέλευση ζημίας του υποκειμένου των δεδομένων.[409] Το υποκείμενο των δεδομένων θα πρέπει επίσης να πληροφορηθεί τις πράξεις επεξεργασίας σε γλώσσα οικεία και κατανοητή, και με διατύπωση μη επιδεκτική παρερμηνειών. Η αυτοτέλεια της υποχρεώσεως καθίσταται προφανής όταν το υποκείμενο έχει συγκατατεθεί στην επεξεργασία καθώς η συγκατάθεση αυτή δεν αναιρεί την υποχρέωση προηγούμενης ενημερώσεως.[410]

---

[406] Βλ. άρθρο 4 (11) σύμφωνα με το οποίο απαιτείται η πλήρη επιγνώσει συγκατάθεση.

[407] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 415.

[408] Πρβλ. άρθρο 83 παρ. 5 ΓΚΠΔ, το οποίο θεσπίζει πλαίσιο διοικητικού προστίμου εάν παραβιασθούν τα «δικαιώματα των υποκειμένων σύμφωνα με τα άρθρα 12-22».

[409] ΣτΕ 150/2017. https://www.taxheaven.gr/circulars/26742/ste-150-2017.

[410] ΕφΑθ 2887/2010 ΧρηΔικ 1/2011, 163: Για την ανάθεση της οχλήσεως σε Εταιρεία Ενημέρωσης Οφειλετών δεν αρκεί η ύπαρξη στη δανειακή σύμβαση όρου σύμφωνα με τον οποίο παρέχεται συγκατάθεση για τήρηση και επεξεργασία των δεδομένων και από συνεργαζόμενα πρόσωπα, αλλά η τράπεζα οφείλει να έχει ενημερώσει τον οφειλέτη για τον σκοπό διαβιβάσεως και τους αποδέκτες. Πρβλ. και ΑΠΔΠΧ 98/2017, ΑΠ 1740/2013, ΕφΑθ 1437/2014, ΕιρΑθ 273/2016 ΤΝΠ ΝΟΜΟΣ.

Η παροχή στα υποκείμενα των δεδομένων με τα απαραίτητα στοιχεία πληροφόρησης όχι μόνο τοποθετεί αυτά σε μια θέση από την οποία μπορούν αποτελεσματικά να ασκήσουν τα δικαιώματά τους ως υποκείμενα των δεδομένων, αλλά συμβάλλει επίσης στην διασφάλιση της ποιότητας των δεδομένων.[411] Ήδη από τη δεκαετία του 1980, το δικαίωμα στην ενημέρωση για τις πράξεις της επεξεργασίας θεωρούνταν θεμελιώδες ανάμεσα στα υπόλοιπα δικαιώματα των υποκειμένων των δεδομένων. Αργότερα, επισημάνθηκε ότι η διάταξη που συμπεριλαμβάνει τις αρχές της νομιμότητας, της αντικειμενικότητας και της διαφάνειας, «εμπεριέχει και παράγει τις άλλες βασικές αρχές που προβλέπονται στους νόμους προστασίας δεδομένων».[412] Η διαφάνεια κρίνεται ολοένα και πιο σημαντική στην αναδυόμενη εποχή της αλγοριθμικής λήψης αποφάσεων, της Τεχνητής Νοημοσύνης και της μηχανικής μάθησης.[413] Η εποχή αυτή χαρακτηρίζεται από την δημιουργία μιας «κοινωνίας του μαύρου κουτιού» («**black box society**»).[414] Μια τέτοιου είδους κοινωνία θα μπορούσε να χαρακτηριστεί ως μια κοινωνία εντός της οποίας οι αποφάσεις που λαμβάνονται μέσω της χρήσης αλγορίθμων ή εφαρμογών τεχνητής νοημοσύνης, συμπεριλαμβανομένων και των εφαρμογών που χρησιμοποιούν αλγορίθμους μηχανικής μάθησης, διεισδύουν σε όλες τις πτυχές της κοινωνικής ζωής, χωρίς οι άνθρωποι να γνωρίζουν πώς αυτές οι αυτοματοποιημένες διεργασίες λειτουργούν και πότε λαμβάνουν χώρα.[415]

Μετά την υιοθέτηση του Κανονισμού, ακολούθησε μια ακαδημαϊκή διαμάχη αναφορικά με το αν υφίσταται το δικαίωμα των υποκειμένων των δεδομένων να λαμβάνουν μια εκ των υστέρων (ex post) επεξήγηση, όταν έχει λάβει χώρα αυτοματοποιημένη ή αλγοριθμική λήψη αποφάσεων.[416] Ανεξάρτητα από την ονομασία του, τέτοιο δικαίωμα στην ουσία έχει διασφαλιστεί μέσω ενός πλέγματος διατάξεων του Κανονισμού, που στόχο έχουν την διασφάλιση της διαφάνειας αναφορικά με συγκεκριμένες πράξεις επεξεργασίας.[417] Θα πρέπει επίσης να ληφθεί υπόψιν ότι η παροχή ουσιώδους διαφάνειας σχετικά με την λειτουργία των αυτοματοποιημένων συστημάτων σε σχέση με τα προσωπικά δεδομένα των υποκειμένων, βρίσκεται στον πυρήνα των πρώτων νομοθετημάτων που τέθηκαν σε ισχύ σε ενωσιακό επίπεδο. Ο πρώτος γαλλικός νόμος περί προστασίας των δεδομένων του 1978, ήδη παρείχε στα υποκείμενα το «δικαίωμα να γνωρίζουν και να αμφισβητούν τις πληροφορίες και την λογική που χρησιμοποιούνται από τα αυτοματοποιημένα συστήματα, τα αποτελέσματα των οποίων τους αφορούν.[418]

---

[411] European Data Protection Supervisor, 'Guidelines on the Rights of Individuals with Regard to Processing of Personal Data' (25 February 2014), 8. https://edps.europa.eu/.

[412] Lee A Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits*, 1st ed. (repr., New York, NY: Wolters Kluwer Law & Business, 2002), 58.

[413] Για την κατανόηση των εννοιών αυτών σε ένα πλαίσιο «προστασίας δεδομένων», σημαντική κρίνεται η συμβολή της Έκθεσης της νορβηγικής αρχής προστασίας δεδομένων, που αναφέρεται εκτενώς στην ένταση ανάμεσα στην αρχή της διαφάνειας και στην έννοια του «μαύρου κουτιού» (**black box**), που συμπεριλαμβάνεται στην αυτοματοποιημένη λήψη αποφάσεων. Βλ. σελ. 19.
Διαθέσιμη στην ιστοσελίδα: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.

[414] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, 1st ed. (repr., Cambridge, MA: Harvard University Press, 2016), 191-194.

[415] Ignas Kalpokas, *Algorithmic Governance: Politics and Law in The Post-Human Era*, 1st ed. (repr., Cham, Switzerland: Palgrave Pivot, 2019), 33.

[416] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, "Why A Right to Explanation of Automated Decision-Making Does Not Exist in The General Data Protection Regulation", *SSRN Electronic Journal*, 2016, 6-9, doi:10.2139/ssrn.2903469.

[417] Άρθρα 5 (1) στοιχ. α', 12, 14 και 15 ΓΚΠΔ.

[418] Γαλλικός νόμος προστασίας δεδομένων 1978, άρθρο 3: «Toute personne a le droit de connaitre et de contester les informations et les raisonnements utilisıs dans les traitements automatisıs dont les rısultats lui sont opposes».

Η αρχή της διαφάνειας απαιτεί κάθε πληροφορία και ενημέρωση που σχετίζεται με την επεξεργασία των εκάστοτε προσωπικών δεδομένων να είναι εύκολα προσβάσιμη και κατανοητή, ενώ θα πρέπει να χρησιμοποιείται καθαρή και απλή γλώσσα.[419] Η ομάδα εργασίας του άρθρου 29, κατέστησε σαφές ότι με βάση το άρθρο 13 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας πρέπει να ενεργεί με αποφασιστικότητα ως προς την παροχή πληροφοριών στο υποκείμενο των δεδομένων, εννοώντας ότι «το υποκείμενο των δεδομένων δεν πρέπει να χρειάζεται να αναζητάει ενεργά τις πληροφορίες που καλύπτουν αυτά τα άρθρα, μεταξύ άλλων πληροφοριών, όπως οι όροι και προϋποθέσεις χρήσης ενός ιστοτόπου ή μιας εφαρμογής».[420] Η βέλτιστη πρακτική για την παροχή των σχετικών πληροφοριών, είναι η υιοθέτηση μιας προσέγγισης πολλαπλών επιπέδων (**layered notices**). Όπως αναφέρει η Ομάδα του άρθρου 29, οι δηλώσεις πολλαπλών επιπέδων «μπορούν να συμβάλουν στην επίλυση της έντασης μεταξύ της πληρότητας και της κατανόησης, ιδίως μέσω της παροχής στους χρήστες της δυνατότητας να μεταβαίνουν απευθείας στην ενότητα της δήλωσης που επιθυμούν να διαβάσουν».[421] Τέλος, διευκρίνισε ότι το άρθρο 13 του Κανονισμού χρήζει εφαρμογής τόσο στην επεξεργασία δεδομένων κατά την οποία το υποκείμενο των δεδομένων παρέχει συνειδητά αυτά σε έναν υπεύθυνο επεξεργασίας δεδομένων (π.χ. συμπλήρωση ηλεκτρονικής φόρμας), όσο και στην περίπτωση που ένας υπεύθυνος επεξεργασίας συλλέγει τα δεδομένα από ένα υποκείμενο των δεδομένων μέσω παρατήρησης (π.χ. μέσω της χρήσης συσκευών ή λογισμικού καταγραφής δεδομένων, μέσω εξοπλισμού δικτύου, μέσω παρακολούθησης από ασύρματα δίκτυα, μέσω αισθητήρων RFID κ.λπ.).[422] Για τις περιπτώσεις αυτές, η Ομάδα συνέστησε διάφορους τρόπους παροχής ενημέρωσης, όπως εικονίδια, κωδικούς QR, φωνητικές ειδοποιήσεις, βίντεο που ενσωματώνονται σε ψηφιακές οδηγίες ρύθμισης, μηνύματα που αποστέλλονται μέσω SMS ή e-mail, γραπτές πληροφορίες σε έξυπνη συσκευή κ.λπ.[423]

Ως προς τον χρόνο ενημέρωσης, αυτή θα πρέπει να παρέχεται «κατά το χρόνο συλλογής των προσωπικών δεδομένων. Αυτό σημαίνει παράλληλα με την συλλογή των δεδομένων από το υποκείμενο και όχι post factum. Για παράδειγμα, ο συνδρομητής του εκάστοτε ενημερωτικού δελτίου θα πρέπει να ενημερώνεται κατά τον χρόνο που παρέχει την ηλεκτρονική διεύθυνσή του για τον σκοπό της εγγραφής στο εν λόγω ενημερωτικό δελτίο. Στην περίπτωση της συλλογής δεδομένων «μέσω παρατήρησης», αναφορικά με τα δεδομένα που συλλέγονται απευθείας από το υποκείμενο των δεδομένων μέσω παρακολούθησης του ασύρματου δικτύου, η ενημέρωση θα πρέπει να παρέχεται κατά την είσοδο στην περιοχή που καλύπτεται από την εν λόγω υπηρεσία παρακολούθησης.[424] Η ενημέρωση θα πρέπει επίσης να είναι ατομική, δηλαδή θα πρέπει να περιέλθει στην σφαίρα εξουσίας του υποκειμένου. Κατ' εξαίρεση μπορεί να πραγματοποιηθεί και δια του τύπου, εφόσον είναι αδύνατη με άλλον τρόπο που κρίνεται πιο ευνοϊκός για το υποκείμενο (ΑΚ 335), αδύνατη φυσικώς ή οικονομικώς, ήτοι στην περίπτωση που «θα απαιτούσε δυσανάλογη προσπάθεια» η ατομική εγγραφή ή ηλεκτρονική ενημέρωση του υποκειμένου (άρθρο 14 παρ. 5

[419] Αιτιολογική σκέψη 39, ΓΚΠΔ.
[420] Ομάδα εργασίας του άρθρου 29, «Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679», 17/EL WP260 rev.01, (29 Νοεμβρίου 2017), 23.
[421] Ibid., 24.
[422] Ibid., 18.
[423] Ibid., 28.
[424] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 427.

ΓΚΠΔ).[425] Στην περίπτωση της διαβίβασης δεδομένων του οφειλέτη από τον δανειστή στον ενδεχόμενο εκδοχέα ή τον δεκτικό καταβολής στο πλαίσιο του θεσμού της πρακτορείας επιχειρηματικών απαιτήσεων (**factoring**), η ενημέρωση πραγματώνεται εν μέρει μέσω της αναγγελίας (ΑΚ 460), εφόσον πριν λάβει χώρα αυτή δεν υφίσταται ισχυρή εκχώρηση. Σύμφωνα με την κρατούσα άποψη, στο πλαίσιο αυτό, επιβάλλεται η ενημέρωση των οφειλετών δανειοληπτών για την επικείμενη πληροφόρηση του αγοραστή τραπεζικής επιχείρησης.[426]

Οι προς το υποκείμενο των δεδομένων υποχρεώσεις διαφώτισης, μπορούν να εκπληρωθούν και προς εξουσιοδοτημένο αντίκλητό του (ΑΚ 417, άρθρο 20 ΓΚΠΔ). Ο υπεύθυνος επεξεργασίας όμως (τράπεζα), βαρύνεται με την ορθή απεύθυνση της πληροφόρησης, δηλαδή της εξακρίβωσης και της απόδειξης της ταυτότητας του προς ον (υποκειμένου) και του κύρους της εξουσιοδότησής του. Περαιτέρω, ο υπεύθυνος επεξεργασίας υποχρεώνεται να τηρεί αρχείο συγκεκριμένων πληροφοριών αναφορικά με την εκάστοτε επεξεργασία του, ώστε να το επιδείξει στην ΑΠΔΠΧ, εφόσον αυτή του ζητήσει το εν λόγω αρχείο (άρθρο 30 ΓΚΠΔ). Περαιτέρω, ο υπεύθυνος επεξεργασίας υπέχει καθήκον πληροφόρησης προς την ΑΠΔΠΧ τυχόν παραβιάσεως των δεδομένων του αρχείου του. Ως παρασχετέες πληροφορίες (άρθρα 13-15 ΓΚΠΔ), ορίζονται τα στοιχεία ταυτότητας και επικοινωνίας του υπευθύνου, του εκπροσώπου του και του υπευθύνου προστασίας, οι σκοποί, η χρονική οριοθέτηση και η νομική βάση της επεξεργασίας (σύμφωνα με άρθρο 6 παρ. 1 στ΄), ο αυτοματοποιημένος χαρακτήρας της ή μη και η σημασία του, οι αποδέκτες των δεδομένων, η πρόθεση διαβίβασής τους σε τρίτη χώρα, ως «λιμένα ασφαλή» ή μη με «κατάλληλες εγγυήσεις», αλλά και τα έννομα μέσα κατ' αυτής προς υπεύθυνο και ΑΠΔΠΧ (π.χ. εναντίωση, καταγγελία, ανάκληση συγκατάθεσης).[427] Επικράτησε επίσης η ορθή σύμφωνα με το δίκαιο της Ε.Ε. ερμηνεία του άρθρου 10 παρ. 10 του νόμου 3156/03 αναφορικά με την τιτλοποίηση απαιτήσεων. Το εν λόγω άρθρο όριζε ότι «λογίζεται ως αναγγελία της μεταβίβασης των απαιτήσεων η απλή καταχώρισή της στο δημόσιο βιβλίο του άρθρου 3 ν. 2844/2000», ότι αρκούσε δηλαδή η εγγραφή στο βιβλίο αυτό ερήμην του οφειλέτη. Ωστόσο, σύμφωνα με την νομολογία της ΑΠΔΠΧ και των δικαστηρίων, προσαπαιτείται πλέον και η αναγγελία της στον οφειλέτη.[428][429]

Αναφορικά με την οριοθέτηση των αποδεκτών, αυτοί θα πρέπει να ανακοινώνονται στο υποκείμενο, ώστε το τελευταίο να γνωρίζει στα χέρια ποιου βρίσκεται το αρχείο, ώστε να μπορεί κατ' επέκταση να αποκτήσει πρόσβαση σε αυτό και να το εξετάσει. Οι αποδέκτες επίσης θα πρέπει να γνωστοποιούνται ατομικώς ο καθένας ή και κατά κατηγορία, δηλαδή να καθίστανται ορισμένοι ή έστω οριστοί. Σύμφωνα με πάγια νομολογία των δικαστηρίων[430] και της ΑΠΔΠΧ[431], στο

---

[425] Αυτό προβλεπόταν μόνο μετά από άδεια της ΑΠΔΠΧ και μόνο προκειμένου για υπερχίλια πρόσωπα από το προισχύον άρθρο 24 παρ. 3 εδ. β' του νόμου 2472/97 σε συνδυασμό με την κανονιστική απόφαση της ΑΠΔΠΧ υπ'αριθμ. 408/1998.

[426] Ετήσια έκθεση ΑΠΔΠΧ 2014, 79. https://www.dpa.gr/sites/default/files/2020-12/ARXH%20PROSTASIAS_APOLOGISMOS%202013.PDF.

[427] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 119-120.

[428] Ετήσια έκθεση ΑΠΔΠΧ 2014, 76-77. www.dpa.gr/sites/default/files/2020-12/ANNUAL_2014_V2.0_WEB_VIEW.PDF

[429] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 123.

[430] Νομιμότητα επεξεργασίας προσωπικών δεδομένων από την «Τειρεσίας ΑΕ», *ΑΠ 1923/2006*, (Χρηματοπιστωτικό Δίκαιο 2/2007).

[431] ΑΠΔΠΧ 24/2004. https://www.dpa.gr/sites/default/files/2019-10/24-04-1_1.doc.

πλαίσιο αυτό, κρίθηκε ότι η Τειρεσίας Α.Ε. απαλλάσσεται από την υποχρέωση να ενημερώσει περαιτέρω τους οφειλέτες των οποίων τα στοιχεία συγκεντρώνει, στο μέτρο που ήδη έχει ενημερώσει αυτούς ότι οι αποδέκτες των αντίστοιχων δεδομένων περιορίζονται σε έναν στενό κύκλο προσώπων, τα μέλη της ελληνικής ενώσεως τραπεζών. Αντίθετα έκρινε η ΑΠΔΠΧ[432], στην περίπτωση των εταιρειών διαπίστωσης πιστοληπτικής ικανότητας, εφόσον πιθανός αποδέκτης των σχετικών πληροφοριών μπορεί να είναι οποιοσδήποτε πελάτης των εταιρειών αυτών. Η διαζευκτική διατύπωση των διατάξεων του Κανονισμού στα άρθρα 13-15, αναφορικά με «τον αποδέκτη ή τις κατηγορίες των αποδεκτών», δεν φαίνεται να παρέχει δικαίωμα επιλογής στον υπεύθυνο επεξεργασίας. Όταν γνωρίζει συγκεκριμένα κάτι, τότε δεν επιτρέπεται να αποκρύψει αυτό με γενικότητες.[433]

4.3.2 Η επεξεργασία των δεδομένων των πελατών με βάση την αρχή του περιορισμού του σκοπού επεξεργασίας

Όταν ένας υπεύθυνος επεξεργασίας (τραπεζικό ίδρυμα) σκοπεύει να επεξεργαστεί περαιτέρω τα προσωπικά δεδομένα των πελατών για σκοπό διαφορετικό από αυτόν για τον οποίο συνελέγησαν, πριν από την περαιτέρω επεξεργασία αυτή, ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει στα υποκείμενα των δεδομένων πληροφορίες σχετικά με τον διαφορετικό αυτό σκοπό καθώς και άλλες περαιτέρω σχετικές πληροφορίες (άρθρο 13 παρ. 3 και 14 παρ. 4 ΓΚΠΔ). Ακόμα και αν το άρθρο 13 παρ. 3 του Κανονισμού δεν κάνει διάκριση ανάμεσα σε έναν περαιτέρω, τελείως διαφορετικό σκοπό και σε ένα περαιτέρω συμβατό σκοπό, η διάταξη αναφέρεται μόνο σε επεξεργασία δεδομένων για συμβατούς μεταξύ τους σκοπούς. Αυτό συμβαίνει διότι το άρθρο 5 παρ. 1 στοιχείο β' του Κανονισμού απαγορεύει την περαιτέρω επεξεργασία δεδομένων για σκοπούς ασύμβατους με τους αρχικούς. Εάν ο υπεύθυνος επεξεργασίας σκοπεύει να ξεκινήσει να επεξεργάζεται τα προσωπικά δεδομένα για έναν νέο, συμβατό σκοπό, θα πρέπει να παρέχει εκ νέου ενημέρωση στα υποκείμενα των δεδομένων ώστε να συμπεριλάβει πληροφορίες σχετικές με τον νέο αυτό σκοπό. Όλα τα στοιχεία της ενημερώσεως που απαιτούνται σύμφωνα με το άρθρο 13 παρ. 2 του Κανονισμού θα πρέπει να ανανεωθούν εάν η επεξεργασία για τον νέο σκοπό δεν καλύπτεται πλήρως από τις υπάρχουσες πληροφορίες. Αυτό θα πρέπει να συμβεί πριν λάβει χώρα η νέα επεξεργασία. Η Ομάδα του άρθρου 29 πρότεινε την ύπαρξη ενός εύλογου διαστήματος ανάμεσα στην ενημέρωση και στην επανέναρξη της επεξεργασίας, αντί της άμεσης εκκίνησής της έπειτα από την ενημέρωση, ώστε να παρέχεται στα υποκείμενα των δεδομένων αρκετός χρόνος για να ασκήσουν τα δικαιώματά τους, εάν κρίνουν αυτό απαραίτητο.[434] Στο άρθρο 31 παρ. 1 του νόμου 4624/2019 προβλέπονται ωστόσο περιπτώσεις στις οποίες δεν υφίσταται η υποχρέωση ενημέρωσης του υποκειμένου κατ' άρθρο 13 παρ. 3 του Κανονισμού. Στις περιπτώσεις αυτές ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για την προστασία των συμφερόντων των υποκειμένων των δεδομένων, συμπεριλαμβανομένης της παροχής στο κοινό πληροφοριών που αναφέρονται στα άρθρα 13 παρ. 1 και 2 ή 14 παρ. 1 και 2.

---

[432] ΑΠΔΠΧ 193/2012. https://www.dpa.gr/sites/default/files/2019-10/193_2012anonym.pdf.

[433] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 120.

[434] Article 29 Working Party, 'Guidelines on Individual Automated Decision- Making and Profiling for the Purposes of Regulation 2016/ 679' (WP251.rev01, as last revised and adopted on 6 February 2018), 24.

4.3.3 Η επεξεργασία των δεδομένων των πελατών με βάση την αρχή της ακρίβειας

Περαιτέρω, τα προσωπικά δεδομένα που έχουν στην κατοχή τους τα τραπεζικά ιδρύματα θα πρέπει να είναι ακριβή και όταν είναι αναγκαίο να επικαιροποιούνται, ενώ θα πρέπει να ανταποκρίνονται συνεχώς στην πραγματικότητα (άρθρο 5 παρ. 1 στοιχείο δ' ΓΚΠΔ). Στο πλαίσιο αυτό, θα πρέπει να λάβουν όλα τα εύλογα μέτρα για να διασφαλίσουν ότι τα δεδομένα είναι ορθά, δίνοντας στους πελάτες τους τη δυνατότητα της διόρθωσης ή της διαγραφής των ανακριβών προσωπικών δεδομένων, χωρίς αδικαιολόγητη καθυστέρηση. Επίσης, η τράπεζα θα πρέπει να διασφαλίζει ότι τα στοιχεία που διαβιβάζει προς τρίτους (π.χ. ύψος οφειλών, ή υπολειπόμενο χρέος) είναι επίσης ακριβή και επικαιροποιημένα.[435][436] Τα μέτρα που απαιτούνται να ληφθούν ώστε να διατηρούνται επικαιροποιημένα τα προσωπικά δεδομένα εξαρτώνται και από τον τύπο των δεδομένων που υφίστανται επεξεργασία αλλά και από τον σκοπό της επεξεργασίας αυτής. Επί παραδείγματι, τα δεδομένα που περιέχονται στα πρακτικά ενός διοικητικού συμβουλίου , δεν θα χρειαστεί να επικαιροποιηθούν εφόσον τηρείται ακριβές αρχείο των πρακτικών αυτών. Αντιθέτως, τα δεδομένα που τηρούνται για να καθοριστεί η φερεγγυότητα ενός φυσικού προσώπου, απαιτούν την συχνή επικαιροποίησή τους.[437]

4.3.4 Η επεξεργασία των δεδομένων των πελατών με βάση την αρχή του περιορισμού της περιόδου αποθήκευσης

Επιπροσθέτως, τα δεδομένα θα πρέπει να διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των πελατών των τραπεζικών ιδρυμάτων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας (άρθρο 5 παρ. 1 στοιχείο ε' ΓΚΠΔ). Η αρχή αυτή, του χρονικού περιορισμού της επεξεργασίας, επιβάλλει την παύση της επεξεργασίας, την καταστροφή δηλαδή των νομίμως κατ' αρχήν συλλεγέντων δεδομένων, μόλις εξυπηρετηθεί ο σκοπός της επεξεργασίας. Στο πεδίο των τραπεζικών συναλλαγών, το χρονικώς αναγκαίο όριο για την διατήρηση των δεδομένων, κρίνεται όχι μόνο με βάση την ολοκλήρωση συγκεκριμένης συναλλαγής, αλλά και με βάση την εύλογη πρόνοια της τράπεζας για την διατήρηση στοιχείων σε περίπτωση που αμφισβητηθεί το κύρος της εκάστοτε συναλλαγής ή ασκηθεί αξίωση εναντίον της. Επίσης, μπορεί ο ίδιος ο πελάτης να ζητήσει στοιχεία, ώστε να θεμελιώσει τυχόν αξίωσή του ή να προσκομίσει αυτά σε δημόσιες αρχές εφόσον του ζητηθούν. Αν ληφθεί υπόψιν και ο μακρύς χρόνος παραγραφής ορισμένων αξιώσεων (π.χ. εικοσαετής παραγραφή σε αξιώσεις από εντολή ή αδικαιολόγητο πλουτισμό), δικαιολογείται η διατήρηση των αρχείων από την τράπεζα για μεγάλο χρονικό διάστημα. Επιπροσθέτως, η διατήρηση των αρχείων από την τράπεζα μπορεί να δικαιολογείται για λόγους που ανάγονται στην εποπτεία αυτής ή στην σχέση της με τις δημόσιες ή φορολογικές αρχές. Για παράδειγμα, οι τράπεζες διαβιβάζουν στοιχεία στην ΤτΕ ή στις φορολογικές αρχές για τους αποστολείς ή δέκτες εμβασμάτων σε πιστωτικά ιδρύματα της αλλοδαπής. Θα πρέπει επίσης να σημειωθεί ότι η διατήρηση στοιχείων στην διάθεση των αρχών αποτελεί διακεκριμένη

---

[435] Sanjay Sharma, *Data Privacy and GDPR Handbook*, 1st ed. (repr., Newark, United States: John Wiley & Sons, Incorporated, 2020), 130.

[436] Για την αντίστροφη περίπτωση, σύμφωνα με την οποία στοιχειοθετείται ευθύνη της Τειρεσίας Α.Ε. για διαβίβαση ανακριβών στοιχείων σε τράπεζα, υπό το καθεστώς της αντίστοιχης διατάξεως του άρθρου 4 παρ. 1 περ. γ' του νόμου 2472/1997 πρβλ. ΕφΑθ. 5717/2008 ΝοΒ 2009, ΠΠρΑθ. 3944/2009 ΤΝΠ ΝΟΜΟΣ.

[437] Peter Carey, *Data Protection - A Practical Guide to UK Law*, 5th ed. (repr., Oxford, UK: Oxford University Press, 2018), 37-38.

επεξεργασία, η νομιμότητα της οποίας κρίνεται αυτοτελώς σε σχέση με την αρχική (διενέργεια επεξεργασίας στο πλαίσιο τραπεζικής συναλλαγής).[438]

4.3.5 Η επεξεργασία των δεδομένων των πελατών με βάση την αρχή της εμπιστευτικότητας και ακεραιότητας

Τέλος, τα δεδομένα θα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη τους ασφάλεια και ιδιαίτερα την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά (άρθρο 5 παρ. 1 στοιχείο στ' ΓΚΠΔ). Η διάταξη επιβάλλει στα τραπεζικά ιδρύματα την υποχρέωση πρόνοιας, ώστε να διαφυλάσσει αποτελεσματικά και να διατηρεί ασφαλή τα δεδομένα που βρίσκονται στην κατοχή της αλλά και να αποτρέπει την διαρροή τους σε τρίτα μέρη. Από τη διατύπωση της διάταξης συνάγεται το συμπέρασμα ότι δεν αρκείται στην εκ μέρους της τράπεζας προσήκουσα οργάνωση των υπηρεσιών της, ώστε να αποτρέπει επιτυχώς την μη εξουσιοδοτημένη επεξεργασία, αλλά επιρρίπτονται σε αυτήν και τυχηρά γεγονότα, η επέλευση των οποίων δεν θα οφείλεται σε πταίσμα των οργάνων της ή των προστηθέντων της. Στο σημείο αυτό θα πρέπει να γίνει αναφορά στην απόφαση 12/2007[439] της ΑΠΔΠΧ, η οποία αφορά περίπτωση στην οποία η τράπεζα δεν τήρησε προσηκόντως τις υποχρεώσεις προνοίας που αφορούν την προστασία των δεδομένων από απώλεια, καταστροφή, μη εξουσιοδοτημένη πρόσβαση ή διαρροή. Συγκεκριμένα, ο υπεύθυνος επεξεργασίας οφείλει να καταστρέψει τα δεδομένα με ασφαλή τρόπο μετά το πέρας της περιόδου που απαιτείται για τον σκοπό της επεξεργασίας. Ωστόσο, η τράπεζα στην προκειμένη περίπτωση εγκατέλειψε έγγραφα πελατών και υπαλλήλων χωρίς προηγουμένως να καταστρέψει αυτά. Αναφορικά με την στοιχειοθέτηση της αστικής ευθύνης, το άρθρο 82 παρ. 3 του ΓΚΠΔ προβλέπει την απαλλαγή του υπευθύνου επεξεργασίας από την ευθύνη του προς αποζημίωση «εάν αποδεικνύει ότι δεν φέρει καμία ευθύνη για το γενεσιουργό γεγονός της ζημίας».[440]

4.4 Τα θεμέλια της νομιμότητας της επεξεργασίας προσωπικών δεδομένων στα πιστωτικά ιδρύματα

Στο πεδίο των τραπεζικών συναλλαγών, η επεξεργασία από τα τραπεζικά ιδρύματα δεδομένων προσωπικού χαρακτήρα είναι σύννομη βάσει κάποιας από τις προβλεπόμενες στον Κανονισμό βάσεις νομιμοποιήσεως της επεξεργασίας (άρθρο 6 παρ. 1 περ. β'- στ'). Αρχικά, η επεξεργασία είναι σύννομη όταν η επεξεργασία είναι απαραίτητη για την εκπλήρωση των συμβατικών υποχρεώσεων των τραπεζών (άρθρο 6 παρ. 1 περ. β' ΓΚΠΔ). Στο πλαίσιο αυτό, η σύναψη τραπεζικών συμβάσεων απαιτεί αναγκαία ορισμένες ενέργειες επεξεργασίας εκ μέρους της τράπεζας, όπως τη συλλογή από τους υπαλλήλους στοιχείων της ταυτότητας και οικονομικών δεδομένων ή την καταχώριση σε αρχεία. Εφόσον κρίνεται ότι η επεξεργασία αυτή είναι απαραίτητη τόσο σε προσυμβατικό ή κατά την εκτέλεση της συμβάσεως, είναι σύννομη, χωρίς να απαιτείται λήψη της συναίνεσης του πελάτη. Όταν η επεξεργασία αποβλέπει όμως σε περαιτέρω

---

[438] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 122-123.

[439]"Ετήσια Έκθεση ΑΠΔΠΧ 2007, 123. Διαθέσιμο στην ιστοσελίδα: https://www.dpa.gr/sites/default/files/2019-09/DPA_ANNUAL_REPORT_2007.PDF.

[440] Ibid., 123.

αξιοποίηση των στοιχείων εκ μέρους της τράπεζας, είναι σύννομη εφόσον έχει ληφθεί η συναίνεση του πελάτη. Η εκδήλωση ενδιαφέροντος από τον πελάτη ως προς την σύναψη συμβάσεως και η εκούσια παράδοση των σχετικών στοιχείων προς την τράπεζα εκφράζει έτσι και αλλιώς σιωπηρή συναίνεση εκ μέρους του για την επεξεργασία. Αυτό όμως δεν αρκεί εφόσον ο Κανονισμός απαιτεί την ρητή συναίνεση των υποκειμένων.[441] Η διάταξη εφαρμόζεται επίσης και στις περιπτώσεις που το υποκείμενο των δεδομένων δεν έχει συμβληθεί με το τραπεζικό ίδρυμα ώστε να εκφράσει τη συναίνεσή του για την επεξεργασία. Παραδείγματα τέτοιων περιπτώσεων αποτελούν η επεξεργασία δεδομένων του λήπτη εμβάσματος ή το άνοιγμα ενεγγύου πιστώσεως. Η εν λόγω επεξεργασία κρίνεται αναγκαία για την εκπλήρωση συμβατικών υποχρεώσεων της τράπεζας, παρά το γεγονός ότι δεν υφίσταται ρητή συγκατάθεση των υποκειμένων.[442]

Περαιτέρω, η επεξεργασία μπορεί να είναι απαραίτητη για τη συμμόρφωση της τράπεζας με έννομη υποχρέωσή της (άρθρο 6 παρ. 1 περ. γ' ΓΚΠΔ). Ως έννομες υποχρεώσεις μπορούν να θεωρηθούν ο έλεγχος πιστοληπτικής ικανότητας του πελάτη αλλά και η διαβίβαση δεδομένων των πελατών της τράπεζας προς εποπτικές ή δημόσιες αρχές (ΕΚΤ, ΤτΕ, φορολογικές, ποινικές κ.ο.κ).[443] Έννομη υποχρέωση όμως υφίσταται και έναντι ιδιωτών.[444] Χαρακτηριστική είναι η προβλεπόμενη στο άρθρο 456 ΑΚ υποχρέωση του εκχωρητή να εκχωρήσει στον εκδοχέα τις αναγκαίες πληροφορίες για την άσκηση της εκχωρούμενης απαιτήσεως.[445] Η διάταξη αυτή καλύπτει την διαβίβαση προσωπικών δεδομένων των οφειλετών σε κάθε περίπτωση εκχωρήσεως από την τράπεζα των απαιτήσεών της εναντίον τους, στο πλαίσιο της μεταβίβασης απαιτήσεων από δάνεια, τιτλοποιήσεις αλλά και εξασφαλιστικές εκχωρήσεις. Ειδικότερα, στις περιπτώσεις της τιτλοποιήσεως και της μεταβιβάσεως απαιτήσεως από δάνεια, η επεξεργασία προσωπικών δεδομένων για τους προαναφερθέντες σκοπούς δεν απαιτεί την συγκατάθεση του οφειλέτη (άρθρο 10 παρ. 21 του νόμου 3156/2003, άρθρο 1 παρ. 21 του νόμου 4354/2015).

Αναφορικά με την επεξεργασία που είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος (άρθρο 6 παρ. 1 περ. δ' ΓΚΠΔ), κρίνεται αμφίβολο εάν το οικονομικό συμφέρον μπορεί να χαρακτηριστεί «ζωτικό» και να επιτραπεί συνεπώς η διαβίβαση των δεδομένων σε άλλο φυσικό πρόσωπο ώστε να αποτραπεί η οικονομική του ζημιά, όπως μπορεί να συμβεί σε περίπτωση ενημέρωσης της τράπεζας προς πελάτη της ότι άλλος πελάτης της, με τον οποίο συνεργάζεται ο πρώτος, έχει καταστεί υπερήμερος έναντι της τράπεζας).[446]

Επιπροσθέτως, η επεξεργασία μπορεί να κρίνεται απαραίτητη για τους σκοπούς των εννόμων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος (άρθρο 6 παρ. 1 περ. στ' ΓΚΠΔ). Εδώ εμπίπτουν οι ενέργειες των τραπεζών για την άσκηση των δικαιωμάτων τους έναντι του πελάτη. Τέτοιες ενέργειες μπορεί επίσης να εντάσσονται στο πλαίσιο πρόληψης εγκλημάτων, ελέγχου ασφάλειας των εγκαταστάσεών τους, ελέγχου και βελτίωσης των πληροφοριακών τους

---

[441] Ibid., 124.
[442] Ibid.
[443] ΑΠΔΠΧ 116/2004, δημοσίευση: www.dpa.gr.
[444] ΑΠ 820/2002, ενημέρωση του κομιστή επιταγής εάν ο λογαριασμός του εκδότη της έχει επαρκές υπόλοιπο, (Δίκαιο Επιχειρήσεων και Εταιρειών, 12/2002).
[445] Δημήτριος Λιάππης, "Το Δίκαιο Των Προσωπικών Δεδομένων - Κατακτήσεις, Αμφισβητήσεις, Προκλήσεις Και Προοπτικές", σε *Προσωπικά Δεδομένα, Ανάλυση - Σχόλια - Εφαρμογή*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2016), 461.
[446] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 126.

συστημάτων, βελτίωσης των τραπεζικών τους προϊόντων κ.λπ. Επίσης, μπορεί να αφορούν την έγερση νομικών αξιώσεων, όπως την σύνταξη και την επίδοση εξώδικων δηλώσεων ή την άσκηση ενδίκων βοηθημάτων ή μέσων κατά του πελάτη.[447] Στις περιπτώσεις αυτές, συμπεριλαμβάνονται στα σχετικά δικόγραφα δεδομένα των πελατών και προσάγονται αποδεικτικά μέσα που τους αφορούν. Στην περίπτωση στ' του άρθρου 6 παρ. 1 ΓΚΠΔ μπορεί να υπαχθεί και η όχληση του πελάτη από την τράπεζα και η ανάθεση της εισπράξεως απαιτήσεων, δια της παροχής εντολής σε Εταιρείες Ενημερώσεως Οφειλετών για ληξιπρόθεσμες απαιτήσεις (νόμος 3758/2009) και εταιρείες Διαχειρίσεως Απαιτήσεων από Δάνεια και Πιστώσεις (νόμος 4354/2015).[448] Ακόμα και αν δεν υφίσταται συναίνεση στις περιπτώσεις αυτές, μπορεί να θεωρηθεί ότι η δικαστική διεκδίκηση απαιτήσεων από την τράπεζα δικαιολογεί την επεξεργασία, που συνίσταται στην διαβίβαση των αναγκαίων δεδομένων στο πρόσωπο που η τράπεζα τις έχει αναθέσει.[449] Πάντως, στις περιπτώσεις αυτές, υποστηρίζεται ότι δεν υφίσταται ζήτημα «διαβιβάσεως» των δεδομένων, καθώς τα προαναφερθέντα νομικά πρόσωπα αποτελούν εκτελούντες την επεξεργασία για λογαριασμό της τράπεζας, ως υπευθύνου επεξεργασίας, και όχι «τρίτους».[450]

4.4.1 Η συγκατάθεση του υποκειμένου ως νομιμοποιητική βάση επεξεργασίας

Ως «συγκατάθεση» του υποκειμένου εννοείται σύμφωνα με τον ορισμό του άρθρου 1 περ. 11 του Κανονισμού «κάθε ένδειξη βουλήσεως, ελεύθερη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν». Η συγκατάθεση του υποκειμένου έχει συλληφθεί ως η κύρια νομιμοποιητική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα εφόσον μέσω της συγκατάθεσής του ή της αρνήσεως αυτής το υποκείμενο ασκεί το δικαίωμά του να αυτοπροσδιορίζεται πληροφοριακά. Η βούληση του υποκειμένου καθιερώνεται σύμφωνα με τα άρθρα 6 παρ. 1 και 9 παρ. 2 στ. α' του Κανονισμού ως λόγος άρσης του άδικου χαρακτήρα της προσβολής της ιδιωτικής σφαίρας. Έννομη συνέπεια της συγκαταθέσεως του υποκειμένου στην επεξεργασία των δεδομένων του είναι η άρση του κατ' αρχήν αδίκου χαρακτήρα της επεξεργασίας αυτής, κατά τούτο δε δεν διαφέρει από οποιαδήποτε άλλη συγκατάθεση σε παράνομη προσβολή διαθετού αγαθού (**volenti non fit injuria**).[451] Η συγκατάθεση του υποκειμένου των δεδομένων τυγχάνει επίσης ειδικής αναφοράς στο άρθρο 8 (2) του ΧΘΔ ως νομιμοποιητική βάση για την επεξεργασία προσωπικών δεδομένων. Επίσης, η σημασία της συνάγεται σιωπηρά από το συνδυασμό των άρθρων 7 ΧΘΔ και 8 της ΕΣΔΑ, καθώς η απουσία της συγκατάθεσης διαδραματίζει σημαντικό ρόλο για να

---

[447] Σχετική είναι η απόφαση 38/2013 ΑΠΔΠΧ, με την οποία έκρινε ότι οι διαβιβάσεις προσωπικών δεδομένων ιδιωτών και επιχειρήσεων είναι νόμιμη και απολύτως αναγκαία για την ικανοποίηση των εννόμων συμφερόντων του υπευθύνου επεξεργασίας σύμφωνα με το άρθρο 5 παρ. 2 εδ. ε του ν. 2472/1997.

[448] Το άρθρο 1 παρ. 21 του νόμου 4354/2015 ορίζει σχετικά ότι χρήζει ανάλογης εφαρμογής η παρ. 21 του άρθρου 10 του νόμου 3156/2003 που ορίζει ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα «δεν προϋποθέτει προηγούμενη άδεια της Αρχής του ν.2472/1997 ή συναίνεση του οφειλέτη».

[449] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 127.

[450] ΟλΑΠΔΠΧ 59/2009, 141-147. Ετήσια Έκθεση ΑΠΔΠΧ 2009. https://www.dpa.gr/sites/default/files/2020-12/DPA_ANNUAL_REPORT_2009.PDF. Επίσης, ΑΠΔΠΧ 98/2017, ΑΠΔΠΧ 20/2001.

[451] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 71.

θεμελιωθεί η παρέμβαση στα δικαιώματα που προβλέπονται στα άρθρα αυτά, παρέμβαση η οποία χρήζει δέουσας αιτιολόγησης ώστε να μην ισοδυναμεί με παραβίαση των σχετικών δικαιωμάτων.

Περαιτέρω, η συγκατάθεση θα πρέπει να αφορά συγκεκριμένα δεδομένα (άρθρο 4, αρ. 11 ΓΚΠΔ) και συγκεκριμένο σκοπό επεξεργασίας (αρχή της ειδικότητας/αρχή του ορισμένου). Αυτό προκύπτει από το άρθρο 6 παρ. 1 στ. α', που κάνει λόγο «για έναν ή περισσότερους σκοπούς». Επίσης προκύπτει και από την αιτιολογική σκέψη 42 του Κανονισμού, που προαπαιτεί την γνώση των σκοπών της επεξεργασίας και του προς όν υπευθύνου αυτής. Σε περίπτωση απρόοπτης μεταβολής των συνθηκών, η συγκατάθεση ανατρέπεται αυτοδίκαια, βάσει της επιταγής για ειδικότητα, χωρίς να απαιτείται προσφυγή σε γενικές ρήτρες των άρθρων 288,388 ΑΚ. Ως προς τη νομική της φύση, η συγκατάθεση αποτελεί δικαιοπραξία, αφού συνίσταται σε δήλωση που κατευθύνεται προς την παραγωγή εννόμου αποτελέσματος (επιτρεπτό της επεξεργασίας), το οποίο επέρχεται εφόσον υπάρχει θέληση του συγκατατιθέμενου υποκειμένου προς αυτό. Περαιτέρω, η συγκατάθεση που προβλέπεται στο άρθρο 4 αρ. 11 του Κανονισμού αποτελεί ειδική περίπτωση εξουσιοδοτήσεως και επομένως είναι εκποιητική και μονομερής. Ως ληψιδεής, απευθύνεται προς τον υπεύθυνο επεξεργασίας, με εξαίρεση την περίπτωση του άρθρου 9 παρ. 2 στ. ε΄, που ορίζει ότι νόμιμη βάση επεξεργασίας αποτελεί και η «δημοσιοποίηση» των δεδομένων από τη μεριά του υποκειμένου. Σε κάθε περίπτωση, το ΕΔΔΑ[452] και η ΑΠΔΠΧ[453] έχουν κρίνει ότι το υποκείμενο χρήζει προστασίας της ιδιωτικότητάς του ακόμα και στον δημόσιο βίο. Παρά το γεγονός ότι στο άρθρο 7 του Κανονισμού χρησιμοποιείται ο όρος «συγκατάθεση», αντί του στενότερου όρου «συναίνεση», από τη διατύπωση του άρθρου 6 παρ. 1 στ. α' («Η επεξεργασία είναι σύννομη εάν το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία»), προκύπτει ότι η συγκατάθεση θα πρέπει να έχει παρασχεθεί από το υποκείμενο πριν λάβει χώρα η επεξεργασία των δεδομένων.

Στο πλαίσιο των τραπεζικών συναλλαγών, η συγκατάθεση των υποκειμένων-πελατών, αποτελεί τη βάση για κάθε επεξεργασία που κρίνεται αναγκαία για την εκτέλεση της συμβάσεως που έχει συνάψει η τράπεζα με τον πελάτη. Η επεξεργασία αυτή μπορεί να συνίσταται στην συλλογή προσωπικών στοιχείων, την καταχώριση, αποθήκευση, διαβίβαση σε τρίτους όπως σε ανταποκρίτριες τράπεζες κ.ο.κ. Αν και η συγκατάθεση αυτή παρέχεται κατά την σύναψη της εκάστοτε συμβάσεως, ο πελάτης συνήθως συγκατατίθεται και στην περαιτέρω επεξεργασία των δεδομένων του, που μπορεί να διενεργείται για την εκπλήρωση των νομίμων υποχρεώσεων της τράπεζας ή για την άσκηση των δικαστικών ή εξώδικων υποχρεώσεών της κατά του πελάτη.[454]

Παρά τον έντονα προσωποπαγή χαρακτήρα της, η αντιπροσώπευση στο πλαίσιο τραπεζικών συναλλαγών ενδέχεται να παρέχεται στο πλαίσιο συμβάσεως που συνάπτεται δι΄αντιπροσώπου. Εάν δεχτούμε επομένως ότι έγκυρα μπορεί να συναφθεί σύμβαση καταθέσεως ή δανείου δι' αντιπροσώπου, θα ήταν παράδοξο να δεχτούμε ότι η συγκατάθεση που παρέχεται στο πλαίσιο της συμβάσεως για την επεξεργασία προσωπικών δεδομένων του δανειολήπτη ή καταθέτη δεν είναι έγκυρη, επειδή ειδικώς η συγκατάθεση δεν είναι δεκτική αντιπροσωπεύσεως.

Καθώς ο Κανονισμός δεν ορίζει τυπικές προϋποθέσεις για τον τρόπο παροχής της συγκατάθεσης, αυτή μπορεί θεωρητικά να δοθεί με προφορική ή γραπτή δήλωση, συμπεριλαμβανομένης της

---

[452] Βλ. υπόθεση Copland κατά Ηνωμένου Βασιλείου.

[453] Βλ. Γνωμοδότηση 1/2009 ΑΠΔΠΧ σχετικά με τη λειτουργία κλειστών κυκλωμάτων τηλεόρασης σε δημόσιους χώρους. Σε Ετήσια Έκθεση ΑΠΔΠΧ 2009, σελ. 174 επ.

[454] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 129.

ηλεκτρονικής. Η συγκατάθεση θα πρέπει πάντως να είναι «ρητή» και «συγκεκριμένη». Ειδικότερα, στην αιτιολογική σκέψη 32 αναφέρεται ότι: «Η συγκατάθεση πρέπει να παρέχεται με σαφή θετική ενέργεια η οποία να συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει ένδειξη της συμφωνίας του υποκειμένου των δεδομένων υπέρ της επεξεργασίας των δεδομένων που το αφορούν, για παράδειγμα με γραπτή δήλωση, μεταξύ άλλων με ηλεκτρονικά μέσα, ή με προφορική δήλωση». Όπως προαναφέρθηκε, τα άρθρα 5 παρ. 1 β' και 6 παρ. 1 α' του Κανονισμού, απαιτούν τον σαφή καθορισμό των σκοπών της επεξεργασίας, συμβάλλοντας έτσι στην πλήρωση του κριτηρίου της εξειδίκευσης. Όπως αναφέρει η Ομάδα του άρθρου 29, η «συγκατάθεση θα πρέπει να παρέχεται για συγκεκριμένο σκοπό»[455] και «ένας σκοπός που είναι ασαφής ή γενικός…δεν θα ανταποκρίνεται στα κριτήρια της ακρίβειας».[456] Επομένως, δεν θα είναι έγκυρη η συναίνεση για διαβίβαση δεδομένων γενικά σε «τρίτους» ή «για κάθε νόμιμο σκοπό». Σύμφωνα με την αιτιολογική σκέψη υπ'αριθ. 32, «Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει να δίνεται συγκατάθεση για όλους αυτούς τους σκοπούς».

Στο πεδίο των τραπεζικών συναλλαγών, τηρείται κατά κανόνα ο έγγραφος τύπος, όταν η συγκατάθεση παρέχεται στο πλαίσιο έγγραφης συνάψεως τραπεζικής σύμβασης. Επιπροσθέτως, με βάση την αρχή της λογοδοσίας, το βάρος απόδειξης για την παροχή έγκυρης συγκατάθεσης φέρει ο υπεύθυνος επεξεργασίας, γι' αυτό είναι προτιμητέος ο έγγραφος τύπος.[457] Με βάση τα άρθρα 1 παρ. 11 και 6 παρ. 1 περ. α' του Κανονισμού, αρκεί πάντως η συγκατάθεση του πελάτη που παρέχεται χωρίς ιδιόχειρη υπογραφή του, ή μέσω της χρήσης των μέσων της σύγχρονης τραπεζική, δηλαδή ηλεκτρονικά με τη συμπλήρωση σχετικού πεδίου ή με ηλεκτρονικό μήνυμα ή και τηλεφωνικώς. Σε κάθε περίπτωση η συγκατάθεση που παρέχει το υποκείμενο θα πρέπει να είναι «ελεύθερη», «ρητή» και «συγκεκριμένη».

Για να είναι «ελεύθερη» η συγκατάθεση, το υποκείμενο θα πρέπει να απολαμβάνει έναν υψηλό βαθμό αυτονομίας όταν επιλέγει εάν θα παρέχει ή όχι τη συγκατάθεσή του. Επίσης δεν θα πρέπει να αποτελεί προϊόν ελαττωματικής βούλησης (πλάνης, απάτης ή απειλής)[458], ειδάλλως θα είναι ακυρώσιμη (ΑΚ 140), ως δήλωση βουλήσεως.[459] Σύμφωνα με την Ομάδα του άρθρου 29, «εάν το υποκείμενο των δεδομένων δεν είναι σε θέση να αρνηθεί ή να αποσύρει τη συγκατάθεσή του χωρίς να ζημιωθεί, τότε η συγκατάθεση δεν θεωρείται ελεύθερη».[460] Το κριτήριο δεν πληροίται στις περιπτώσεις στις οποίες το υποκείμενο των δεδομένων βρίσκεται σε άνιση θέση ή θέση εξάρτησης σε σχέση με τον υπεύθυνο επεξεργασίας. Η αιτιολογική σκέψη υπ'αριθ. 43 αναφέρεται σε αυτού του είδους τη σχέση στο πλαίσιο «μιας σαφούς ανισότητας ανάμεσα στο υποκείμενο τον δεδομένων και τον υπεύθυνο επεξεργασίας». Η διατύπωση είναι κατά μια έννοια ασαφής, καθώς δεν υπογραμμίζει ρητά την βασική φύση της ανισότητας, αλλά το πλαίσιο εντός του οποίου

---

[455] Ομάδα εργασίας του άρθρου 29, «Κατευθυντήριες γραμμές σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679», 17/EL WP259 αναθ.01, (28 Νοεμβρίου 2017), 15.
[456] Article 29 Working Party, 'Opinion 3/ 2013 on Purpose Limitation' (WP 203, 2 April 2013), 16.
[457] Ειρηνικός Πλατής, *Προσωπικά Δεδομένα-Προστασία GDPR*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Παπαδόπουλος, 2018), 42.
[458] Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, *Προσωπικά Δεδομένα*, 1η εκδ. (Θεσσαλονίκη: Νομική Βιβλιοθήκη, 2016), 89.
[459] Αντίθετη άποψη υποστηρίζει ο Χριστοδούλου, Κ., Δίκαιο Προσωπικών Δεδομένων, 2η εκδ., 86, σύμφωνα με την οποία η συγκατάθεση θα είναι άκυρη, καθώς το γενικό δίκαιο των ελαττωμάτων της βούλησης εκτοπίζεται από το ειδικότερο και τυπικώς υπέρτερο άρθρο 4, αρ. 11 ΓΚΠΔ.
[460] Ομάδα εργασίας του άρθρου 29, «Κατευθυντήριες γραμμές σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679», 17/EL WP259 αναθ.01, (28 Νοεμβρίου 2017), 6.

εμφανίζεται καθιστά σαφές ότι η ανισότητα αυτή είναι θέμα ισχύος. Παράδειγμα σχέσεως που χαρακτηρίζεται από μια ξεκάθαρη ανισότητα ισχύος αποτελεί η σχέση ανάμεσα σε εργοδότη και εργαζόμενο. Επομένως, σύμφωνα με την Ομάδα του άρθρου 29, «οι εργαζόμενοι ως υποκείμενα των δεδομένων είναι απίθανο να είναι σε θέση να αρνηθούν να παράσχουν στον εργοδότη τους συγκατάθεση για την επεξεργασία των δεδομένων τους χωρίς να φοβούνται ή χωρίς να διατρέχουν πραγματικό κίνδυνο να υποστούν αρνητικές συνέπειες λόγω της άρνησής τους».[461][462] Κρίσιμη με βάση τα προαναφερθέντα θεωρείται και η Οδηγία 115/2001 της ΑΠΔΠΧ για την επεξεργασία των προσωπικών δεδομένων στο πεδίο των εργασιακών σχέσεων, η οποία θέτει τα νόμιμα πλαίσια της σχετικής επεξεργασίας τους.[463] Ένα άλλο παράδειγμα σχέσεως στην οποία η συγκατάθεση δεν προκύπτει πάντοτε από την ελεύθερη βούληση του υποκειμένου είναι οι συμβάσεις προσχώρησης. Εδώ εντάσσεται και η συναλλακτική σχέση τραπεζών και δανειοληπτών, ιδιαίτερα απλών καταναλωτών, οι οποίοι για να πάρουν δάνειο συγκατατίθενται, μέσω της υπογραφής συμβάσεως, να δηλώσουν πλήθος προσωπικών τους δεδομένων, που πολλές φορές ξεπερνούν τον επιδιωκόμενο σκοπό (π.χ. ποια είναι η οικογενειακή κατάσταση, εάν και πόσα παιδιά έχουν, την ηλικία ή το στάδιο εκπαίδευσής τους κ.α.)[464]

Περαιτέρω, σε εξειδίκευση της προβλέψεως που αφορά την «ελεύθερη» συγκατάθεση, το άρθρο 7 παρ. 4 του Κανονισμού αναφέρει ότι «Κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης». Η κρίση στην περίπτωση αυτή θα αφορά αποκλειστικά επεξεργασία που δεν ήταν αντικειμενικώς αναγκαία για την εκτέλεση της εκάστοτε συμβάσεως. Εάν για παράδειγμα, ο πελάτης αναγκαστεί να προσκομίσει τα αιτούμενα οικονομικά στοιχεία και να συναινέσει στην επεξεργασία τους από την τράπεζα, διότι σε διαφορετική περίπτωση δεν θα εγκριθεί η αίτησή του για δάνειο, δεν πρόκειται για συγκατάθεση που δεν έχει παρασχεθεί «ελευθέρως». Αντιθέτως, όταν η τράπεζα αρνηθεί να αξιολογήσει αίτημα πελάτη εάν αυτός δεν συναινέσει σε περαιτέρω χρήση και διαβίβαση των στοιχείων του σε θυγατρικές της τράπεζας για διαφημιστικούς σκοπούς, πρόκειται για επεξεργασία που δεν είναι αναγκαία για να εκτελεστεί η υπό διαπραγμάτευση σύμβαση.[465]Στο πλαίσιο αυτό σχετική είναι η απόφαση υπ'αριθ. 18/2007 της Αρχής, με την οποία η Αρχή απεφάνθη ότι ο όρος που συμπεριλαμβανόταν σε προεκτυπωμένη αίτηση για χορήγηση χρεωστικής κάρτας και με τον οποίο παρέχεται εκ των προτέρων συγκατάθεση του

---

[461] Ibid., 8.

[462]Στην υπόθεση Υπόθεση C-673/17, *Planet49 GmbH κατά Bundesverband der Verbraucherzentralen und Verbraucherverbände*, παρ. 66, ο ΓΕ Szpunar χαρακτηριστικά ανέφερε ότι: «Για να μπορεί να θεωρηθεί ότι η συγκατάθεση παρέχεται «ελεύθερα» και «εν πλήρει επιγνώσει», δεν αρκεί αυτή να είναι μόνο ενεργή, αλλά πρέπει να είναι και διακριτή. Η δραστηριότητα του χρήστη στο Διαδίκτυο (ανάγνωση ιστοσελίδας, συμμετοχή σε κερδοφόρο παιχνίδι, παρακολούθηση βίντεο κ.λπ.) και η χορήγηση συγκατάθεσης δεν μπορούν να εντάσσονται στην ίδια πράξη. Ειδικότερα, από τη σκοπιά του χρήστη, η χορήγηση συγκατάθεσης δεν μπορεί να φαίνεται ότι έχει παρεπόμενο χαρακτήρα σε σχέση με τη συμμετοχή στο κερδοφόρο παιχνίδι. Αμφότερες οι πράξεις πρέπει να εκδηλώνονται, ιδίως οπτικά, επί ίσοις όροις. Κατά συνέπεια, εκτιμώ ότι είναι αμφίβολο κατά πόσον μια δέσμη δηλώσεων βουλήσεως η οποία περιλαμβάνει τη χορήγηση συγκατάθεσης μπορεί να θεωρηθεί ότι συνάδει με την έννοια της συγκατάθεσης κατά την οδηγία 95/46».

[463] Βλ. την Οδηγία αυτή σε https://www.dpa.gr/sites/default/files/2019-10/2001_115_1.doc.

[464] Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, *Προσωπικά Δεδομένα*, 1η εκδ. (Θεσσαλονίκη: Νομική Βιβλιοθήκη, 2016), 91.

[465] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 132.

προσφεύγοντος για επεξεργασία των προσωπικών του δεδομένων για διαφημιστικούς ή προωθητικούς σκοπούς, είναι παράνομος. Η συγκατάθεση στην περίπτωση αυτή δεν ήταν ειδική και ελεύθερη, καθώς ο προσφεύγων υποχρεώθηκε να αποδεχτεί τον συγκεκριμένο όρο, εφόσον σε αντίθετη περίπτωση δεν θα γινόταν κάτοχος της χρεωστικής κάρτας. Επιπροσθέτως, δεν είχε προηγηθεί η απαιτούμενη ενημέρωση του προσφεύγοντος με βάση τις διατάξεις του ν. 2472/1997.[466]

Η απαίτηση σύμφωνα με την οποία η συγκατάθεση πρέπει βασίζεται σε προηγούμενη πλήρη ενημέρωση του υποκειμένου για να είναι έγκυρη, προϋποθέτει ότι θα πρέπει να διασφαλιστεί ότι το υποκείμενο των δεδομένων έχει προηγουμένως ενημερωθεί σχετικά με τις παραμέτρους της διαδικασίας της επεξεργασίας στην οποία πρόκειται να συναινέσει.[467] Η απαίτηση ενισχύεται από την θεμελιώδη αρχή της διαφάνειας, όπως διατυπώνεται στο άρθρο 5 παρ. 1 στοιχείο α' του Κανονισμού, σε συνδυασμό με τις γενικές απαιτήσεις για την παροχή πληροφοριών στα υποκείμενα των δεδομένων, όπως αυτές διατυπώνονται στα άρθρα 7 παρ. 3 και 12-14 του Κανονισμού. Στην αιτιολογική σκέψη υπ'αριθ. 42 αναφέρεται επίσης ότι «για να θεωρηθεί η συγκατάθεση εν επιγνώσει, το υποκείμενο των δεδομένων θα πρέπει να γνωρίζει τουλάχιστον την ταυτότητα του υπευθύνου επεξεργασίας και τους σκοπούς της επεξεργασίας για την οποία προορίζονται τα δεδομένα προσωπικού χαρακτήρα». Ωστόσο, η ομάδα του άρθρου 29 διατύπωσε μια εκτενέστερη λίστα σχετικά με τις «ελάχιστες απαιτήσεις του περιεχομένου» ώστε η συγκατάθεση να θεωρείται «εν πλήρει επιγνώσει», προσθέτοντας στοιχεία όπως τα είδη των δεδομένων που υφίστανται επεξεργασία, την ύπαρξη του δικαιώματος ανακλήσεως της συναίνεσης και τις κατηγορίες ή τις ταυτότητες των αποδεκτών των δεδομένων.[468]Επίσης, σχετική είναι η διάταξη του άρθρου 49 παρ. 1 στ. α' του Κανονισμού που επιτρέπει την διαβίβαση των προσωπικών δεδομένων σε Τρίτη χώρα ή σε διεθνή οργανισμό, σε περίπτωση απουσίας απόφασης επάρκειας ή κατάλληλων εγγυήσεων, «όταν το υποκείμενο των δεδομένων συγκατατέθηκε ρητώς στην προτεινόμενη διαβίβαση, αφού ενημερώθηκε για τους πιθανούς κινδύνους που εγκυμονούν τέτοιες διαβιβάσεις δεδομένων για το υποκείμενο των δεδομένων». Στην υπόθεση Planet49, ο ΓΕ Szpunar χαρακτήρισε την υποχρέωση για πλήρη ενημέρωση του υποκειμένου πριν αναζητηθεί η συγκατάθεσή του σε επιγραμμικό πλαίσιο ως εξής: «Στο πλαίσιο αυτό, πρέπει να καθίσταται απολύτως σαφές στον χρήστη κατά πόσον η δραστηριότητά του στο Διαδίκτυο εξαρτάται από τη χορήγηση συγκατάθεσης. Ο χρήστης πρέπει να είναι σε θέση να εκτιμήσει σε ποιον βαθμό είναι διατεθειμένος να παράσχει τα δεδομένα του, προκειμένου να δραστηριοποιηθεί στο Διαδίκτυο. Δεν πρέπει να καταλείπεται περιθώριο για οποιαδήποτε ασάφεια . Ο χρήστης πρέπει να γνωρίζει αν και, σε περίπτωση καταφατικής απάντησης, σε ποιον βαθμό η χορήγηση της συγκατάθεσής του ασκεί επιρροή όσον αφορά τη δραστηριοποίησή του στο Διαδίκτυο.»[469]

Η τράπεζα επομένως, θα πρέπει στο πλαίσιο της συναλλακτικής της σχέσης με τον πελάτη, να ενημερώσει αυτόν με διαφανή και κατανοητό, αναφορικά με το είδος της επεξεργασίας, τους

---

[466] Ετήσια έκθεση ΑΠΔΠΧ 2007, απόφαση 18/2007, σελ. 127-129. https://www.dpa.gr/sites/default/files/2019-09/DPA_ANNUAL_REPORT_2007.PDF.

[467] Βλ. και υπόθεση C-40/17, *Fashion ID*, παράγραφοι 102–106 (ερμηνεία των απαιτήσεων συγκατάθεσης και ενημέρωσης υπό την Οδηγία 95/46). Επίσης, κατ' αναλογία, βλ. υποθέσεις C-397/ 01 to C-403/ 01, *Pfeiffer*, παρ. 82.

[468] Ομάδα εργασίας του άρθρου 29, «Κατευθυντήριες γραμμές σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679», 17/EL WP259 αναθ.01, (28 Νοεμβρίου 2017), 16.

[469] Υπόθεση C-673/17, *Planet49 GmbH κατά Bundesverband der Verbraucherzentralen und Verbraucherverbände*, παρ. 67. https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:62017CC0673&from=GA.

σκοπούς αυτής, αλλά και την ταυτότητα ενδεχόμενων τρίτων αποδεκτών[470]. Σύμφωνα με την 1/1999 κανονιστική πράξη της Αρχής, η ενημέρωση για να είναι πλήρης πρέπει επίσης να περιλαμβάνει την ακριβή διεύθυνση και τον αριθμό τηλεφώνου του υπευθύνου επεξεργασίας ή του εκπροσώπου του και την ύπαρξη δικαιώματος αντίρρησης για τα δεδομένα που αφορούν το υποκείμενο.[471] Εάν λείπει η ενημέρωση αυτή, η συγκατάθεση πάσχει και δεν δύναται να λειτουργήσει ως νομιμοποιητική βάση επεξεργασίας. Περαιτέρω η συγκατάθεση θα πρέπει να είναι «ρητή», δηλαδή να εκδηλώνεται με τέτοια μέσα (π.χ. προφορικός λόγος, έγγραφο, ηλεκτρονικά) ώστε να συνάγεται η βούληση του υποκειμένου. Ως ρητή θεωρείται και η συγκατάθεση που παρέχεται αθόρυβα (μέσω χειρονομιών ή νευμάτων), αρκεί να συνάγεται με σαφή τρόπο ότι άμεσος σκοπός είναι η εξωτερίκευση της βούλησης για συγκατάθεση.[472]Όπως χαρακτηριστικά αναφέρει η Κώστα, «η συγκατάθεση που δίνεται με διφορούμενο τρόπο, ισοδυναμεί με μια ασαφή ένδειξη των επιθυμιών του υποκειμένου των δεδομένων… και επομένως δεν μπορεί να θεωρηθεί ως έγκυρη συγκατάθεση».[473] Σχετικά με την απαίτηση σύμφωνα με την οποία η συγκατάθεση του υποκειμένου θα πρέπει να είναι «ρητή», θα πρέπει να γίνει αναφορά στην απόφαση 39/2015 της Αρχής, με βάση την οποία η τελευταία απεφάνθη ότι η επεξεργασία που πραγματοποιείται στο πλαίσιο λειτουργίας της υπηρεσίας «Winbank for cards», δεν μπορεί να θεωρηθεί ως απολύτως απαραίτητη στο πλαίσιο των συμβατικών σχέσεων ανάμεσα στον υπεύθυνο επεξεργασίας και τον εκάστοτε πελάτη της τράπεζας, εφόσον η πληροφόρηση για τις κινήσεις των καρτών μπορεί να παρέχεται και με άλλους τρόπους (π.χ. μέσω ταχυδρομείου). Επομένως, για την εν λόγω επεξεργασία δεν συντρέχει το στοιχείο της αναγκαιότητας και δεν μπορεί να τύχει εφαρμογής η εξαίρεση του άρθρου 5 παρ. 2 στοιχ. α' του ν. 2472/1997. Με βάση τα προαναφερθέντα, η Αρχή κάλεσε την τράπεζα να διασφαλίσει ότι όσον αφορά τους νέους πελάτες-κατόχους πιστωτικών καρτών, η εν λόγω υπηρεσία θα παρέχεται αφού προηγηθεί η ρητή και ειδική συγκατάθεσή τους ότι επιθυμούν αυτήν (σύστημα opt-in) και αφού ενημερωθούν προσηκόντως ως προς αυτήν. Η δήλωση συγκατάθεσης θα πρέπει να παρέχεται από τους πελάτες, με φυσική τους παρουσία, σε κατάστημα της τράπεζας ή ηλεκτρονικά, κατά τρόπο που να διασφαλίζει την πιστοποίηση της ταυτότητας των αιτούντων. Αναφορικά με τους νυν πελάτες-κατόχους πιστωτικών καρτών, που δεν έχουν δηλώσει την αντίρρησή τους για την συγκεκριμένη υπηρεσία, θα πρέπει η τράπεζα να προβεί σε ατομική ενημέρωσή τους, στην οποία θα αναφέρεται ότι η υπηρεσία είναι ενεργή και θα περιγράφονται τα χαρακτηριστικά της αλλά και ο τρόπος διακοπής της. Η τράπεζα υποχρεώθηκε περαιτέρω να διασφαλίζει ότι σε περίπτωση που

---

[470] Αποδέκτες των προσωπικών δεδομένων των πελατών των τραπεζών είναι οι υπάλληλοι και τα στελέχη της τράπεζας, στελέχη θυγατρικών εταιρειών του πιστωτικού ιδρύματος, άλλα πιστωτικά ή χρηματοδοτικά ιδρύματα (ν. 3156/2003), φορείς στους οποίους το πιστωτικό ίδρυμα αναθέτει τη διεκπεραίωση εργασιών για λογαριασμό του, φορείς συγχρηματοδότησης ή παροχής εγγυήσεων, εταιρείες ενημέρωσης οφειλετών (ν. 3758/2009) ή διαχείρισης απαιτήσεων (ν. 4354/2015), δικηγόροι ή δικηγορικές εταιρείες, εταιρείες που αναλαμβάνουν την επικαιροποίηση στοιχείων ταυτοποίησης, εταιρείες ή φορείς που αποκτούν απαιτήσεις του πιστωτικού ιδρύματος, εποπτικές των πιστωτικών ιδρυμάτων αρχές, η εταιρεία ΤΕΙΡΕΣΙΑΣ Α.Ε., εταιρείες προβολής και προώθησης προϊόντων και υπηρεσιών. (βλ. Κώδικα δεοντολογίας ελληνικών τραπεζών, σχέδιο 16/1/2019, σελ. 21-23.)

[471] Ετήσια έκθεση ΑΠΔΠΧ 2007, 128.
https://www.dpa.gr/sites/default/files/2019-09/DPA_ANNUAL_REPORT_2007.PDF.

[472] Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, *Προσωπικά Δεδομένα*, 1η εκδ. (Θεσσαλονίκη: Νομική Βιβλιοθήκη, 2016), 91.

[473] Eleni Kosta, *Consent in European Data Protection Law*, 1st ed. (repr., Leiden: Martinus Nijhoff Publishers, 2013), 235.

προχωρήσει στο μέλλον σε τροποποίηση της υπηρεσίας, θα παρέχει πρόσφορη σχετική ενημέρωση στους πελάτες-χρήστες αυτής.[474]

Αν και δεν απαιτείται η συγκατάθεση να είναι έγγραφη, σύμφωνα με το άρθρο 7 (1) και την αιτιολογική σκέψη υπ'αριθ. 42, ο υπεύθυνος επεξεργασίας θα πρέπει να είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων έχει συγκατατεθεί στις πράξεις επεξεργασίας. Επομένως, θα πρέπει να υπάρχει κάποιου είδους έγγραφη τεκμηρίωση της διαδικασίας παροχής συναινέσεως. Η Ομάδα εργασίας του άρθρου 29 αναφέρει σχετικά ότι: «Ένας προφανής τρόπος για να διασφαλίζεται ότι η συγκατάθεση είναι ρητή είναι να επιβεβαιώνεται ρητώς σε γραπτή δήλωση. Όπου ενδείκνυται, ο υπεύθυνος επεξεργασίας μπορεί να διασφαλίζει ότι το υποκείμενο των δεδομένων υπογράφει τη γραπτή δήλωση, προκειμένου να αρθεί κάθε ενδεχόμενη αμφιβολία και δυνητική έλλειψη αποδείξεων στο μέλλον».[475]

Περαιτέρω, η συγκατάθεση μπορεί να παρέχεται σε προδιατυπωμένους Γενικούς Όρους Συναλλαγών της τράπεζας. Στην περίπτωση αυτή, πέρα από την εφαρμογή των γενικών διατάξεων του άρθρου 2 του ν. 2251/1994, θα εφαρμόζονται και οι ειδικότερες διατάξεις του Κανονισμού. Επομένως, θα πρέπει να αποχωρίζεται η υπόδειξη του ΓΟΣ της συγκαταθέσεως από το υπόλοιπο σώμα της συμβάσεως προσχώρησης και επιπλέον να μην γίνεται διαπραγμάτευση *in totto* ως προς αυτήν.Ο όρος περί συγκαταθέσεως θα πρέπει να είναι διακεκριμένος από τους υπολοίπους («σαφώς διακριτός», άρθρο 7 παρ. 2) και, σε περίπτωση που αφορά επεξεργασία που δεν είναι αναγκαία για να εκτελεστεί η σύμβαση στην οποία αφορούν οι ΓΟΣ, να απαιτείται επιπλέον διακεκριμένη αποδοχή ή απόρριψη (άρθρο 7 παρ. 4 ΓΚΠΔ). Αυτό μπορεί να εξασφαλιστεί μέσω της προσθήκης χωριστού τετραγωνιδίου, που θα αφορά την αποδοχή ή μη του συγκεκριμένου όρου και το οποίο ο καταναλωτής-πελάτης καλείται να επισημειώσει ανάλογα με το αν προσχωρεί στον συγκεκριμένο ΓΟΣ ή όχι. Η επεξεργασία των προσωπικών δεδομένων υποβάλλεται κατά αυτόν τον τρόπο σε χωριστό *opt-in* από την υπόλοιπη σύμβαση στην οποία περιλαμβάνεται ως όρος. Στην περίπτωση που το υποκείμενο δεν συμφώνησε χωριστά να δώσει τη συγκατάθεσή του, δηλαδή δεν προσχώρησε στον σχετικό όρο, τότε γίνεται δεκτό ότι ο όρος αυτός δεν έχει ενταχθεί νομίμως στη σύμβαση, όπως συμβαίνει και με τους ανέντακτους ΓΟΣ.[476]

Η ανάκληση της συγκατάθεσης μπορεί να λάβει χώρα οποτεδήποτε, χωρίς να έχει όμως αναδρομικό αποτέλεσμα. Από τη στιγμή που θα περιέλθει στον υπεύθυνο επεξεργασίας των εν λόγω δεδομένων, καθιστά παράνομη κάθε περαιτέρω επεξεργασία, εφόσον προφανώς δεν συντρέχει άλλη νομιμοποιητική βάση. Εφόσον η ανάκληση δεν δρα αναδρομικώς, τα δεδομένα που είχαν αποτελέσει αντικείμενο επεξεργασίας κατά τον χρόνο από την περιέλευση της συναινέσεως στον υπεύθυνο επεξεργασίας και πριν από την ανάκλησή της νομίμως έχουν τύχει επεξεργασίας.[477]

---

[474] Ετήσια έκθεση ΑΠΔΠΧ 2015, απόφαση 39/2015, σελ. 165-169. https://www.dpa.gr/sites/default/files/2020-12/ANNUAL%202015%20V2.0%20WEB%20VIEW2.PDF.

[475] Ομάδα εργασίας του άρθρου 29, «Κατευθυντήριες γραμμές σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679», 17/EL WP259 αναθ.01, (28 Νοεμβρίου 2017), 23.

[476] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 88.

[477]Γεώργιος Καλλιμόπουλος, "Ανάκληση Συναίνεσης Του Υποκειμένου Περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Γνωμ.)", *Χρηματοπιστωτικό Δίκαιο*, no. 3 (2010): 285-295.

4.5 Οι σκοποί επεξεργασίας των προσωπικών δεδομένων των πελατών των τραπεζικών ιδρυμάτων

Στο πλαίσιο των ενεργητικών και παθητικών εργασιών τους, τα τραπεζικά ιδρύματα επεξεργάζονται πληθώρα προσωπικών δεδομένων των υποκειμένων-πελατών τους, ώστε να εκπληρώνουν τις συμβατικές υποχρεώσεις τους[478], αλλά και να διαχειρίζονται τις συναλλαγές και τα αιτήματα των πελατών τους για την λήψη τραπεζικών υπηρεσιών. Παραδοσιακή είναι η διάκριση, από την πλευρά της τράπεζας, ανάμεσα σε ενεργητικές και παθητικές εργασίες, αναλόγως του αν η τελευταία εμφανίζεται ως δανείστρια ή οφειλέτης. Ως τυπικές περιπτώσεις ενεργητικών τραπεζικών εργασιών μπορούν να αναφερθούν το δάνειο, η παροχή πιστώσεως και οι διάφορες μορφές αναλήψεως εγγυητικής ευθύνης από την τράπεζα. Ως παθητική τραπεζική εργασία μπορεί να χαρακτηριστεί η αποδοχή καταθέσεων από την τράπεζα. Πέραν όμως των ενεργητικών και παθητικών εργασιών, υπάρχει ένα ευρύ και ολοένα διευρυνόμενο φάσμα τραπεζικών εργασιών, που συνίσταται στην επ'αμοιβή παροχή υπηρεσιών από την τράπεζα στους πελάτες της. Ανάμεσα στις υπηρεσίες αυτές βρίσκεται η απλή μεταφορά χρημάτων από πελάτη σε πελάτη της τράπεζας, η περίπλοκη παροχή επενδυτικών συμβουλών αλλά και η διαχείριση χαρτοφυλακίου των πελατών. Οι παροχή των σύγχρονων αυτών υπηρεσιών αυτών εγείρει ζητήματα που αφορούν τα προσωπικά δεδομένα των πελατών, τόσο ως προς το εύρος των εξουσιών της τράπεζας όσο και ως προς το περιεχόμενο και την έκταση της ευθύνης της.[479][480]

Στο πλαίσιο αυτό, οι τράπεζες διαθέτουν στους πελάτες τους καταθετικά, επενδυτικά, χορηγητικά και προϊόντα μεικτής φύσης (π.χ. καταθέσεις μέρος των οποίων επενδύεται σε αξίες).Επίσης, αποδέχονται καταθέσεις και χορηγούν δάνεια, ενώ συχνά παρέχουν και επενδυτικές υπηρεσίες (ν. 4514/2018). Για να χορηγήσουν τα προϊόντα αυτά και να παρέχουν στους πελάτες τους τις υπηρεσίες αυτές, οι τραπεζικές επιχειρήσεις προχωρούν στην επεξεργασία προσωπικών δεδομένων, τόσο σε προσυμβατικό στάδιο αλλά και κατά τη διάρκεια της ισχύος των σχετικών συμβάσεων, για τη λειτουργία αυτών, αλλά και μετά τη λήξη της ισχύος τους, προασπίζοντας παράλληλα τα έννομα συμφέροντα τους, αλλά και τα αντίστοιχα των πελατών τους. Περαιτέρω, η επεξεργασία των προσωπικών δεδομένων των πελατών διενεργείται για την ταυτοποίηση και την επαλήθευση των στοιχείων τους κατά τη διενέργεια συναλλαγών, για την αξιολόγηση των αιτήσεων των πελατών αλλά και γενικότερα των αιτημάτων τους, για την εξυπηρέτηση, την υποστήριξη και την εκτέλεση πάσης φύσεως συναλλαγών, συμπεριλαμβανομένων αυτών που διενεργούνται σε περιβάλλον ηλεκτρονικής τραπεζικής (**e-banking, mobile banking, phone**

---

[478] Βλ. αποφάσεις 60/2009 και 59/2009 ΑΠΔΠΧ, στις οποίες η Αρχή έκρινε ότι δεν απαιτείται η συγκατάθεση του υποκειμένου (άρθρο 5 παρ. 1 α ν. 2497/1997) για την τήρηση σε ηλεκτρονικό η μη αρχείο των ατομικών στοιχείων του συμβαλλομένου και την περαιτέρω επεξεργασία τους, που γίνεται για σκοπούς εκτέλεσης σύμβασης στην οποία συμβαλλόμενο μέρος είναι το υποκείμενο των δεδομένων.

[479] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 154.

[480] Βλ. **ΑΠ 1352/2011**, σύμφωνα με την οποία: «Οι τράπεζες, ως χρηματοδοτικοί οργανισμοί που ασκούν αποφασιστική επίδραση στην ανάπτυξη και στη λειτουργία των χρηματοδοτούμενων από αυτές επιχειρήσεων, έχουν αυξημένη ευθύνη κατά την άσκηση του χρηματοδοτικού τους έργου και οφείλουν να μεριμνούν για τα συμφέροντα των επιχειρήσεων που χρηματοδοτούν, αφού από τη φύση της η πιστωτική σχέση, ως διαρκής έννομη σχέση ιδιαίτερης εμπιστοσύνης μεταξύ των συμβαλλομένων, επιβάλλει την υποχρέωση πίστης και προστασίας από την πλευρά των τραπεζών των συμφερόντων των πελατών τους, ώστε να αποφεύγονται υπέρμετρα επαχθείς γι' αυτούς συνέπειες. Συνεπώς και για το λόγο αυτό η άσκηση των δικαιωμάτων τους θα πρέπει να κυριαρχείται από τις αρχές της καλόπιστης και σύμφωνης με τα χρηστά συναλλακτικά ήθη εκπλήρωσης των οφειλόμενων παροχών (ΑΚ 178, 200, 288) και να αποφεύγεται αντίστοιχα κάθε κατάχρηση στη συμπεριφορά τους».

banking, v-banking), αλλά και για την κατάταξη των πελατών ως ιδιωτών ή επαγγελματιών βάσει της ενωσιακής νομοθεσίας (Οδηγία 2014/65/ΕΕ - **MIFID II**) που ενσωματώθηκε στο ελληνικό δίκαιο με τον Ν. 4514/2018 και των εκτελεστικών της μέτρων). Επιπροσθέτως, οι τράπεζες συχνά προχωρούν στην αξιολόγηση της καταλληλότητας και της συμβατότητας των πελατών ώστε να χορηγήσουν σε αυτούς επενδυτικά ή ασφαλιστικά προϊόντα και υπηρεσίες.

4.5.1 Η καταγραφή τηλεφωνικών συνομιλιών

Παράλληλα, οι τράπεζες στο πλαίσιο εκπλήρωσης των συμβατικών και συναλλακτικών τους υποχρεώσεων, προχωρούν στην καταγραφή των τηλεφωνικών συνομιλιών που πραγματοποιούν με τους πελάτες τους. Η καταγραφή αυτή διενεργείται αρχικά για την διασφάλιση της ασφάλειας και της προστασίας των συναλλαγών αλλά και για να υπάρχει η δυνατότητα απόδειξης της διεκπεραίωσης της εκάστοτε συναλλαγής και του περιεχομένου αυτής, σε περίπτωση που τα υποκείμενα των δεδομένων κάνουν χρήση των υπηρεσιών τηλεφωνικής εξυπηρέτησης (phone banking). Περαιτέρω, η καταγραφή αυτή μπορεί να λαμβάνει χώρα σε περίπτωση που πρόκειται να ληφθούν χρηματιστηριακές εντολές μέσω τηλεφώνου από τους πελάτες των τραπεζών (άρθρο 43 ν. 4443/2016). Τέλος, η καταγραφή των τηλεφωνικών συνομιλιών μπορεί να διενεργείται κατά την τηλεφωνική ενημέρωση των πελατών για την ύπαρξη ληξιπρόθεσμων απαιτήσεων του πιστωτικού ιδρύματος και τη διαπραγμάτευση της ρύθμισης της εκάστοτε οφειλής, σύμφωνα με τις διατάξεις και τις εγγυήσεις των νόμων 3758/2009 και 4354/2015, όπως ισχύουν. Εάν οι ενέργειες αυτές κρίνονται αναγκαίες για να αξιολογηθεί η πιστοληπτική ικανότητα και η φερεγγυότητα των πελατών, τα πιστωτικά ιδρύματα προχωρούν σε άντληση των δεδομένων των πελατών από διατραπεζικά αρχεία οικονομικών πληροφοριών. Τα πιστωτικά ιδρύματα στο πλαίσιο αυτό θα πρέπει να προχωρούν σε προηγούμενη ενημέρωση των πελατών και να λαμβάνουν την συγκατάθεσή τους για την άντληση αυτή και την περαιτέρω επεξεργασία των δεδομένων τους.[481]

Αναφορικά με τη νομιμότητα της καταγραφής των τηλεφωνικών συνομιλιών κατά την παροχή επενδυτικών υπηρεσιών, η Αρχή με την απόφαση 72/2013 απεφάνθη, ότι σύμφωνα με το ενωσιακό δίκαιο επιτρέπεται η καταγραφή και αρχειοθέτηση εντολών που δίνουν πελάτες για την κατάρτιση συναλλαγών επί χρηματοπιστωτικών μέσων και ιδίως η ηχογράφηση εντολών που δίνονται τηλεφωνικώς, αλλά και η αποθήκευση εντολών που δίδονται μέσω τηλεομοιοτυπίας ή ηλεκτρονικού μέσου.[482] Περαιτέρω, η καταγραφή αυτή θα πρέπει να λαμβάνει χώρα με τρόπο που να εγγυάται την αξιοπιστία, την ασφάλεια και την πληρότητα των καταγεγραμμένων στοιχείων, αλλά και την δυνατότητα ευχερούς πρόσβασης και έρευνας των καταγεγραμμένων στοιχείων. Περαιτέρω, με βάση το άρθρο 4 παρ. 3 του νόμου 3471/2006, «Επιτρέπεται η καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης, όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων εμπορικής

---

[481] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 154-155.

[482] Άρθρο 18 **ν. 3340/2005** (ΦΕΚ Α΄ 112/10.5.2005) «Για την προστασία της Κεφαλαιαγοράς από πράξεις προσώπων που κατέχουν προνομιακές πληροφορίες και πράξεις χειραγώγησης της αγοράς», όπως τροποποιήθηκε και ισχύει, ενσωματώθηκε στην ελληνική έννομη τάξη η **Οδηγία 2003/6/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 28ης Ιανουαρίου 2003 για τις πράξεις προσώπων που κατέχουν προνομιακές πληροφορίες και τις πράξεις χειραγώγησης της αγοράς (κατάχρηση αγοράς), καθώς και μέρος των Οδηγιών 2003/124/ΕΚ, 2003/125/ΕΚ και 2004/72/ΕΚ της Επιτροπής (άρθρο 1 σε συνδυασμό με σελ. 1 της Αιτιολογικής Έκθεσης του ίδιου νόμου).

συναλλαγής ή άλλης επικοινωνίας επαγγελματικού χαρακτήρα, υπό την προϋπόθεση ότι και τα δύο μέρη, μετά από προηγούμενη ενημέρωση σχετικά με το σκοπό της καταγραφής, παρέχουν τη συγκατάθεση τους».

Στο πλαίσιο της μη ικανοποίησης δικαιώματος πρόσβασης σε καταγεγραμμένες συνομιλίες[483], η Αρχή εξέδωσε την απόφαση 47/2018. Ειδικότερα, η Αρχή δέχθηκε καταγγελία από πελάτη τράπεζας ο οποίος δέχθηκε τηλεφωνική όχληση στα γραφεία της επιχείρησής του σχετικά με οφειλή του από επιχειρηματικό δάνειο. Στο εν λόγω τηλεφώνημα όμως απάντησε συγγενής του που δεν είχε σχέση με την εν λόγω οφειλή και ο οποίος ήταν ανταγωνιστής του. Ο προσφεύγων μέσω γραπτού αιτήματος αιτήθηκε να λάβει αντίγραφα των δύο συνομιλιών με υπαλλήλους της τράπεζας σχετικά με το συγκεκριμένο περιστατικό. Η Αρχή έκρινε ότι το αίτημα του προσφεύγοντος που ασκήθηκε εγγράφως ήταν ορισμένο και σαφές, ενώ η τράπεζα δεν εκπλήρωσε εμπροθέσμως την αντίστοιχη υποχρέωσή της να απαντήσει εγγράφως με σαφήνεια και πληρότητα αλλά ούτε κοινοποίησε την απάντησή της στην Αρχή, ενημερώνοντας τον ενδιαφερόμενο ότι μπορεί να προσφύγει σε αυτήν (άρθρο 12 παρ. 2 και 4 του ν. 2472/1997). Τέλος, η Αρχή επέβαλλε πρόστιμο στην τράπεζα για μη εκπλήρωση της υποχρέωσής της να απαντήσει στον προσφεύγοντα εντός της προβλεπόμενης προθεσμίας, παραβιάζοντας το κατ' άρθρο 12 του ν. 2472/1997 δικαίωμα πρόσβασής του. Επίσης, απηύθυνε σε αυτήν σύσταση, επισημαίνοντας ότι κατά την τηλεφωνική επικοινωνία με τους πελάτες της οφείλει να μεριμνά για την ταυτοποίηση του συνομιλητή, πριν προχωρήσει σε συνομιλία που αφορά τα δεδομένα συναλλαγών ή οφειλών του ίδιου του πελάτη ή προσώπων που συνδέονται συναλλακτικά με αυτό.[484]

4.5.2 Προώθηση τραπεζικών υπηρεσιών

Με απώτερο στόχο την εξυπηρέτηση των επιχειρηματικών τους στόχων αλλά και την επέκταση της πελατειακής τους βάσης, οι τράπεζες επεξεργάζονται προσωπικά δεδομένα των πελατών στο πλαίσιο προώθησης των προϊόντων και των υπηρεσιών τους. Η προώθηση αυτή διενεργείται μέσω τηλεφωνικών συνομιλιών, ενημερωτικού υλικού που αποστέλλεται μέσω ηλεκτρονικού ή παραδοσιακού ταχυδρομείου ή άλλων ηλεκτρονικών μέσω επικοινωνίας (π.χ. sms), αλλά και μέσω προσκλήσεων που στόχο έχουν την εγγραφή των πελατών σε ενημερωτικά δελτία (newsletters). Η άμεση αυτή προώθηση αυτή για να θεωρείται νόμιμη θα πρέπει να διενεργείται υπό το θεσμικό και νομοθετικό πλαίσιο που καθορίζεται από τις διατάξεις του Κανονισμού.[485] Το υποκείμενο των δεδομένων στις περιπτώσεις αυτές έχει το δικαίωμα να εναντιωθεί αναιτιολογήτως (opt-out) και δη χωρίς περιθώριο (αντ)ένστασης κατ' αυτής ανά πάσα στιγμή στην επεξεργασία που διενεργείται για σκοπούς απευθείας εμπορικής προώθησης, περιλαμβανομένης της κατάρτισης προφίλ εάν έχει σχέση με την συγκεκριμένη απευθείας εμπορική προώθηση (άρθρο 21 παρ. 2-3 ΓΚΠΔ). Ομοίως, σύμφωνα με το άρθρο 22 του Κανονισμού, το υποκείμενο δικαιούται να εναντιωθεί σε αποφάσεις-προϊόντα ακόμη και κατ' αρχήν επιτρεπτής εκ του νόμου αλλά απολύτως αυτοματοποιημένης επεξεργασίας (ιδίως profiling). Στις περιπτώσεις αυτές, η τυχόν εκ προοιμίου συγκατάθεση του υποκειμένου δεν θα ήρε τον αυτοματοποιημένο χαρακτήρα της επεξεργασίας, ούτε και θα μπορούσε να συνιστά ισχυρή παραίτηση του υποκειμένου από το

[483] Βλ. και σχετικές αποφάσεις ΑΠΔΠΧ υπ'αριθμ. 65/2010 και 72/2013.
[484] Ετήσια έκθεση ΑΠΔΠΧ 2018, 55-56.
https://www.dpa.gr/sites/default/files/2020-02/ANNUAL2018V30WEBPAGE_01.PDF.
[485] Ibid., 155

δικαίωμά του αυτό. Στις περιπτώσεις αυτές, ο υπεύθυνος επεξεργασίας δύναται να αποκρούσει την εναντίωση του υποκειμένου μέσω της άσκησης δύο (αντ)ενστάσεων: την ένσταση της ρητής συγκατάθεσης του υποκειμένου, προκειμένου δε για απλά δεδομένα και της σιωπηρής επί εκτελέσεως συμβατικής του υποχρεώσεως (άρθρο 22 παρ. 2 γ' , α , 4) και της ένστασης που βασίζεται σε ρητή νομοθετική πρόβλεψη (άρθρο 22 παρ. 2 β' ΓΚΠΔ), προκειμένου δε για ευαίσθητα δεδομένα μόνο για λόγους ουσιώδους δημοσίου συμφέροντος, που σταθμίζεται δηλαδή ως υπερέχον έναντι του ατομικού συμφέροντος του υποκειμένου των δεδομένων.[486]

Αναφορικά με την αυτόκλητη εμπορική επικοινωνία, ο νόμος (άρθρο 11 ν. 3471/2006), κάνει διάκριση ανάλογα με το αν αυτή διενεργείται μέσω ανθρώπινης παρέμβασης (προσωπικό τηλεφώνημα) ή με αυτοματοποιημένο τρόπο (ηλεκτρονικό ταχυδρομείο, αυτόματες κλήσεις, fax κ.α.). Στην πρώτη περίπτωση επικρατεί το σύστημα opt-out, δηλαδή επιτρέπεται αρχικά, εκτός αν το υποκείμενο εναντιωθεί, ενώ στην δεύτερη περίπτωση επικρατεί το σύστημα opt-in, δηλαδή για να θεωρηθεί νόμιμη απαιτείται συγκατάθεση του υποκειμένου. Στην συγκατάθεση αυτή στην αυτόκλητη εμπορική επικοινωνία εφαρμόζονται συμπληρωματικά (αναλογικά) οι διατάξεις που διέπουν την συγκατάθεση στην επεξεργασία προσωπικών δεδομένων (άρθρο 8 ΓΚΔΠ). Αλλιώς έχουν τα πράγματα σε περίπτωση που η συγκατάθεση του υποκειμένου για δημοσίευση στοιχείων επαφής του υπηρετεί αποκλειστικά επαγγελματικούς σκοπούς.[487][488]

Εξαίρεση από τον κανόνα της απαγόρευσης της αυτόκλητης επαγγελματικής επικοινωνίας προβλέπεται επίσης με το θεσμό του opt-out της συνάφειας (άρθρο 11 παρ. 3 ν. 3471/2006). Η περίπτωση αυτή αφορά μη ζητηθείσα ηλεκτρονική επικοινωνία όπου «τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου αποκτήθηκαν νόμιμα στο πλαίσιο παρόμοιων σκοπών». Επί παραδείγματι, ο προμηθευτής ενός προϊόντος δικαιούται να απευθυνθεί και πάλι στον πελάτη του κάνοντας χρήση των στοιχείων επαφής του τελευταίου, τα οποία είχε ήδη αποκτήσει κατά τη διενέργεια της προηγούμενης συναλλαγής ανάμεσά τους, εφόσον αυτή αφορούσε παρόμοια αγαθά, προϊόντα ή υπηρεσίες. Η περίπτωση αυτή αποτελεί εξαίρεση από τον κανόνα που καθιερώνεται στο άρθρο 4 παρ. 11 του Κανονισμού, της εν αμφιβολία μη σιωπηρής συγκατάθεσης για την επεξεργασία των προσωπικών δεδομένων, καθώς οι προγενέστερες συναλλαγές και δοσοληψίες αποτελούν μορφές «συγκείμενων» περιστάσεων και θα πρέπει σε κάθε περίπτωση να ερμηνεύεται η δικαιοπραξία ώστε να ανιχνευθεί η σιωπηρή ή εικαζόμενη συναίνεση του υποκειμένου.[489]

Ειδικότερα, όσον αφορά τις τηλεφωνικές κλήσεις που πραγματοποιούνται με ανθρώπινη παρέμβαση, θα πρέπει να σημειωθεί ότι οι συνδρομητές έχουν τη δυνατότητα να δηλώσουν ατελώς στους παρόχους τηλεπικοινωνιακών υπηρεσιών ότι δεν επιθυμούν στο εξής να λαμβάνουν διαφημιστικά τηλεφωνήματα. Οι πάροχοι με τη σειρά τους οφείλουν να τηρούν μητρώο που περιλαμβάνει τις δηλώσεις αυτές, στο οποίο έχει πρόσβαση οποιοσδήποτε επιθυμεί να κάνει χρήση αυτού για σκοπούς εμπορικής προώθησης. Τα υποκείμενα δύνανται επίσης να δηλώσουν

---

[486] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 131.

[487] Επιτρέπεται επομένως η αυτόκλητη εμπορική επικοινωνία, εάν τα στοιχεία επαφής του υποκειμένου δημοσιεύονται έπειτα από συγκατάθεσή του στον «Χρυσό Οδηγό». Σε τέτοιες περιπτώσεις έχει ήδη επιτραπεί η άμεση επαγγελματική επικοινωνία, εάν φυσικά συνέχεται με το δημοσιευμένο επιτήδευμα του υποκειμένου.

[488] Κωνσταντίνος Ν. Χριστοδούλου, *Δίκαιο Προσωπικών Δεδομένων*, 2η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2020), 249.

[489] Ibid., 251.

την αντίρρησή τους και στον καλούντα, αλλά στην περίπτωση αυτή η αντίρρηση θα αφορά αποκλειστικά αυτόν.[490]

Σύμφωνα με την απόφαση 26/2004 της Αρχής, η συλλογή δεδομένων για σκοπούς απευθείας διαφήμισης και προώθησης πωλήσεων προϊόντων και υπηρεσιών θεωρείται νόμιμη εφόσον το υποκείμενο έχει δώσει τη συγκατάθεσή του σύμφωνα με τα άρθρα 2 εδάφιο ια) και 5 παρ. 1 του νόμου 2472/1997. Η συγκατάθεση είναι επίσης απαραίτητη στις περιπτώσεις που διενεργείται έρευνα καταναλωτικής συμπεριφοράς με σκοπό την άμεση ή έμμεση διαφήμιση προϊόντων ή παροχή υπηρεσιών. Σε περιπτώσεις που το υποκείμενο δεν έχει δώσει τη συγκατάθεσή του, η επεξεργασία θεωρείται κατ' εξαίρεση νόμιμη βάσει του άρθρου 5 παρ. 2, εδάφιο ε', διότι α) κρίνεται απολύτως αναγκαία για την ικανοποίηση του εννόμου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας, β) το έννομο συμφέρον του υπευθύνου επεξεργασίας υπερέχει έναντι του αντίστοιχου του υποκειμένου των δεδομένων. Για να τύχει εφαρμογής η εξαίρεση που καθιερώνεται μέσω της διάταξης του άρθρου 5 παρ. 2, εδάφιο ε', πρέπει αρχικά τα δεδομένα να προέρχονται από καταλόγους που απευθύνονται στο ευρύ κοινό (π.χ. κατάλογος του ΟΤΕ) και να έχει διασφαλιστεί ότι τα υποκείμενα που συμπεριλαμβάνονται στον εν λόγω κατάλογο έχουν δώσει τη συγκατάθεσή τους. Τα δεδομένα μπορούν επίσης να προέρχονται από δημόσια προσβάσιμες πηγές που έχουν ως στόχο την παροχή υπηρεσιών στο ευρύ κοινό, εφόσον έχουν τηρηθεί οι νόμιμες προϋποθέσεις που αφορούν την πρόσβαση σε αυτές. Τέλος, για να εφαρμοστεί η προαναφερθείσα εξαίρεση, θα πρέπει το ίδιο το υποκείμενο να έχει δημοσιοποιήσει τα προσωπικά του δεδομένα για συναφείς σκοπούς. Επιπροσθέτως, ο υπεύθυνος επεξεργασίας θα πρέπει να περιορίζεται στην επεξεργασία των απολύτως αναγκαίων δεδομένων για την επίτευξη του συγκεκριμένου σκοπού.[491]

Σχετική στο πλαίσιο αυτό είναι και η απόφαση 50/2000 της Αρχής, με την οποία διασαφηνίζονται οι όροι και οι προϋποθέσεις υπό τις οποίες είναι ανεκτή η επεξεργασία προσωπικών δεδομένων των υποκειμένων, για την οποία αυτά δεν έχουν δώσει τη συγκατάθεσή τους, όταν η επεξεργασία γίνεται με σκοπό την άμεση εμπορία. Στην εν λόγω απόφαση, η Αρχή επίσης σε περιοριστική απαρίθμηση των δεδομένων, τα οποία επιτρέπεται να συλλέγουν εταιρείες (π.χ. Τειρεσίας Α.Ε.) με στόχο την διαπίστωση της πιστοληπτικής ικανότητας των υποκειμένων. Απαγορεύεται επίσης η συλλογή «ευμενών» στοιχείων (**whitelist**), για τα οποία το υποκείμενο πρέπει να έχει δώσει τη συγκατάθεσή του, εν αντιθέσει με τη συλλογή «δυσμενών» στοιχείων (**blacklist**), τα οποία μπορούν να συλλέγονται και χωρίς να συντρέχει η συγκατάθεση του υποκειμένου.[492]

4.5.3 Επεξεργασία δεδομένων στο πλαίσιο ερευνών ικανοποίησης πελατών

Μέσω των ερευνών ικανοποίησης πελατών τα πιστωτικά ιδρύματα διαπιστώνουν το βαθμό ικανοποίησης των πελατών τους με βάση τα παρεχόμενα προϊόντα και τις υπηρεσίες αλλά και να λάβουν γνώση των αναγκών αυτών με στόχο την βελτίωση των υπηρεσιών τους και την ανάπτυξη νέων. Οι έρευνες ικανοποίησης πελατών εμπεριέχουν επεξεργασία προσωπικών δεδομένων καθώς δεν γίνονται ανώνυμα και δεν αποτελούν προωθητικές ενέργειες. Επιπροσθέτως, μέσω της

---

[490] Άρθρο 11, νόμος 3471/2006.

[491] Απόφαση 26/2004 ΑΠΔΠΧ, διαθέσιμη στην διεύθυνση: https://www.dpa.gr/sites/default/files/2019-10/ap_26-2004_1.pdf.

[492] Βασίλης Σωτηρόπουλος, "Προστασία Προσωπικών Δεδομένων", Digestaonline.Gr, 2005, http://www.digestaonline.gr/pdfs/Digesta%202005/DIGESTA%201-2005/5%20SOTOU.pdf.

διενέργειας αυτών των ερευνών, οι τράπεζες εξυπηρετούν τα έννομα συμφέροντά τους και αποβλέπουν στην ενίσχυση των πελατειακών τους σχέσεων και στην προαγωγή της επιχειρηματικής δραστηριότητας μέσω της ανάπτυξης καινοτόμων υπηρεσιών. Η αποστολή των ερωτηματολογίων προς τους πελάτες εντάσσεται στο νομοθετικό και κανονιστικό πλαίσιο για την επικοινωνία με αυτούς.[493]

4.5.4 Επεξεργασία δεδομένων στο πλαίσιο των δημοσίων σχέσεων των πιστωτικών ιδρυμάτων

Οι τράπεζες συχνά επεξεργάζονται προσωπικά δεδομένα πελατών ή μη, με στόχο την ενίσχυση της δημόσιας εικόνας τους, αλλά και για την προβολή των δραστηριοτήτων τους που μπορεί να αφορούν θέματα περιβάλλοντος, ανάπτυξης και κοινωνικής ευθύνης. Επιπροσθέτως, επεξεργάζονται δεδομένα υποκειμένων στο πλαίσιο παροχών αριστείας ή παροχών κοινωνικού και φιλανθρωπικού χαρακτήρα. Στις περιπτώσεις αυτές, η συμμετοχή των προσώπων αυτών στις δραστηριότητες αυτές, αφού έχει προηγηθεί η προσήκουσα ενημέρωσή τους σχετικά με το είδος της επεξεργασίας, των σκοπών αυτής, αλλά και τους αποδέκτες τους, συνιστά έμπρακτη συγκατάθεση για αυτήν. Περαιτέρω, η επεξεργασία για να θεωρηθεί νόμιμη, θα πρέπει να στηρίζεται σε κάποια από τις βάσεις επεξεργασίας που απαριθμούνται στο άρθρο 6 του Κανονισμού.

4.5.5 Επεξεργασία δεδομένων στο πλαίσιο λειτουργίας συστημάτων πρόσβασης και ασφάλειας των τραπεζών

Με στόχο την πρόληψη και την αποτροπή εγκληματικών πράξεων κατά της ζωής και της περιουσίας των φυσικών προσώπων-πελατών τους, οι τράπεζες προχωρούν στη λήψη μέτρων φυσικής ή τεχνικής προστασίας των εγκαταστάσεών τους, τα οποία μπορεί να απαιτούν και την επεξεργασία των προσωπικών δεδομένων των φυσικών αυτών προσώπων. Τα μέτρα αυτά εφαρμόζονται στα συστήματα και τις εγκαταστάσεις των τραπεζών, αλλά και στα αποθηκευμένα σε αυτά δεδομένα, χωρίς να γίνεται διάκριση ανάμεσα στις εγκληματικές πράξεις που προέρχονται από το εσωτερικό της τράπεζας ή από εξωγενείς παράγοντες.[494] Τα τραπεζικά ιδρύματα στο πλαίσιο αυτό εγκαθιστούν συστήματα καταγραφής εικόνας στους χώρους συναλλαγών εντός των καταστημάτων τους ή εκτός αυτών στις θέσεις των μηχανημάτων αυτόματων συναλλαγών. Επίσης, εγκαθιστούν μηχανισμούς ηλεκτρονικής πρόσβασης και ελέγχου, που αφορούν τόσο την φυσική πρόσβαση στους χώρους των υπηρεσιών των πιστωτικών ιδρυμάτων, με τον έλεγχο και την καταγραφή της εισόδου και της εξόδου των φυσικών προσώπων, αλλά και την ηλεκτρονική πρόσβαση ή εκτέλεση εργασιών, μέσω της χρήσης μηχανισμών ταυτοποίησης και καταγραφής της ιστορικότητας των ενεργειών (**audit trails**) για την παρακολούθηση και τη δημιουργία αναφορών που σχετίζονται με τις δραστηριότητες στα ηλεκτρονικά συστήματα των τραπεζών.[495]

---

[493] Ελληνική Ένωση Τραπεζών, "Κώδικας Δεοντολογίας Για Την Επεξεργασία Προσωπικών Δεδομένων Στο Τραπεζικό Σύστημα" (repr., Σχέδιο 16.1.2019), 13. https://www.hba.gr/UplDocs/GDPR/%CE%9A%CE%A9%CE%94%CE%99%CE%9A%CE%91%CE%A3%20%CE%94%CE%95%CE%9F%CE%9D%CE%A4%CE%9F%CE%9B%CE%9F%CE%93%CE%99%CE%91%CE%A3.pdf

[494] Ibid.,14

[495] Ibid.

Εντός ενός οργανισμού που χειρίζεται ενεργά δεδομένα προσωπικού χαρακτήρα, είναι σημαντικό να διατηρείται ένα κατάλληλο επίπεδο «υγείας των δεδομένων» κατά την επεξεργασία. Αυτό απαιτεί την προστασία των δεδομένων καθ' όλη τη διάρκεια της ζωής τους: από τον σχεδιασμό νέων επιγραμμικών λειτουργιών και υπηρεσιών μέχρι την αποθήκευση παλαιότερων δεδομένων. Το επίπεδο προστασίας δεδομένων που επιθυμεί μια εταιρεία να διατηρήσει, μπορεί να διασφαλιστεί μέσω μέτρων προστασίας όπως η κρυπτογράφηση, η ανωνυμοποίηση, η διενέργεια εκτιμήσεων αντικτύπου (άρθρο 35 ΓΚΠΔ) αλλά και η εκπαίδευση των υπαλλήλων σχετικά με τις πρακτικές της ασφάλειας των δεδομένων.[496]

4.5.6 Επεξεργασία δεδομένων στο πλαίσιο της πρόληψης και της καταστολής εσόδων από εγκληματικές δραστηριότητες

Με στόχο την πρόληψη, τον εντοπισμό αλλά και την καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, οι τράπεζες εγκαθιστούν και κάνουν χρήση συστημάτων ταυτοποίησης και αξιολόγησης των πελατών και των τραπεζικών συναλλαγών τους. Η επεξεργασία των δεδομένων από τα συστήματα αυτά πραγματοποιείται βάσει μοντέλων και πραγματοποιούν ελέγχους σε διεθνείς καταλόγους πολιτικώς εκτεθειμένων προσώπων ή επιβολής κυρώσεων. Στόχος της επεξεργασίας αυτής είναι η διερεύνηση των ύποπτων ή ασυνήθιστων συναλλαγών, αλλά και η πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και άλλων άδικων πράξεων (π.χ. απάτη). Στο πλαίσιο αυτό, οι τράπεζες συχνά καταρτίζουν και προφίλ των πελατών τους μέσω της χρήσης αυτοματοποιημένων συστημάτων, ώστε να εκδίδουν αναφορές που σχετίζονται με ύποπτες δραστηριότητες.[497]

Με την απόφαση υπ'αριθμ. 91/2014[498], η Αρχή έκρινε ότι ο νόμος 3691/2008 για την πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, εισάγει ειδικότερες διατάξεις αναφορικά με την επεξεργασία δεδομένων χρηματοπιστωτικής φύσεως από τα πιστωτικά ιδρύματα, επιβάλλοντας έτσι τη συλλογή, τήρηση και επεξεργασία δεδομένων που αφορούν τις συναλλαγές των πελατών τους και την δραστηριότητα των υπαλλήλων τους ως πελατών τους, όταν συντρέχουν συγκριμένες περιστάσεις. Οι διατάξεις του νόμου αυτού εξειδικεύονται περαιτέρω μέσω αποφάσεων και πράξεων της ΤτΕ, είναι δημόσιας τάξεως και επιβάλλουν αντίστοιχες υποχρεώσεις στα πιστωτικά ιδρύματα. Το άρθρο 31 του ν. 3691/2008 θεσπίζει παρέκκλιση από την υποχρέωση ενημέρωσης του υποκειμένου, όπως αυτό προβλέπεται στο άρθρο 11 του ν. 2472/1997 που αφορά τόσο τους πελάτες όσο και τους υπαλλήλους των τραπεζών. Στο πλαίσιο αυτό κρίθηκε αναγκαία η επεξεργασία, που συνίστατο στον έλεγχο των τραπεζικών λογαριασμών της προσφεύγουσας, για την εκπλήρωση της υποχρέωσης του υπευθύνου επεξεργασίας όπως αυτή απορρέει από την προαναφερθείσα νομοθεσία. Με την απόφαση υπ'αριθμ. 66/2008, η Αρχή έκρινε ότι η

---

[496] Sanjay Sharma, *Data Privacy and GDPR Handbook*, 1st ed. (repr., Newark, United States: John Wiley & Sons, Incorporated, 2020), 69.

[497] Ελληνική Ένωση Τραπεζών, "Κώδικας Δεοντολογίας Για Την Επεξεργασία Προσωπικών Δεδομένων Στο Τραπεζικό Σύστημα" (repr., Σχέδιο 16.1.2019), 15. https://www.hba.gr/UplDocs/GDPR/%CE%9A%CE%A9%CE%94%CE%99%CE%9A%CE%91%CE%A3%20%CE%94%CE%95%CE%9F%CE%9D%CE%A4%CE%9F%CE%9B%CE%9F%CE%93%CE%99%CE%91%CE%A3.pdf

[498] Με την απόφαση 58/2015, η Αρχή προέβη σε διόρθωση της αποφάσεως 91/2014. https://www.dpa.gr/sites/default/files/2019-10/58_2015anonym.pdf.

προσφεύγουσα έχει δικαίωμα πρόσβασης στα δεδομένα που είχαν συλλεχθεί κατά τη συνήθη διερεύνηση της συνολικής εικόνας της ως πελάτισσα και αξιολογήθηκαν στο πλαίσιο της συναλλακτικής σχέσης της τράπεζας με αυτήν. Περαιτέρω, το δικαίωμα πρόσβασης των υποκειμένων των δεδομένων σε στοιχεία που το αφορούν νομίμως περιορίζεται, για τον σκοπό της διερεύνησης ποινικών αδικημάτων που είναι συναφή προς τη νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες (άρθρο 31 του ν. 3691/2008 και ν. 3601/2007). Ο περιορισμός αυτός όμως του δικαιώματος πρόσβασης παύει να ισχύει, αφότου το τραπεζικό ίδρυμα ολοκληρώσει την έρευνα και δεν διαβιβάσει τα εν λόγω στοιχεία στην αρμόδια Επιτροπή, εκτιμώντας ότι αυτά δεν συνιστούν ένδειξη νομιμοποίησης εσόδων από εγκληματική δραστηριότητα.[499]

4.5.7 Επεξεργασία δεδομένων υποκειμένων που έχουν τη μετοχική ιδιότητα

Στο πλαίσιο των δραστηριοτήτων τους, τα πιστωτικά ιδρύματα τηρούν και επεξεργάζονται δεδομένα προσωπικού χαρακτήρα των υποκειμένων που συμμετέχουν στη μετοχική τους σύνθεση ή είναι ενεχυρούχοι δανειστές των μετόχων. Παράλληλα, σε πολλά πιστωτικά ιδρύματα λειτουργούν υπηρεσίες εξυπηρέτησης μετόχων, με στόχο την άμεση και σύμμετρη πληροφόρησή τους αλλά και την εξυπηρέτησή τους ως προς την άσκηση των εκ του νόμου δικαιωμάτων τους. Οι υπηρεσίες αυτές, ενημερώνουν τους μετόχους σχετικά με τη διανομή μερισμάτων, τις πράξεις έκδοσης νέων μετοχών, τη μεταβίβαση των μετοχών λόγω κληρονομιάς, την έκδοση βεβαιώσεων σχετικά με εταιρικές πράξεις, αλλά και τις τακτικές ή έκτακτες συνελεύσεις μετόχων και τις αποφάσεις αυτών. Παράλληλα, αναλαμβάνουν να διανείμουν την ετήσια οικονομική έκθεση στους μετόχους, αλλά και να τηρούν και να επικαιροποιούν το μετοχολόγιο της εταιρείας.[500] [501]

4.5.8 Επεξεργασία δεδομένων στο πλαίσιο της άσκησης αξιώσεων και της υπεράσπισης εννόμων συμφερόντων

Στο πλαίσιο της εξυπηρέτησης του συγκεκριμένου σκοπού, τα πιστωτικά ιδρύματα επεξεργάζονται προσωπικά προσωπικού χαρακτήρα των πελατών και γενικότερα των υποκειμένων, εφόσον αυτό κριθεί αναγκαίο για να διασφαλιστούν τα έννομα συμφέροντα και η άσκηση των δικαιωμάτων των πιστωτικών ιδρυμάτων. Για την υποστήριξή τους δικαστικά και εξώδικα, τα πιστωτικά ιδρύματα χρησιμοποιούν τις υπηρεσίες που παρέχονται από δικηγόρους, συμβολαιογράφους, δικαστικούς επιμελητές κ.λπ. και απευθύνονται σε αρμόδιους φορείς και αρχές προς τους οποίους διαβιβάζονται και κοινοποιούνται τα προσωπικά δεδομένα των φυσικών προσώπων που εμπλέκονται (αντίδικοι, ομόδικοι, αντίκλητοι, προστηθέντες, δημόσιοι λειτουργοί, δανειστές των πελατών κ.λπ.). Νομική βάση για την επεξεργασία αυτή αποτελεί η προάσπιση των εννόμων συμφερόντων του πιστωτικού ιδρύματος, υπό τον όρο ότι έχει προηγουμένως ενημερώσει τους πελάτες-υποκείμενα, όχι για κάθε συγκεκριμένο αποδέκτη, αλλά για τις κατηγορίες αποδεκτών. Σε περίπτωση διαβίβασης προσωπικών δεδομένων πελατών σε εταιρείες

---

[499] Απόφαση 66/2008 ΑΠΔΠΧ, σελ. 5-7, https://www.dpa.gr/sites/default/files/2019-10/66_08anonym.pdf.

[500] Ελληνική Ένωση Τραπεζών, "Κώδικας Δεοντολογίας Για Την Επεξεργασία Προσωπικών Δεδομένων Στο Τραπεζικό Σύστημα" (repr., Σχέδιο 16.1.2019), 15. https://www.hba.gr/UplDocs/GDPR/%CE%9A%CE%A9%CE%94%CE%99%CE%9A%CE%91%CE%A3%20%CE%94%CE%95%CE%9F%CE%9D%CE%A4%CE%9F%CE%9B%CE%9F%CE%93%CE%99%CE%91%CE%A3.pdf

[501] https://www.piraeusholdings.gr/el/investors/metochologio.

ενημέρωσης οφειλετών (ν. 3758/2009) και εταιρείες διαχείρισης απαιτήσεων (ν.4354/2015 και ν. 4469/2017), ισχύουν οι ίδιες προϋποθέσεις.

4.5.9 Επεξεργασία δεδομένων για ιστορικούς και εκπαιδευτικούς σκοπούς

Τα πιστωτικά ιδρύματα διατηρούν αρχείο που περιλαμβάνει στοιχεία, πληροφορίες και δεδομένα προσωπικού χαρακτήρα των μετόχων, των μελών του Διοικητικού Συμβουλίου ή και της διοίκησής τους, αλλά και πελατών που επηρέασαν την πορεία του πιστωτικού ιδρύματος ή και την οικονομία της χώρας, για ερευνητικούς και ιστορικούς σκοπούς. Τέτοια προσωπικά δεδομένα αποτελούν τα στοιχεία ταυτοπροσωπίας, τα βιογραφικά σημειώματα και το φωτογραφικό υλικό.

4.5.10 Διαβίβαση δεδομένων σε δημόσιες και ελεγκτικές αρχές

Τα πιστωτικά ιδρύματα συχνά διαβιβάζουν δεδομένα προσωπικού χαρακτήρα των πελατών τους ή και υπαλλήλων τους σε φορολογικές, ανακριτικές , εποπτικές[502] , εισαγγελικές ή δικαστικές αρχές, αλλά και σε διεθνείς οργανισμούς, ώστε να προσδιοριστεί η φορολογητέα ύλη (π.χ. περίπτωση γνωστοποίησης των τόκων των καταθέσεων), να διερευνηθούν οι παράνομες δραστηριότητες (π.χ. φοροδιαφυγή, απάτη), ή για την εκπλήρωση διεθνών υποχρεώσεων της χώρας (FATCA). Τα πιστωτικά ιδρύματα, θα πρέπει να εγγυόνται ως υπεύθυνοι επεξεργασίας, ότι οι διαβιβάσεις των προσωπικών δεδομένων πραγματοποιούνται σύμφωνα με τις διατάξεις του Κανονισμού και του νόμου 4624/2019 και να διασφαλίζουν ότι οι εκτελούντες την επεξεργασία που ενεργούν για λογαριασμό του, εφαρμόζουν τα κατάλληλα τεχνικά οργανωτικά μέτρα και παρέχουν επαρκείς διαβεβαιώσεις, ώστε να πληρούνται οι διατάξεις του Κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του πελάτη-υποκειμένου των δεδομένων.[503]

Στις ανωτέρω περιπτώσεις, η διαβίβαση των προσωπικών δεδομένων αποτελεί υποχρέωση που πηγάζει εκ του νόμου και για την εκπλήρωσή της δεν απαιτείται να έχει ληφθεί η συγκατάθεση των υποκειμένων για τα διαβιβαζόμενα δεδομένα, αλλά ούτε να έχει προηγηθεί ειδική ενημέρωση αυτών. Πρόσβαση στα δεδομένα αυτά μπορούν επίσης να αποκτήσουν η Τράπεζα της Ελλάδος, η Ευρωπαϊκή Κεντρική Τράπεζα, ο Ενιαίος Εποπτικός Μηχανισμός (**SSM**) αλλά και η Επιτροπή Κεφαλαιαγοράς, κατά την άσκηση των εποπτικών τους αρμοδιοτήτων. Και στην περίπτωση αυτή δεν απαιτείται προηγούμενη λήψη συγκατάθεσης ή ενημέρωσης των υποκειμένων.[504]

Αναφορικά με την διαβίβαση δεδομένων προσωπικού χαρακτήρα των πελατών σε εταιρείες του ομίλου του πιστωτικού ιδρύματος, θα πρέπει να σημειωθεί ότι αυτή έχει ως νομική βάση την εξυπηρέτηση υπέρτερου έννομου συμφέροντος του πιστωτικού ιδρύματος, ως υπευθύνου επεξεργασίας (άρθρο 6 παρ. 1 στοιχείο στ' ΓΚΠΔ). Θα πρέπει στην περίπτωση αυτή να έχει προηγηθεί η σαφής και προσήκουσα ενημέρωση του υποκειμένου-πελάτη βάσει των άρθρων 13

---

[502] Βλ. άρθρο 58 παρ. 1 ΓΚΠΔ.

[503] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 79.

[504] Ελληνική Ένωση Τραπεζών, "Κώδικας Δεοντολογίας Για Την Επεξεργασία Προσωπικών Δεδομένων Στο Τραπεζικό Σύστημα" (repr., Σχέδιο 16.1.2019), 16. https://www.hba.gr/UplDocs/GDPR/%CE%9A%CE%A9%CE%94%CE%99%CE%9A%CE%91%CE%A3%20%CE%94%CE%95%CE%9F%CE%9D%CE%A4%CE%9F%CE%9B%CE%9F%CE%93%CE%99%CE%91%CE%A3.pdf

παρ. 3 και 14 παρ. 4 του Κανονισμού.[505]Επιπροσθέτως, η διαβίβαση προσωπικών δεδομένων από το πιστωτικό ίδρυμα κρίνεται επιτρεπτή, βάσει του άρθρου 25 παρ. 1 του νόμου 4624/2019 στις ακόλουθες περιπτώσεις: α) για να αποτραπούν οι απειλές κατά της εθνικής ή της δημόσιας ασφάλειας αφού έχει προηγηθεί αίτημα δημόσιου φορέα, β) για την δίωξη ποινικών αδικημάτων ή γ) για να θεμελιωθούν, ασκηθούν ή υποστηριχθούν νομικές αξιώσεις, εκτός εάν υπερτερεί το συμφέρον του υποκειμένου των δεδομένων να μην τύχουν επεξεργασίας τα εν λόγω δεδομένα.

Όταν το πιστωτικό ίδρυμα, ως υπεύθυνος επεξεργασίας, διαβιβάζει δεδομένα προσωπικού χαρακτήρα σε εκτελούντες την επεξεργασία, θα πρέπει να διασφαλίσει ότι οι τελευταίοι παρέχουν τις κατάλληλες εγγυήσεις ως προς την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων, ώστε η επεξεργασία των δεδομένων αυτών να ανταποκρίνεται στις απαιτήσεις που θέτει ο Κανονισμός και να διασφαλίζονται τα δικαιώματα των υποκειμένων. Επομένως, ο υπεύθυνος επεξεργασίας, θα πρέπει να επιλέγει τους εκτελούντες την επεξεργασία, βάσει της αξιοπιστίας τους, των απαιτούμενων τεχνικών γνώσεων, της εμπειρογνωμοσύνης και των πόρων, ώστε να παρέχονται κατάλληλες εγγυήσεις. Για να διασφαλιστεί η διαφανής κατανομή των ευθυνών και των υποχρεώσεων, τόσο στο πλαίσιο της εσωτερικής τους σχέσης (ανάμεσα σε υπεύθυνο και εκτελούντα την επεξεργασία) αλλά και στο πλαίσιο εξωτερικών σχέσεων έναντι των υποκειμένων των δεδομένων και των εποπτικών αρχών, η επεξεργασία από τον εκτελούντα θα πρέπει να καλύπτεται από γραπτές συμβάσεις ή άλλα νομικώς δεσμευτικά κείμενα, ανάμεσα στον υπεύθυνο επεξεργασίας και τον εκτελούντα αυτήν. Τα δεσμευτικά αυτά κείμενα τεκμηριώνουν γραπτώς τις οδηγίες του υπευθύνου προς τον εκτελούντα την επεξεργασία, καθώς και το αντικείμενο, τη διάρκεια, τη φύση και τους σκοπούς της επεξεργασίας. Επίσης, τεκμηριώνουν τα δικαιώματα και τις υποχρεώσεις του εκτελούντος την επεξεργασία.[506] Αναφορικά με το αντικείμενο της επεξεργασίας, αυτό θα πρέπει να αναφέρεται σαφώς στη φύση, την έκταση και το πλαίσιο της επεξεργασίας. Η διάρκεια της επεξεργασίας, μπορεί να ορίζεται μέσω του καθορισμού της ημερομηνίας έναρξης και λήξης και ο σκοπός θα πρέπει να είναι είναι σύμφωνος με την αρχή του περιορισμού του σκοπού, που προβλέπεται στο άρθρο 5 παρ. 1 στοιχείο β' του Κανονισμού. Τέτοια σύμβαση μπορεί να έχει τη μορφή συμφωνίας επιπέδου υπηρεσιών (**Service Level Agreement**), σύμβασης πλαισίου παροχής υπηρεσιών (**Framework Service Agreement**), ή συμφωνίας διαβίβασης δεδομένων (**Data Transfer Agreement**).[507]

Η σύμβαση που συνάπτεται ανάμεσα στον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία θα πρέπει να είναι έγγραφη και να περιλαμβάνει όσα προβλέπονται στο άρθρο 28 παρ. 3 του Κανονισμού. Περαιτέρω, ο εκτελών την επεξεργασία θα πρέπει να ενεργεί βάσει αναλυτικών έγγραφων οδηγιών του υπευθύνου επεξεργασίας (πιστωτικού ιδρύματος), ακόμα και σε περιπτώσεις διασυνοριακών διαβιβάσεων, εκτός αν η επεξεργασία απαιτείται βάσει ενωσιακού

---

[505] Η ύπαρξη εννόμου συμφέροντος του υπευθύνου επεξεργασίας που δικαιολογεί την διαβίβαση δεδομένων προσωπικού χαρακτήρα εντός του ομίλου, αναγνωρίζεται και από την αιτ. σκέψη 48 του ΓΚΠΔ, στην οποία αναφέρεται σχετικά: «*Οι υπεύθυνοι επεξεργασίας που είναι μέλη ομίλου επιχειρήσεων ή ιδρυμάτων που συνδέονται με κεντρικό φορέα ενδέχεται να έχουν έννομο συμφέρον να διαβιβάζουν δεδομένα προσωπικού χαρακτήρα εντός του ομίλου επιχειρήσεων για εσωτερικούς διοικητικούς σκοπούς, συμπεριλαμβανομένης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα πελατών ή εργαζομένων*..»

[506] Christopher Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, 1st ed. (repr., Kettering: Oxford University Press, 2019), 606.

[507] Alfred Büllesbach and Serge Gijrath, *Concise European IT Law*, 2nd ed. (repr., Alphen aan den Rijn, The Netherlands: Wolters Kluwer Law & Business, 2010), 86.

ή εθνικού δικαίου (άρθρο 28 παρ. 3 στοιχείο α'). Η σύμβαση θα πρέπει επίσης να καθορίζει ότι τα φυσικά πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα προσωπικά δεδομένα υπόκεινται σε κανονιστικές υποχρεώσεις τήρησης της εμπιστευτικότητας (άρθρο 28 παρ. 3 στοιχείο β') και ο εκτελών την επεξεργασία θα πρέπει ταυτόχρονα να υπογράφει συμφωνίες εμπιστευτικότητας με τους εργαζόμενους του και τους υπεργολάβους του. Μετά το πέρας της παροχής υπηρεσιών, ο εκτελών την επεξεργασία θα πρέπει να διαγράφει ή να επιστρέφει τα προσωπικά δεδομένα στον υπεύθυνο επεξεργασίας και να διαγράφει όλα τα υπάρχοντα αντίγραφα εκτός αν απαιτείται βάσει ενωσιακού ή εθνικού δικαίου να διατηρεί αυτά (άρθρο 28 παρ. 3 στοιχείο ζ'). Ανάμεσα στα τεχνικά και οργανωτικά μέτρα που πρέπει να εφαρμόζει ο εκτελών την επεξεργασία (άρθρο 28 παρ. 3 στοιχείο γ, άρθρο 32 ΓΚΠΔ), είναι η ψευδωνυμοποίηση (άρθρο 32), η κρυπτογράφηση (αιτ. σκέψη 83), η ικανότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε προσωπικά δεδομένα σε εύθετο χρόνο έπειτα από φυσικό ή τεχνικό συμβάν (άρθρο 32 παρ. 1 στοιχείο γ') και η θέσπιση διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση των μέτρων ασφαλείας ώστε να διασφαλιστεί η αποτελεσματικότητά τους (άρθρο 32 παρ. 1 στοιχείο δ'). Τέλος, θα πρέπει να ενημερώνουν το πιστωτικό ίδρυμα αμελλητί, μόλις αντιληφθούν ότι παραβιάστηκαν τα προσωπικά δεδομένα των πελατών-υποκειμένων.

4.5.10.1 Διαβίβαση δεδομένων σε εταιρείες ενημέρωσης οφειλετών

Ο νόμος 3758/2009 («Εταιρείες ενημέρωσης οφειλετών για ληξιπρόθεσμες απαιτήσεις και άλλες διατάξεις») που διέπει τη λειτουργία των εταιρειών ενημέρωσης οφειλετών, ως ειδικότερος του Κανονισμού, έχει το προβάδισμα εφαρμογής έναντι αυτού.[508] Τα τραπεζικά ιδρύματα έχουν δικαίωμα να χορηγούν στις εταιρείες αυτές στοιχεία που αφορούν ληξιπρόθεσμες απαιτήσεις έναντι των οφειλετών. Επομένως, στις περιπτώσεις αυτές υπεύθυνος επεξεργασίας είναι το τραπεζικό ίδρυμα και εκτελούσα την επεξεργασία η εταιρεία ενημέρωσης οφειλετών που ενεργεί για λογαριασμό του.[509] Στο πλαίσιο αυτό, η εταιρεία ενημέρωσης οφειλετών θα πρέπει να ενεργεί κατόπιν γραπτής συμβάσεως ή άλλης νομικής πράξης, που προβλέπεται στο άρθρο 28 παρ. 3 του Κανονισμού και θα πρέπει να έχει λάβει και να τηρεί τα τεχνικά και οργανωτικά μέτρα, ώστε να διασφαλίζεται η ασφάλεια των δεδομένων των υποκειμένων. Εάν, η εταιρεία ενημέρωσης οφειλετών, ως εκτελούσα την επεξεργασία, υπερβεί τις εντολές του πιστωτικού ιδρύματος ή συνεχίσει να επεξεργάζεται τα δεδομένα μετά το πέρας της συμβατικής διάρκειας, τότε νοείται ως υπεύθυνος επεξεργασίας και οφείλει να αποδεικνύει τη νομιμότητα της επεξεργασίας.

Για να εξασφαλιστεί η νομιμότητα της διαβίβασης δεδομένων από το πιστωτικό ίδρυμα στην εταιρεία ενημέρωσης οφειλετών, θα πρέπει το πιστωτικό ίδρυμα να έχει ενημερώσει προηγουμένως ειδικά και συγκεκριμένα για την διαβίβαση αυτή. Η ενημέρωση αυτή μπορεί να λάβει χώρα είτε κατά τη σύναψη της σύμβασης με τον εκάστοτε πελάτη, είτε μέσω της τελευταίας έγγραφης ενημέρωσης του οφειλέτη ότι η οφειλή του κατέστη ληξιπρόθεσμη και ότι σε περίπτωση που δεν προχωρήσει σε τακτοποίηση αυτής, τα συναφή στοιχεία του θα ανακοινωθούν σε εταιρεία ενημέρωσης οφειλετών, με σκοπό την ενημέρωσή του σύμφωνα με το νόμο 3758/2009. Στην πρώτη περίπτωση, η ενημέρωση συμπεριλαμβάνεται στο κείμενο της σύμβασης, εντός του οποίου

[508] Η Αρχή έχει επισημάνει ότι ο ν. 3758/2009, θα πρέπει να αναμορφωθεί εκ νέου, ώστε να μην έρχεται σε αντίθεση με τις διατάξεις του ΓΚΠΔ. Βλ. συστάσεις Αρχής, Γ/ΕΞ/2964-1/30-04-2018.
[509] Βλ. άρθρο 4 αρ. 8 και άρθρο 28 του ΓΚΠΔ. Επίσης, απόφαση ΕιρΠειρ 92/2018 και αποφάσεις 20/2001, 59/2009, 49/2011, 98/2017 ΑΠΔΠΧ.

θα πρέπει να καθίσταται σαφές ότι ο δανειστής έχει δικαίωμα, εφόσον η οφειλή καταστεί ληξιπρόθεσμη, να ανακοινώσει τα δεδομένα του πελάτη του σε εταιρεία ενημέρωσης οφειλετών, ώστε να ενημερωθεί σύμφωνα με τους όρους που προβλέπονται στις διατάξεις του νόμου 3758/2009.[510] Επισημαίνεται δε ότι οι παλαιοί πελάτες, δηλαδή εκείνοι που υπέγραψαν συμβάσεις με τους δανειστές πριν την έναρξη ισχύος του ν. 3758/2009 (05-05-2009), πρέπει να ενημερώνονται για την εν λόγω νέα επεξεργασία με τρόπο πρόσφορο και σαφή, για παράδειγμα με συστημένη επιστολή που θα περιλαμβάνει την ανωτέρω πληροφόρηση ή με ενσωμάτωση της σχετικής πληροφόρησης στα αντίγραφα λογαριασμών.[511]

Με το υπ'αριθμ. Πρωτοκόλλου Γ/ΕΞ/73-1/28-01-2013 έγγραφό της, η Αρχή διευκρίνισε ότι σε περίπτωση επιτρεπτής επεξεργασίας, όπως συμβαίνει κατά την επεξεργασία που είναι απαραίτητη για την εκτέλεση σύμβασης, η χορήγηση και ανακοίνωση των στοιχείων των οφειλετών από τραπεζικό ίδρυμα προς την εκάστοτε συνεργαζόμενη με αυτό εταιρεία ενημέρωσης οφειλετών (εκτελούσα την επεξεργασία), επιτρέπεται και χωρίς να έχει συγκατατεθεί ο οφειλέτης-υποκείμενο των δεδομένων, εφόσον όμως η τράπεζα έχει προβεί σε σαφή ενημέρωση σχετικά με την κατηγορία αυτή των αποδεκτών των δεδομένων του. Θα πρέπει επίσης να τηρούνται απαρεγκλίτως σε τέτοιες περιπτώσεις οι υποχρεώσεις σχετικά με τη διασφάλιση του απορρήτου και της ασφάλειας των δεδομένων.[512]

Βάσει του άρθρου 4 παρ. 4 του νόμου 3758/2009, θα πρέπει επίσης να λαμβάνεται ειδική μέριμνα, με στόχο τη εξασφάλιση της ακρίβειας των δεδομένων που αφορούν τον πελάτη-υποκείμενο αυτών. Ο δανειστής επομένως θα πρέπει να επιβεβαιώνει τις οφειλές και να έχει ταυτοποιήσει τον οφειλέτη πριν προβεί σε οποιαδήποτε ενέργεια ενημέρωσης των οφειλετών από τον ίδιο ή πριν ανακοινώσει τα σχετικά στοιχεία σε εταιρεία ενημέρωσης οφειλετών. Η επικαιροποίηση του αρχείου γίνεται με κάθε πρόσφορο τρόπο. Εάν διαπιστωθεί ότι τα στοιχεία που είχαν δηλωθεί στο δανειστή είναι ψευδή ή λανθασμένα, το βάρος για την εύρεση των αληθών στοιχείων του οφειλέτη φέρει ο δανειστής.

Με την υπ'αριθμ. Πρωτοκόλλου Γ/ΕΞ/1325-1/12-07-2013 γνωμοδότησή της[513], η Αρχή έκρινε ότι η καταγραφή κάθε επικοινωνίας με τρίτο πρόσωπο-οφειλέτη συνιστά αναγκαία επεξεργασία για την εκπλήρωση της υποχρέωσης του υπευθύνου επεξεργασίας να παρέχει στη Γενική Γραμματεία Καταναλωτή κάθε στοιχείο που αποτελεί απόδειξη της συμμόρφωσή του με τις επιταγές του νόμου 3758/2009, ήτοι αν πραγματοποίησε την εν λόγω επικοινωνία σύμφωνα με τους όρους που προβλέπονται στο άρθρο 4 του νόμου αυτού, αλλά και αν κατά την επικοινωνία αυτή όχλησε ή όχι οικεία πρόσωπα του οφειλέτη. Κατά την τηλεφωνική ομιλία, ο καλών οφείλει να ενημερώσει τόσο για την ιδιότητά του (εταιρεία ενημέρωσης ή δανειστής) και τα λοιπά στοιχεία που προβλέπονται στο νόμο 3758/2009, όσο και το γεγονός της καταγραφής πριν την έναρξη κάθε επικοινωνίας από οποιοδήποτε πρόσωπο και αν απαντηθεί η κλήση, είτε δηλαδή αυτή απαντηθεί από τον ίδιο τον οφειλέτη είτε από τρίτο πρόσωπο (άρθρα 6 παρ. 2 και 8 παρ. 2

---

[510] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 82-83.
[511] Απόφαση 98/2017 ΑΠΔΠΧ. https://www.dpa.gr/sites/default/files/2019-10/98_2017anonym.pdf.
[512] https://www.hellenicparliament.gr/UserFiles/67715b2c-ec81-4f0c-ad6a-476a34d732bd/7970809.pdf.
[513] https://www.dpa.gr/sites/default/files/2020-05/ENIMEROSI%20OFEILETON%20-%20KATAGRAFI%20SYNOMILION%20ME%20TRITOYS_FINAL.PDF.

του ν. 3758/2009 σε συνδυασμό με άρθρο 4 παρ. 3 του ν. 3471/2006). Η καλούσα εταιρεία οφείλει καταρχάς να βεβαιωθεί για την ταυτότητα του καλούμενου, δηλαδή αν πρόκειται για τον ίδιο τον οφειλέτη ή τρίτο πρόσωπο, και μόνον στην πρώτη περίπτωση να προβεί σε ενημέρωση σχετικά με την οφειλή, ενώ στη δεύτερη περίπτωση θα πρέπει να διακόψει τη συνομιλία. Το τρίτο πρόσωπο-οικείος του οφειλέτη αλλά και ο ίδιος ο οφειλέτης έχουν, ως υποκείμενα των δεδομένων, δικαίωμα πρόσβασης στα δεδομένα που τους αφορούν και περιέχονται στο σύνολο των ηχογραφημένων αυτών συνομιλιών, το οποίο ο υπεύθυνος επεξεργασίας οφείλει να ικανοποιήσει σύμφωνα με τους όρους του άρθρου 15 του Κανονισμού σε συνδυασμό με το άρθρο 6 παρ. 7 και το άρθρο 8 παρ. 2 του ν. 3758/2009.

Με την υπ'αριθμ. 98/2017 απόφαση της, η Αρχή απεφάνθη ότι θα πρέπει να λαμβάνει χώρα ειδική ενημέρωση των οφειλετών σχετικά με τη διάθεση των δεδομένων τους από τους δανειστές σε Εταιρείες Ενημέρωσης οφειλετών, δηλαδή οι δανειστές, ως υπεύθυνοι επεξεργασίας, οφείλουν να ενημερώνουν τους οφειλέτες για τη διάθεση των δεδομένων του στην εκάστοτε συγκεκριμένη εταιρεία ενημέρωσης οφειλετών να παρέχει ένα εύλογο διάστημα (π.χ. ενδεικτικά, 10-15 ημερών) πριν από τη διάθεση για την άσκηση των δικαιωμάτων πρόσβασης και αντίρρησης και να μμεριμνήσει, ώστε η ενημέρωση αυτή να γίνεται με κάθε πρόσφορο τρόπο (π.χ. με ενσωμάτωση της σχετικής πληροφόρησης στα αντίγραφα λογαριασμών και σε ευδιάκριτο σημείο αυτών ή μέσω ηλεκτρονικού ταχυδρομείου (email).[514]

4.6 Ο χρόνος τήρησης των δεδομένων των πελατών των τραπεζικών ιδρυμάτων

Τα δεδομένα προσωπικού χαρακτήρα τηρούνται από τα τραπεζικά ιδρύματα για το χρόνο που είναι απαραίτητος ώστε να εκπληρωθεί ο σκοπός που εξυπηρετεί η επεξεργασία αυτών, άλλως για τον ελάχιστο χρόνο που απαιτείται σύμφωνα με την εκάστοτε ισχύουσα νομοθεσία που διέπει τη λειτουργία των τραπεζικών ιδρυμάτων, αλλά όχι για χρόνο μεγαλύτερο των είκοσι ετών από τη λήξη της σύμβασης ή της συναλλαγής, που αποτελεί τον χρόνο της κατ' άρθρο 249 ΑΚ γενικής παραγραφής των αξιώσεων. Εάν μέχρι τη λήξη της προθεσμίας αυτής βρίσκονται σε εξέλιξη δικαστικές ενέργειες σε σχέση με το πιστωτικό ίδρυμα, οι οποίες αφορούν άμεσα ή έμμεσα το υποκείμενο των δεδομένων, ο προαναφερθείς χρόνος τήρησης των δεδομένων προσωπικού χαρακτήρα παρατείνεται μέχρι να εκδοθεί αμετάκλητη δικαστική απόφαση.[515]

Ειδικότερα, τα αρχεία που σχετίζονται άμεσα με την κατάρτιση και τη λειτουργία της σύμβασης που έχει συνάψει ο πελάτης με το τραπεζικό ίδρυμα, τα υποστηρικτικά έγγραφα αυτής, αλλά και τα έγγραφα που παρήχθησαν κατά τη διάρκεια της ισχύος της σύμβασης (π.χ. πρόσθετες πράξεις, επιστολές για την ερμηνεία των όρων της σύμβασης) με πιστωτικό ίδρυμα ή εγχρήματη συναλλαγή σε αυτό, διατηρούνται τουλάχιστον καθ' όλη τη διάρκεια της σχέσης του πιστωτικού ιδρύματος με τον πελάτη, έως την ολοσχερή εξόφληση κάθε σχετικής οφειλής ή απαίτησης και τη συμπλήρωση του κατά νόμου χρόνου παραγραφής κάθε τυχόν αξίωσης.[516]

---

[514] Απόφαση 98/2017 ΑΠΔΠΧ, https://www.dpa.gr/sites/default/files/2019-10/98_2017anonym.pdf.

[515] Ελληνική Ένωση Τραπεζών, "Κώδικας Δεοντολογίας Για Την Επεξεργασία Προσωπικών Δεδομένων Στο Τραπεζικό Σύστημα" (repr., Σχέδιο 16.1.2019), 24. https://www.hba.gr/UplDocs/GDPR/%CE%9A%CE%A9%CE%94%CE%99%CE%9A%CE%91%CE%A3%20%CE%94%CE%95%CE%9F%CE%9D%CE%A4%CE%9F%CE%9B%CE%9F%CE%93%CE%99%CE%91%CE%A3.pdf

[516] Ibid., 24.

Περαιτέρω, τα πιστωτικά ιδρύματα φυλάσσουν τα στοιχεία πιστοποίησης και επαλήθευσης της ταυτότητας του πελάτη κατά τη σύναψη κάθε είδους σύμβασης, τα νομιμοποιητικά έγγραφα, τα αντίγραφα εγγράφων με βάση τα οποία έγινε η πιστοποίηση της ταυτότητας, τα πρωτότυπα έγγραφα ή τα αντίγραφα παραστατικά κάθε είδους συναλλαγών, τα εσωτερικά έγγραφα που αφορούν εγκρίσεις ή διαπιστώσεις ή εισηγήσεις για υποθέσεις που σχετίζονται με τη διερεύνηση αδικημάτων του άρθρου 2 του νόμου 3691/2008, αλλά και την αλληλογραφία με τους πελάτες. Τα έγγραφα αυτά τηρούνται για χρονικό διάστημα τουλάχιστον πέντε (5) ετών από τη λήξη της επιχειρηματικής σχέσης με τους πελάτες ή την εκτέλεση κάθε συναλλαγής, εκτός εάν η τήρησή τους επιβάλλεται από διάταξη νόμου για μεγαλύτερο χρονικό διάστημα.[517]

Επιπροσθέτως, τα δεδομένα που αφορούν τηλεφωνικές συνομιλίες με αντικείμενο συναλλαγές επί χρηματοπιστωτικών μέσων, διατηρούνται για χρονικό διάστημα τουλάχιστον πέντε (5) ετών ή για πρόσθετη περίοδο δύο (2) ετών μετά από απόφαση της Επιτροπής Κεφαλαιαγοράς όταν διενεργεί έρευνα για κατάχρηση της αγορά (άρθρο 43 νόμος 4443/2016). Οι τηλεφωνικές επικοινωνίες με πελάτες στο πλαίσιο των διατάξεων των νόμων 3758/2009 και 4354/2015, διατηρούνται υποχρεωτικά για ένα έτος από την συνομιλία, εκτός αν έχει αιτηθεί την λήψη της συνομιλίας το υποκείμενο ή η εποπτική αρχή.[518]

Σχετικά με τα εικόνες που λαμβάνονται από συστήματα βιντεοεπιτήρησης στους χώρους των συναλλαγών ή στις εισόδους των υπηρεσιών των τραπεζικών ιδρυμάτων, θα πρέπει να σημειωθεί ότι αυτές διατηρούνται για χρονικό διάστημα που δεν ξεπερνά τις σαράντα πέντε (45) ημέρες από τη λήψη τους. Αν στη διάρκεια αυτής της χρονικής περιόδου καταγραφούν περιστατικά απάτης ή αμφισβήτησης οικονομικής συναλλαγής, τα σχετικά τμήματα των δεδομένων του συστήματος βιντεοεπιτήρησης μπορούν να διατηρηθούν σε ξεχωριστό αρχείο ανάλογα με τα μέτρα ασφαλείας που τηρούνται, για όσο διάστημα απαιτείται για να ολοκληρωθεί η διερεύνηση και η πειθαρχική ή δικαστική δίωξη των περιστατικών αυτών (άρθρο 16 της υπ'αριθ. 1/2011 Οδηγίας της ΑΠΔΠΧ).[519]

Τα αρχεία τα οποία περιλαμβάνουν δεδομένα των υποκειμένων-πελατών που δημιουργούνται από την εφαρμογή του Κώδικα Δεοντολογίας του νόμου 4224/2013 στο πλαίσιο της διαδικασίας επίλυσης καθυστερήσεων, διατηρούνται για ελάχιστη περίοδο έξι (6) ετών από την ημερομηνία που κάθε ένα από τα στοιχεία περιήλθε στην κατοχή του πιστωτικού ιδρύματος και για όλα τα στοιχεία κάθε πελάτη-δανειολήπτη για τουλάχιστον έξι (6) έτη μετά την λήξη της συνεργασίας του με αυτόν. Στο αρχείο αυτό περιλαμβάνονται επίσης τα δικαιολογητικά που τεκμηριώνουν την επιδίωξη λύσης με την διαδικασία επίλυσης καθυστερήσεων του Κώδικά ή τους λόγους που

---

[517] Επιτροπή τραπεζικών και πιστωτικών θεμάτων της Τράπεζας της Ελλάδος, "ΕΤΠΘ 281/5/17.3.2009, Πρόληψη Της Χρησιμοποίησης Των Εποπτευομένων Από Την Τράπεζα Της Ελλάδος Πιστωτικών Ιδρυμάτων Και Χρηματοπιστωτικών Οργανισμών Για Τη Νομιμοποίηση Εσόδων Από Παράνομες Δραστηριότητες Και Τη Χρηματοδότηση Της Τρομοκρατίας", 2009.

[518] Ελληνική Ένωση Τραπεζών, "Κώδικας Δεοντολογίας Για Την Επεξεργασία Προσωπικών Δεδομένων Στο Τραπεζικό Σύστημα" (repr., Σχέδιο 16.1.2019), 24. https://www.hba.gr/UplDocs/GDPR/%CE%9A%CE%A9%CE%94%CE%99%CE%9A%CE%91%CE%A3%20%CE%94%CE%95%CE%9F%CE%9D%CE%A4%CE%9F%CE%9B%CE%9F%CE%93%CE%99%CE%91%CE%A3.pdf

[519] Ibid.

εμπόδισαν την επιδίωξη λύσης μέσω της διαδικασίας αυτής (υπό κεφάλαιο 7 της υπ'αριθ. 195/2016 Απόφασης της Επιτροπής Πιστωτικών και Ασφαλιστικών Θεμάτων της ΤτΕ).[520]

Περαιτέρω, τα δεδομένα που αφορούν σε επικοινωνίες με υποκείμενα για την λήψη συγκατάθεσης, για επεξεργασία με σκοπό την προώθηση προϊόντων ή υπηρεσιών, τηρούνται μέχρι την ανάκλησή της και τα δεδομένα αυτής τηρούνται μέχρι την επαναχορήγηση συγκατάθεσης, ενώ τα δεδομένα που αφορούν σε επικοινωνίες προς υποκείμενα για σκοπούς προώθησης, διατηρούνται για ένα (1) έτος από τη διενέργεια της τελευταίας επικοινωνίας μαζί τους.[521]

Τέλος, με την επιφύλαξη τυχόν ειδικότερης νομοθεσίας, τα δεδομένα των πελατών των τραπεζών που έχουν υποβάλλει αίτηση δανειοδότησης ή παροχής εγγυοδοσίας υπέρ πελάτη, και το αίτημα δεν ικανοποιήθηκε, διατηρούνται για πέντε (5) χρόνια από την απόρριψή του, δηλαδή όσο διαρκεί η 5ετής παραγραφή των αξιώσεων κατά το προσυμβατικό στάδιο, για την προάσπιση των έννομων συμφερόντων του πιστωτικού ιδρύματος που συνίσταται : α) στην απόδειξη τήρησης της νομιμότητας για την άντληση δεδομένων οικονομικής συμπεριφοράς του αιτούντος από διατραπεζικά αρχεία πληροφοριών, β) στην αξιολόγηση της πιστοληπτικής ικανότητας του υποψηφίου δανειολήπτη σε περίπτωση που αυτός επανέλθει με νέο αίτημα εντός του ως άνω χρονικού διαστήματος τήρησης και γ) στην προάσπιση των συμφερόντων της Τράπεζας, σε περίπτωση προβολής αντιρρήσεων ή ενστάσεων του υποψηφίου πελάτη για την απόρριψη του αιτήματός του ή τη διαδικασία εξέτασης του αιτήματός του. Στην περίπτωση αυτή, τα δεδομένα των αιτήσεων που έχουν απορριφθεί, τηρούνται για το χρόνο που δικαιολογείται από το σκοπό που εξυπηρετεί η διατήρηση της πληροφόρησης με απώτατο χρονικό διάστημα τα 5 έτη, που συμπίπτει με το χρόνο παραγραφής των αξιώσεων κατά το προσυμβατικό στάδιο. Η εκκίνηση του χρόνου αυτού τοποθετείται κατά τη στιγμή που το μέρος που επικαλείται την ευθύνη του άλλου μέρους έλαβε γνώση της ζημίας του. Με την επιφύλαξη της ΕΤΠΘ 281/2009, τα παραπάνω δεν ισχύουν για τα δικαιολογητικά που έχει προσκομίσει ο πελάτης, τα οποία πρέπει να καταστρέφονται ή να επιστρέφονται σε αυτόν μετά την απόρριψη.[522]

4.7 Η λειτουργία συστημάτων βιντεοεπιτήρησης και ασφάλειας εισόδου στις εγκαταστάσεις των πιστωτικών ιδρυμάτων

Το άρθρο 16 της Οδηγίας 1/2011[523] της Αρχής[524] ορίζει τις προϋποθέσεις της νόμιμης εγκατάστασης και λειτουργίας συστημάτων βιντεοεπιτήρησης στους χώρους των τραπεζικών ιδρυμάτων. Συγκεκριμένα, στην παράγραφο 1 του άρθρου 16 καθιερώνεται το σύννομο της εποπτείας μέσω συστημάτων βιντεοεπιτήρησης σε όλους τους χώρους των εγκαταστάσεων των τραπεζών, εκτός των χώρων στους οποίους τα υποκείμενα των δεδομένων έχουν αυξημένες προσδοκίες για την ιδιωτικότητά τους, όπως α) χώρους και προθαλάμους τουαλετών ανεξάρτητα του είδους της επιχείρησης ή του φορέα που βρίσκονται οι χώροι αυτοί και β) αποδυτήρια και

[520] Ibid.,25.
[521] Ibid.
[522] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 75.
[523] https://www.dpa.gr/sites/default/files/2020-01/ODIGIA_CCTV_FINAL_1_2011.PDF.
[524] Η Οδηγία διατηρείται σε ισχύ κατά το άρθρο 83 παρ. 2 του νόμου 4624/2019.

λουτρά προσωπικού ή πελατών.[525] Ειδικά για την αποφυγή κλοπών, το πιστωτικό ίδρυμα, οφείλει να προβεί στη λήψη εναλλακτικών μέτρων, όπως της χρήση ερμαρίων που διαθέτουν κλειδαριά ή διαχωρισμένων χώρων φύλαξης.

Περαιτέρω, η διαβίβαση σε τρίτους δεδομένων και αποσπασμάτων υλικού που προέρχονται από συστήματα βιντεοσκόπησης, επιτρέπεται κατόπιν προηγούμενης συγκατάθεσης του υποκειμένου των δεδομένων που απεικονίζεται σε αυτό (άρθρο 9 παρ. 1 Οδηγία 1/2011 ΑΠΔΠΧ). Ωστόσο, ο υπεύθυνος επεξεργασίας, δηλαδή στην περίπτωση αυτή το πιστωτικό ίδρυμα, έχει υποχρέωση να διαβιβάζει στις αρμόδιες δικαστικές, εισαγγελικές και αστυνομικές αρχές, δεδομένα που ζητούν οι τελευταίες νομίμως κατά την άσκηση των καθηκόντων τους, ενώ δύναται να διαβιβάζει σε αυτές και αποσπάσματα που ενδεχομένως αποτελούν αποδεικτικά στοιχεία αξιόποινων πράξεων (π.χ. κλοπή, ξυλοδαρμός), που τελέστηκαν στον χώρο τον οποίο έχει συμφέρον ή νομική υποχρέωση να προστατεύσει με σύστημα βιντεοεπιτήρησης και που μπορούν να συνεισφέρουν στη διερεύνηση των πραγματικών περιστατικών ή στην αναγνώριση των δραστών (άρθρο 9 Οδηγία 1/2011 ΑΠΔΠΧ). Επιπλέον, ο υπεύθυνος επεξεργασίας επιτρέπεται να διαβιβάσει αποσπάσματα που ενδέχεται να αποτελούν αποδεικτικά στοιχεία μιας αξιόποινης πράξης στο ίδιο πρόσωπο που απεικονίζεται ως θύμα ή δράστης της πράξης (άρθρο 9 παρ. 4 Οδηγία 1/2011 ΑΠΔΠΧ). Στην περίπτωση αυτή, κατά την διαβίβαση των σχετικών αρχείων, ειδικά εάν αυτά αφορούν εσωτερικούς χώρους του καταστήματος, θα πρέπει να λαμβάνεται μέριμνα ώστε να μην αποκαλύπτονται στοιχεία που προστατεύονται από τις διατάξεις περί τραπεζικού απορρήτου (Ν.Δ. 1059/1971), εφόσον δεν έχει προηγηθεί νόμιμη άρση αυτού.[526]

Με την απόφαση 40/2001, η Αρχή αποφάσισε στο πλαίσιο της πρόληψης και αποτροπής εγκλημάτων σε τράπεζες, να επιτρέψει σε αυτές να διατηρούν αρχεία που συλλέγονται από την εγκατάσταση κλειστών κυκλωμάτων, για χρονικό διάστημα που δεν ξεπερνά τις σαράντα πέντε (45) ημερολογιακές μέρες, σε αντίθεση με το προηγούμενο όριο των 15 ημερών, το οποίο προβλεπόταν αρχικά στην υπ'αριθμ. 1122 (Φ.Ε.Κ. αρ. 1234/9-10-2000) Οδηγία της.[527] Η Οδηγία αυτή καταργήθηκε με την Οδηγία 1/2001 που αφορά τη χρήση συστημάτων βιντεοεπιτήρησης στα πιστωτικά ιδρύματα.

Στο πλαίσιο της συμμόρφωσης προς την υποχρέωση αυξημένης διαφάνειας, οι υπεύθυνοι επεξεργασίας που κάνουν χρήση συστημάτων βιντεοεπιτήρησης, οφείλουν να παρέχουν πλήρη ενημέρωση στα υποκείμενα για τη λειτουργία καμερών πριν την είσοδο κάποιου στην εμβέλεια του συστήματος βιντεοεπιτήρησης. Η σχετική ενημέρωση θα πρέπει να διενεργείται με τρόπο εμφανή και κατανοητό, μέσω ανάρτησης ευδιάκριτων πινακίδων σε επαρκή αριθμό και εμφανές μέρος, στις οποίες θα αναγράφεται το πρόσωπο για λογαριασμό του οποίου διενεργείται η επεξεργασία, ο σκοπός, καθώς και το άτομο με το οποίο τα υποκείμενα των δεδομένων μπορούν να επικοινωνήσουν για να ασκήσουν τα δικαιώματα πρόσβασης και εναντίωσης σχετικά με το βιντεοληπτικό υλικό στο οποίο καταγράφεται η εικόνα τους (άρθρο 12 Οδηγία 1/2011 ΑΠΔΠΧ).

---

[525] Άρθρο 6 παρ. 3 Οδηγία 1/2011 ΑΠΔΠΧ.
[526] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 76.
[527] Ετήσια έκθεση ΑΠΔΠΧ 2001, 41.
https://www.dpa.gr/sites/default/files/2019-09/DPA_ANNUAL_REPORT_2001.PDF.

Αναφορικά με την λειτουργία συστημάτων ασφαλείας εισόδου, η Αρχή με την απόφαση 194/2012, απεφάνθη ότι είναι νόμιμη η εγκατάσταση συστήματος που καταγράφει την εικόνα και στοιχεία της γεωμετρίας του προσώπου του εισερχόμενου στο κατάστημα, στην είσοδο του καταστήματος του πιστωτικού ιδρύματος. Η επεξεργασία αυτή επιτρέπεται στο πλαίσιο της ικανοποίησης του υπέρτερου έννομου συμφέροντος του υπευθύνου επεξεργασίας (άρθρο 6 παρ. 1 στοιχείο στ' Κανονισμού). Ως υπέρτερο έννομο συμφέρον που δικαιολογεί την εγκατάσταση του συστήματος αυτού, νοείται στην περίπτωση αυτή το έννομο συμφέρον ή η νομική υποχρέωση του ιδιοκτήτη ή του διαχειριστή ενός χώρου να διασφαλίσει την προστασία του χώρου αυτού αλλά και τα αγαθά που βρίσκονται εντός αυτού από παράνομες πράξεις, αλλά και την ασφάλεια της ζωής, της σωματικής ακεραιότητας και της υγείας του συναλλακτικού κοινού και του προσωπικού εντός του επιτηρούμενου χώρου. Η λειτουργία του συστήματος αυτού θα πρέπει όμως να είναι σύμφωνη και με την αρχή της αναλογικότητας, υπό την ειδικότερη έκφανση της αναγκαιότητας και επομένως θα πρέπει να επιτρέπεται μόνο στην περίπτωση που πληρούνται προϋποθέσεις ανάλογες με αυτές που προβλέπονται στο άρθρο 2 παρ. 3 στοιχ. β΄ της υπουργικής απόφασης 3015/30/6/2009 για την εγκατάσταση άθραυστων υαλοπινάκων. Συγκεκριμένα, απαιτείται για τη νόμιμη εγκατάσταση του συστήματος αυτού, να έχει προηγηθεί ειδικά αιτιολογημένη απόφαση του διευθυντή της οικείας Διεύθυνσης Ασφαλείας ή Αστυνομικής Διεύθυνσης, η οποία θα λαμβάνει ιδίως υπόψη την εγκληματικότητα, την πραγματοποίηση συναθροίσεων ή συγκεντρώσεων στην περιοχή, τη διάπραξη στο συγκεκριμένο κατάστημα φθορών ή ληστείας κατά το παρελθόν, την απόστασή του από το πλησιέστερο αστυνομικό τμήμα, καθώς και τη διακίνηση από το συγκεκριμένο κατάστημα μεγάλων χρηματικών ποσών ή τη φύλαξη σε αυτό αντικειμένων σημαντικής αξίας.[528]

Επίσης, το πιστωτικό ίδρυμα για να διασφαλίσει τη νομιμότητα της επεξεργασίας δεδομένων που καταγράφονται από το σύστημα ασφαλείας, θα πρέπει, ως υπεύθυνος επεξεργασίας, κατά το στάδιο συλλογής των προσωπικών δεδομένων, να ενημερώνει με τρόπο πρόσφορο και σαφή τα υποκείμενα για την ταυτότητά του, την ταυτότητα του τυχόν εκπροσώπου του, τον σκοπό της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων, την ύπαρξη δικαιώματος πρόσβασης και αντίρρησης και τον τρόπο με τον οποίο αυτά μπορούν να ασκηθούν. Τέλος, με βάση την απόφαση της Αρχής, τα δεδομένα που καταγράφονται από τα συστήματα ασφαλείας εισόδου θα πρέπει να τηρούνται για χρονικό διάστημα είκοσι τεσσάρων (24) ωρών, με εξαίρεση τα Σαββατοκύριακα, οπότε η διαγραφή των δεδομένων θα πραγματοποιείται τις Δευτέρες, καθώς ο χρόνος αυτός επαρκεί για να επιτευχθεί ο σκοπός της επεξεργασίας. [529]

[528] Απόφαση 194/2012 ΑΠΔΠΧ, σελ. 16. https://www.dpa.gr/sites/default/files/2019-10/194_2012anonym.pdf.
[529] Ibid.,16.

ΠΕΜΠΤΟ ΚΕΦΑΛΑΙΟ
ΤΟ ΤΡΑΠΕΖΙΚΟ ΑΠΟΡΡΗΤΟ ΚΑΙ Η ΦΥΣΗ ΤΟΥ ΩΣ ΔΕΔΟΜΕΝΟ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

5.1 Το γενικό τραπεζικό απόρρητο

Οι τράπεζες στο πλαίσιο των συναλλακτικών και έννομων τους σχέσεων με τους πελάτες τους, έχουν υποχρέωση να τηρούν το τραπεζικό απόρρητο. Ως γενικό τραπεζικό απόρρητο νοείται η υποχρέωση της τράπεζας να μην αποκαλύπτει σε τρίτους (οικονομικές ή προσωπικές) πληροφορίες των πελατών τους, τις οποίες αυτοί εμπιστεύθηκαν σε αυτήν ή οι οποίες περιήλθαν στην αντίληψη της τράπεζας κατά την άσκηση των δραστηριοτήτων της. Η υποχρέωση αυτή των τραπεζών να μην αποκαλύπτουν σε τρίτους πληροφορίες των πελατών τους δεν πηγάζει από μια ρητά ή σιωπηρά συνομολογημένη συμβατική ρήτρα μεταξύ τράπεζας και πελάτη αλλά από τον ίδιο το νόμο. Επιπλέον, το τραπεζικό απόρρητο διαφέρει ως προς την έκταση και τις έννομες συνέπειες από το ειδικό απόρρητο των τραπεζικών καταθέσεων (ν.δ. 1059/1071), αλλά και από τις υποχρεώσεις που επιβάλλονται με βάση τη νομοθεσία περί προστασίας των προσωπικών δεδομένων.

Το γενικό τραπεζικό απόρρητο απορρέει από τη σχέση πίστεως και προστασίας που συνδέει τα τραπεζικά ιδρύματα με τους πελάτες τους. Οι συναλλασσόμενοι έχουν επομένως έντονο και προστατευτέο συμφέρον να μην γίνονται ευρύτερα γνωστές οι οικονομικές τους συναλλαγές. Αυτό εντάσσεται στο γενικότερο συμφέρον των προσώπων προς διαφύλαξη των ιδιωτικών τους απορρήτων, τα οποία αποτελούν στοιχεία του δικαιώματος της προσωπικότητας. Το δικαίωμα αυτό της προσωπικότητας ανήκει και στα νομικά πρόσωπα, στο πλαίσιο προστασίας και διατήρησης τη καλής τους φήμης και της πίστεως, στοιχεία που προστατεύονται και με την τήρηση του τραπεζικού απορρήτου. Το δικαίωμα της προσωπικότητας κατοχυρώνεται από το Σύνταγμα, μέσω της διάταξης του άρθρου 5 παρ. 1 και περιορισμοί του επιτρέπονται και στην έκφανση της διαφυλάξεως των τραπεζικών απορρήτων, πάντοτε με βάση την αρχή της αναλογικότητας. Ωστόσο, η τήρηση του επαγγελματικού απορρήτου θεραπεύει και το γενικό συμφέρον, καθώς εμπεδώνει την εμπιστοσύνη του κοινού σε δραστηριότητες που παρουσιάζουν μεγάλη κοινωνική και οικονομική σπουδαιότητα, όπως η τραπεζική λειτουργία. Περαιτέρω, η υποχρέωση τήρησης του απορρήτου θεμελιώνεται ως παρεπόμενη υποχρέωση και στην καλή πίστη (ΑΚ 288), στο πλαίσιο των συμβατικών σχέσεων των τραπεζικών ιδρυμάτων με τους πελάτες τους, ενώ παράλληλα μπορεί να προβλεφθεί και ως όρος στις συμβάσεις αυτές, όταν τα μέρη επιθυμούν να εξασφαλίσουν την έκταση της δεσμεύσεως της τράπεζας και να ενισχύσουν με ποινική ρήτρα τη δέσμευση αυτή. Από το τραπεζικό απόρρητο δεσμεύονται οι νόμιμα λειτουργούσες τράπεζες στον ελληνικό χώρο, τα νομικά πρόσωπα που παρέχουν τραπεζικές υπηρεσίες χωρίς να είναι τράπεζες, όπως το Ταμείο Παρακαταθηκών και Δανείων, αλλά και τα χρηματοδοτικά ιδρύματα.[530]

Η υποχρέωση τηρήσεως του γενικού τραπεζικού απορρήτου νοείται ευρύτατη, καθώς κριτήριο προστασίας του δεν αποτελεί μόνο η βούληση, πραγματική ή εικαζόμενη, του πελάτη, αλλά και

[530] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 80.

το αντικειμενικώς νοούμενο συμφέρον αυτού, ο οποίος μπορεί να μην έχει εκ των προτέρων διαμορφωμένη βούληση επί του προκειμένου. Στο απόρρητο περιλαμβάνονται όλα τα περιστατικά και οι πληροφορίες των οποίων έλαβε γνώση και έχει στη διάθεσή της η τράπεζα, ανεξάρτητα από την πηγή προελεύσεώς τους, αλλά και αξιολογικές κρίσεις που βασίζονται στα περιστατικά αυτά. Οι πληροφορίες αυτές μπορεί να περιήλθαν στην κατοχή της τράπεζας, εξαιτίας της συναλλακτικής της σχέσης με τον πελάτη, τόσο κατά το προσυμβατικό στάδιο όσο και κατά τη διάρκεια της σύμβασης και μετά την ολοκλήρωσή της. Περαιτέρω, οι πληροφορίες αυτές μπορεί να μην περιορίζονται μόνο στις στενά συνδεδεμένες με την ή τις τραπεζικές συναλλαγές, αλλά να περιλαμβάνουν και κάθε ιδιωτικής φύσεως πληροφορίες που περιήλθαν στην τράπεζα επ'ευκαιρία κάποιας συναλλαγής. Αυτό ισχύει και για μη επιχειρηματίες συναλλασσομένους με την τράπεζα, καθώς δίνεται μέσω των σχετικών κινήσεων των λογαριασμών η δυνατότητα σχηματισμού εικόνας για την οικονομική και προσωπική κατάσταση των προσώπων. Από το τραπεζικό απόρρητο δεν καλύπτονται πληροφορίες που κατά την κοινή πείρα κρίνονται ασήμαντες ή κατά την αντίληψη των συναλλαγών ανακοινώσιμες.[531] Οι πληροφορίες που δεν αφορούν σε συγκεκριμένο συναλλασσόμενο με την τράπεζα, αλλά γενικότερα σε κλάδους της οικονομίας ή σε οικονομικές τάσεις, έστω και αν αυτές έχουν συγκεντρωθεί επαγωγικά από τα οικονομικά και άλλα στοιχεία της πελατείας της τράπεζας, δεν συνιστούν παραβίαση του απορρήτου.

Περιορισμοί που αφορούν την τήρηση του απορρήτου θα πρέπει να ισχύουν και για την μεταξύ των ιδίων των τραπεζών, απ' ευθείας ή μέσω διατραπεζικών οργανώσεων ανταλλαγή πληροφοριών. Δεν πρέπει επομένως να αναγνωρίζεται γενικό και απεριόριστο δικαίωμα αλληλοπληροφορήσεως ως προς το γενικώς αξιόχρεο των συναλλασσομένων με τις τράπεζες.[532]Αντίστοιχοι περιορισμοί θα πρέπει να ισχύουν και ως προς τρίτα πρόσωπα, δηλαδή υπαλλήλους άλλων τμημάτων της τράπεζας, συνδεδεμένων επιχειρήσεων και κυρίως ασφαλιστικών εταιρειών, που δύνανται να λάβουν γνώση των απόρρητων στοιχείων μόνο όταν αυτό επιτρέπεται από ειδική διάταξη νόμου ή όταν υπάρχει η προς τούτο συναίνεση του πελάτη ή συντρέχει άλλος νόμιμος δικαιολογητικός λόγος (σύμφωνα με την παρ. 4 του άρθρου 371 ΠΚ).[533]

Το γενικό τραπεζικό απόρρητο δεν επιβάλλεται από συγκεκριμένη νομοθετική διάταξη, αλλά θεμελιώνεται στις συνταγματικές διατάξεις των άρθρων 2 παρ. 1, 5 παρ. 1, 9 παρ. 1, 19 και 25, αλλά και σε νομοθετικές διατάξεις που αφορούν το επαγγελματικό και το υπηρεσιακό απόρρητο του πιστωτικού ιδρύματος (άρθρα 252 και 371 ΠΚ, 402 αρ. 2 ΚΠολΔ). Παράλληλα μπορεί να θεμελιωθεί στην ιδιαίτερη σχέση ανάμεσα σε τράπεζα και πελάτη και ιδίως στην υποχρέωση εχεμύθειας που υπέχει το πιστωτικό ίδρυμα (ΑΚ197, 198, 200, 281, 288).[534] Το ειδικό τραπεζικό απόρρητο, στο οποίο εμπίπτουν οι πάσης φύσεως χρηματικές καταθέσεις προστατεύεται με βάση τις διατάξεις του Ν.Δ. 1059/1971, όπως ισχύει σήμερα. Σε περίπτωση παραβίασης του, οι υπάλληλοι του τραπεζικού ιδρύματος αλλά και των δημοσίων υπηρεσιών που αποκτούν

---

[531] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 99.
[532] Γεώργιος Αθ. Γραμματίκας, *Το Τραπεζικό Απόρρητο*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Σάκκουλα, 1991), 69.
[533] Ibid.,60.
[534] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 101.

πρόσβαση σε στοιχεία που καλύπτονται από το ειδικό τραπεζικό απόρρητο, υπέχουν ποινικές ευθύνες σύμφωνα με το άρθρο 2 του Ν.Δ. 1059/1971 και το άρθρο 371 Π.Κ.[535]

5.1.1 Η υποχρέωση τήρησης του γενικού τραπεζικού απορρήτου

Η υποχρέωση τήρησης του γενικού τραπεζικού απορρήτου γεννάται από τη στιγμή της ενάρξεως της συναλλακτικής σχέσης ανάμεσα σε τράπεζα και πελάτη, πριν την εκκίνηση συγκεκριμένων διαπραγματεύσεων για τη σύναψη της εκάστοτε έννομης σχέσης, ενώ διαρκεί και μετά την καθ' οιονδήποτε λήξη της εννόμου σχέσεως την οποία αφορά.[536]Τα καταστατικά όργανα, οι υπάλληλοι και οι εντολοδόχοι του τραπεζικού ιδρύματος έχουν υποχρέωση έναντι αυτού και των πελατών του να τηρούν το απόρρητο και μετά την καθ' οιονδήποτε λήξη της σχέσεώς τους με το τραπεζικό ίδρυμα.[537] Η υποχρέωση τήρησης του γενικού τραπεζικού απορρήτου καλύπτει και το χρονικό διάστημα που προηγείται της καταρτίσεως της σύμβασης καταθέσεως, η οποία από τη στιγμή της συνάψεώς της καλύπτεται από την υποχρέωση τήρησης του ειδικού τραπεζικού απορρήτου.

Περαιτέρω, το δικαίωμα επί το απόρρητο είναι προσωπικό, προσωποπαγές[538] αλλά και απόλυτο, εφόσον αποτελεί εκδήλωση του δικαιώματος της προσωπικότητας του ατόμου. Αναφορικά με τη φύση του ως προσωπικό και απόλυτο, τα χαρακτηριστικά του αυτά δικαιολογούνται λόγω του γεγονότος ότι αποτελεί ενοχικό δικαίωμα.[539] Ως προς τον προσωποπαγή χαρακτήρα του όμως, θα πρέπει να γίνουν κάποιες διευκρινίσεις που αφορούν το δικαίωμα παραιτήσεως από αυτό αλλά και την μεταβίβασή του. Ειδικότερα, το δικαίωμα της προσωπικότητας είναι αμεταβίβαστο, ακληρονόμητο αλλά και ανεπίδεκτο παραιτήσεως, όχι μόνο στο σύνολό του αλλά και στις σημαντικότερες εκφάνσεις του. Αναφορικά με το γενικό τραπεζικό απόρρητο, γίνεται δεκτό ότι ο δικαιούχος του δύναται να παραιτηθεί από αυτό.[540] Η παραίτηση αυτή μπορεί να αφορά μόνο σε συγκεκριμένη σχέση ή κύκλο προσώπων. Ωστόσο, γενική εκ των προτέρων παραίτηση από αυτό και από τις αξιώσεις που απορρέουν από την παράβαση του δικαιώματος, θα ήταν άκυρη ως αντιβαίνουσα στα χρηστά ήθη και θα χαρακτηριζόταν ειδικότερα ως καταπλεονεκτική.[541]Υπό ορισμένους όρους, γίνεται δεκτή και η εν ζωή μεταβίβαση, στην περίπτωση που ο δικαιούχος μεταβιβάσει σε τρίτο, με τη συναίνεση της τράπεζας, όπου αυτό απαιτείται, την έννομη σχέση που τον συνέδεε με αυτήν και η οποία παρήγαγε το δικαίωμα επί του απορρήτου.[542]

Το τραπεζικό ίδρυμα έχει υποχρέωση τήρησης του απορρήτου επί του συνόλου της σχέσεως και ως προς το μέρος που ανάγεται στον χρόνο προ της μεταβιβάσεως. Ο αρχικός δικαιούχος δεν δικαιούται να απαλλάξει την τράπεζα εκ των υστέρων από την τήρηση του απορρήτου καθ' ο μέρος τον αφορούσε. Σε άλλη περίπτωση θα μπορούσε να βλάψει ή να διακινδυνέψει τα συμφέροντα του νέου δικαιούχου. Ταυτόχρονα, ο αρχικός δικαιούχος έχει αξίωση κατά της τράπεζας για τήρηση της εχεμύθειας, αφού η γενικότερη υποχρέωση τήρησης του απορρήτου, ως

---

[535] Ibid.
[536] Ibid.,72.
[537] Ibid., 59.
[538] Βλ. απόφαση ΕφΑθ 2257/1985 ΕΕΝ 52, 411.
[539] Γεώργιος Αθ. Γραμματίκας, *Το Τραπεζικό Απόρρητο*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Σάκκουλα, 1991), 53.
[540] Ibid.,109.
[541] Ibid., 110.
[542] Μιχαήλ Θ. Ντόστας, *Γενικό Τραπεζικό Απόρρητο Και Απόρρητο Των Καταθέσεων. Κατάσχεση Των Καταθέσεων*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Αντ. Ν. Σάκκουλα Ε.Ε, 2000), 45.

εκδήλωση της υποχρεώσεως προστασίας (ΑΚ 288), εκτείνεται και σε χρόνο μεταγενέστερο της λήξης της έννομης σχέσεως.[543]

Στην περίπτωση θανάτου, ο σύζυγος, οι κατιόντες, οι ανιόντες και οι αδελφοί του θανόντος, ανεξάρτητα από την ιδιότητά τους ως κληρονόμων, αλλά και οι κληρονόμοι από διαθήκη, θεωρούνται από τον νόμο (ΑΚ 57 παρ. 1 εδ.2) ως θεματοφύλακες της προσωπικότητας του θανόντος, η οποία εξακολουθεί να θεωρείται προστατευτέα από την έννομη τάξη. Κατά το μέρος λοιπόν που το δικαίωμα του τραπεζικού απορρήτου αποτελεί έκφανση του δικαιώματος της προσωπικότητας, τα προαναφερθέντα πρόσωπα έχουν τις αξιώσεις που πηγάζουν από τη διάταξη του άρθρου 57 παρ. 1 εδάφιο 1 ΑΚ. Το δικαίωμα της προσωπικότητας παραμένει σεβαστό ακόμα και μετά το θάνατο του δικαιούχου, με αποτέλεσμα η τράπεζα να υποχρεούται να τηρεί τα μυστικά του θανόντος, τα οποία σε περίπτωση διαρροής τους, μπορούν να διασύρουν αυτόν και μεταθανατίως.

Και με βάση το κληρονομικό δίκαιο όμως, η τράπεζα συνεχίζει να υποχρεούται να τηρεί το απόρρητο. Η έννομη σχέση πίστεως και προστασίας μεταξύ τράπεζας και πελάτη έχει πέρα από προσωπικό και περιουσιακό χαρακτήρα, ειδικά όταν απορρέει από μια κύρια σχέση, η οποία εξακολουθεί να υφίσταται κατά τον χρόνο του θανάτου του αντισυμβαλλομένου της τράπεζας. Η κύρια αυτή σχέση (π.χ. σύμβαση καταθέσεως), μεταβιβάζεται σύμφωνα με τους κανόνες της κληρονομικής διαδοχής στους κληρονόμους του θανόντος καταθέτη. Στην μεταβίβαση αυτή περιλαμβάνονται όχι μόνο τα βασικά δικαιώματα του θανόντος, όπως το δικαίωμα για ανάληψη της καταθέσεως, αλλά και όσα αντιστοιχούν σε παρεπόμενες υποχρεώσεις του πιστωτικού ιδρύματος, όπως η τήρηση της πίστεως και προστασίας, άρα και η προστασία του απορρήτου. Ακόμα όμως και σε περίπτωση λήξεως της σχέσης ανάμεσα σε τράπεζα και πελάτη πριν το θάνατο του τελευταίου, δεν καταλύεται η σχέση πίστεως και προνοίας, η οποία ως ενέχουσα και περιουσιακό χαρακτήρα μεταβαίνει στους κληρονόμους.[544]

5.2 Το ειδικό τραπεζικό απόρρητο

Όπως προαναφέρθηκε, το γενικό τραπεζικό απόρρητο καλύπτει το σύνολο των συναλλαγών των τραπεζών με την πελατεία τους. Πρόκειται για μια μορφή του γενικού επαγγελματικού απορρήτου, το οποίο πρέπει να τηρούν τα πρόσωπα που τελούν σε ιδιαίτερη σχέση εμπιστοσύνης προς τρίτους. Αναφορικά με τις τραπεζικές καταθέσεις, ειδικές διατάξεις επιβάλλουν στα τραπεζικά ιδρύματα ένα απόρρητο πιο αυστηρό από το γενικό. Μέσω αυτού επιδιώκεται η περαιτέρω κατοχύρωση της σχέσης εμπιστοσύνης ανάμεσα σε τράπεζες και πελάτες, ώστε να προστατεύονται πιο αποτελεσματικά τα συμφέροντα των τελευταίων. Αυτό συμβαίνει διότι οι τραπεζικές καταθέσεις αποτελούν το κατ' εξοχήν σημείο επαφής ανάμεσα στις τράπεζες και το κοινό, αλλά και την βασική πηγή πορισμού χρήματος για τις τράπεζες και διοχετεύσεώς του στην κρατική οικονομία. Για το λόγο αυτό, οι κυρώσεις που επιβάλλονται σε περίπτωση παραβίασης του ειδικού τραπεζικού απορρήτου είναι αυστηρότερες σε σχέση με τις αντίστοιχες που επιβάλλονται για την παραβίαση του γενικού. Το ειδικό απόρρητο των τραπεζικών καταθέσεων

---

[543] Μιχαήλ Θ. Ντόστας, *Γενικό Τραπεζικό Απόρρητο Και Απόρρητο Των Καταθέσεων. Κατάσχεση Των Καταθέσεων*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Αντ. Ν. Σάκκουλα Ε.Ε, 2000), 46-47.

[544] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 86.

θεσπίστηκε[545] από το ομότιτλο ν.δ. 1059/1951, το οποίο έκτοτε έχει τροποποιηθεί επανειλημμένα.[546]Με τις επιμέρους τροποποιήσεις αίρεται το απόρρητο των καταθέσεων έναντι των δικαστικών, φορολογικών και εποπτικών αρχών. Με τις διατάξεις του ν.δ. 1059/1971, όπως ισχύει, ορίζονται τα πρόσωπα που υποχρεώνονται να τηρούν το απόρρητο, οι τραπεζικές καταθέσεις που προστατεύονται από το απόρρητο, οι κυρώσεις για την παραβίασή του και οι εξαιρετικές περιπτώσεις που οδηγούν σε άρση αυτού.

Σύμφωνα με το άρθρο 1 του ν.δ. 1059/1971, το ειδικό τραπεζικό απόρρητο καλύπτει κάθε μορφή καταθέσεων σε πιστωτικά ιδρύματα. Επομένως, καταλαμβάνονται όλα τα είδη των χρηματικών καταθέσεων σε ευρώ και σε συνάλλαγμα, ταμιευτηρίου, όψεως, προθεσμίας, σε κοινό λογαριασμό κ.λπ.[547] Ως προς το αν καλύπτονται από το ειδικό τραπεζικό απόρρητο και καταθέσεις άλλων αξιών, ιδίως χρεογράφων κάθε είδους, προς φύλαξη ή λόγω ενεχύρου, έχουν διατυπωθεί δύο διαφορετικές απόψεις. Την αρχική αποφατική άποψη είχε δεχθεί το 1975 η Ολομέλεια του Αρείου Πάγου, με βάση την αρχική διατύπωση του άρθρου 1 του ν.δ. 1059/1071 και την συστηματική και τελολογική του ερμηνεία.[548]Η σημερινή διατύπωση της εν λόγω διάταξης κάνει λόγο για «κάθε μορφής» καταθέσεις, ενώ το άρθρο 3 του ν.δ. 1059/1971, όπως αντικαταστάθηκε από το άρθρο 27 παρ. 1 του ν. 1868/1989, αναφέρεται σε «απόρρητες χρηματικές ή άλλες καταθέσεις». Εν όψει τούτων, κρατεί σήμερα ή άποψη σύμφωνα με την οποία το ειδικό τραπεζικό απόρρητο καταλαμβάνει και τις μη χρηματικές καταθέσεις (μετοχών, ομολογιών, χρεογράφων).[549] Κατά μια παραλλάσσουσα άποψη, δεν εμπίπτουν στις προστατευτικές διατάξεις του ν.δ. οι συμβάσεις με τις οποίες η τράπεζα αναλαμβάνει τη φύλαξη συγκεκριμένων κινητών αξιών, υπό τη μορφή της ομαλής παρακαταθήκης, αλλά μόνο η κατάθεση κινητών αξιών με τη μορφή της ανώμαλης παρακαταθήκης, που παρέχει στην τράπεζα δικαίωμα χρήσεως.[550] Με τη διάταξη του άρθρου 12 παρ. 2 του νόμου 2198/1994, έχει επεκταθεί η προστασία του τραπεζικού απορρήτου στους λογαριασμούς τίτλων με λογιστική μορφή του Ελληνικού Δημοσίου.

---

[545] Το απόρρητο των τραπεζικών καταθέσεων θεσπίστηκε αρχικά έναντι της φορολογικής αρχής με το άρθρο 17 παρ. 2 του α.ν. 942/1949, που αφορούσε τις καταθέσεις ταμιευτηρίου και τις προθεσμιακές, και με το άρθρο 50 παρ. 1 περ. α' του ν.δ. 3323/1953, που κάλυπτε όλα τα είδη των καταθέσεων.

[546] Από τις τροποποιήσεις που προηγήθηκαν θα πρέπει να γίνει αναφορά στο άρθρο 40 του νόμου 1806/1988, στην υπ'αριθ. 376/29.11.1988 κοινή απόφαση των Υπουργών Εθνικής Οικονομίας και Εμπορίου που κυρώθηκε με το άρθρο 38 του νόμου 1828/1989 και τα άρθρα 10 του νόμου 1858/1989 και 27 του νόμου 1868/1989. Occasio legum αποτέλεσε η «υπόθεση Κοσκωτά» στην Τράπεζα Κρήτης. Η ανεπάρκεια της πρώτης νομοθετικής ρύθμισης οδήγησε στις επόμενες. Πριν επέλθουν οι τροποποιήσεις αυτές, ο νομοθέτης θεωρούσε ότι το απόρρητο του άρθρου 1 του ν.δ. 1059/1971 ίσχυες και έναντι της Τράπεζας της Ελλάδος. Η συγκεκριμένη υπόθεση όμως θα μπορούσε να έχει εξαρχής αντιμετωπιστεί με την έκδοση πράξεως νομοθετικού περιεχομένου.

[547] Μιχαήλ Θ. Ντόστας, *Γενικό Τραπεζικό Απόρρητο Και Απόρρητο Των Καταθέσεων. Κατάσχεση Των Καταθέσεων*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Αντ. Ν. Σάκκουλα Ε.Ε, 2000), 69-70.

[548] Βλ. ΑΠ 1225/1975 NoB 24, 189, σύμφωνα με την οποία «*εκ του συνδυασμού των ανωτέρω διατάξεων (άρθρων 1-3 ν.δ. 1059/1971 και του άρθρου 2 του ν.δ. 1325/1971) και του σκοπού του νομοθέτου επιδιώξαντος την επαύξησιν των τραπεζικών καταθέσεων προς εξυπηρέτησιν δια τούτων της χρηματοδοτήσεως της εθνικής οικονομίας σαφώς προκύπτει ότι ως τραπεζικαί καταθέσεις, δι' ας ισχύει το κατά το άνω καθιερούμενον απόρρητον νοούνται αι εις χρήμα τοιαύται και ουχί αι καταθέσεις μετοχών, ομολογιών ή άλλων χρεογράφων*».

[549] Βλ. ΕφΠατρ 14/2011 ΑχΝομ 2012, 18, ΕφΘες 1013/2011 ΤΝΠ Νόμος, ΕφΑθ. 1597/2007 ΔΕΕ 2008, 603, ΕφΘες 702/2005 Αρμ 2006, 1226.

[550] Σπυρίδων Δ. Ψυχομάνης, *Τραπεζικό Δίκαιο, δίκαιο τραπεζικών συμβάσεων Ι:Γενικό Μέρος*, 6η εκδ. (repr., Αθήνα, Θεσσαλονίκη: Εκδόσεις Σάκκουλα, 2008), 58.

5.2.1 Τα υπόχρεα προς τήρηση του ειδικού τραπεζικού απορρήτου πρόσωπα

Σύμφωνα με το άρθρο 1 παρ. 1 του ν.δ. 1059/1971, «Οι κάθε μορφής καταθέσεις σε πιστωτικά ιδρύματα είναι απόρρητες». Εννοούνται στην περίπτωση αυτή τα πιστωτικά ιδρύματα που λειτουργούν νόμιμα στην Ελλάδα, όπως αυτά προσδιορίζονται στο άρθρο 3 του νόμου 4261/2014, συμπεριλαμβανομένων και των υποκαταστημάτων αλλοδαπών πιστωτικών ιδρυμάτων. Το απόρρητο καταλαμβάνει επίσης και τις καταθέσεις σε αλλοδαπά πιστωτικά ιδρύματα που λειτουργούν νόμιμα στην Ελλάδα, δεδομένου ότι με βάση τη διάταξη του άρθρου 1 του ν.δ. 1059/1971, όπως ισχύει σήμερα, γίνεται λόγος γενικώς για πιστωτικά ιδρύματα, ενώ στην αρχική του διατύπωση, αναφερόταν μόνο σε ελληνικές τράπεζες.[551] Υπόχρεο προς τήρηση του ειδικού τραπεζικού απορρήτου είναι μεν το νομικό πρόσωπο του πιστωτικού ιδρύματος στο οποίο τηρείται η κατάθεση, η ποινική όμως ευθύνη την οποία καθιερώνει το άρθρο 2 παρ. 1 του ν.δ 1059/1971, αφορά μόνο σε φυσικά πρόσωπα. Ποινικώς υπεύθυνοι είναι επομένως οι διοικητές, μέλη διοικητικών συμβουλίων ή άλλων συλλογικών οργάνων καθώς και υπάλληλοι, οι οποίοι εκ της ασκήσεως των καθηκόντων τους λαμβάνουν γνώση των τραπεζικών καταθέσεων. Τα προαναφερθέντα πρόσωπα, εφόσον παράσχουν οποιαδήποτε πληροφορία με οποιονδήποτε τρόπο, τιμωρούνται με φυλάκιση τουλάχιστον έξι μηνών. Πέραν των ποινικών ευθυνών των προσώπων αυτών, το πιστωτικό ίδρυμα θα υποχρεωθεί να αποκαταστήσει στον δικαιούχο της καταθέσεως την υλική ή ηθική ζημιά που προκλήθηκε εξ αιτίας της παραβιάσεως του απορρήτου. Η ευθύνη αυτή θεμελιώνεται στα άρθρα 71, 334 και 922 ΑΚ. Σύμφωνα με την παράγραφο 1 του άρθρου 63 του νόμου 4170/2013, οι διατάξεις του άρθρου 2 του ν.δ. 1059/1971 και του άρθρου 371 ΠΚ ισχύουν και για τους υπαλλήλους, το προσωπικό που υπηρετεί με οποιαδήποτε σχέση εργασίας, καθώς και τους λειτουργούς των αρχών, υπηρεσιών και φορέων του Δημοσίου.[552]

5.2.2 Τα προστατευόμενα από το ειδικό τραπεζικό απόρρητο πρόσωπα

Το ειδικό τραπεζικό απόρρητο ισχύει υπέρ των καταθετών. Ως καταθέτες νοούνται όχι μόνο τα πρόσωπα τα οποία έχουν ανοίξει το λογαριασμό και έχουν προβεί στην αρχική και στις τυχόν επόμενες καταθέσεις, αλλά και κάθε πρόσωπο το οποίο αντλεί δικαιώματα από την εκάστοτε σύμβαση καταθέσεως που έχει συναφθεί από άλλον.[553]Στην κατάθεση σε κοινό λογαριασμό, επομένως, προστατεύονται και οι συνδικαιούχοι ανεξάρτητα από το αν έχουν προβεί σε κατάθεση ή όχι χρηματικών ποσών. Το ίδιο θα πρέπει να γίνεται δεκτό και σε περίπτωση κατάθεσης υπέρ τρίτου, τόσο σε περίπτωση που η κατάθεση γίνεται σε προϋπάρχοντα λογαριασμό τρίτου, αλλά και όταν η κατάθεση γίνεται σε λογαριασμό που ανοίγεται υπέρ τρίτου επ' ευκαιρία της καταθέσεως. Σε περίπτωση που γίνεται διάθεση της καταθέσεως με οποιονδήποτε τρόπο, λ.χ. με εκχώρηση ή ενεχύραση, το απόρρητο καλύπτει και τον δικαιοπάροχο αλλά και τον δικαιοδόχο.

Οι διατάξεις του ν.δ. 1059/1971 έχουν τεθεί για να προστατεύονται οι καταθέτες. Επομένως, το απόρρητο δεν ισχύει έναντι των κληρονόμων του καταθέτη, διότι αυτοί υπεισέρχονται στη θέση του και καθίστανται δικαιούχοι των περιουσιακών του δικαιωμάτων, άρα και των τραπεζικών του

---

[551] Μιχαήλ Θ. Ντόστας, *Γενικό Τραπεζικό Απόρρητο Και Απόρρητο Των Καταθέσεων. Κατάσχεση Των Καταθέσεων*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Αντ. Ν. Σάκκουλα Ε.Ε, 2000), 71-72.

[552] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 434-435.

[553] Σωτήριος Καλαμίτσης, *Το Απόρρητο Των Τραπεζικών Καταθέσεων*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Π. Χιωτέλλη, 1993), 24.

καταθέσεων. Το ίδιο θα πρέπει να γίνεται δεκτό και για τους ειδικούς διαδόχους του καταθέτη, δηλαδή τους κληρονόμους του και τους εκδοχείς. Επιπροσθέτως, το τραπεζικό απόρρητο των καταθέσεων δεν ισχύει έναντι των νόμιμων ή εκούσιων αντιπροσώπων του, οι οποίοι εκφράζουν τη βούλησή του κατά την άσκηση των δικαιωμάτων του και ενεργούν στο όνομά του.[554][555]

Όσον αφορά στη διάρκεια της υποχρεώσεως του πιστωτικού ιδρύματος να τηρεί το απόρρητο των καταθέσεων, ισχύουν όσα εκτέθηκαν ανωτέρω για το γενικό τραπεζικό απόρρητο. Επειδή όμως το άρθρο 1 παρ. 1 εδάφιο 1 του ν.δ. 1059/1971 ορίζει ότι οι καταθέσεις έχουν απόρρητο χαρακτήρα, κρίνεται ορθό να δεχθούμε ότι το ειδικό τραπεζικό απόρρητο καλύπτει μόνο τις υφιστάμενες καταθέσεις και όχι το μη ευοδωθέν προσυμβατικό, διαπραγματευτικό στάδιο. Το στάδιο αυτό όμως καταλαμβάνεται εφόσον καταρτισθεί η σύμβαση καταθέσεως.[556]Μετά τον θάνατο του καταθέτη, δικαιούχοι της καταθέσεως και των δικαιωμάτων που απορρέουν από αυτήν καθίστανται οι κληρονόμοι αυτού. Ήδη από τον χρόνο της επαγωγής, το δικαίωμα ανήκει στους κληρονόμους εξ ιδίου δικαίου, ως δικαιούχους της καταθέσεως. Αναφορικά με την κατάθεση κατά τον χρόνο προ της επαγωγής της κληρονομίας, οπότε δικαιούχος του απορρήτου ήταν ο κληρονομούμενος, θα πρέπει να σημειωθεί ότι το σχετικό δικαίωμα μεταβιβάζεται στους κληρονόμους του. Αυτό γίνεται δεκτό διότι το δικαίωμα προς τήρηση του απορρήτου δεν μπορεί να ενταχθεί στην κατηγορία των άκρως προσωποπαγών και μη κληρονομητών δικαιωμάτων, ανεξαρτήτως του αν προέχει ή όχι ο περιουσιακός του χαρακτήρας.[557]

5.3 Η φύση του τραπεζικού απορρήτου ως προσωπικό δεδομένο

Το τραπεζικό απόρρητο (γενικό και ειδικό) καλύπτεται σήμερα από το νομοθετικό πλαίσιο της προστασίας των δεδομένων του υποκειμένου (Κανονισμός ΕΕ 2016/679, νόμος 4624/2019). Το τραπεζικό απόρρητο από κοινού με την προστασία των προσωπικών δεδομένων δημιουργούν ένα πλέγμα σωρευτικής προστασίας για το υποκείμενο των δεδομένων. Το αντικείμενο προστασίας τους διατέμνεται καθώς και οι δύο θεσμοί εφαρμόζονται σε φυσικά πρόσωπα, ενώ μόνο το τραπεζικό απόρρητο εφαρμόζεται και σε νομικά πρόσωπα. Οι νομικές βάσεις από τις οποίες πηγάζουν είναι επίσης κοινές, καθώς ανάγονται στις συνταγματικές αρχές προστασίας της προσωπικότητας και της ιδιωτικής σφαίρας.[558] Το τραπεζικό απόρρητο συγκεντρώνει επίσης όλα τα στοιχεία που προβλέπονται στο άρθρο 4 παρ. 1 του Κανονισμού και τα οποία πρέπει να συντρέχουν ώστε μια πληροφορία να αποτελέσει «δεδομένο προσωπικού χαρακτήρα». Συνεπώς, και το τραπεζικό απόρρητο αποτελεί πληροφορία που αναφέρεται σε φυσικό πρόσωπο, του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί.[559]

---

[554] Μιχαήλ Θ. Ντόστας, *Γενικό Τραπεζικό Απόρρητο Και Απόρρητο Των Καταθέσεων. Κατάσχεση Των Καταθέσεων*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Αντ. Ν. Σάκκουλα Ε.Ε, 2000), 75-76.

[555] Βλ. και απόφαση ΕφΑθ 1664/2001 ΕλλΔνη 2002, 1704, σύμφωνα με την οποία: «*Το απόρρητο δεν αντιτάσσεται έναντι προσώπων δικαιούμενων κατά το νόμο να λάβουν γνώση των τραπεζικών λογαριασμών του πελάτη, όπως λ.χ. των συνδίκων της πτώχευσης, των πληρεξουσίων, εκτελεστών διαθήκης κ.λπ. και κατά τα ενδιαφέροντα εν προκειμένω, έναντι των ασκούντων τη γονική μέριμνα σε σχέση με καταθέσεις του ανηλίκου*».

[556] Σωτήριος Καλαμίτσης, *Το Απόρρητο Των Τραπεζικών Καταθέσεων*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Π. Χιωτέλλη, 1993), 24.

[557] Μιχαήλ Θ. Ντόστας, *Γενικό Τραπεζικό Απόρρητο Και Απόρρητο Των Καταθέσεων. Κατάσχεση Των Καταθέσεων*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Αντ. Ν. Σάκκουλα Ε.Ε, 2000), 73-74.

[558] Λάμπρος Κοτσίρης, "Τραπεζικό Απόρρητο και Κατάσχεση Τραπεζικών Καταθέσεων", Dsanet.Gr, http://www.dsanet.gr/ekpaideush/seminaria/KOTSIRIS.htm.

[559] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 102.

Επιπροσθέτως, το τραπεζικό απόρρητο δεν αναφέρεται ρητώς στο άρθρο 9 του Κανονισμού ως δεδομένο που ανήκει σε κάποια ειδική κατηγορία και επομένως αποτελεί απλό προσωπικό δεδομένο του πελάτη και δεν εφαρμόζονται στην περίπτωσή του οι αυξημένες εγγυήσεις προστασίας του Κανονισμού και του νόμου 4624/2019 ως προς τα δεδομένα ειδικών κατηγοριών.

Παρά το γεγονός ότι έχουν κοινές νομικές βάσεις, το τραπεζικό απόρρητο παρέχει αφενός ευρύτερη προστασία σε σχέση με την προστασία που παρέχεται από τον Κανονισμό και τον νόμο 4624/2019, αφετέρου δε στενότερη. Το τραπεζικό απόρρητο παρέχει ευρύτερη προστασία καθώς λειτουργεί όχι μόνο υπέρ των φυσικών προσώπων αλλά και υπέρ των νομικών προσώπων, ενώ παρέχει στενότερη προστασία καθώς εφαρμόζεται αποκλειστικά στο πλαίσιο λειτουργίας των τραπεζικών ιδρυμάτων και δεν αφορά περιπτώσεις επιχειρήσεων ή οργανισμών που συλλέγουν και επεξεργάζονται δεδομένα και πληροφορίες που παρουσιάζουν ομοιότητες με τα αντίστοιχα που συλλέγονται και υφίστανται επεξεργασία από τα τραπεζικά ιδρύματα κατά την διενέργεια των δραστηριοτήτων τους. Επιπροσθέτως, οι διατάξεις περί προστασίας του τραπεζικού απορρήτου δεσμεύουν τα πιστωτικά ιδρύματα σχετικά με την προστασία των πληροφοριών των πελατών τους που βρίσκονται στη διάθεσή τους και όχι στη διάθεση τρίτων προσώπων, ενώ, αντιθέτως, βάσει της νομοθεσίας περί προστασίας των δεδομένων προσωπικού χαρακτήρα, τα πιστωτικά ιδρύματα, ακόμη και για τα δεδομένα τρίτων, που δεν είναι πελάτες τους, που βρίσκονται στη διάθεσή τους, βαρύνονται από την υποχρέωση εχεμύθειας. Αυτό συμβαίνει διότι τα πιστωτικά ιδρύματα αποτελούν υπευθύνους επεξεργασίας και συνεπώς η επεξεργασία προσωπικών δεδομένων τρίτων από αυτά θα πρέπει να διενεργείται για νόμιμους σκοπούς και να στηρίζεται σε κάποια νόμιμη βάση του άρθρου 6 του Κανονισμού.[560]

5.3.1 Η υποχώρηση της προστασίας των προσωπικών δεδομένων σε ποινικές διαδικασίες που σχετίζονται με φορολογικά αδικήματα

Όπως προαναφέρθηκε, η νομοθεσία περί προστασίας προσωπικών δεδομένων, καταλαμβάνει τόσο το φορολογικό, όσο και το τραπεζικό απόρρητο υπό την ευρύτερη δυνατή έννοια της υπαγωγής δεδομένων με οικονομικό χαρακτήρα κάθε μορφής τραπεζικών ή άλλου είδους συναλλαγών.[561] Κατά ταύτα, τα πιστωτικά ιδρύματα, αλλά και όλοι οι υπόλοιποι εμπλεκόμενοι φορείς, οικονομικές υπηρεσίες κ.α. θα πρέπει να εφαρμόζουν την σχετική νομοθεσία[562] χωρίς ακραίες συμπεριφορές και ερμηνείες από όλους τους παράγοντες που εμπλέκονται, με βάση την αρχή της αναλογικότητας.

Ειδικότερα, η κάμψη ή μη του γενικού τραπεζικού απορρήτου σε περίπτωση που συντρέχει σπουδαίος λόγος που να δικαιολογεί την άρνηση επίδειξης εγγράφων σύμφωνα με την προαναφερθείσα διάταξη 450 παρ. 2 ΚΠολΔ, έχει κριθεί ότι αφορά στην αίτηση επίδειξης από τρίτο ενδιαφερόμενο, όχι όμως από το ίδιο το υποκείμενο στοιχείου με χαρακτήρα προσωπικών δεδομένων.[563] Αντιθέτως, ορθά θεωρείται ότι το τραπεζικό απόρρητο ευρύτερα δεν μπορεί να εμποδίσει την εκχώρηση κατά το άρθρο 455 ΑΚ προστατευόμενων αντίστοιχα απαιτήσεων ούτε

---

[560] Ibid.
[561] Βλ. ΑΠΔΠΧ 26/2003, 1/2007, 18/2007, 22/2007, 33/2008, 66/2008, 54/2010, 122/2011 και 27/2012, www.dpa.gr. Ακόμη, ΠΠρΘες 6657/2010 ΧρηΔικ 2010, 394 επ., ΜΠρΑθ 1654/2010 ΧρηΔικ 2010, 391 επ.
[562] Βλ. ΕφΑθ 1597/2007 ΔιμΕΕ 2007, 117 επ. Ακόμη, ΑΠ 1923/2006 ΕΕμπΔ 2007, 352 επ., ΕφΑθ. 3727/2007 ΕπισκΕΔ 2007,1208 επ.
[563] Βλ. ΕφΑθ 1664/2001 ΕλλΔνη 2002, 1703 επ., ΕφΑθ 7277/2003 ΕλλΔνη 2004, 1446 επ.

φυσικά την επιβαλλόμενη πληροφόρηση και παράδοση σχετικών αποδεικτικών στοιχείων σύμφωνα με το άρθρο 456 ΑΚ από τον εκχωρητή προς τον εκδοχέα, εφόσον μάλιστα ο τελευταίος ή ο τυχόν εντολέας του τηρούν νόμιμο αρχείο δεδομένων προσωπικού χαρακτήρα, χωρίς να τίθεται θέμα προηγούμενης συγκατάθεσης του οφειλέτη στην επιχειρούμενη εκχώρηση και συναφή αναγγελία του άρθρου ΑΚ 460. Τέλος, είναι δυνατή η παροχή απλών αλλά και ευαίσθητων προσωπικών δεδομένων σε πιστωτικό ίδρυμα, έπειτα από άδεια της Αρχής, ώστε να χρησιμοποιηθούν αυτά σε πολιτική δίκη.[564]

Στο πεδίο των ποινικών διαδικασιών, η κατάσταση είναι μεταβάλλεται. Σε σχέση καταρχάς με τα ευαίσθητα προσωπικά δεδομένα, όπως αυτά προσδιορίζονται στο άρθρο 2, α' του νόμου 2472/1997 (άρθρα 4 παρ. 13-14-15, άρθρο 9 ΓΚΠΔ), η περίπτωση β' του ίδιου άρθρου προβλέπει ότι «Ειδικά για τα σχετικά με ποινικές διώξεις ή καταδίκες δύναται να επιτραπεί η δημοσιοποίηση μόνον από την εισαγγελική αρχή για τα αδικήματα που αναφέρονται στο εδάφιο β' της παρ. 2 του άρθρου 3 με διάταξη του αρμόδιου Εισαγγελέα Πρωτοδικών ή του Εισαγγελέα Εφετών, εάν η υπόθεση εκκρεμεί στο Εφετείο. Η διάταξη πρέπει να είναι ειδικώς και πλήρως αιτιολογημένη, να προσδιορίζει τον τρόπο δημοσιοποίησης και το χρονικό διάστημα που θα διαρκέσει. Η δημοσιοποίηση αυτή αποσκοπεί στην προστασία του κοινωνικού συνόλου, των ανηλίκων, των ευάλωτων ή ανίσχυρων πληθυσμιακών ομάδων και προς ευχερέστερη πραγμάτωση της αξίωσης της Πολιτείας για τον κολασμό των παραπάνω αδικημάτων». Στη συνέχεια το άρθρο 3 παρ. 2 β' του ίδιου νόμου ορίζει ότι «οι διατάξεις του παρόντος νόμου δεν εφαρμόζονται στην επεξεργασία δεδομένων η οποία πραγματοποιείται: α)…β) από τις δικαστικές - εισαγγελικές αρχές και τις υπηρεσίες που ενεργούν υπό την άμεση εποπτεία τους στο πλαίσιο της απονομής της δικαιοσύνης ή για την εξυπηρέτηση των αναγκών της λειτουργίας τους με σκοπό τη βεβαίωση εγκλημάτων, που τιμωρούνται ως κακουργήματα ή πλημμελήματα με δόλο και ιδίως εγκλημάτων κατά της ζωής, κατά της γενετήσιας ελευθερίας, της οικονομικής εκμετάλλευσης της γενετήσιας ζωής, κατά της προσωπικής ελευθερίας, κατά της ιδιοκτησίας, κατά των περιουσιακών δικαιωμάτων, παραβάσεων της νομοθεσίας περί ναρκωτικών, επιβουλής της δημόσιας τάξης, ως και τελουμένων σε βάρος ανηλίκων θυμάτων. Ως προς τα ανωτέρω εφαρμόζονται οι ισχύουσες ουσιαστικές και δικονομικές ποινικές διατάξεις».[565]

Με βάση τα ανωτέρω, έχει επικρατήσει η άποψη ότι η νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα υποχωρεί σε σχέση με τις ειδικότερες ποινικές δικονομικές αρχές, όπως αυτές προβλέπονται στον ΚΠΔ. Στις περιπτώσεις αυτές συμπεριλαμβάνονται και οι ποινικές διαδικασίες που άπτονται των φορολογικών αδικημάτων. Εδώ εντάσσεται και η πρακτική έκδοσης εισαγγελικών παραγγελιών, για γνωστοποίηση σε τρίτους απλών ή ευαίσθητων προσωπικών δεδομένων από υπεύθυνους επεξεργασίας, των οποίων τα υποκείμενα είναι πελάτες ή συναλλασσόμενοι μαζί τους. Οι σχετικές παραγγελίες-εντολές, οι οποίες μπορούν να σχετίζονται

[564] Βλ. απόφαση ΑΠΔΠΧ 122/2011 (διαβίβαση προσωπικών δεδομένων στην Εθνική τράπεζα της Ελλάδας για τη ρύθμιση οφειλών υπερχρεωμένου οφειλέτη) και ΑΠΔΠΧ 50/2011 (νομιμότητα τήρησης στοιχείων αιτήσεων εξωδικαστικού συμβιβασμού από την Τειρεσίας Α.Ε.).

[565] Βάσει του άρθρου 84 του νόμου 4624/2019, διατηρούνται σε ισχύ οι διατάξεις του άρθρου 2, όπου γίνεται ρητή παραπομπή σε αυτούς σε σχετική με τα προσωπικά δεδομένα νομοθεσία, του δεύτερου έως και του τελευταίου εδαφίου της περίπτωσης β΄ του άρθρου 2 για την ανακοίνωση και δημοσιοποίηση δεδομένων προσωπικού χαρακτήρα. Επίσης, διατηρούνται σε ισχύ οι διατάξεις του εδαφίου β΄ της παραγράφου 2 του άρθρου 3, μόνο ως προς τα αδικήματα που περιγράφονται σε αυτό, του τρίτου έως και του τελευταίου εδαφίου της περίπτωσης β΄ της παραγράφου 2 του άρθρου 3 του ανωτέρου νόμου για την εγκατάσταση και λειτουργία συστημάτων επιτήρησης.

έμμεσα και με πληροφόρηση φορολογικού χαρακτήρα, έχει κριθεί από την Αρχή ότι δεν δεσμεύουν τους υπεύθυνους επεξεργασίας, ώστε να χορηγήσουν τα αιτούμενα στοιχεία, εφόσον δεν εκδίδονται βάσει των σχετικών διατάξεων του ΚΠΔ. Επομένως, στην περίπτωση που ο εισαγγελέας που επιλαμβάνεται της υποθέσεως κρίνει ad hoc απαραίτητη την παροχή τέτοιου είδους απόρρητων πληροφοριών, οφείλει να παραπέμψει το ζήτημα στην Αρχή, η οποία ως μόνη αρμόδια δικαιούται να παράσχει τη σχετική άδεια.[566] Πέραν αυτών, δυνατότητα συλλογής προσωπικών στοιχείων οικονομικού χαρακτήρα έχει αναγνωρισθεί ότι διαθέτει και το Σώμα Δίωξης Οικονομικού Εγκλήματος (ΣΔΟΕ) κατά την διενέργεια των φορολογικών ελέγχων από αυτό, χωρίς αντίστοιχη υποχρέωση ενημέρωσης των υποκειμένων των δεδομένων.[567]Στο πλαίσιο αυτό, τα πιστωτικά ιδρύματα ως υπεύθυνα επεξεργασίας αυξημένου όγκου προσωπικών δεδομένων οικονομικού χαρακτήρα, ενημερώνουν τους πελάτες τους μέσω του τύπου σχετικά με τις υποχρεώσεις παροχής στοιχείων, πληροφόρησης κ.λπ. προς τις αρμόδιες δικαστικές, φορολογικές, και λοιπές εποπτικές αρχές.[568]

5.4 Οι περιπτώσεις άρσης του τραπεζικού απορρήτου

Το τραπεζικό απόρρητο δεν δύναται να αρθεί, ωστόσο η προστασία που παρέχει δεν είναι απόλυτη και πολλές φορές καθίσταται αντικείμενο στάθμισης με έννομα αγαθά και συμφέροντα τρίτων μερών.

5.4.1 Οι περιπτώσεις άρσης του γενικού τραπεζικού απορρήτου

Η συγκατάθεση του πελάτη της τράπεζας δύναται να οδηγήσει σε άρση του τραπεζικού απορρήτου, αρκεί να είναι ελεύθερη και απαλλαγμένη ελαττωμάτων, να είναι δε αρκούντος ειδική και ορισμένη, ώστε να μην προσλαμβάνει τον χαρακτήρα (ανεπίτρεπτης) γενικής παραιτήσεως από την προστασία που παρέχει το απόρρητο.[569] Το τραπεζικό απόρρητο δεν ισχύει έναντι προσώπων τα οποία κατά το νόμο ενεργούν αντί του δικαιούχου του αντίστοιχου δικαιώματος, όπως λ.χ. ο εκπρόσωπος του νομικού προσώπου, ο ασκών τη γονική μέριμνα, ο επίτροπος ανηλίκου, ο δικαστικός συμπαραστάτης, ο εντολοδόχος ή πληρεξούσιος, οι καθολικοί και ειδικοί ου διάδοχοι, ο σύνδικος της πτωχεύσεως, ο εκκαθαριστής, ο αναγκαστικός διαχειριστής, ο εκτελεστής διαθήκης, ο κηδεμόνας σχολάζουσας κληρονομίας κ.α. Το ίδιο γίνεται ευλόγως δεκτό και για τους έναντι της τράπεζας συνδικαιούχους ή συνυποχρέους ως προς την κοινή τους υπόθεση.[570]

Δικαίωμα πληροφορήσεως έχει και ο εγγυητής ως προς την πορεία της έναντι της τράπεζας πρωτοφειλής, για να γνωρίζει εκάστοτε το ενδεχόμενο ύψος αυτής, ακόμα και μέλλουσας, ευθύνης του, κατά μείζονα δε λόγο όταν η τράπεζα στραφεί εναντίον του προς ικανοποίηση της απαιτήσεώς της.[571] Επιπροσθέτως, οι κάθε είδους ελεγκτές της ανώνυμης εταιρείας, τους οποίους

---

[566] Βλ. Γνωμοδότηση 3/2009 ΑΠΔΠΧ, σελ. 6.
[567] Βλ. απόφαση 113/2001 ΑΠΔΠΧ.
[568] Βασίλης Α. Δουβλής, "Τραπεζικό Απόρρητο, Προστασία Προσωπικών Δεδομένων Και Νομιμοποίηση Παράνομων Εσόδων Κατά Τη Διεξαγωγή Φορολογικών Ελέγχων", *Δίκαιο Επιχειρήσεων Και Εταιρειών,* 12, (2012): 1101-1102.
[569] Μιχαήλ Θ. Ντόστας, *Γενικό Τραπεζικό Απόρρητο Και Απόρρητο Των Καταθέσεων. Κατάσχεση Των Καταθέσεων*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Αντ. Ν. Σάκκουλα Ε.Ε, 2000), 30-31.
[570] Γεώργιος Α. Γραμματίκας, *Το Τραπεζικό Απόρρητο*, 1η εκδ. (repr., Αθήνα: Π. Σάκκουλας, 1991), 63.
[571] Ibid., 64. Αμφίβολο είναι ωστόσο εάν η τράπεζα υποχρεούται να ενημερώσει τον εγγυητή για τις κατ' αυτής μη προσωποπαγείς ενστάσεις του πρωτοφειλέτη (ΑΚ 853).

ορίζει η γενική συνέλευση των μετόχων, είναι όργανα αυτής και, ανεξαρτήτως της υπάρξεως ειδικών επιτρεπτικών διατάξεων[572], έχουν τη δυνατότητα να λαμβάνουν από τις τράπεζες, με τις οποίες έχει συναλλαγές η ελεγχόμενη ανώνυμη εταιρεία, κάθε πληροφορία που είναι αναγκαία για την εκτέλεση του έργου τους. Όταν διενεργείται έλεγχος που διατάσσεται από δικαστική ή διοικητική αρχή, η κάμψη του τραπεζικού απορρήτου μπορεί να δικαιολογείται είτε με βάση τις ειδικές εκάστοτε διατάξεις, είτε με βάση τα προστατευτέα εκατέρωθεν συμφέροντα, κατ' εφαρμογή του άρθρου 371 παρ. 4 ΠΚ.

Το γενικό τραπεζικό απόρρητο δύναται επίσης να καμφθεί δυνάμει εξαιρέσεων που προβλέπονται σε ειδικές διατάξεις νόμων. Συγκεκριμένα, σύμφωνα με το άρθρο 985 παρ. 1 ΚΠολΔ, η τράπεζα υποχρεούται να προβαίνει στην σχετική θετική ή αρνητική δήλωση, όταν διενεργείται κατάσχεση είτε αναγκαστική είτε συντηρητική (ΚΠολΔ 712 παρ. 1 εδάφιο 2) πράγματος ή απαιτήσεως εις χείρας της ως τρίτης. Μέση οδό ακολουθεί το άρθρο 402 περ. 2 ΚΠολΔ, σύμφωνα με το οποίο επιτρέπεται η άρνηση μαρτυρίας, όταν πρόκειται για περιστατικά που αποτελούν επαγγελματικό απόρρητο, και σαν τέτοιο θα πρέπει να θεωρείται και το τραπεζικό. Σύμφωνα όμως με το άρθρο 403 παρ. 3 ΚΠολΔ, ο μάρτυρας οφείλει να αναφέρει στο δικαστήριο τον λόγο για τον οποίο δεν υποχρεούται να καταθέσει, κατά δεν την παράγραφο 4 του ίδιου άρθρου το δικαστήριο κρίνει και με απλή πιθανολόγηση, εάν ο λόγος αρνήσεως της μαρτυρίας είναι ή όχι βάσιμος. Στην τελευταία περίπτωση ο μάρτυρας έχει υποχρέωση να καταθέσει, υποκείμενος άλλως στις κυρώσεις που προβλέπονται στο άρθρο 404 ΚΠολδ. Εννοείται ότι ο μάρτυρας, όταν συμμορφωθεί προς την απόφαση του δικαστηρίου και προβεί σε κατάθεση, δεν υπέχει την ποινή του άρθρου 371 παρ. 1 ΠΚ, διότι στην περίπτωση αυτή εφαρμόζεται η παράγραφος 4 του άρθρου αυτού. Το ίδιο συμβαίνει και όταν ο υπέρ ού το απόρρητο διάδικος απαλλάξει τον μάρτυρα από την υποχρέωση τηρήσεως του απορρήτου.[573] Σε κάθε περίπτωση, η ύπαρξη του τραπεζικού απορρήτου δεν αποτελεί, κατά το άρθρο 400 ΚΠολΔ, λόγο εξαιρέσεως του μάρτυρα, λόγω της περιοριστικής απαριθμήσεως στην οποία προβαίνει η εν λόγω διάταξη.

Για τις ποινικές υποθέσεις, το άρθρο 212 ΚΠολΔ δεν αναφέρει το γενικό τραπεζικό απόρρητο ως λόγο αρνήσεως της μαρτυρίας. Συνεπώς πρέπει να γίνει δεκτό ότι σε όλες τις φάσεις της ποινικής διαδικασίας οι δεσμευόμενοι από το γενικό τραπεζικό απόρρητο υποχρεούνται να καταθέσουν ως μάρτυρες. Για την ταυτότητα του νομικού λόγου, πρέπει επίσης να γίνει δεκτό ότι κατά την ποινική διαδικασία η δικαστική αρχή έχει πρόσβαση και στα βιβλία και στοιχεία της τράπεζας.[574]

Προς τις προαναφερθείσες ρυθμίσεις του ΚΠολΔ, ταυτίζεται σχεδόν το άρθρο 183 ΚΔΔ (νόμος 2717/1999), το οποίο ορίζει ότι αποκλείεται η εξέταση ως μαρτύρων προσώπων που ασκούν επάγγελμα για όσα θέματα τους έχουν εμπιστευτεί λόγω της ιδιότητάς τους αυτής εφόσον για τα θέματα αυτά υφίσταται υποχρέωση εχεμύθειας. Κατά ρητή δε πρόβλεψη του άρθρου 183 ΚΔΔ, ο αποκλεισμός αυτός μπορεί να αρθεί εφόσον το επιτρέψουν τόσο εκείνος που τους εμπιστεύθηκε το σχετικό θέμα όσο και αυτός στον οποίο αφορά το απόρρητο. Με την παράγραφο 2 του άρθρου 183 ΚΔΔ, ρυθμίζεται το δικαίωμα αρνήσεως μαρτυρίας των προσώπων που δεσμεύονται από το

---

[572] Βλ. άρθρο 12 παρ. 2 του ν.δ. 3329/1955 «περί συστάσεως σώματος ορκωτών λογιστών», το οποίο εκτός του ελέγχου κάνει λόγο και για τη διενέργεια πραγματογνωμοσύνης.
[573] Γεώργιος Α. Γραμματίκας, *Το Τραπεζικό Απόρρητο*, 1η εκδ. (repr., Αθήνα: Π. Σάκκουλας, 1991), 98.
[574] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 89.

επαγγελματικό απόρρητο. Υπάρχουν, ωστόσο, διατάξεις φορολογικού περιεχομένου που αποκλίνουν από τη ρύθμιση του ΚΔΔ. Στόχος των διατάξεων αυτών είναι η αντιμετώπιση της φοροδιαφυγής και η παροχή της εξουσίας στην φορολογούσα αρχή να λαμβάνει πληροφορίες για τις συναλλαγές του φορολογουμένου με την τράπεζα, περιλαμβανομένων και των λογαριασμών καταθέσεων. Στις περιπτώσεις αυτές δηλαδή αίρεται τόσο το γενικό όσο και το ειδικό τραπεζικό απόρρητο. Θα πρέπει επίσης να γίνει δεκτό ότι όπου με ειδική διάταξη αίρεται το ειδικό απόρρητο των καταθέσεων, κατά μείζονα λόγο αίρεται και το γενικό.[575]

Ειδικότερα, το άρθρο 15 παρ. 3 του νόμου 4174/2013, προβλέπει γενικευμένη άρση του τραπεζικού απορρήτου με απλή αίτηση του Γενικού Γραμματέα Δημοσίων Εσόδων προς πιστωτικό ίδρυμα, το οποίο έχει υποχρέωση να χορηγήσει τις σχετικές πληροφορίες, αφού αυτές «αφορούν οικονομικές συναλλαγές τους με τον φορολογούμενο». Επίσης, σύμφωνα με το άρθρο 50 του νόμου 3323/1955 για τη φορολογία εισοδήματος, όπως ισχύει, η φορολογούσα αρχή δικαιούται να λαμβάνει και από τις τράπεζες όσες πληροφορίες θεωρεί αναγκαίες για τον έλεγχο της ακρίβειας των υποβληθεισών φορολογικών δηλώσεων και για την ανακάλυψη των υποχρέων που δεν υπέβαλαν δήλωση.[576] Επίσης, βάσει του άρθρου 14 του νόμου 2523/1997, επί ορισμένων σοβαρών φορολογικών παραβάσεων, οι τράπεζες υποχρεούνται να παρέχουν στην αρμόδια διεύθυνση του Υπουργείου Οικονομικών όλες τις σχετικές πληροφορίες και, επιπλέον, να δεσμεύουν υπέρ του Δημοσίου το 50% των καταθέσεων ή του περιεχομένου των θυρίδων του φορολογούμενου. Το γενικό τραπεζικό απόρρητο δεν ισχύει έναντι της φορολογικής αρχής για τις εκμισθώσεις από την τράπεζα χρηματοκιβωτίων στα θησαυροφυλάκιά της και για τα παραδιδόμενα σε αυτήν προς φύλαξη αντικείμενα εντός σφραγισμένων φακέλων ή κιβωτιδίων (άρθρο 109 του νόμου 2961/2001). Η διάταξη αυτή σκοπεί στην διαφύλαξη της δυνατότητας συλλήψεως της φορολογητέας ύλης στην περίπτωση θανάτου του μισθωτή ή παρακαταθέτη.

Επιπροσθέτως, στο άρθρο 62 του νόμου 4170/2013 για τη διοικητική συνεργασία στο φορολογικό τομέα προβλέπεται η σύσταση Συστήματος Μητρώων Τραπεζικών Λογαριασμών και Λογαριασμών Πληρωμών (Σ.Μ.Τ.Λ. και Λ.Π.) των πιστωτικών ιδρυμάτων, των ιδρυμάτων πληρωμών και των ιδρυμάτων ηλεκτρονικού χρήματος που λειτουργούν στην Ελλάδα, καθώς και των παρόχων υπηρεσιών πληρωμών που αποδέχονται συναλλαγές καρτών πληρωμών (card acquirers) με έδρα το εξωτερικό και οι οποίοι δραστηριοποιούνται στην Ελλάδα, εξυπηρετώντας επιχειρήσεις στην Ελληνική επικράτεια, «με σκοπό τη διευκόλυνση της διαβίβασης των αιτημάτων παροχής πληροφοριών από το σύνολο των υπηρεσιών της Γενικής Γραμματείας Δημοσίων Εσόδων και του Σώματος Δίωξης Οικονομικού Εγκλήματος του Υπουργείου Οικονομικών, την Οικονομική Αστυνομία, τον Οικονομικό Εισαγγελέα, τον Εισαγγελέα Εγκλημάτων Διαφθοράς, την Αρχή Καταπολέμησης της νομιμοποίησης των εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας και ελέγχου των δηλώσεων περιουσιακής κατάστασης». Στο ίδιο άρθρο προβλέπεται ότι «τα αιτήματα παροχής πληροφοριών αφορούν σε κάθε στοιχείο και πληροφορία για φυσικό ή νομικό πρόσωπο ή νομική οντότητα που τηρούνται στα πιστωτικά ιδρύματα και τα ιδρύματα πληρωμών, σύμφωνα με τις διατάξεις της κείμενης νομοθεσίας για την άρση του τραπεζικού και επαγγελματικού απορρήτου».

---

[575] Γεώργιος Α. Γραμματίκας, *Το Τραπεζικό Απόρρητο*, 1η εκδ. (repr., Αθήνα: Π. Σάκκουλας, 1991), 85.
[576] Διευκρινίστηκε περαιτέρω μέσω της διάταξης του άρθρου 25 παρ. 1 του νόμου 2214/1994.

Τέλος, σύμφωνα με το άρθρο 4 του νόμου 4261/2014, το τραπεζικό απόρρητο κάμπτεται κατά την άσκηση από την Τράπεζα της Ελλάδος της εποπτείας και του ελέγχου επί των ιδιωτικών τραπεζών, με αντίστοιχη όμως υποχρέωση, κατά το άρθρο 54 του νόμου 4261/2014, των οργάνων και υπαλλήλων της να τηρούν το δικό τους επαγγελματικό απόρρητο έναντι τρίτων, με την απειλή των κυρώσεων του άρθρου 371 ΠΚ. Η Τράπεζα της Ελλάδος δεν επιτρέπεται να παρέχει πληροφορίες σε τρίτους και δημόσιες αρχές με τρόπο αναλυτικό και συγκεκριμένο και με εμφανή την ταυτότητα ορισμένου πιστωτικού ιδρύματος.

Δύο είναι πάντως τα βασικά κριτήρια με βάση τα οποία μπορεί να θεωρηθεί προστατευτέο το συμφέρον ενώπιον του οποίου δύναται να υποχωρήσει το τραπεζικό απόρρητο: το εν λόγω συμφέρον θα πρέπει να είναι ουσιώδες και να μην δύναται να διαφυλαχθεί παρά μόνο με την παραβίαση του απορρήτου. Ο δημόσιος χαρακτήρας του συμφέροντος αυτού δεν αρκεί για να καταστήσει αυτό και ουσιώδες. Το τελευταίο αυτό κριτήριο είναι γενικό και αυτοτελές και προϋποθέτει λογικά και την ύπαρξη δημοσίων συμφερόντων που δεν είναι ουσιώδη. Επιπροσθέτως, τα συμφέροντα των οποίων η προάσπιση επιτρέπει την παραβίαση του τραπεζικού απορρήτου μπορεί να ανήκουν και στην ίδια την τράπεζα. Συνεπώς, η τράπεζα, κατά την δικαστική επιδίωξη των απαιτήσεών της κατά των οφειλετών της, δεν κωλύεται να αποκαλύψει τα στοιχεία που αφορούν τις έννομες σχέσεις της με τους οφειλέτες αυτούς και τα οποία θεμελιώνουν τις αξιώσεις ή τους ισχυρισμούς της.[577] Ορθώς παρατηρείται, ότι και σε αυτήν την περίπτωση πρέπει να τηρείται η αρχή της αναλογικότητας, η οποία είναι μια από τις εκφάνσεις της καταχρήσεως δικαιώματος. Οι τράπεζες επομένως δεν θα πρέπει να προσκομίζουν στο δικαστήριο αποδεικτικά στοιχεία που απλώς διασύρουν τον οφειλέτη, χωρίς να βοηθούν στο σχηματισμό δικαστικής κρίσεως.[578][579]

Η άρση του απορρήτου για τις έννομες σχέσεις ενός πελάτη μπορεί επίσης να επιβάλλεται ώστε να προστατευθούν υπέρτερα συμφέροντα άλλου πελάτη της τράπεζας. Σε τέτοιες περιπτώσεις, η τράπεζα έχει υποχρέωση να συμπεριφέρεται καλόπιστα έναντι αμφότερων των πελατών με αντικρουόμενα συμφέροντα, οπότε θα πρέπει να υπάρξει ad hoc στάθμιση κατά την οποία θα συναξιολογηθούν τα εκατέρωθεν συμφέροντα που διακυβεύονται. Την ευθύνη για την εν λόγω στάθμιση έχει σε κάθε περίπτωση ο επιχειρών αυτήν. Η καταβολή από αυτόν επιμέλειας η οποία εντούτοις καταλήγει σε εσφαλμένη στάθμιση, δεν οδηγεί στην πλήρη απαλλαγή του από την αστική ευθύνη. Αυτό συμβαίνει διότι στην αστική ευθύνη η αμέλεια κρίνεται αντικειμενικώς (ΑΚ 330 εδ. 2), η δε τελική δικαστική κρίση περί το ουσιώδες του συμφέροντος και την ανυπαρξία άλλης δυνατότητας προς διαφύλαξη αυτού διαμορφώνεται με βάση αντικειμενικών κριτηρίων.[580]

---

[577] Δημήτριος Β. Κουτσούκης, *Τραπεζικό Απόρρητο (Νομοθεσία-Νομολογία)*, 1η εκδ. (repr., Αθήνα: Αντ. Ν. Σάκκουλας, 1998), 170.

[578] Γεώργιος Α. Γραμματίκας, *Το Τραπεζικό Απόρρητο*, 1η εκδ. (repr., Αθήνα: Π. Σάκκουλας, 1991), 106.

[579] Η χρησιμοποίηση από την τράπεζα ένδικων βοηθημάτων που είναι δυσανάλογα προς το μέγεθος της απαιτήσεως της, λ.χ. αιτήσεως πτωχεύσεως για μικρή σχετικώς οφειλή, αποτελεί παράβαση της αρχής της αναλογικότητας μεταξύ μέσων και σκοπού, όχι όμως, καθαυτή, και του τραπεζικού απορρήτου. (*Γραμματίκας*, 106.)

[580] Γεώργιος Δ. Καλλιμόπουλος, Κωνσταντίνος Γ. Καραγιάννης και Ζαφείριος Ν. Τσολακίδης, *Δίκαιο Τραπεζικών Συναλλαγών*, 1η εκδ. (repr., Αθήνα: Π.Ν. Σάκκουλας, 2019), 97.

5.4.2 Οι περιπτώσεις άρσης του ειδικού τραπεζικού απορρήτου

Η προστασία που παρέχει το ειδικό τραπεζικό απόρρητο δεν είναι τόσο ευρεία όσο μπορεί να φαίνεται εξ 'αρχής, καθώς τόσο στο ίδιο το ν.δ. 1059/1971 όσο και σε άλλα νομοθετήματα περιλαμβάνονται διατάξεις που αίρουν το ειδικό αυτό απόρρητο, με στόχο την εξυπηρέτηση κυρίως σκοπών δημοσίου συμφέροντος. Η έκταση των νομοθετικών αυτών εξαιρέσεων, εγείρει το ερώτημα μήπως είναι προτιμότερη η κατάργηση των ρυθμίσεων για το ειδικό τραπεζικό απόρρητο και η υπαγωγή του ζητήματος στο γενικό τραπεζικό απόρρητο.

Στο άρθρο 1 του ν.δ. 1059/1971, όπως αυτό ισχύει σήμερα, προβλέπεται ότι το απόρρητο των καταθέσεων δεν ισχύει έναντι της Τράπεζας της Ελλάδος κατά την άσκηση των εποπτικών και ελεγκτικών της αρμοδιοτήτων. Η ρύθμιση αυτή που εισήχθη με το άρθρο 10 παρ. 1 του νόμου 1858/1989 συμπληρώνεται και από το εδάφιο γ' της παραγράφου 1 του άρθρου 2 του ν.δ. σύμφωνα με το οποίο οι κυρώσεις που προβλέπονται σε περίπτωση παραβιάσεως του απορρήτου δεν εφαρμόζονται από την Διοίκηση και τα λοιπά όργανα της Τράπεζας της Ελλάδος προκειμένου να επιβληθούν διοικητικές κυρώσεις για παραβάσεις νομισματικών, πιστωτικών ή συναλλαγματικών κανόνων. Οι διατάξεις αυτές ακολούθησαν το άρθρο 40 παρ. 3 του νόμου 1806/1988 το οποίο αντιθέτως προέβλεπε ότι τα άρθρα 2 και 3 του ν.δ ισχύουν κατ' αρχήν και για τα όργανα της ΤτΕ. Μετά τη θέσπιση του άρθρου 10 του νόμου 1858/1989, το οποίο εξαίρεσε από την εφαρμογή των διατάξεων για το απόρρητο την ΤτΕ, εισήχθη και το άρθρο 27 παρ. 2 του νόμου 1868/1989 το οποίο αντικατέστησε το άρθρο 40 παρ. 2 του νόμου 1806/1988 και το οποίο εισήγαγε μια ευρεία εξαίρεση από το ειδικό τραπεζικό απόρρητο, όχι μόνο για τα ελεγκτικά όργανα της ΤτΕ αλλά και για τις δικαστικές αρχές και τις προανακριτικές κοινοβουλευτικές επιτροπές, στις οποίες κατά το νόμο ανατίθεται ο έλεγχος των πιστωτικών ιδρυμάτων και η ορθή εφαρμογή της πιστωτικής ή νομισματικής νομοθεσίας ή της νομοθεσίας περί προστασίας του εθνικού νομίσματος.

Επιπροσθέτως, σύμφωνα με το δεύτερο εδάφιο του άρθρου 2 του ν.δ., όπως αυτό συμπληρώθηκε με την παράγραφο 3 του άρθρου 63 του νόμου 4170/2013, «*το απόρρητο δεν ισχύει έναντι των αρμόδιων για την είσπραξη και τον έλεγχο στον τομέα των δημοσίων εσόδων υπηρεσιών Φορολογικής Διοίκησης καθώς και των αρμόδιων υπηρεσιών και ασφαλιστικών ταμείων για την είσπραξη κοινωνικοασφαλιστικών εισφορών*», ενώ και το εδάφιο γ' του άρθρου 1 του ν.δ. επιτρέπει την άρση του απορρήτου με ενέργεια του Προϊσταμένου της ΔΟΥ σε περίπτωση που προσκομίζεται προσωπική επιταγή ποσού άνω του ενός εκατομμυρίου δραχμών, για εξόφληση χρεών προς το Δημόσιο , οπότε και δίδεται πρόβλεψη και δέσμευση ποσού υπέρ της ΔΟΥ.

Περαιτέρω, στο άρθρο 3 του ν.δ. 1059/1971 ρυθμίζεται κατ' εξαίρεση «*η παροχή πληροφοριών για τις απόρρητες χρηματικές ή άλλες καταθέσεις μετά από ειδικά αιτιολογημένη παραγγελία ή αίτηση ή απόφαση του αρμόδιου για την άσκηση ποινικής δίωξης ή τη διενέργεια προκαταρκτικής εξέτασης ή προανάκρισης ή κύριας ανάκρισης οργάνου δια του δικαστικού συμβουλίου ή δικαστηρίου, στο οποίο διενεργείται η σχετική διαδικασία, εφόσον η παροχή των πληροφοριών αυτών είναι απολύτως αναγκαία για την ανίχνευση και τον κολασμό του κακουργήματος*». Στις περιπτώσεις αυτές, οι δικαστικές αρχές αποστέλλουν τις αποφάσεις ή τα βουλεύματα στην ΤτΕ και η τελευταία με ευθύνης της διαβιβάζει αυτά αμέσως στα τραπεζικά ιδρύματα.

Το ειδικό τραπεζικό απόρρητο δύνανται επίσης να αρθεί βάσει ειδικών νομοθετημάτων. Συγκεκριμένα, το ειδικό τραπεζικό απόρρητο δεν ισχύει σύμφωνα με την πρόβλεψη του άρθρου

2 του ν.δ. 1325/1972 σε περίπτωση μη πληρωμής επιταγής λόγω ελλείψεως διαθέσιμων κεφαλαίων, οπότε η Τράπεζα έχει υποχρέωση να βεβαιώσει αυτό είτε στο σώμα της επιταγής, είτε με ίδιο έγγραφο που συνοδεύεται από σημείωση της ημέρας εμφανίσεως της επιταγής.

Απόκλιση από τις διατάξεις για την προστασία του ειδικού τραπεζικού απορρήτου προβλέπει και το άρθρο 48 του νόμου 4370/2016 για το Ταμείο Εγγύησης Καταθέσεων και Επενδύσεων (ΤΕΚΕ). Στις παραγράφους 19 και 20 του άρθρου αυτού προβλέπεται ότι τα μέλη του Διοικητικού Συμβουλίου και το προσωπικό του ΤΕΚΕ είναι κατ' αρχήν υπόχρεα στην τήρηση του επαγγελματικού απορρήτου και του απορρήτου των τραπεζικών καταθέσεων. Στο πλαίσιο όμως των αρμοδιοτήτων τους, επιτρέπεται βάσει του άρθρου 48 του νόμου 4370/2016, η ανταλλαγή πληροφοριών μεταξύ του ΤΕΚΕ και των αρχών που είναι αρμόδιες για την εξυγίανση και την εποπτεία των πιστωτικών ιδρυμάτων στα κράτη-μέλη της ΕΕ, χωρίς η ανταλλαγή αυτή να συνιστά παραβίαση του επαγγελματικού απορρήτου και του απορρήτου των τραπεζικών καταθέσεων. Και στον νόμο αυτό εφαρμόζονται πάντως οι κυρώσεις του άρθρου 371 ΠΚ και του άρθρου 2 του ν.δ. 1059/1971 αναλόγως.

Σε ισχύ έχουν, επίσης, παραμείνει οι ΥΑ 376/29.11.2018, η οποία μάλιστα κυρώθηκε με το άρθρο 38 του νόμου 1828/1989, καθώς και 60013/14.10.1988, οι οποίες προβλέπουν περιπτώσεις ελεγκτικών αρμοδιοτήτων της ΤτΕ, στις οποίες δεν ισχύει το ειδικό τραπεζικό απόρρητο. Επιπροσθέτως, σύμφωνα με το άρθρο 23 παρ. 5 του νόμου 4364/2016 για την ιδιωτική ασφάλιση, κατά τη διενέργεια ελέγχων από την Εποπτική Αρχή ή τις αρμόδιες αρχές των άλλων κρατών-μελών, τα υποκείμενα στους ελέγχους αυτούς πρόσωπα «δεν δικαιούνται να επικαλεσθούν το απόρρητο των τραπεζικών καταθέσεων ή τη νομοθεσία περί προστασίας των προσωπικών δεδομένων ή άλλο απόρρητο έναντι των αρμόδιων αρχών ή των εξουσιοδοτημένων από αυτές για τη διενέργεια του ελέγχου προσώπων».

Περαιτέρω περιπτώσεις άρσεως του ειδικού τραπεζικού απορρήτου προβλέπονται στο νόμο 4549/2018, ανάγοντας όμως την άρση αυτή στη βούληση του φορέα της καταθέσεως. Ειδικότερα στο άρθρο 54 προβλέπεται ότι με την αίτηση επιχειρηματία οφειλέτη για την ένταξη στην εξωδικαστική διαδικασία ρυθμίσεως χρηματικών οφειλών «παρέχεται από τον οφειλέτη άδεια για κοινοποίηση στον πιστωτή, επεξεργασία και διασταύρωση από αυτόν των δεδομένων του, τα οποία περιλαμβάνονται στην αίτηση και τα συνοδευτικά έγγραφα για τους σκοπούς της διαδικασίας ρύθμισης οφειλών», η δε άδεια αυτή «συνεπάγεται την άρση του απορρήτου των τραπεζικών καταθέσεων του άρθρου 1 του ν.δ. 1059/1971 και του φορολογικού απορρήτου του άρθρου 17 του ν. 4174/2013».

ΕΚΤΟ ΚΕΦΑΛΑΙΟ
Η ΜΕΤΑΒΙΒΑΣΗ «ΚΟΚΚΙΝΩΝ» ΔΑΝΕΙΩΝ ΑΠΟ ΤΙΣ ΤΡΑΠΕΖΕΣ ΚΑΙ Η ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΤΩΝ ΔΑΝΕΙΟΛΗΠΤΩΝ

6.1 Η επεξεργασία δεδομένων στο πλαίσιο της πώλησης και μεταβίβασης (εκχώρησης) απαιτήσεων

Στην εποχή μας, αποτελεί συχνό φαινόμενο οι τράπεζες να προβαίνουν σε μαζικές πωλήσεις απαιτήσεων κατά των πελατών τους από δάνεια και πιστωτικές κάρτες σε εταιρείες διαχείρισης ή απόκτησης δανείων. Πρόκειται για τα λεγόμενα «κόκκινα» (μη εξυπηρετούμενα) δάνεια, δηλαδή εκείνα στα οποία καταγράφεται ήδη υπερημερία του οφειλέτη ως προς την εκπλήρωση των υποχρεώσεών του ή προβλέπεται ότι λόγω οικονομικών δυσχερειών, ότι αυτά δεν θα αποπληρωθούν κατά την λήξη τους. Οι τράπεζες προχωρούν επομένως όλο και πιο συχνά στην μεταβίβαση των δανείων αυτών, με στόχο την εξυγίανση των ισολογισμών τους, με δεδομένο ότι η πλειοψηφία των πωλούμενων δανείων βρίσκονται σε καθυστέρηση ετών και δεν έχουν καθόλου ή έχουν μη επαρκείς εξασφαλίσεις. Το ειδικό νομοθετικό πλαίσιο για την μεταβίβαση των τραπεζικών δανείων διαμορφώθηκε με την ψήφιση του νόμου 4354/2015, ο οποίος διέπει την μεταβίβαση κάθε είδους απαιτήσεων από δάνεια ή πιστώσεις που έχουν χορηγηθεί από πιστωτικά ή χρηματοδοτικά ιδρύματα, είτε πρόκειται για καθυστερούμενες, είτε για ενήμερες οφειλές. Συμπληρωματικά με τις διατάξεις του νόμου αυτού (άρθρα 1-3), εφαρμόζεται και το γενικό δίκαιο της εκχώρησης (άρθρα 455 επ.) του Αστικού Κώδικα.[581]

Ο νόμος 4354/2015 προβλέπει δύο μορφές μεταβίβασης απαιτήσεων από τραπεζικά δάνεια ή πιστώσεις. Η ανάθεση της διαχείρισης, ως πρώτη μορφή μεταβίβασης, έχει ως συνέπεια ότι οι τράπεζες παραμένουν δικαιούχοι των μεταβιβαζόμενων απαιτήσεων και απλώς αναθέτουν, δυνάμει έγγραφης συμβάσεως, τη διαχείριση αυτών σε ειδικές εταιρείες αποκλειστικού σκοπού («Εταιρείες Διαχείρισης Απαιτήσεων από Δάνεια και Πιστώσεις»). Η διαχείριση των απαιτήσεων περιλαμβάνει κάθε πράξη την οποία θα μπορούσε να διενεργήσει το ίδιο το πιστωτικό ίδρυμα (είσπραξη, λογιστική και νομική παρακολούθηση, ρύθμιση οφειλών, σύναψη συμβάσεων συμβιβασμού, άσκηση ένδικων βοηθημάτων, επίσπευση αναγκαστικής εκτέλεσης κ.ο.κ). Για να διασφαλιστεί η προστασία των δανειοληπτών, ο νόμος (άρθρο 1) προβλέπει ότι οι εταιρείες αυτές λαμβάνουν ειδική άδεια από την ΤτΕ και υπόκεινται σε αυστηρή εποπτεία από αυτήν. Επίσης, δεσμεύονται από τη νομοθεσία περί προστασίας των καταναλωτών, τον Κώδικα Δεοντολογίας για τα μη εξυπηρετούμενα δάνεια[582], αλλά και τους κανόνες που διέπουν τη χορήγηση δανείων και πιστώσεων από τις τράπεζες.

Περαιτέρω, η μεταβίβαση με αιτία την πώληση (εκχώρηση) των απαιτήσεων (άρθρο 3), έχει ως αποτέλεσμα οι τράπεζες να αποξενώνονται πλήρως από τις μεταβιβαζόμενες απαιτήσεις, οι οποίες

---

[581] Απόστολος Γεωργιάδης, "Η Μεταβίβαση «Κόκκινων» Δανείων από τις Τράπεζες και η Προστασία Προσωπικών Δεδομένων του Δανειολήπτη", σε *Συλλογικό Έργο, Τιμητικός Τόμος, Νικολάου Θ. Νίκα*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Σάκκουλα, 2018), 153-154.

[582] Ο Κώδικας Δεοντολογίας για τις μη εξυπηρετούμενες ιδιωτικές οφειλές θεσπίστηκε για πρώτη φορά, κατ' εξουσιοδότηση του άρθρου 1 παρ. 2 του ν. 4224/2013, με την υπ'αριθμ. 116/25.8.2014 απόφαση της Επιτροπής Πιστωτικών και Ασφαλιστικών Θεμάτων (ΕΠΑΘ) της Τράπεζας της Ελλάδος. Ήδη έχει τεθεί σε ισχύ νέα, αναθεωρημένη μορφή του Κώδικα, που περιλαμβάνεται στην ΕΠΑΘ 195/29.7.2016 (ΦΕΚ Β' 2376).

ανήκουν πλέον εξ 'ολοκλήρου στον εκδοχέα. Προϋπόθεση για την προσφορά προς πώληση των απαιτήσεων, όταν πρόκειται για μη εξυπηρετούμενα δάνεια, είναι να έχει προηγηθεί, πριν από τουλάχιστον δώδεκα μήνες, εξώδικη πρόσκληση προς τον δανειολήπτη και τον εγγυητή να τακτοποιήσουν τις οφειλές τους σύμφωνα με τον Κώδικα Τραπεζικής Δεοντολογίας. Για τους εκδοχείς, όπως τις Εταιρείες Απόκτησης Απαιτήσεων από Δάνεια και Πιστώσεις, δεν τίθενται ιδιαίτερες προδιαγραφές, αρκεί να έχουν τη δυνατότητα, με βάση το καταστατικό τους, να προβαίνουν σε απόκτηση απαιτήσεων από τραπεζικά δάνεια και να μην εδρεύουν σε χώρα με «προνομιακό φορολογικό καθεστώς» ή σε «μη συνεργάσιμο κράτος». Οι εταιρείες αυτές, όμως δεν μπορούν να ασκήσουν οι ίδιες τα δικαιώματα που απορρέουν από τις αποκτώμενες απαιτήσεις, αλλά έχουν υποχρέωση να προχωρήσουν σε ανάθεση της διαχείρισής των απαιτήσεων αυτών σε μια από τις Εταιρείες Διαχείρισης. Η σύμβαση εκχωρήσεως καταρτίζεται εγγράφως, αναγγέλλεται στον εκάστοτε δανειολήπτη και υπόκειται σε ειδική δημοσιότητα, από την οποία και μόνο επέρχονται τα αποτελέσματά της.[583]

6.2 Το ζήτημα της πώλησης και μεταβίβασης (εκχώρησης) απαιτήσεων από τη σκοπιά της νομοθεσίας προσωπικών δεδομένων

Η διαχείριση και μεταβίβαση μη εξυπηρετούμενων δανείων, γεννά σημαντικά ζητήματα που άπτονται της νομοθεσίας περί προστασίας δεδομένων προσωπικού χαρακτήρα. Αυτό συμβαίνει διότι τόσο η σύμβαση ανάθεσης της διαχείρισης όσο και η σύμβαση εκχώρησης των δανείων αυτών ιδρύουν υποχρέωση των τραπεζικών ιδρυμάτων να μεταβιβάσουν στον αποκτώντα πλήθος δεδομένων προσωπικού χαρακτήρα του οφειλέτη-φυσικού προσώπου, υπό την έννοια του άρθρου 4 παρ. 1 του Κανονισμού (ΕΕ) 2016/679, καθώς οι πληροφορίες αυτές[584] είναι αναγκαίες για την ενάσκηση των μεταβιβαζόμενων απαιτήσεων (ΑΚ 465).

Στον όγκο των διαβιβαζόμενων δεδομένων προστίθεται και το γεγονός ότι η διαβίβαση των οικονομικών δεδομένων του οφειλέτη στον εκδοχέα συχνά δεν πραγματοποιείται μετά τη μεταβίβαση των αντίστοιχων πιστώσεων αλλά ήδη κατά το προσυμβατικό στάδιο. Αυτό συμβαίνει διότι μόνο με τη γνώση αυτών των οικονομικών δεδομένων είναι σε θέση ο υποψήφιος αντισυμβαλλόμενος της τράπεζας να εξετάσει εάν τον συμφέρει -και σε ποια τιμή- να προβεί στην απόκτηση των απαιτήσεων αυτών. Επιπροσθέτως, ενδέχεται η διασπορά των δεδομένων προσωπικού χαρακτήρα του δανειολήπτη να ενισχυθεί ακόμα περισσότερο μετά την αρχική διαβίβαση στον εκδοχέα σε αμφότερες τις μορφές μεταβίβασης «κόκκινων» δανείων. Στη μεν

---

[583] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 128.

[584] Οι εν λόγω πληροφορίες κατηγοριοποιούνται ως εξής: α) στοιχεία ταυτοποίησης του δανειολήπτη, β) στοιχεία ταυτότητας τρίτων προσώπων-υπόχρεων προς καταβολή του μεταβιβαζόμενου δανείου ή προσώπων που συνδέονται με αυτό με άλλο τρόπο (π.χ. συνοφειλέτες, εγγυητές, ενεχυρικοί ή υποθηκικοί οφειλέτες, ειδικοί ή καθολικοί διάδοχοι των παραπάνω κ.λπ.), γ) δεδομένα σχετικά με το ύψος, τις ασφάλειες και τους όρους των πιστώσεων, από τις οποίες απορρέουν οι μεταβιβαζόμενες απαιτήσεις, δ) πληροφορίες για την οικονομική συμπεριφορά του δανειολήπτη στο πλαίσιο της συγκεκριμένης πίστωσης (π.χ. καθυστέρηση πληρωμών, τυχόν ήδη περιέλευση σε υπερημερία συνεπεία προηγούμενης όχλησης) και λοιπά στοιχεία του λεγόμενου «φακέλου χρηματοδότησης», (στάδιο στο οποίο βρίσκεται ο διακανονισμός της οφειλής σύμφωνα με τον Κώδικα Τραπεζικής Δεοντολογίας, τυχόν υπαγωγή του οφειλέτη στον νόμο για τα υπερχρεωμένα νοικοκυριά κ.α.) και ε) πληροφορίες για την γενικότερη οικονομική και περιουσιακή κατάσταση του οφειλέτη. [Απόστολος Γεωργιάδης, "Η Μεταβίβαση «Κόκκινων» Δανείων από τις Τράπεζες και η Προστασία Προσωπικών Δεδομένων του Δανειολήπτη", σε *Συλλογικό Έργο, Τιμητικός Τόμος, Νικολάου Θ. Νίκα*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Σάκκουλα, 2018), 156].

ανάθεση της διαχείρισης, η εταιρεία που αποκτά τις απαιτήσεις δύναται να επιστρατεύσει και τις αποκαλούμενες «Εταιρείες Ενημέρωσης Οφειλετών για ληξιπρόθεσμες οφειλές» του νόμου 3758/2009 κατά τη διαχείριση της απαίτησης (άρθρο 2 παρ. 5 του νόμου 4354/2015). Στην περίπτωση της πλήρους μεταβιβάσεως (εκχωρήσεως), ο εκδοχέας υποχρεούται να αναθέσει, τη διαχείριση των απαιτήσεων σε μια από τις εταιρείες διαχείρισης.[585]

Η διαβίβαση των προσωπικών πληροφοριών του δανειολήπτη αλλά και των λοιπών υποχρέων στον εκδοχέα, υπάγεται στην έννοια της «επεξεργασίας» βάσει του άρθρου 4 αριθ. 2 του Κανονισμού. Επομένως, για να θεωρείται θεμιτή η πραγματοποίησή της θα πρέπει να συντρέχει κάποια από τις νόμιμες βάσεις που προβλέπονται στο άρθρο 6 παρ. 1 του ίδιου Κανονισμού. Θα έπρεπε επομένως να απαιτείται η προηγούμενη συγκατάθεση του υποκειμένου των δεδομένων ή εναλλακτικά, η συνδρομή κάποιας νόμιμης βάσης του άρθρου 6 του Κανονισμού. Ο νόμος 4354/2015 ορίζει όμως στο άρθρο 1 παρ. 21, ότι στο πλαίσιο της μεταβίβασης δανείων εφαρμόζονται ανάλογα οι διατάξεις που αφορούν την τιτλοποίηση απαιτήσεων, οι οποίες, μεταξύ άλλων, προβλέπουν ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα διενεργείται βάσει της ισχύουσας νομοθεσίας περί προστασίας προσωπικών δεδομένων, χωρίς να απαιτείται η προηγούμενη συναίνεση του οφειλέτη ή η σχετική άδεια της Αρχής (άρθρο 10 παρ. 21, νόμος 3156/2003).[586]

Η ρύθμιση αυτή έχει ως βάση δύο θεμελιώδεις αξιολογήσεις. Αρχικά, στηρίζεται στην ανάγκη να διευκολυνθεί η μαζική μεταβίβαση «κόκκινων» δανείων, ώστε να ωφεληθούν οι τράπεζες και κατ' επέκταση το σύνολο του χρηματοπιστωτικού συστήματος. Δευτερευόντως, στηρίζεται στην πεποίθηση του νομοθέτη, όπως αυτή αποτυπώνεται και στο «γενικό μέρος» της εισηγητικής έκθεσης του νόμου 4354/2015 (άρθρο 3 παρ. 7), ότι η έννομη θέση του δανειολήπτη όχι μόνο δεν χειροτερεύει, αλλά ενδέχεται να βελτιωθεί από τη μεταβίβαση των εν λόγω δανείων. Στο πλαίσιο αυτό, ο δανειολήπτης αλλά και οι λοιποί υπόχρεοι έχουν τα ίδια δικαιώματα (π.χ. ενστάσεις) και τις ίδιες υποχρεώσεις (π.χ. υπόκεινται στα ίδια μέτρα αναγκαστικής εκτέλεσης) έναντι του εκδοχέα, που υπήρχαν και έναντι της τράπεζας. Ο δανειολήπτης επίσης προστατεύεται σε σημαντικό βαθμό, χάρη στην υπαγωγή των εταιρειών διαχείρισης απαιτήσεων σε αυστηρή εποπτεία. Τέλος, επειδή ο εκδοχέας αποκτά τις απαιτήσεις σε τιμή αρκετά μικρότερη από την ονομαστική τους αξία, βρίσκεται σε θέση να προτείνει στον δανειολήπτη τρόπους διευθέτησης της οφειλής του (π.χ. σημαντικά «κουρέματα») που συχνά είναι πολύ πιο ευνοϊκοί σε σχέση με τους αντίστοιχους που προσφέρουν οι τράπεζες. Όπως και να έχει, η προαναφερθείσα νομοθετική ρύθμιση (άρθρο 1 παρ. 21 του νόμου 4354/2015 σε συνδυασμό με το άρθρο 10 παρ. 21 του νόμου 3156/2003) καθιστά σαφές ότι για τη διαβίβαση των δεδομένων προσωπικού χαρακτήρα των οφειλετών (δανειοληπτών και λοιπών υποχρέων) από το τραπεζικό ίδρυμα στον εκδοχέα δεν απαιτείται προηγούμενη συγκατάθεση των προσώπων αυτών.[587]

Οι δανειολήπτες σε κάθε περίπτωση συνεχίζουν να προστατεύονται από την νομοθεσία περί προστασίας προσωπικών δεδομένων. Ειδικότερα, οι τράπεζες συνεχίζουν να δεσμεύονται από τις διατάξεις των άρθρων 13 παρ. 3 και 14 παρ. 4 του Κανονισμού, σχετικά με την προηγούμενη

---

[585] Απόστολος Γεωργιάδης, "Η Μεταβίβαση «Κόκκινων» Δανείων από τις Τράπεζες και η Προστασία Προσωπικών Δεδομένων του Δανειολήπτη", σε *Συλλογικό Έργο, Τιμητικός Τόμος, Νικολάου Θ. Νίκα*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Σάκκουλα, 2018), 156.
[586] Ibid., 157.
[587] Ibid., 158.

ενημέρωση των υποκειμένων των δεδομένων για τη διαβίβαση των προσωπικών τους δεδομένων στις Εταιρείες που ορίζονται στον νόμο 4354/2015. Επίσης, δεσμεύονται από τις γενικές αρχές που ορίζονται στο άρθρο 5 του Κανονισμού, οι οποίες διέπουν κάθε επεξεργασία προσωπικών δεδομένων, αλλά και από τις διατάξεις του άρθρου 32 του Κανονισμού που θεσπίζουν υποχρέωση του προσώπου που προβαίνει στην επεξεργασία των δεδομένων να φροντίζει για την ασφάλεια αυτής. [588]

6.3 Η ενημέρωση των δανειοληπτών σχετικά με τη διαβίβαση των προσωπικών τους δεδομένων

Όπως προαναφέρθηκε, τα τραπεζικά ιδρύματα δεν έχουν υποχρέωση προς λήψη της συναίνεσης των οφειλετών πριν από τη διαβίβαση των στοιχείων των προσώπων αυτών στις Εταιρείες Διαχείρισης ή Απόκτησης Απαιτήσεων από Δάνεια και Πιστώσεις. Τα πιστωτικά ιδρύματα, ωστόσο, δεν απαλλάσσονται από την υποχρέωση να ενημερώσουν τους οφειλέτες πριν διαβιβάσουν τα δεδομένα αυτών, σύμφωνα με τα άρθρα 13 παρ. 3 και 14 παρ. 4 του Κανονισμού (ΕΕ) 2016/679. Στο πεδίο της ανάθεσης διαχείρισης των απαιτήσεων στις αρμόδιες εταιρείες, η υποχρέωση αυτή των τραπεζικών ιδρυμάτων αποκτά μάλιστα ιδιαίτερη βαρύτητα, δεδομένου ότι δεν υφίσταται υποχρέωση αναγγελίας της εν λόγω ανάθεσης στους οφειλέτες, όπως στην περίπτωση της πλήρους μεταβίβασης (εκχώρησης) των απαιτήσεων.[589]

Η προαναφερθείσα ενημέρωση πρέπει να διεξάγεται, όπως προκύπτει από το συνδυασμό των παρ. 1 και 3 του άρθρου 13 του Κανονισμού, είτε κατά το στάδιο της συλλογής των σχετικών στοιχείων από το τραπεζικό ίδρυμα είτε πάντως, το αργότερο, πριν διαβιβαστούν στον εκδοχέα. Επιπροσθέτως, η ενημέρωση πρέπει να περιλαμβάνει τουλάχιστον τα στοιχεία που ορίζονται στο άρθρο 13 (παρ. 1) του Κανονισμού και ιδίως α) το είδος και τις κατηγορίες των αποδεκτών στους οποίους ενδέχεται να διαβιβάσει το τραπεζικό ίδρυμα τα προσωπικά και οικονομικά δεδομένα του δανειολήπτη. Από τη στιγμή που το τραπεζικό ίδρυμα πληροφορηθεί την ταυτότητα του συγκεκριμένου εκδοχέα, έχει υποχρέωση να ενημερώσει σχετικά με αυτήν τον δανειολήπτη το ταχύτερο δυνατόν και πάντως το αργότερο προτού διαβιβάσει τα δεδομένα του. Συνεπώς, τυχόν γενικόλογη γνωστοποίηση, κατά την υπογραφή της δανειακής σύμβασης, σχετικά με το ενδεχόμενο διαβίβασης των δεδομένων σε εταιρείες απόκτησης απαιτήσεων από δάνεια δεν είναι αρκετή.[590] Η ενημέρωση στην οποία προβαίνει το τραπεζικό ίδρυμα θα πρέπει επίσης να περιλαμβάνει τον συγκεκριμένο σκοπό (υλοποίηση της μεταβίβασης δανείου), για τον οποίο το τραπεζικό ίδρυμα προχωρά στη διαβίβαση των δεδομένων στα προαναφερθέντα πρόσωπα. Σε περίπτωση που η σχετική γνωστοποίηση περιλαμβάνεται ήδη στη δανειακή σύμβαση, πρέπει να γίνεται συγκεκριμένη αναφορά στο ενδεχόμενο μεταβίβασης των απαιτήσεων της τράπεζας κατά του δανειολήπτη σε τρίτους, να αποτυπώνονται οι όροι υπό τους οποίους ενδέχεται να λάβει χώρα μια τέτοια μεταβίβαση (π.χ. μόνο προκειμένου για μη εξυπηρετούμενα δάνεια) και να απαριθμούνται οι συγκεκριμένοι σκοποί, του οποίους είναι θεμιτό να επιδιώκει το τραπεζικό ίδρυμα μέσω μιας τέτοιου είδους μεταβίβασης. Επίσης, θα πρέπει να υπάρχει σχετική ενημέρωση

---

[588] Ibid., 158.

[589] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 131.

[590] Βλ. Απόφαση 98/2017 ΑΠΔΠΧ, η οποία αφορά την διαβίβαση προσωπικών δεδομένων του οφειλέτη σε Εταιρείες Ενημέρωσης Οφειλετών, σύμφωνα με την οποία: «*…ο δανειστής, ως υπεύθυνος επεξεργασίας, οφείλει να ενημερώνει τους οφειλέτες για τη διάθεση των δεδομένων τους στην εκάστοτε συγκεκριμένη Εταιρεία Ενημέρωσης Οφειλετών…*»

ως προς την ύπαρξη δικαιώματος πρόσβασης (άρθρο 15 ΓΚΠΔ) των υποκειμένων των δεδομένων που διαβιβάζονται.[591] [592]

Σε κάθε περίπτωση, βάσει του ισχύοντος νομοθετικού πλαισίου, η ενημέρωση θα πρέπει να διενεργείται με τρόπο πρόσφορο και σαφή, ώστε τα υποκείμενα των δεδομένων να λαμβάνουν πράγματι γνώση των σχετικών στοιχείων και να έχουν ξεκάθαρη εικόνα για αυτά. Οι τράπεζες επομένως δεν θα πρέπει να προβαίνουν σε παραπλανητικές, αόριστες και γενικόλογες αναφορές, είτε αυτές γίνονται εξατομικευμένα, είτε περιέχονται σε ΓΟΣ δανειακών συμβάσεων, καθώς στις περιπτώσεις αυτές δεν θα πληρούν τις προϋποθέσεις που ορίζει ο νόμος. Εδώ υπάγεται λ.χ. η γνωστοποίηση, εκ μέρους της τράπεζας, ότι τα δεδομένα προσωπικού χαρακτήρα του δανειολήπτη θα χρησιμοποιούνται για την εκτέλεση των σχετικών δανειακών συμβάσεων, την προάσπιση των συμφερόντων της τράπεζας και την εκπλήρωση των υποχρεώσεών της ή θα γίνονται αντικείμενο επεξεργασίας με σκοπό την είσπραξη, για λογαριασμό των δόσεων του δανείου.[593] Εξάλλου, όπως έχει ορθά επισημανθεί, η προαναφερθείσα ενημέρωση δεν ταυτίζεται με την αναγγελία της μεταβίβασης του δανείου στον οφειλέτη[594], αν και δεν αποκλείεται η ταυτόχρονη πραγματοποίησή της με αυτήν. Αυτό συμβαίνει διότι η προαναφερθείσα ενημέρωση επιβάλλεται να έχει το συγκεκριμένο περιεχόμενο που ορίζεται στον Κανονισμό και είναι επίσης πιθανό να απαιτείται να πραγματοποιηθεί πριν συντελεστεί η εκχώρηση, όταν τα δεδομένα προσωπικού χαρακτήρα του οφειλέτη παρέχονται σε περισσότερους του ενός εκδοχείς κατά το προσυμβατικό στάδιο.[595]

Συγκεκριμένα, με την απόφαση του το Ειρηνοδικείο Αθηνών (273/2016) έκρινε ότι «…κατά την κατάρτιση δανειακής συμβάσεως - προσωπικών δεδομένων της, με τη διαβίβαση στην δεύτερη εναγομένη εισπρακτική εταιρία, παραλείποντας να την ενημερώσει, όπως όφειλε, αφ' ενός κατ` άρθρο 11 παρ.1 Ν.2472/1997 με τρόπο σαφή για τους σκοπούς της επεξεργασίας κατά το στάδιο συλλογής των δεδομένων αυτών κατά το χρόνο καταρτίσεως της επίδικης συμβάσεως δανείου, αφετέρου δε κατ` άρθρο 11 παρ.3 του ίδιου νόμου, κατά το χρόνο πριν από τη διαβίβαση τους στην επικαλούμενη από τον ίδιο δεύτερη εναγομένη εισπρακτική εταιρία (αποδέκτρια) για τη μέλλουσα ανακοίνωση των προσωπικών του δεδομένων προς αυτήν…» η εναγόμενη τράπεζα παρενέβη το Νόμο.[596]

Επιπλέον, το Μονομελές Πρωτοδικείο Αθηνών (3428/2016) έκρινε ότι εκ μόνης της ύπαρξης όρου «συγκατάθεσης» στα πλαίσια ενός κειμένου με Γενικούς Όρους Συναλλαγών (ΓΟΣ) «... ουδόλως αποδεικνύεται από την εν λόγω εναγόμενη, που έχει το βάρος απόδειξης της ενημέρωσης ως

---

[591] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 131.

[592] Απόστολος Γεωργιάδης, "Η Μεταβίβαση «Κόκκινων» Δανείων από τις Τράπεζες και η Προστασία Προσωπικών Δεδομένων του Δανειολήπτη", σε *Συλλογικό Έργο, Τιμητικός Τόμος, Νικολάου Θ. Νίκα*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Σάκκουλα, 2018), 159.

[593] Ibid., 160.

[594] Η οποία απαιτείται τόσο σύμφωνα με την διάταξη ΑΚ 460, όσο και με βάση τον νόμο 4354/2015 (άρθρο 3 παρ. 4) στην περίπτωση που η τράπεζα προβαίνει σε εκχώρηση των σχετικών απαιτήσεων. Επίσης, πρβλ. άρθρο 17 της ΚΥΑ Ζ-699/2010, σύμφωνα με το οποίο επιτάσσεται η αναγγελία της εκχωρήσεως στον οφειλέτη στο πεδίο της καταναλωτικής πίστης. [Ibid., 168]

[595] Απόστολος Γεωργιάδης, "Η Μεταβίβαση «Κόκκινων» Δανείων από τις Τράπεζες και η Προστασία Προσωπικών Δεδομένων του Δανειολήπτη", σε *Συλλογικό Έργο, Τιμητικός Τόμος, Νικολάου Θ. Νίκα*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Σάκκουλα, 2018), 160.

[596] Απόφαση διαθέσιμη στη διεύθυνση http://www.dsanet.gr/Epikairothta/Nomologia/eirath273.htm.

υπεύθυνος επεξεργασίας κατά τα προαναφερθέντα στη μείζονα σκέψη - ότι αυτή κατά τον παραπάνω χρόνο της συλλογής δεδομένων είχε ενημερώσει τον ενάγοντα κατά τρόπο σαφή για την ταυτότητα του υπευθύνου επεξεργασίας, την ταυτότητα του τυχόν εκπροσώπου του, για τον σκοπό της επεξεργασίας (διαβίβασης) και για τους αποδέκτες ή τις κατηγορίες αποδεκτών, όπως απαιτείτο κατ` άρθρο 11 παρ. 1 α', β', γ' Ν. 2472/1997».[597][598]

6.3.1 Η ενημέρωση των δανειοληπτών δια του τύπου

Ο ήδη καταργηθείς νόμος 2472/1997 περιλάμβανε μια μεταβατική διάταξη (άρθρο 24 παρ. 3), η οποία όριζε ότι η ενημέρωση σχετικά με τα αρχεία δεδομένων προσωπικού χαρακτήρα τα οποία ήδη βρίσκονταν σε λειτουργία κατά την έναρξη της ισχύος του, μπορούσε, εφόσον αφορούσε μεγάλο αριθμό υποκειμένων, να διενεργηθεί και δια του τύπου. Μέσω μιας σειράς αποφάσεών της, η Αρχή έκρινε ότι η προαναφερθείσα διάταξη αποτυπώνει ευρύτερη και πάγια βούληση του νομοθέτη. Συνεπώς, η ενημέρωση που προβλέπεται στο άρθρο 11 του νόμου 2472/1997 (νυν άρθρα 13 παρ. 3 και 14 παρ. 4 του Κανονισμού), δύναται να διενεργηθεί όχι εξατομικευμένα, αλλά δια του τύπου, εφόσον αφορά μεγάλο αριθμό υποκειμένων (πάνω από 1000) και χορηγηθεί σχετική άδεια από την Αρχή.[599] Στο πλαίσιο της χορήγησης της άδειας αυτής, η Αρχή λαμβάνει υπόψιν την αδυναμία ενημέρωσης με άλλο πρόσφορο τρόπο, τον μεγάλο αριθμό των υποκειμένων που πρόκειται να ενημερωθούν, τον σκοπό της εκάστοτε επεξεργασίας αλλά και τις ειδικές συνθήκες συλλογής των δεδομένων. Η εν λόγω άποψη της Αρχής υιοθετήθηκε και από τη νομολογία.[600]

Χαρακτηριστική είναι η απόφαση 75/2009 της Αρχής, με την οποία αυτή απέρριψε το αίτημα της ενημέρωσης δια του τύπου και έκρινε ότι η εταιρεία με την επωνυμία «3DUBEE» υποχρεούται να ενημερώσει ατομικώς με συστημένη επιστολή τα υποκείμενα των δεδομένων για την σκοπούμενη επεξεργασία. Στην υπό κρίση περίπτωση ο αριθμός των μελών του Ι.Σ.Α υπερέβαινε τα χίλια άτομα, αλλά ήταν γνωστά τα στοιχεία ταυτοποίησης και οι διευθύνσεις των υποκειμένων. Επομένως, υπήρχε ασφαλέστερος και προσφορότερος τρόπος ώστε να ενημερωθούν τα υποκείμενα.[601]

Λαμβάνοντας υπόψιν τα παραπάνω δεδομένα, δύο ελληνικές τράπεζες γνωστοποίησαν στην Αρχή την πρόθεσή τους να προβούν σε ανάθεση της διαχείρισης, όπως αυτή νοείται βάσει του νόμου 4354/2015, ενός σημαντικού αριθμού καθυστερούμενων δανείων τους και ζήτησαν την άδεια να προχωρήσουν σε ενημέρωση των δανειοληπτών δια του τύπου. Με την απόφαση 87/2017, η Αρχή υιοθέτησε κατά πλειοψηφία σε μεγάλο βαθμό το σκεπτικό των αιτούντων τραπεζών αλλά και της Ένωσης Ελληνικών Τραπεζών που παρενέβη υπέρ αυτών και χορήγησε τη σχετική άδεια, αν και καταρχήν μόνο για τη μεταβίβαση απαιτήσεων που ήταν ήδη ληξιπρόθεσμες κατά τη δημοσίευση της απόφασής της. Η Αρχή προχώρησε σε χορήγηση των σχετικών αδειών λόγω α) του πολύ μεγάλου αριθμού των υποκειμένων (εκατοντάδων χιλιάδων φυσικών προσώπων, εκ των οποίων, βάσει σχετικού ισχυρισμού των αιτουσών Τραπεζών και της Ελληνικής Ένωσης Τραπεζών,

---

[597] Απόφαση διαθέσιμη στη διεύθυνση http://www.dsanet.gr/Epikairothta/Nomologia/mprath3428.htm.
[598] Βλ. αντίστοιχα και αποφάσεις ΕιρΑθ 3277/2014, ΤΝΠ ΝΟΜΟΣ, ΕιρΑθ 415/2016 ΤΝΠ ΝΟΜΟΣ, ΜΕφΑθ 1437/2014, ΤΝΠ ΝΟΜΟΣ.
[599] Βλ. τις Κανονιστικές πράξεις της Αρχής με αριθμό 1/1999 (ΦΕΚ Β'555) και 408/1998 (ΦΕΚ Β' 1250).
[600] Βλ. ΑΠ 1923/2006, ΝοΒ 2007, 367, ΕφΑθ 3833/2003, ΝοΒ 2004, 247, ΜΠρΑθ 2828/2014, ΤΝΠ ΝΟΜΟΣ.
[601] "Ετήσια Έκθεση ΑΠΔΠΧ 2009, 155. Διαθέσιμη στην ιστοσελίδα: https://www.dpa.gr/sites/default/files/2020-12/DPA_ANNUAL_REPORT_2009.PDF.

πιθανολογείται ότι πολλοί έχουν αλλάξει διεύθυνση κατοικίας και δεν έχουν ενημερώσει την τράπεζα συνεργασίας τους) που καθιστά δυσχερή την ατομική και έγκαιρη ενημέρωσή τους, β) του σύντομου χρονικού διαστήματος, εντός του οποίου θα πρέπει να ολοκληρωθεί η ενημέρωση για την χορήγηση των σχετικών δεδομένων, βάσει των ισχυρισμών των αιτούντων Τραπεζών και της Ελληνικής Ένωσης Τραπεζών[602] και γ) του γεγονότος ότι τα συνδεόμενα με το χρέος δικαιώματα των υποκειμένων και οι θεμελιώδεις ελευθερίες τους δεν θίγονται, καταρχάς, από την εν λόγω επεξεργασία.[603]

Στην εν λόγω απόφαση της Αρχής συμπεριλαμβάνονται επίσης ορισμένες επιπλέον εγγυήσεις που αποσκοπούν στην προστασία των υποκειμένων. Η Αρχή στο πλαίσιο αυτό επεσήμανε ότι: «για την ίδια κατηγορία δεδομένων πρέπει να πραγματοποιηθεί εξατομικευμένη ηλεκτρονική ενημέρωση μέσω ηλεκτρονικού ταχυδρομείου (e-mail), σε όλες τις περιπτώσεις, στις οποίες τα σχετικά στοιχεία (διευθύνσεις ηλεκτρονικού ταχυδρομείου) έχουν χορηγηθεί στην Τράπεζα από τα υποκείμενα των δεδομένων και , συνεπώς , καθίσταται εφικτή η ηλεκτρονική ενημέρωση».[604]Επιπροσθέτως, επέβαλε την δημοσίευση της ενημέρωσης σε πέντε (5) διαδικτυακούς τόπους με τη μεγαλύτερη επισκεψιμότητα στην Ελλάδα. Η εν λόγω ενημέρωση θα πρέπει επίσης να επαναλαμβάνεται ανά μήνα μέχρι να ολοκληρωθεί η διάθεση των δεδομένων στην αποδέκτρια Εταιρεία Διαχείρισης Απαιτήσεων και να επαναληφθεί δύο φορές, ανά τρίμηνο, μετά την ολοκλήρωση της διάθεσης.[605] Τέλος, η Αρχή μέσω της αποφάσεώς της αντέστρεψε τον παραπάνω κανόνα σε σχέση με τις απαιτήσεις που δεν είναι ήδη καθυστερούμενες, αλλά γίνονται ληξιπρόθεσμες μετά τη δημοσίευση της αποφάσεώς της, επειδή στις περιπτώσεις αυτές δεν συντρέχουν οι πρακτικοί λόγοι (ανάγκη μαζικής και άμεσης ενημέρωσης) που δικαιολογούν την παράκαμψη της εξατομικευμένης ενημέρωσης. Για τις μη ληξιπρόθεσμες αυτές απαιτήσεις επιτρέπεται κατ' εξαίρεση η δια του τύπου ενημέρωση μόνον αν η εξατομικευμένη ενημέρωση αποδεδειγμένα δεν είναι δυνατή (π.χ. ελλείψει στοιχείων επικοινωνίας, πρόσωπα αγνώστου διαμονής).[606]

Το τελευταίο σκέλος της απόφασης της Αρχής σχετικά με την εξατομικευμένη ενημέρωση των οφειλετών των απαιτήσεων που δεν είναι ακόμα καθυστερούμενες δεν μπορεί παρά να χαιρετιστεί, ωστόσο, το πόρισμά της για τα ήδη καθυστερούμενα κατά τη δημοσίευση της απόφαση δάνεια, υπόκειται σε σοβαρές επιφυλάξεις, εφόσον μέσω της ενημέρωσης «δια του τύπου» η επιταγή της νομοθεσίας περί προστασίας των δεδομένων προσωπικού χαρακτήρα για πρόσφορη και σαφή ενημέρωση του υποκειμένου των δεδομένων καταλήγει να αποτελεί «κενό γράμμα».[607] Συγκεκριμένα, όπως επισημαίνει και η μειοψηφία στην ανωτέρω απόφαση της Αρχής, το πιο πιθανό σενάριο θέλει τους δανειολήπτες να μη λάβουν καν γνώση της παραπάνω

---

[602] Λαμβάνοντας παράλληλα υπόψιν ότι: «*στις αρχές του 2018 οι ελληνικές συστημικές τράπεζες θα υποβληθούν σε αυστηρά "stress tests" με βάση τα οικονομικά στοιχεία του 2017, στα οποία περιλαμβάνονται και τα ήδη υπάρχοντα μη εξυπηρετούμενα δάνεια*».
[603] Απόφαση 87/2017 ΑΠΔΠΧ, σελ. 12. https://www.dpa.gr/sites/default/files/2019-10/87_2017anonym.pdf.
[604] Ibid.
[605] Ibid., 14.
[606] Ibid., 13.
[607] Απόστολος Γεωργιάδης, "Η Μεταβίβαση «Κόκκινων» Δανείων από τις Τράπεζες και η Προστασία Προσωπικών Δεδομένων του Δανειολήπτη", σε *Συλλογικό Έργο, Τιμητικός Τόμος, Νικολάου Θ. Νίκα*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Σάκκουλα, 2018), 162.

καταχώρισης στα ηλεκτρονικά και έντυπα μέσα. Ακόμη όμως και σε περίπτωση που πληροφορηθούν αυτήν, δεν θα μπορούν με ευκολία να αναγνωρίσουν ότι τους αφορά. Στις μέρες μας, η κυκλοφορία των έντυπων μέσων ενημέρωσης έχει περιοριστεί, ενώ όσον αφορά τον ηλεκτρονικό τύπο, η πλειοψηφία των συμπολιτών μας απλά προσπερνά ανακοινώσεις που αφορούν τέτοια ζητήματα. Παραμένει φυσικά η ασφαλιστική δικλείδα της αναγγελίας της εκχώρησης, η οποία όμως πραγματοποιείται αφού έχουν διαβιβαστεί τα δεδομένα των δανειοληπτών στις εταιρείες απόκτησης απαιτήσεων. Αυτό έχει ως αποτέλεσμα να μην απομένει στο υποκείμενο των δεδομένων ένα εύλογο χρονικό διάστημα εντός του οποίου θα έχει τη δυνατότητα να ασκήσει το δικαίωμα πρόσβασης και ενδεχομένως και αντίρρησης (άρθρα 15 και 21 ΓΚΠΔ).[608]

Το ζήτημα της διά του τύπου ενημέρωσης παρουσιάζει ενδιαφέρον στο πλαίσιο εφαρμογής του Κανονισμού, ο οποίος δεν περιλαμβάνει διάταξη που να αφορά το συγκεκριμένο ζήτημα.[609] Βάσει των διατάξεων των άρθρων 31 παρ. 2 και 32 παρ. 2 του νόμου 4624/2019, εφόσον δεν παρέχονται πληροφορίες στο υποκείμενο των δεδομένων για τους λόγους που αναφέρονται στην παράγραφο 1 του άρθρου 31 και του άρθρου 32, ή για τους λόγους που αναφέρονται στα άρθρα 13 και 14 του Κανονισμού, ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για την προστασία των εννόμων συμφερόντων των υποκειμένων, «συμπεριλαμβανομένης της παροχής στο κοινό πληροφοριών που αναφέρονται στο άρθρο 13 παράγραφοι 1 και 2 του Κανονισμού, σε ακριβή, διαφανή, κατανοητή και ευχερώς προσβάσιμη μορφή, σε σαφή και απλή γλώσσα, χωρίς προηγούμενη άδεια της Αρχής, ωστόσο, ο υπεύθυνος επεξεργασίας θα πρέπει να αιτιολογεί γραπτώς τους λόγους για τους οποίους απέφυγε να παράσχει πληροφορίες.[610]

Εν πάση περιπτώσει, θα πρέπει να γίνει δεκτό, τηρουμένης της αρχής της αναλογικότητας, ότι τα τραπεζικά ιδρύματα οφείλουν να εξαντλούν κάθε πρακτική δυνατότητα και κάθε χρονικό περιθώριο για την εξατομικευμένη ενημέρωση των οφειλετών σε κάθε μεταβίβαση δανείου και αν αυτή η ενημέρωση κρίνεται αδύνατη ή δυσχερής με βάση τα δεδομένα της εκάστοτε περίπτωσης, να προβαίνουν στην δια του τύπου ενημέρωση.[611]

6.3.1.1 Οι συνέπειες της παραλείψεως της ενημέρωσης των οφειλετών

Εάν το τραπεζικό ίδρυμα παραλείψει να ενημερώσει το υποκείμενο για τη διαβίβαση των δεδομένων του , προβεί σε ενημέρωση δια του τύπου χωρίς να έχει προηγουμένως λάβει άδεια της Αρχής, ή προβεί σε ενημέρωση δια του τύπου παρά το γεγονός ότι η εξατομικευμένη γνωστοποίηση είναι ευχερώς δυνατή, τότε η διαβίβαση των προσωπικών δεδομένων είναι παράνομη. Η τράπεζα επομένως υποχρεούται στην αποκατάσταση της (πλήρους) περιουσιακής ζημίας και της ηθικής βλάβης που προκλήθηκε στον οφειλέτη χάρη στην παράνομη ενημέρωση των δεδομένων του στην εταιρεία διαχείρισης ή απόκτησης απαιτήσεων, σύμφωνα με τα οριζόμενα στο άρθρο 82 του Κανονισμού. Ο οφειλέτης έχει επίσης, βάσει του άρθρου ΑΚ 57,

---

[608] Ibid., 163.

[609] Η διάταξη του άρθρου 14 παρ. 5, που ορίζει ότι η ενημέρωση δεν πραγματοποιείται εφόσον αυτή είναι αδύνατη ή απαιτεί δυσανάλογη προσπάθεια, αφενός αφορά την περίπτωση που τα δεδομένα έχουν συλλεγεί χωρίς συνδρομή του υποκειμένου τους και αφετέρου εφαρμόζεται σε περίπτωση επεξεργασίας δεδομένων που διενεργείται για σκοπούς επιστημονικούς, στατιστικούς ή ιστορικής έρευνας.

[610] Γεώργιος Ε. Πλιαβέσης, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. (repr., Αθήνα: Νομική Βιβλιοθήκη, 2019), 134.

[611] Ibid.

αξίωση προς παράλειψη της παράνομης μεταβίβασης των προσωπικών του δεδομένων στον εκδοχέα. Η εν λόγω αξίωση όμως έχει ελάχιστη σημασία, καθώς αυτός τις περισσότερες φορές λαμβάνει γνώση της παράνομης διαβίβασης αφού αυτή έχει ολοκληρωθεί.[612]

6.4 Η τήρηση των αρχών επεξεργασίας στις διαδικασίες του νόμου 4354/2015

Ο Κανονισμός περιλαμβάνει στο άρθρο 5 ορισμένες αρχές που πρέπει να διέπουν κάθε μορφή επεξεργασίας προσωπικών δεδομένων, επομένως και τη διαβίβαση τους σε τρίτους αποδέκτες, όπως είναι οι εταιρείες διαχείρισης και απόκτησης απαιτήσεων από δάνεια. Στο πεδίο που είναι υπό εξέταση, μπορούν να βρουν εφαρμογή κυρίως η αρχή της αναγκαιότητας και η αρχή της ακρίβειας κατά την τήρηση των δεδομένων.

Οι τράπεζες, στο πλαίσιο των συναλλακτικών τους σχέσεων με τους δανειολήπτες πελάτες τους, συλλέγουν πλήθος προσωπικών δεδομένων που τους αφορούν και διαθέτουν μια σφαιρική εικόνα της περιουσιακής και οικονομικής τους κατάστασης. Ωστόσο, βάσει του άρθρου 5 παρ. 1 γ' του Κανονισμού 2016/679, η επεξεργασία των προσωπικών δεδομένων δεν πρέπει να υπερβαίνει την έκταση εκείνη που είναι αναγκαία για την επίτευξη των σκοπών της συγκεκριμένης επεξεργασίας. Αυτό προκύπτει και από το συνδυασμό του άρθρου 1 παρ. 21 του νόμου 4354/2015 με την αιτιολογική έκθεση του νόμου («γενικό μέρος» αιτ. έκθεσης) που κάνουν λόγο για άρση του επαγγελματικού απορρήτου και ανακοίνωση των προσωπικών δεδομένων μόνο στο μέτρο που είναι αναγκαίο για τους σκοπούς της μεταβίβασης των απαιτήσεων.

Στην περίπτωση της ανάθεσης διαχείρισης ή εκχώρησης «κόκκινων» (ή μη) δανείων επιτρέπεται να διαβιβάζονται στον «διαχειριστή» ή τον εκδοχέα μόνο τα απολύτως απαραίτητα δεδομένα για την ενάσκηση των μεταβιβαζόμενων απαιτήσεων. Είναι για παράδειγμα, προφανές ότι στοιχεία που έχει συλλέξει η τράπεζα και αφορούν το όνομα και τον αριθμό των τέκνων του οφειλέτη δεν πρέπει σε καμία περίπτωση να ανακοινώνονται στον εκδοχέα. Το ίδιο ισχύει κατά κανόνα λ.χ. προκειμένου για ευμενή οικονομικά στοιχεία του οφειλέτη (π.χ. στοιχεία που αφορούν την ύπαρξη πιστωτικής κάρτας ή άλλης πιστωτικής σύμβασης η οποία εξυπηρετείται κανονικά). Τα τραπεζικά ιδρύματα οφείλουν γενικότερα να είναι ιδιαίτερα φειδωλά στη διαβίβαση περισσότερο «προσωπικών» πληροφοριών του οφειλέτη, καθώς και κάθε στοιχείου που δεν συνδέεται άμεσα με τη συγκεκριμένη μεταβιβαζόμενη πίστωση και τις εξασφαλίσεις αυτής. Μπορεί μάλιστα να υποστηριχθεί ότι ακόμη και η έκταση των διαβιβαζόμενων οικονομικών πληροφοριών που συνδέονται άμεσα με τη μεταβιβαζόμενη απαίτηση πρέπει να εξαρτάται και από το πόσο δυσχερής προβλέπεται να είναι η απαίτηση αυτής. Επί παραδείγματι, το τραπεζικό ίδρυμα δεν έχει λόγο να μεταβιβάσει στην εκάστοτε εταιρεία διαχείρισης στοιχεία που αφορούν τις τραπεζικές καταθέσεις του πελάτη της, εφόσον για το δάνειο έχουν συσταθεί επαρκείς εμπράγματες εξασφαλίσεις.[613]

Με βάση την αρχή της αναγκαιότητας, εγκαθιδρύεται μια ακόμα υποχρέωση της τράπεζας, που αφορά αποκλειστικά το στάδιο των διαπραγματεύσεων προτού συντελεστεί η μεταβίβαση των δανείων. Κατά το στάδιο αυτό, η τράπεζα πρέπει να προχωρά σε παράδοση των προσωπικών και οικονομικών δεδομένων των δανειοληπτών στην εταιρεία που σκοπεύει να αποκτήσει τα δάνεια,

---

[612] Απόστολος Γεωργιάδης, "Η Μεταβίβαση «Κόκκινων» Δανείων από τις Τράπεζες και η Προστασία Προσωπικών Δεδομένων του Δανειολήπτη", σε *Συλλογικό Έργο, Τιμητικός Τόμος, Νικολάου Θ. Νίκα*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Σάκκουλα, 2018), 164.
[613] Ibid., 165.

σε «ανώνυμη» ή κρυπτογραφημένη μορφή, για να αποτραπεί η ταυτοποίηση του οφειλέτη. Αυτό συμβαίνει γιατί ο «διαχειριστής» ή εκδοχέας των απαιτήσεων δεν χρειάζεται να έχει γνώση της ταυτότητας του οφειλέτη, αλλά αρκεί να γνωρίζει το περιεχόμενο και τα χαρακτηριστικά των απαιτήσεων που πρόκειται να μεταβιβαστούν.[614]

Σύμφωνα με τα άρθρα 5 παρ. 1 δ' και 16 του Κανονισμού 2016/679 η τράπεζα θα πρέπει να καταβάλλει την απαιτούμενη επιμέλεια, ώστε τα προσωπικά δεδομένα των οφειλετών που βρίσκονται στην κατοχή της να είναι ακριβή, δηλαδή να ανταποκρίνονται στην πραγματικότητα. Επίσης, θα πρέπει να διατηρεί αυτά ενημερωμένα, δηλαδή να διορθώνει αυτά κάθε φορά που σημειώνεται κάποια αλλαγή σε αυτά. Ιδίως, η τράπεζα οφείλει να επιβεβαιώνει τα στοιχεία της οφειλής και να έχει προβεί, στο μέτρο του δυνατού, σε επικαιροποίηση των προσωπικών πληροφοριών των οφειλετών, προτού διαβιβάσει αυτές στον εκδοχέα.[615] Σε περίπτωση που η τράπεζα (ή η εταιρεία που έχει αποκτήσει τις απαιτήσεις) παραβιάσει τις προαναφερθείσες υποχρεώσεις της, η Αρχή έχει τη δυνατότητα, κατόπιν υποβολής καταγγελίας, να επιβάλει τη διακοπή της συλλογής ή την καταστροφή του συγκεκριμένου αρχείου προσωπικών δεδομένων.

Τέλος, με απώτερο στόχο την προστασία των δανειοληπτών, μπορεί να αξιοποιηθούν και οι υποχρεώσεις που επιβάλλονται σε κάθε υπεύθυνο επεξεργασίας βάσει των άρθρων 5 παρ. 1 στ', 24 επ. και 32 επ. του Κανονισμού. Ειδικότερα, η τράπεζα και ο εκδοχέας πρέπει να μεριμνούν ώστε κάθε επεξεργασία και διαβίβαση των προσωπικών δεδομένων να γίνεται από περιορισμένο κύκλο προσώπων (π.χ. να μην υπάρχει διασπορά σε μεγάλο αριθμό υπαλλήλων), τα οποία διαθέτουν επαγγελματικά προσόντα που είναι σε θέση να παράσχουν κατάλληλες εγγυήσεις για την τήρηση του απορρήτου. Επιπροσθέτως, οφείλουν να προχωρούν στη λήψη όλων των απαραίτητων τεχνικών και οργανωτικών μέτρων, για να αποτρέπεται η ενδεχόμενη υποκλοπή και περαιτέρω διάδοση των προσωπικών δεδομένων των οφειλετών.[616]

[614] Ibid.
[615] Ibid.
[616] Ibid., 166.

ΜΕΡΟΣ Γ'

ΕΒΔΟΜΟ ΚΕΦΑΛΑΙΟ
Η ΧΡΗΣΗ ΥΠΗΡΕΣΙΩΝ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ (CLOUD COMPUTING) ΑΠΟ ΤΑ ΧΡΗΜΑΤΟΠΙΣΤΩΤΙΚΑ ΙΔΡΥΜΑΤΑ

7.1 Εισαγωγικές παρατηρήσεις

Τα τελευταία χρόνια, οι υπηρεσίες υπολογιστικού νέφους (***cloud computing***) αποτελούν το τεχνολογικό εργαλείο που επιτρέπει την ανάπτυξη καινοτόμων υπηρεσιών. Η υπολογιστική νέφους επιτρέπει στις τραπεζικές επιχειρήσεις να αξιοποιήσουν νέα επιχειρηματικά μοντέλα, κάνοντας χρήση της τεχνολογικής της προόδου για την παροχή νέων και βελτιωμένων υπηρεσιών στους πελάτες, μέσω της βελτίωσης της παραγωγικότητας, της αποδοτικότητας και της ευελιξίας των εσωτερικών επιχειρηματικών διεργασιών. Σε τελική ανάλυση, οι τεχνολογίες υπολογιστικής νέφους μπορούν να αποτελέσουν το θεμέλιο για τον ψηφιακό μετασχηματισμό της χρηματοπιστωτικής βιομηχανίας.

Ο χρηματοπιστωτικός τομέας βρίσκεται στη διαδικασία υιοθέτησης των τεχνολογιών υπολογιστικής νέφους ώστε να εκμεταλλευτεί τα προαναφερθέντα πλεονεκτήματα. Οι νέες ευκαιρίες για την παροχή υπηρεσιών στους πελάτες, εξυπηρετώντας τις ανάγκες και τις προσδοκίες τους, είναι εξίσου σχετικές με την βελτίωση της ασφάλειας, την μείωση του κόστους και την ευελιξία κατά τη διεξαγωγή των επιχειρηματικών διεργασιών. Οι τεχνολογίες υπολογιστικής νέφους έχουν επίσης τη δυνατότητα να ανοίξουν νέες αγορές και να δώσουν την ευκαιρία στους «ώριμους» χρηματοπιστωτικούς θεσμούς να βρουν νέους τρόπους ώστε να ανταγωνιστούν τις νεοεισερχόμενες στην αγορά επιχειρήσεις χρηματοοικονομικής τεχνολογίας (***fintech companies***). Ωστόσο, η υιοθέτηση των τεχνολογιών υπολογιστικού νέφους από την χρηματοπιστωτική βιομηχανία θα πρέπει να προχωρήσει λαμβάνοντας υπόψιν την υψηλά διαρρυθμισμένη φύση του τομέα αυτού και δίνοντας εξέχουσα σημασία στην σταθερότητα και την ασφάλεια. Οι ευρωπαϊκές τράπεζες λειτουργούν εντός ενός πλαισίου οικονομικών κανόνων που στοχεύουν στην διασφάλιση της ορθής διακυβέρνησης και του ελέγχου των κινδύνων (**οδηγίες εσωτερικής διακυβέρνησης - internal governance guidelines**), ειδικά στις περιπτώσεις όπου τρίτα μέρη εμπλέκονται στη λειτουργία συστημάτων που βασίζονται στις τεχνολογίες πληροφορικής και επικοινωνιών (**Information and communication technologies - ICT**).[617]Οι κανόνες αυτοί θέτουν το πλαίσιο για την εποπτική εμπλοκή με τις ευρωπαϊκές τράπεζες καθ' όλη τη διάρκεια ζωής της σχέσης που βασίζεται στις τεχνολογίες υπολογιστικού νέφους στον ενωσιακό χρηματοπιστωτικό τομέα.

Τα ειδικότερα χαρακτηριστικά των τεχνολογιών υπολογιστικής νέφους στο πλαίσιο εφαρμογής τους στον χρηματοπιστωτικό τομέα απαιτούν ιδιαίτερη προσοχή και δέουσα εξέταση. Η συνεχής και ταχύτατη εξέλιξη του περιβάλλοντος των υπηρεσιών υπολογιστικής νέφους καθώς και η στενή διάδραση των ευρωπαϊκών τραπεζών με τις επιβλέπουσες αρχές, απαιτεί μια συστηματική

[617] EBA Guidelines on ICT and security risk management (under development): https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management.

προσέγγιση και μια αρμονική κατανόηση των τεχνολογιών νέφους στον ενωσιακό χώρο, ώστε να ενθαρρυνθεί η υιοθέτηση των δημοσίων/υβριδικών νεφών και η χρήση πολύπλευρων τεχνολογιών υπολογιστικής νέφους από τις ευρωπαϊκές τράπεζες με έναν πιο ενιαίο τρόπο.

Το κεφάλαιο αυτό εστιάζει στην πιθανή επίδραση των τεχνολογιών υπολογιστικής νέφους για την βιομηχανία παροχής χρηματοπιστωτικών υπηρεσιών εξετάζοντας το τρέχων πλαίσιο και διερευνώντας τις ποικίλες θεωρήσεις που συνδέονται με την υιοθέτηση των υπηρεσιών υπολογιστικής νέφους. Παράλληλα, εξετάζονται οι κίνδυνοι που μπορούν να αντιμετωπίσουν οι διαχειριστές των συστημάτων υπολογιστικής νέφους αλλά και οι πελάτες αυτών, οι οποίοι υποχρεώνονται να διατηρήσουν ακέραια την ασφάλεια των δεδομένων των πελατών τους τα οποία αποθηκεύονται στα συστήματα αυτά.

7.2 Θεωρητικό πλαίσιο του υπολογιστικού νέφους (Cloud Computing)

Κατά τη διάρκεια της τελευταίας δεκαετίας, η χρήση των υπηρεσιών υπολογιστικής νέφους έχει αυξηθεί σημαντικά. Με βάση τις σχετικές έρευνες που αφορούν την υιοθέτηση των τεχνολογιών υπολογιστικής νέφους μέχρι το έτος 2020, το ενενήντα τοις εκατό των εταιρειών χρησιμοποιούσαν ενεργά τις τεχνολογίες αυτές, ενώ το υπόλοιπο δέκα τις εκατό των εταιρειών σκόπευαν να υιοθετήσουν τις εν λόγω τεχνολογίες.[618]Περαιτέρω, οι εταιρείες εκτελούσαν το μεγαλύτερο μέρος των εργασιών τους και αποθήκευαν τα μισά από τα δεδομένα τους σε πλατφόρμες δημοσίου νέφους (**public cloud**).[619]Ως αποτέλεσμα, η αγορά για τις υπηρεσίες υπηρεσιών δημοσίου νέφους αυξήθηκε σημαντικά, σε πάνω από 140 δισεκατομμύρια λίρες.[620]΄Οσο η αγορά αναπτύσσεται, μια σειρά εταιρειών έχουν ηγηθεί των υπολοίπων. Ενώ οι εκτιμήσεις ποικίλουν, υπάρχει ευρεία συναίνεση ότι ο μεγαλύτερος πάροχος υπηρεσιών υπολογιστικού νέφους είναι πλέον η Amazon Web Services (AWS), ο οποίος έχει δυναμική παρουσία στην αγορά παροχής υποδομών ως υπηρεσιών (**infrastructure-as-a-service - IaaS**) που αποτελεί τύπο υπηρεσίας υπολογιστικού νέφους. Την AWS ακολουθούν η Microsoft και η Google, που συνεχώς αυξάνουν το μερίδιό τους στην αγορά, βασιζόμενες εν μέρει στην παροχή επιχειρηματικών υπηρεσιών ως υπηρεσία (**Software as a Service - SaaS**). Οι εταιρείες αυτές έχουν αποκτήσει και ανταγωνισμό από τις κινέζικες εταιρείες Alibaba και Tencent, οι οποίες έχουν ισχυρή παρουσία στην αγορά της Κίνας.[621]

Παρά την ανάπτυξη της αγοράς αυτής, ο όρος «υπολογιστική νέφους» συνεχίζει να δημιουργεί σύγχυση και αβεβαιότητα, ειδικά σε σχέση με τις πολύπλοκες υποβόσκουσες τεχνικές και εμπορικές διευθετήσεις. Πράγματι, η «υπολογιστική νέφους», συχνά αντιμετωπίζεται ως μια σφαιρική έννοια. Ο όρος όμως εμπεριέχει μια σειρά διαφορετικών πραγμάτων. Στην πιο απλή της μορφή, η υπολογιστική νέφους αποτελεί ένα τρόπο για την παράδοση υπολογιστικών πόρων ως

---

[618] Flexera, 'State of the Cloud Report 2020' (2020) <https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020> accessed 10 January 2022 (εφεξής Flexera, 'State of the Cloud 2020').
[619] Ibid., no 1.
[620] Σύμφωνα με έρευνα της Gartner, η παγκόσμια αγορά για υπηρεσίες δημοσίου νέφους υπολογίστηκε ότι ανέρχεται σε ποσό της τάξεως των 140 δις λιρών κατά το έτος 2018 και σύμφωνα με υπολογισμούς θα αυξανόταν κατά 19% κατά το έτος 2019. Gartner, 'Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019' (2019)
https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwidepublic-cloud-revenue-to-g, accessed 7 October 2020.
[621] Christopher J Millard, *Cloud Computing Law*, 2nd ed. (repr., Oxford, United Kingdom: Oxford University Press, 2021), 26.

υπηρεσία ωφέλειας μέσω ενός δικτύου, συχνότερα του διαδικτύου, ενώ ως υπηρεσία είναι κλιμακούμενη από κάτω προς τα πάνω και αντιστρόφως, ανάλογα με τις απαιτήσεις των χρηστών. Η παροχή των υπηρεσιών υπολογιστικού νέφους συχνά εξαρτάται από πολύπλοκες, πολυεπίπεδες διευθετήσεις ανάμεσα στους διαφορετικούς παρόχους παροχής των εν λόγω υπηρεσιών. Οι χρεώσεις για τους παρόχους αυτούς, εάν υπάρχουν, συχνά είναι ανάλογες με τους πόρους που χρησιμοποιούνται.[622]Συνεπώς, το νέφος μπορεί να αποδειχτεί σαν καινοτομία εξίσου επαναστατική όπως η εμφάνιση του φτηνού κατά παραγγελία ηλεκτρισμού πριν έναν αιώνα. Οι υπολογιστικοί πόροι κυμαίνονται από την «ωμή» επεξεργαστική ισχύ και αποθήκευση, που προσφέρεται μέσω εξυπηρετητών και μονάδων αποθήκευσης, έως τα πλήρη πακέτα εφαρμογών λογισμικού. Οι πελάτες μπορούν να «μισθώσουν» υπολογιστικούς πόρους από τρίτα μέρη όταν παρουσιάζεται η ανάγκη, αντί να προβαίνουν στην αγορά ιδιόκτητων, μετατρέποντας έτσι τα έξοδα κεφαλαίου σε λειτουργικά έξοδα («**turning capex to opex**»).

Στο παρών κεφάλαιο, γίνεται αναφορά στους οργανισμούς ή στα άτομα που εισέρχονται σε συμβατικές σχέσεις με παρόχους υπηρεσιών νέφους για τη χρήση των υπηρεσιών αυτών ως «πελάτες». Επίσης, γίνεται αναφορά στα άτομα που χρησιμοποιούν μια υπηρεσία νέφους, ανεξαρτήτως εάν αποτελούν συμβατικά μέρη ως «τελικούς χρήστες» ή «χρήστες». Η χρήση των όρων αυτών όμως δεν είναι αποκλειστική. Για παράδειγμα, σε περιπτώσεις στις οποίες ένα άτομο κάνει χρήση μια υπηρεσίας νέφους σε ιδιωτικό πλαίσιο, η έννοια του πελάτη και του χρήστη θα ταυτίζονται. Σε άλλες περιπτώσεις, για παράδειγμα όταν μια υπηρεσία νέφους χρησιμοποιείται στο πλαίσιο εργασιακής σχέσης, ο εργοδότης μπορεί να είναι ο πελάτης του παρόχου υπηρεσιών νέφους και οι εργαζόμενοι του οι χρήστες της υπηρεσίας αυτής.

Εξετάζοντας την τεχνολογία υπολογιστικού νέφους με πιο τεχνικούς όρους, συμπεραίνουμε ότι η τεχνολογία αυτή συνεπάγεται την απομακρυσμένη (δικτυωμένη) πρόσβαση σε συστήματα και πόρους. Στο πλαίσιο αυτό, οι πελάτες που κάνουν χρήση των υπηρεσιών αυτών, μπορούν να εκτελούν ή να χρησιμοποιούν, για παράδειγμα, μέσω περιηγητών (web browsers), ή μέσω άλλων εφαρμογών, όπως εφαρμογών τηλεφωνίας, το λογισμικό ή τις υπηρεσίες που είναι εγκατεστημένες σε απομακρυσμένους εξυπηρετητές διαμέσω του διαδικτύου. Αυτό σημαίνει ότι οι συσκευές που χαρακτηρίζονται από περιορισμένους πόρους, όπως τα κινητά τηλέφωνα, οι ταμπλέτες αλλά και οι συσκευές του διαδικτύου των πραγμάτων (**Internet of Things – IoT devices**), συχνά αλληλεπιδρούν με υπηρεσίες νέφους για να μοχλεύσουν υπολογιστικούς πόρους, ή για να ενσωματωθούν σε ευρύτερα συστήματα.[623]

7.2.1 Ορισμοί του υπολογιστικού νέφους

Ο όρος «υπολογιστική νέφους» έχει οριστεί με πολλούς διαφορετικούς τρόπους από επιχειρήσεις ανάλυσης, ακαδημαϊκούς ερευνητές, επαγγελματίες του χώρου αλλά και εταιρείες πληροφορικής. Ειδικότερα, η εταιρεία τεχνολογικών ερευνών «Gartner, Inc» έχει προσδιορίσει την υπολογιστική

---

[622] Οι χρεώσεις χρήσεως των υπηρεσιών μπορούν να υπολογιστούν ανά χρήστη, σε μηνιαία βάση. Υπάρχουν όμως και εναλλακτικά μοντέλα. Για παράδειγμα, το νέφος της IBM, χρεώνει τους χρήστες ανάλογα με τους πόρους που χρησιμοποιούνται, συμπεριλαμβανομένων των μνημών και των χώρων αποθήκευσης. IBM, 'How you're Charged' https://cloud.ibm.com/docs/billing-usage?topic=billing-usage-charges.

[623] Christopher J Millard, *Cloud Computing Law*, 2nd ed. (repr., Oxford, United Kingdom: Oxford University Press, 2021), 27.

νέφους ως «ένα τύπο υπολογιστικής εντός του οποίου παρέχονται εξαιρετικά κλιμακούμενες δυνατότητες που σχετίζονται με την πληροφορική, ως υπηρεσία, κάνοντας χρήση των διαδικτυακών τεχνολογιών σε πολλαπλούς εξωτερικούς πελάτες». Με την σειρά της η Ομάδα 451 («**The 451 Group**») προσδιόρισε την τεχνολογία υπολογιστικής νέφους ως «ένα μοντέλο παροχής υπηρεσιών που συνδυάζει μια γενικότερη οργανωτική αρχή για την παροχή πληροφορικών υπηρεσιών, εξαρτημάτων υποδομών, μια αρχιτεκτονική προσέγγιση αλλά και ένα οικονομικό μοντέλο και γενικότερα μια συμβολή υπολογιστικής δικτύου, εικονικής παρουσίασης, υπολογιστικής ωφέλειας, φιλοξενίας και λογισμικού ως υπηρεσία».

Source	Definition
Gartner	"a style of computing in which massively scalable IT-related capabilities are provided "as a service" using Internet technologies to multiple external customers" (Gartner 2008b)
IDC	"an emerging IT development, deployment and delivery model, enabling real-time delivery of products, services and solutions over the Internet (i.e., enabling cloud services)" (Gens 2008)
The 451 Group	"a service model that combines a general organizing principle for IT delivery, infrastructure components, an architectural approach and an economic model – basically, a confluence of grid computing, virtualization, utility computing, hosting and software as a service (SaaS)" (Fellows 2008)
Merrill Lynch	"the idea of delivering personal (e.g., email, word processing, presentations.) and business productivity applications (e.g., sales force automation, customer service, accounting) from centralized servers" (Merrill Lynch 2008)

Εικόνα 2. Ορισμοί υπολογιστικής νέφους από εταιρείες ανάλυσης

Όλοι οι ανωτέρω ορισμοί έχουν ένα κοινό χαρακτηριστικό: επιχειρούν να περιγράψουν και να καθορίσουν την υπολογιστική νέφους από τη σκοπιά των τελικών χρηστών και εστιάζουν στον τρόπο με τον οποίο αυτοί βιώνουν την χρήση της τεχνολογίας αυτής. Σύμφωνα με τους ορισμούς αυτούς, το κύριο χαρακτηριστικό της υπολογιστικής νέφους είναι η παροχή υποδομών πληροφορικής και εφαρμογών ως υπηρεσία με τρόπο κλιμακούμενο.

Ο ορισμός της υπολογιστικής νέφους έχει επίσης προκαλέσει αντιπαραθέσεις και ανάμεσα στα μέλη της επιστημονικής κοινότητας. Όπως συμβαίνει και με τον εμπορικό τύπο, υπάρχουν διαφορετικές απόψεις σχετικά με τον καθορισμό της υπολογιστικής νέφους και τα χαρακτηριστικά που την κάνουν να ξεχωρίζει. Συγκριτικά με τους ορισμούς που έχουν διατυπωθεί από τον εμπορικό τύπο, οι ορισμοί στην επιστημονική βιβλιογραφία συμπεριλαμβάνουν όχι μόνο την οπτική του τελικού χρήστη αλλά και τα αρχιτεκτονικά χαρακτηριστικά. Για παράδειγμα, το εργαστήριο RAD του Πανεπιστημίου Berkeley έχει προσδιορίσει την υπολογιστική νέφους ως εξής: «Το υπολογιστικό νέφος (Cloud Computing) αναφέρεται στις εφαρμογές που παραδίδονται ως υπηρεσίες μέσω του διαδικτύου και στα υπολογιστικά μηχανήματα (hardware) και στο λογισμικό (software) που βρίσκονται σε ένα κέντρο πληροφοριών που παρέχει αυτές τις υπηρεσίες. Οι υπηρεσίες συχνά αναφέρονται ως Λογισμικό ως Υπηρεσία (SaaS – Software as a Service). Το hardware και το software στο κέντρο πληροφοριών είναι αυτά που αποκαλούμε συχνά ως Νέφος (Cloud). Όταν ένα Νέφος είναι διαθέσιμο στο κοινό με έναν τρόπο χρονικής μίσθωσης, αυτό αποκαλείται Δημόσιο Νέφος (**Public Cloud**), ενώ οι υπηρεσίες που πωλούνται είναι επονομαζόμενες ως Υπολογιστικές Δημόσιες Υπηρεσίες (**Utility Computing**).

Χρησιμοποιούμε τον όρο Ιδιωτικό Νέφος (**Private Cloud**) για να αναφερθούμε σε εσωτερικά κέντρα πληροφοριών μιας επιχείρησης ή ενός οργανισμού, τα οποία δεν είναι διαθέσιμα στο ευρύ κοινό. Επομένως το Cloud Computing είναι το σύνολο των SaaS και του Utility Computing, αλλά δεν περιλαμβάνει το Private Cloud. Ο κόσμος μπορεί να είναι χρήστης ή πάροχος των SaaS ή χρήστης ή πάροχος του Utility Computing».[624]

Ο ορισμός αυτός συνενώνει τις διαφορετικές θεωρήσεις που αφορούν την υπολογιστική νέφους: με βάση την θεώρηση του παρόχου, το κύριο συστατικό του νέφους είναι το κέντρο δεδομένων. Το κέντρο δεδομένων περιέχει τους πόρους υλισμικού για τη διενέργεια υπολογισμών και την αποθήκευση, που από κοινού με το λογισμικό προσφέρονται με ένα τρόπο διανεμητικό (**pay - as-you – go**). Υπό την οπτική του σκοπού τους, τα νέφη ταξινομούνται σε ιδιωτικά και δημόσια. Ανεξαρτήτως του σκοπού αυτού, ένα από τα κυριότερα χαρακτηριστικά των υπολογιστικών νεφών είναι ο συγκερασμός λογισμικού και υλισμικού των συστημάτων με εφαρμογές. Ο Reese επίσης αναφέρει ότι το υπολογιστικό νέφος μπορεί να αποτελείται τόσο από λογισμικό όσο και από υποδομές και δίνει έμφαση στον τρόπο με τον οποίο μπορεί να γίνει χρήση των υπηρεσιών υπολογιστικής νέφους: «Η υπηρεσία υπολογιστικής νέφους είναι προσβάσιμη μέσω περιηγητή διαδικτύου ή μέσω διεπαφών (**API**) διαδικτυακών υπηρεσιών. Δεν απαιτείται δαπάνη κεφαλαίων για να ξεκινήσει κανείς καθώς πληρώνεις μόνο για ότι χρησιμοποιείς και καθώς χρησιμοποιείς αυτό».[625] Σύμφωνα με τον Ian Foster, το υπολογιστικό νέφος προσδιορίζεται ως «ένα ευρείας κλίμακας κατανεμητέο υπολογιστικό πρότυπο που καθοδηγείται από την οικονομία της κλίμακας, εντός του οποίου μια «δεξαμενή» αφαιρετικών, εικονικών, δυναμικά κλιμακούμενων, διαχειριζόμενης υπολογιστικής ισχύος, αποθήκευσης, πλατφόρμες και υπηρεσίες παρέχονται κατά παραγγελία σε εξωτερικούς πελάτες διαμέσω του Διαδικτύου».[626]

Οι δύο σημαντικοί παράγοντες που προστέθηκαν μέσω του ορισμού του Foster είναι η «εικονικότητα» («**virtualization**») και η δυνατότητα επέκτασης («**scalability**»). Η υπολογιστική νέφους αποσπάται από τις υποβόσκουσες υποδομές υλισμικού και το λογισμικό του συστήματος μέσω της εικονικότητας. Οι εικονικοί πόροι παρέχονται μέσω ενός καθορισμένου περιβάλλοντος διεπαφής (**Application Programming Interface – API**). Επομένως, σε επίπεδο υλισμικού οι πόροι μπορούν να προστίθενται ή να αποσύρονται σύμφωνα με την ζήτηση που υποδηλώνεται μέσω της διεπαφής, ενώ η διεπαφή αυτή για τον χρήστη δεν μεταβάλλεται. Η αρχιτεκτονική αυτή επιτρέπει την επεκτασιμότητα και την ευελιξία στο φυσικό επίπεδο του νέφους χωρίς να υπάρχουν επιπτώσεις στην διεπαφή που συναντά ο τελικός χρήστης.

Όλοι οι ανωτέρω ορισμοί υποδεικνύουν ότι η υπολογιστική νέφους είναι ένα φαινόμενο που αποτελείται από μια σειρά παραγόντων και σχετίζεται με ένα νέο παράδειγμα παροχής και ανάπτυξης της πληροφορικής (υλισμικό και εφαρμογές). Σε γενικές γραμμές, η υπολογιστική νέφους αφορά την παροχή δυνατοτήτων της πληροφορικής σε εξωτερικούς πελάτες, ή με βάση την οπτική των χρηστών, την λήψη των δυνατοτήτων αυτών από έναν εξωτερικό πάροχο, ως υπηρεσία, με έναν τρόπο κοστολόγησης ανάλογης της χρήσης και διαμέσω του Διαδικτύου.

---

[624] Santi Ristol, Katarina Stanoevska-Slabeva and Thomas Wozniak, *Grid and Cloud Computing: A Business Perspective on Technology and Applications*, 1st ed. (repr., Heidelberg: Springer, 2010), 48.
[625] George Reese, *Web Architecture and Programming in The Cloud*, 1st ed. (repr., Sebastopol, Calif.: O'Reilly Media, Inc., 2009), 2-3.
[626] Ian Foster et al., "Cloud Computing and Grid Computing 360-Degree Compared", *Grid Computing Environments Workshop*, 2008, 1, doi:10.1109/gce.2008.4738445.

Περαιτέρω, η επεκτασιμότητα και η εικονικότητα συχνά αντιμετωπίζονται ως βασικά χαρακτηριστικά της υπολογιστικής νέφους. Η επεκτασιμότητα αναφέρεται στην δυναμική προσαρμογή των προβλεπόμενων υπολογιστικών πόρων ανάλογα με το μεταβαλλόμενο φορτίο, δηλαδή στην αύξηση ή στην μείωση του αριθμού των χρηστών, την απαιτούμενη αποθηκευτική χωρητικότητα ή επεξεργαστική ισχύ. Η εικονικότητα, που θεωρείται ως ακρογωνιαίος τεχνολογικός λίθος για όλες τις αρχιτεκτονικές υπολογιστικού νέφους, χρησιμοποιείται κυρίως για την απόσπαση και την ενθυλάκωση. Η απόσπαση επιτρέπει τον συγκερασμό των «ωμών» υπολογιστικών, αποθηκευτικών και δικτυακών πόρων ως «δεξαμενή» πόρων και την δόμηση επιστρώσεων πόρων, όπως υπηρεσιών αποθήκευσης δεδομένων πάνω από αυτούς. Η ενθυλάκωση εφαρμογών εν τέλει βελτιώνει την ασφάλεια, την διαχείριση και την απομόνωση. Ένα ακόμα βασικό χαρακτηριστικό των υπολογιστικών νεφών είναι ο συγκερασμός υλισμικού και λογισμικού με τις εκάστοτε εφαρμογές. Τόσο το υλισμικό αλλά και το λογισμικό των συστημάτων, ή οι υποδομές, αλλά και οι εφαρμογές, προσφέρονται ως υπηρεσία με έναν ενιαίο τρόπο.[627]

7.2.2 Τα ουσιώδη χαρακτηριστικά του υπολογιστικού νέφους

Όπως αναφέρθηκε, υπάρχουν πέντε ουσιώδη χαρακτηριστικά της υπολογιστικής νέφους, τα οποία εξηγούν τη σχέση και τη διαφορά που υφίσταται συγκριτικά με τις παραδοσιακές υπολογιστικές μεθόδους. Τα χαρακτηριστικά αυτά καθιερώθηκαν μέσω του ορισμού του cloud computing, ο οποίος διατυπώθηκε από το Εθνικό Ινστιτούτο Τυποποιήσεων και Τεχνολογίας (***NIST – National Institute of Standards and Technology***). Το ίδρυμα αυτό είναι ευρέως γνωστό σε παγκόσμιο επίπεδο για τη δουλειά του στο πεδίο της τεχνολογίας των πληροφοριών. Σύμφωνα με το Ινστιτούτο το υπολογιστικό νέφος αποτελεί: «Ένα μοντέλο που δίνει τη δυνατότητα της συνεχούς, εύκολης και υψηλών απαιτήσεων πρόσβασης σε μια κοινόχρηστη συλλογή ρυθμιζόμενων υπολογιστικών πόρων, οι οποίοι τροφοδοτούνται και απελευθερώνονται με ελάχιστη προσπάθεια διαχείρισης και αλληλεπίδρασης παροχής υπηρεσιών».[628]

Με βάση τον ορισμό αυτό, μια «υπολογιστική δυνατότητα» θα θεωρείται ως «υπηρεσία νέφους» εφόσον έχει τα ακόλουθα χαρακτηριστικά: α) αυτό-εξυπηρέτηση κατά απαίτηση (on – demand – self – service) β) ευρεία πρόσβαση στο δίκτυο (παρέχεται ικανότητα κάλυψης δικτύου και πρόσβαση μέσω τυποποιημένων μηχανισμών), γ) διάθεση πόρων[629] (resource pooling), δ) ταχεία ελαστικότητα (οι υπηρεσίες μπορούν να παρέχονται γρήγορα και ελαστικά) ε) μετρούμενη υπηρεσία (τα συστήματα υπολογιστικής νέφους οργανώνουν και βελτιστοποιούν αυτόματα τη διάθεση πόρων παρέχοντας δυνατότητα μέτρησης των χρησιμοποιούμενων υπηρεσιών ανάλογα το είδος λ.χ. αποθήκευσης, επεξεργασίας, εύρους σύνδεσης ή διαθέσιμων λογαριασμών χρηστών).[630]

---

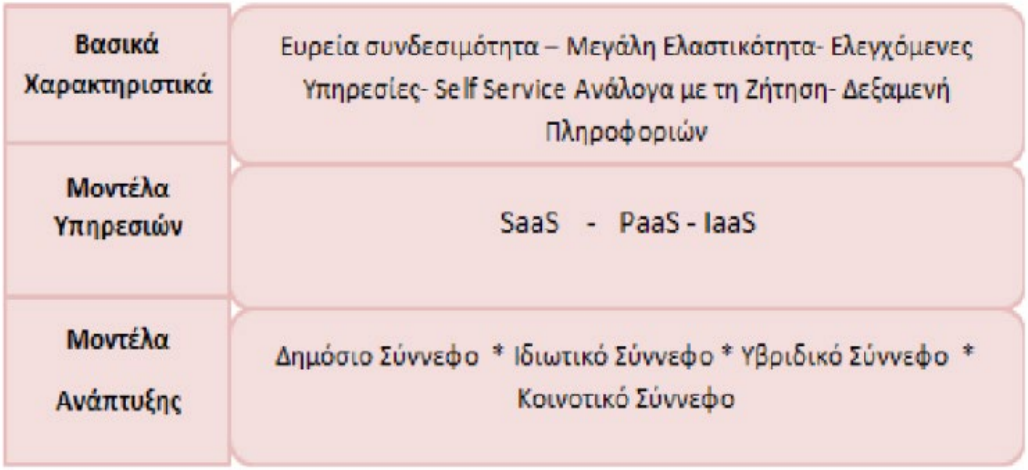
[627] Santi Ristol, Katarina Stanoevska-Slabeva and Thomas Wozniak, *Grid and Cloud Computing: A Business Perspective on Technology and Applications*, 1st ed. (repr., Heidelberg: Springer, 2010), 49-50.

[628] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, Special Publication 800-146, National Institute of Standards and Technology (NIST), May 2012, p. 2-1.

[629] Οι πόροι του παρόχου που χρησιμοποιούνται για υπολογιστικές διαδικασίες διατίθενται για να εξυπηρετούν πολλαπλούς χρήστες. Οι πόροι χρησιμοποιούν ένα μοντέλο «πολύ – ενοικιαστή» (multi – tenant model) και συνδυάζοντας δυναμικά φυσικούς και εικονικούς πόρους ανταποκρίνονται στην εκάστοτε καταναλωτική ζήτηση.

[630] Christopher J Millard, *Cloud Computing Law*, 2nd ed. (repr., Oxford, United Kingdom: Oxford University Press, 2021), 28-29.

Ο ορισμός του NIST έχει επηρεάσει και τη σχετική νομοθεσία. Για παράδειγμα, η Οδηγία (ΕΕ) 2016/1148 (**NIS Directive**) υιοθέτησε μια παρόμοια προσέγγιση με το NIST κάνοντας αναφορά στις «υπηρεσίες υπολογιστικής νέφους ως εξής: «ο όρος υπηρεσίες νεφουπολογιστικής καλύπτει τις υπηρεσίες που επιτρέπουν την πρόσβαση σε κλιμακοθετήσιμο και ελαστικό σύνολο κοινόχρηστων υπολογιστικών πόρων».[631]



Εικόνα 3. Απεικόνιση ορισμού υπολογιστικού νέφους

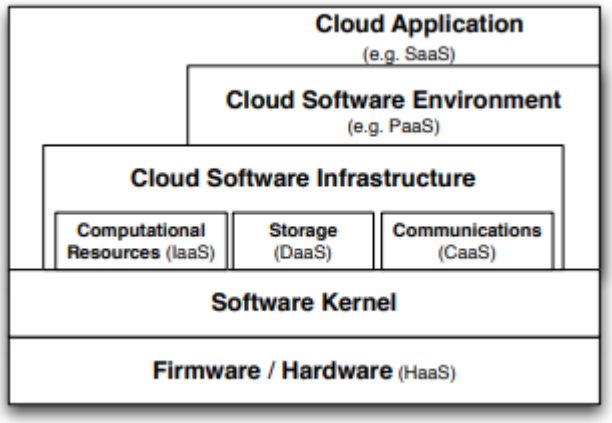
7.3 Αρχιτεκτονική και μοντέλα του υπολογιστικού νέφους

Κατά την εξέταση της αρχιτεκτονικής και της δομής των υπηρεσιών της νεφουπολογιστικής είναι δυνατόν να εντοπιστούν πολλαπλές έννοιες που αφορούν τις δομές αυτές. Αρχικά, οι ταξινομήσεις αυτές φαίνονται να διαφέρουν η μια από την άλλη σε σημαντικό βαθμό. Τελικά, όμως, κατατάσσουν και περιγράφουν το ίδιο φαινόμενο και μοιράζονται έναν κοινό παρονομαστή.

Ειδικότερα, η Menken παρέχει μια πολύ αναλυτική εννοιολόγηση που αποτελείται από επτά κύρια συστατικά της υπολογιστικής νέφους και συγκεκριμένα από την εφαρμογή, τον πελάτη, την υποδομή, την πλατφόρμα, την υπηρεσία, την αποθήκευση και την υπολογιστική ισχύ.[632] Ο Miller με τη σειρά του εξετάζει του «διαφορετικούς τρόπους μέσω των οποίων μια επιχείρηση μπορεί να αξιοποιήσει την υπολογιστική νέφους για να αναπτύξει τις δικές τις επιχειρηματικές εφαρμογές», και κάνει διάκριση ανάμεσα σε τέσσερεις τύπους ανάπτυξης των υπηρεσιών υπολογιστικής νέφους: α) το λογισμικό ως υπηρεσία (**Software as a Service**), β) την πλατφόρμα ως υπηρεσία (**Platform as a Service**), γ) τις διαδικτυακές υπηρεσίες (**Web Services**) και δ) την υπολογιστική κατά παραγγελία (**On demand computing**).[633] Ο Miller επίσης αναφέρει ότι η υπολογιστική κατά

[631] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[632] Ivanka Menken and Gerard Blokdijk, *Cloud Computing - Complete Cornerstone Guide to Cloud Computing Best Practices*, 2nd ed. (repr., London, United Kingdom: Emereo Pty Ltd, 2009), 36.
[633] Michael Miller, *Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online*, 1st ed. (repr., Indianapolis, Ind.: Que Publishing, 2009), 40-41.

παραγγελία χαρακτηρίζεται και ως υπολογιστική ωφέλειας (**utility computing**).[634] Η Youseff με τη σειρά της διακρίνει πέντε επίπεδα της υπολογιστικής νέφους: α) το επίπεδο της εφαρμογής του νέφους (**cloud application**), β) το επίπεδο του περιβάλλοντος του λογισμικού του νέφους (**cloud software environment**), γ) το επίπεδο της υποδομής του λογισμικού (**cloud software infrastructure**), δ) το επίπεδο του πυρήνα του λογισμικού (**software kernel**) και ε) το επίπεδο του σταθερισμικού/υλισμικού (**firmware/hardware**).[635]



Εικόνα 4. Η προτεινόμενη από τη Youseff οντολογία του υπολογιστικού νέφους

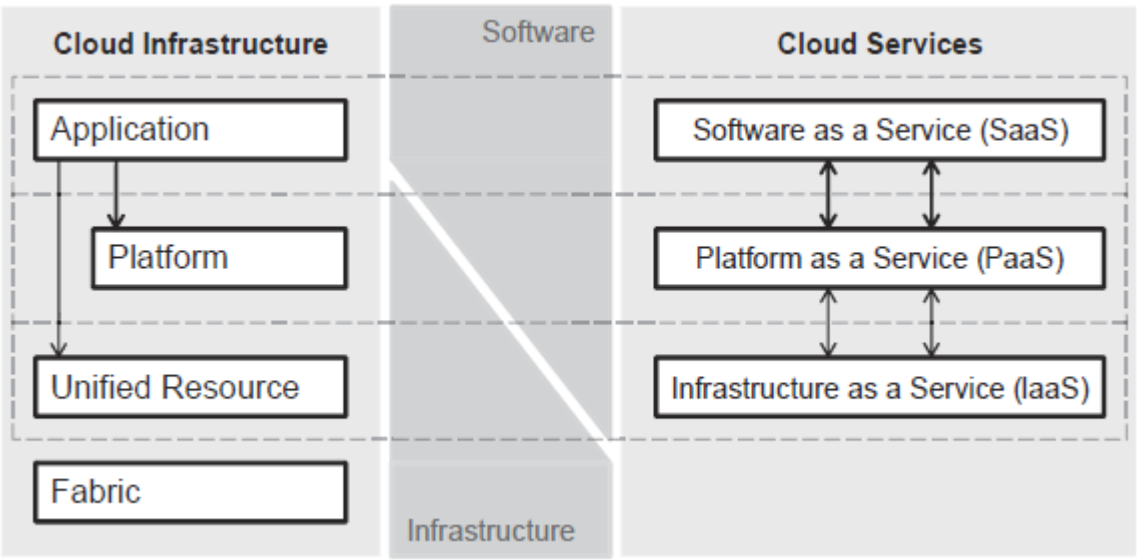
Όλες οι προαναφερθείσες εννοιολογήσεις είναι αρκετά λεπτομερείς και έχουν επηρεαστεί από συγκεκριμένες θεωρήσεις των υπολογιστικών νεφών των συγγραφέων που τις έχουν διατυπώσει. Κάποιες εννοιολογήσεις επίσης συμπεριλαμβάνουν παράγοντες όπως τα ιδιωτικά νέφη (private clouds) και περιέχουν διαφορετικά επίπεδα λεπτομέρειας για συστατικά που συνθέτουν μια λογική οντότητα.[636] Λαμβάνοντας υπόψιν τα δεδομένα αυτά, οι εννοιολογήσεις αυτές δεν παρέχουν μια αρκούντως γενική περιγραφή της δομής των υπολογιστικών νεφών και των συστατικών τους στοιχείων. Για το λόγο αυτό έχει επικρατήσει μια εννοιολόγηση που περιλαμβάνει τρία δομικά επίπεδα των υπολογιστικών νεφών.

Οι ορισμοί για τους οποίους έγινε λόγος παραπάνω, υποδεικνύουν ότι η υπολογιστική νέφους ενέχει διαφορετικές υπολογιστικές δυνατότητες και συγκεκριμένα αυτές που αφορούν τις υποδομές, τις πλατφόρμες και το λογισμικό. Αυτές μπορεί να αναφέρονται και ως διαφορετικά «σχήματα», «κομμάτια», «στιλ», «τύποι», «επίπεδα», ή «στρώματα» της υπολογιστικής νέφους. Αντί επομένως να γίνεται λόγος για «δυνατότητες», προτιμότερο είναι να εξετάζουμε τα διαφορετικά «επίπεδα» καθώς οι υποδομές, οι πλατφόρμες και το λογισμικό δομούνται σε διαδοχικά επίπεδα και είναι λογικά συνδεδεμένα ως διαφορετικά επίπεδα σε μια αρχιτεκτονική

[634] Ibid.
[635] Lamia Youseff, Maria Butrico and Dilma Da Silva, "Toward A Unified Ontology of Cloud Computing", *Grid Computing Environments Workshop*, 2008, 3-4, doi:10.1109/gce.2008.4738443.
[636] George Reese, *Web Architecture and Programming in The Cloud*, 1st ed. (repr., Sebastopol, Calif.: O'Reilly Media, Inc., 2009), 2-3.

νέφους. Ανεξαρτήτως της ορολογίας που χρησιμοποιείται, αυτή η τριμερής ταξινόμηση της υπολογιστικής νέφους έχει επικρατήσει στους ακαδημαϊκούς και επιχειρηματικούς κύκλους.

Επομένως, υπάρχουν τρία μοντέλα υπηρεσίας νέφους και τρεις θεμελιώδεις κατηγορίες οι οποίες συχνά αναφέρονται και ως «μοντέλο SPI» (Software, Platform or Infrastructure as a service – Λογισμικό, Πλατφόρμα ή Δομή μιας υπηρεσίας). Η πρώτη αποτελεί την υποδομή νέφους ως υπηρεσία (SaaS), και δίνεται ως δυνατότητα στους καταναλωτές που εφοδιάζει αυτούς με λειτουργίες επεξεργασίας, αποθήκευσης, δικτύωσης, και άλλους θεμελιώδεις υπολογιστικούς πόρους στους οποίους ο χρήστης μπορεί να αναπτύξει και να εκτελέσει οποιασδήποτε μορφής λογισμικού, όπως λειτουργικά συστήματα ή προγράμματα. Χαρακτηριστικό παράδειγμα αποτελεί το «Elastic Compute Cloud» (EC2) των διαδικτυακών υπηρεσιών της Amazon (AWS), το οποίο πουλάει 1.0 GHz x 86 ISA «κομμάτια» στην τιμή των $ 0.10 ανά ώρα και αν επιθυμεί ο χρήστης μπορεί να προσθέσει επιπλέον «κομμάτια» που προστίθενται ενός 2 με 5 λεπτών. Η Amazon προσφέρει επίσης την υπηρεσία αποθήκευσης «Simple Storage Service» (S3) ενώ η υπηρεσία της «Joyent» παρέχει μια υψηλά κλιμακούμενη κατά παραγγελία υποδομή για την εκτέλεση ιστοσελίδων και εφαρμογών δικτύου. Οι πάροχοι υπηρεσιών πλατφόρμας ως υπηρεσία (PaaS) και λογισμικού ως υπηρεσία (SaaS) μπορούν να χρησιμοποιήσουν τις παροχές υποδομών νέφους ως υπηρεσία (IaaS) οι οποίες βασίζονται σε τυποποιημένες διεπαφές. Αντί να πωλούν υποδομές υλισμικού, οι πάροχοι υποδομών νέφους ως υπηρεσία προσφέρουν συνήθως εικονικές υποδομές ως υπηρεσία. Μέσω της εικονικότητας, οι πόροι στο επίπεδο του υλισμικού αποσπώνται και ενθυλακώνονται και επομένως μπορούν να εκτεθούν στο ανώτερο επίπεδο και στους τελικούς χρήστες μέσω μιας τυποποιημένης διεπαφής ως ενοποιημένοι πόροι με τη μορφή υποδομών νέφους ως υπηρεσία.[637]



Εικόνα 5. Αρχιτεκτονική υπολογιστικού νέφους σχετιζόμενη με τις υπηρεσίες νέφους (πηγή: Cloud Security Alliance, 2009)

[637] Santi Ristol, Katarina Stanoevska-Slabeva and Thomas Wozniak, *Grid and Cloud Computing: A Business Perspective on Technology and Applications*, 1st ed. (repr., Heidelberg: Springer, 2010), 52-53.

Συγκριτικά με τις πρώιμες παροχές των υπολογιστικών δημοσίων υπηρεσιών (***utility computing***), η παροχή υποδομών ως υπηρεσία νέφους υποδηλώνει την εξέλιξή του προς μια ενοποιημένη υποστήριξη και για τα τρία επίπεδα (IaaS, PaaS, SaaS) εντός του υπολογιστικού νέφους. Ήδη από την εποχή παροχής των δημοσίων υπολογιστικών υπηρεσιών, κατέστη σαφές ότι για να επιτύχουν οι πάροχοι των υπηρεσιών αυτών, θα έπρεπε να παρέχουν μια διεπαφή που είναι εύκολα προσβάσιμη, κατανοητή και εύχρηστη. Επίσης θα έπρεπε να χρησιμοποιεί διεπαφή προγράμματος εφαρμογής (API) που θα επέτρεπε την εύκολη ενσωμάτωση με τις υποδομές των πιθανών πελατών και των πιθανών προγραμματιστών των εφαρμογών λογισμικού ως υπηρεσία (SaaS). Ως συνέπεια της απαίτησης για μια εύκολη και αποσπώμενη πρόσβαση στο φυσικό επίπεδο του υπολογιστικού νέφους, η εικονικότητα του φυσικού επιπέδου και οι προγραμματιστικές πλατφόρμες για τους προγραμματιστές αναδύθηκαν ως κύρια χαρακτηριστικά των υπολογιστικών νεφών. [638]

Το δεύτερο επίπεδο αφορά το μοντέλο της πλατφόρμας νέφους ως υπηρεσία (**Platform as a Service – PaaS**). Οι πλατφόρμες αποτελούν ένα επίπεδο απόσπασης ανάμεσα στις εφαρμογές λογισμικού και στις εικονικές υποδομές. Οι παροχές του μοντέλου αυτού έχουν ως στόχο τους φορείς ανάπτυξης λογισμικού. Οι φορείς ανάπτυξης λογισμικού μπορούν να «γράψουν» τις εφαρμογές τους σύμφωνα με τις προδιαγραφές μιας συγκεκριμένης πλατφόρμας χωρίς να ανησυχούν για τις υποβόσκουσες υποδομές υλισμικού (IaaS). Οι φορείς αυτοί μεταφορτώνουν τον κώδικα της εφαρμογής τους σε μια πλατφόρμα, η οποία συνήθως διαχειρίζεται την αυτόματη κλιμάκωση (upscaling) όταν η χρήση της εφαρμογής αυξάνεται. Οι παροχές του μοντέλου αυτού μπορούν να καλύψουν όλες τις φάσεις της ανάπτυξης λογισμικού ή μπορεί να εξειδικεύονται σε ένα συγκεκριμένο πεδίο, όπως το πεδίο της διαχείρισης περιεχομένου. Παραδείγματα αποτελούν η μηχανή εφαρμογών της Google (**Google App Engine**), που επιτρέπει στις εφαρμογές να εκτελεστούν στις υποδομές της Google και η πλατφόρμα Force.com της Salesforce. Το επίπεδο PaaS ενός υπολογιστικού νέφους βασίζεται στην τυποποιημένη διεπαφή του επιπέδου IaaS, η οποία καθιστά εικονική την πρόσβαση στους απαραίτητους πόρους και παρέχει τις τυποποιημένες διεπαφές καθώς και μια πλατφόρμα ανάπτυξης για το επίπεδο SaaS του νέφους.[639]

Το επίπεδο που αφορά το λογισμικό νέφους ως υπηρεσία (SaaS) αφορά το λογισμικό που παραδίδεται και διαχειρίζεται απομακρυσμένα από έναν ή περισσότερους παρόχους και συνήθως προσφέρεται μέσω ενός μοντέλου πληρωμής ανάλογα με τη χρήση (pay – per – use manner). Το επίπεδο αυτό αποτελεί το πιο ορατό επίπεδο στη δομή των υπολογιστικών νεφών για τους τελικούς χρήστες, καθώς αφορά αποκλειστικά τις εφαρμογές λογισμικού στις οποίες αυτοί αποκτούν πρόσβαση και χρησιμοποιούν. Από την πλευρά του χρήστη, η λήψη του λογισμικού ως υπηρεσία υποκινείται κυρίως από τα οφέλη κόστους εξαιτίας του μοντέλου πληρωμής που εφαρμόζεται. Συγκεκριμένα, δεν απαιτείται κάποια αρχική επένδυση σε υποδομές. Κάποια από τα πιο γνωστά παραδείγματα παροχών υπηρεσιών ως λογισμικό είναι οι εφαρμογές της Google όπως το Google Mail, το Google Docs και το Spreadsheets. Ο τυπικός χρήστης αυτού του μοντέλου παροχής υπηρεσιών συνήθως δεν έχει ειδικές γνώσεις ή έλεγχο επί της υποβόσκουσας υποδομής, είτε αυτή αφορά την πλατφόρμα λογισμικού στην οποία βασίζεται το μοντέλο αυτό (PaaS), είτε αφορά την υποδομή του υλισμικού (IaaS). Ωστόσο, τα επίπεδα αυτά είναι αρκετά σχετικά για τον πάροχο υπηρεσιών SaaS καθώς είναι απαραίτητα και μπορούν να αποτελέσουν αντικείμενο εξωτερικής

[638] Ibid., 54.
[639] Ibid.

ανάθεσης (**outsourcing**). Για παράδειγμα, μια εφαρμογή SaaS μπορεί να αναπτυχθεί πάνω σε μια υπάρχουσα πλατφόρμα και να εκτελεστεί στις υποδομές ενός τρίτου μέρους. Η λήψη πλατφορμών αλλά και υποδομών ως υπηρεσία αποτελεί ιδιαίτερα ελκυστική τακτική για τους παρόχους SaaS καθώς μπορεί να τους διευκολύνει ως προς την επένδυση σε υποδομές και σε αδειοδοτήσεις. Επίσης τους επιτρέπει να είναι ευέλικτοι και να εστιάζουν στις κεντρικές τους δραστηριότητες.[640]

Παρά το γεγονός ότι τα μοντέλα IaaS, PaaS και SaaS αποτελούν τα παραδοσιακά μοντέλα της νεφουπολογιστικής, τα τελευταία χρόνια έχουν αναπτυχθεί περαιτέρω μοντέλα παροχής των υπηρεσιών νέφους. Ένα από αυτά τα μοντέλα είναι το μοντέλο της λειτουργίας ως υπηρεσία (**Function as a Service – FaaS**). Το μοντέλο αυτό επιτρέπει στους πελάτες να κάνουν χρήση μιας συγκεκριμένης λειτουργίας, ενώ ο πάροχος επικαλείται, κατά παραγγελία, τους απαραίτητους πόρους ώστε να ανταποκριθεί σε ένα συγκεκριμένο υπολογιστικό αίτημα ή να αναλάβει την επεξεργασία ως απάντηση στην εμφάνιση κάποιο υπολογιστικού συμβάντος. Αυτή η δυναμική κατανομή πόρων σε απάντηση σε κάποιο αίτημα ή συμβάν, αποκαλείται υπολογιστική χωρίς εξυπηρετητή (**serverless computing**). Η έννοια της υπολογιστικής χωρίς εξυπηρετητή δεν σημαίνει ότι δεν εμπλέκεται κάποιος εξυπηρετητής, αλλά ότι αυτός ο τύπος παροχών εστιάζει στην θέση σε ισχύ και την εκτέλεση μιας συγκεκριμένης λειτουργίας, αντί να εστιάζει στους υποβόσκοντες ή υποστηρικτικούς υπολογιστικούς πόρους. Με βάση τα δεδομένα αυτά, η χρέωση τέτοιων υπηρεσιών συνδέεται συνήθως με την επίκληση και τους πόρους που καταναλώνονται από την εκτέλεση της λειτουργίας, αντί να συνδέεται με τον χρόνο χρήσης κάποιου εξυπηρετητή.

Πέρα από αυτό το μοντέλο υπηρεσιών, προσφέρονται πλέον περαιτέρω υπηρεσίες υπολογιστικού νέφους. Παραδείγματα αποτελούν η βάση δεδομένων ως υπηρεσία (**Database as a Service – DbaaS**), το δίκτυο ως υπηρεσία (**Network as a Service – NaaS**), η κινητή μονάδα υποστήριξης ως υπηρεσία (**Mobile Backend as a Service – MbaaS**), το blockchain ως υπηρεσία (**Blockchain as a Service – BaaS**) και η ρομποτική ως υπηρεσία (**Robotics as a Service – RaaS**). Περαιτέρω, ταχέως αναπτυσσόμενη θεωρείται και η μηχανική μάθηση ως υπηρεσία (ή τεχνητή νοημοσύνη ως υπηρεσία – AiaaS), η οποία υποστηρίζει τη διαδικασία της χρήσης της μηχανικής μάθησης, συμπεριλαμβανομένης της πρόσβαση σε υπολογιστικές υποδομές, ώστε να διευκολύνει την μάθηση, ή παρέχει πρόσβαση σε ήδη εκπαιδευμένα μοντέλα, όπως αυτά της αναγνώρισης προσώπου και ομιλίας, επεξεργασίας φυσικής γλώσσας (**natural language processing – NLP**). Παρά τον πολλαπλασιασμό των νέων αυτών κατηγοριών, πολλές από αυτές μπορούν να θεωρηθούν εκφάνσεις των SaaS, PaaS και IaaS. Πράγματι, το NIST κάνει αναφορά στους ανεπίσημους διαφημιστικούς όρους που συχνά κατοχυρώνονται και χρησιμοποιούνται από την βιομηχανία προσθέτοντας την κατάληξη «aaS» μετά από μια υπολογιστική δυνατότητα.[641]

7.3.1 Τα μοντέλα ανάπτυξης του υπολογιστικού νέφους

Οι υπηρεσίες νέφους μπορούν να διευθετηθούν ή να αναπτυχθούν με πολλούς διαφορετικούς τρόπους. Η επιλογή του τρόπου ανάπτυξης εξαρτάται από τις απαιτήσεις της οργάνωσης των καταναλωτών. Το μοντέλο ανάπτυξης περιγράφει την χρήση του υπολογιστικού νέφους και ορίζει

---

[640] Santi Ristol, Katarina Stanoevska-Slabeva and Thomas Wozniak, *Grid and Cloud Computing: A Business Perspective on Technology and Applications*, 1st ed. (repr., Heidelberg: Springer, 2010), 54.
[641] Christopher J Millard, *Cloud Computing Law*, 2nd ed. (repr., Oxford, United Kingdom: Oxford University Press, 2021), 36-37.

παράλληλα τα όρια της πρόσβασης σε αυτό. Το μοντέλο επίσης υποδεικνύει την σχετική τοποθεσία του υπολογιστικού νέφους σε σχέση με την τοποθεσία της οργάνωσης του εκάστοτε καταναλωτή. Ο ορισμός του NIST αναφέρει τέσσερα συνηθισμένα μοντέλα ανάπτυξης: α) το δημόσιο νέφος, β) το ιδιωτικό, γ) το κοινοτικό, και δ) το υβριδικό. Όλα τα υπολογιστικά νέφη υπάγονται σε κάποια από αυτές τις κατηγορίες.[642]

Το μοντέλο ανάπτυξης δημοσίου νέφους (**public cloud**) παρέχει την ευρύτερη δυνατή πρόσβαση στους καταναλωτές σε σχέση με τα υπόλοιπα μοντέλα ανάπτυξης. Οποιοσδήποτε εγγράφεται σε αυτό αποκτά ανοιχτή πρόσβαση σε αυτήν την εγκατάσταση νέφους. Ο καταναλωτής μπορεί να είναι είτε κάποιος ατομικός χρήστης ή μια ομάδα ατόμων που εκπροσωπούν κάποιον οργανισμό ή μια επιχείρηση. Το δημόσιο νέφος αποκαλείται και εξωτερικό νέφος καθώς όσον αφορά την τοποθεσία του παραμένει εξωτερικό ή εκτός των εγκαταστάσεων και οι καταναλωτές μπορούν να αποκτήσουν πρόσβαση στην υπηρεσία απομακρυσμένα. Ένα δημόσιο νέφος φιλοξενείται και διαχειρίζεται από κάποιους πωλητές υπολογιστικής (**computing vendors**) οι οποίοι εγκαθιδρύουν κέντρα δεδομένων για να παρέχουν την υπηρεσία στους καταναλωτές. Οι καταναλωτές που υπάγονται σε αυτό το μοντέλο ανάπτυξης είναι ελεύθεροι από τις εντάσεις που προκύπτουν από τη διαχείριση των υποδομών και τα θέματα που αφορούν την διοίκηση των συστημάτων. Παράλληλα όμως οι καταναλωτές έχουν χαμηλό βαθμό ελέγχου επί του νέφους. Κάποια από τα πιο γνωστά δημόσια νέφη είναι οι υπηρεσίες δικτύου της Amazon (**Amazon Web Services**), η υπηρεσία Azure της Microsoft και η υπηρεσία Salesforce.com. Η ανάπτυξη δημοσίων νεφών προωθεί την πολλαπλή μίσθωση (**multi – tenancy**) στον υψηλότερο βαθμό καθώς οι ίδιοι φυσικοί υπολογιστικοί πόροι μπορούν να διαμοιραστούν από πολλούς καταναλωτές που δεν σχετίζονται μεταξύ τους. Αυτό παρέχει πολλαπλά οφέλη καθώς επιτρέπει σε έναν πάροχο υπηρεσιών νέφους να εξυπηρετήσει πολλούς καταναλωτές. Όταν ένας διάσπαρτος αριθμός καταναλωτών σε όλο τον κόσμο μοιράζεται πόρους που βρίσκονται στο κέντρο δεδομένων ενός πωλητή, αυτό αυτομάτως αυξάνει τα ποσοστά χρήσης των πόρων και μειώνει το κόστος παράδοσης της υπηρεσίας του πωλητή. Επομένως, για τους καταναλωτές, το κύριο όφελος της χρήσης δημοσίων νεφών είναι το οικονομικό πλεονέκτημα που προσφέρει.

Οι πάροχοι δημοσίων νεφών από την άλλη μεριά, εκμεταλλεύονται το μέγεθος της επιχείρησής τους. Όντας μεγάλοι σε όγκο και επιχειρηματικές δραστηριότητες, έχουν τη δυνατότητα να επενδύσουν σε τεχνολογίες αιχμής και σε εξειδικευμένο προσωπικό. Αυτό διασφαλίζει την ποιότητα των παρεχόμενων υπηρεσιών. Μέσω του μοντέλου αυτού, οι καταναλωτές μπορούν να έχουν πρόσβαση σε μια δυνητικά υπέρτερη υπηρεσία με μειωμένο κόστος. Εφόσον διαφορετικοί καταναλωτές (από διαφορετικά μέρη του κόσμου) έχουν διαφοροποιημένες εργασιακές απαιτήσεις κατά τη διάρκεια της ημέρας, της εβδομάδας, του μήνα ή του έτους, ένας πάροχος υπηρεσιών νέφους μπορεί πάντοτε να υποστηρίξει τα φορτία αιχμής όταν η ζήτηση αυξάνεται.[643]

Ο δεύτερος τύπος αφορά το ιδιωτικό νέφος (**private cloud**). Χρησιμοποιούμε τον όρο ιδιωτικό νέφος για να περιγράψουμε ένα κέντρο δεδομένων νεφουπολογιστικής το οποίο ανήκει και βρίσκεται σε λειτουργία από έναν οργανισμό και περιορίζεται στις υπολογιστικές διεργασίες του οργανισμού αυτού. Η φιλοξενία και λειτουργία των ιδιωτικών νεφών μπορεί επίσης να ανατεθεί σε εξωτερικούς παρόχους υπηρεσιών. Θα πρέπει να σημειωθεί ότι το μοντέλο αυτό δεν είναι

[642] Sandeep Bhowmik, *Cloud Computing*, 1st ed. (repr., Cambridge, UK: Cambridge University Press, 2017), 66.
[643] Ibid., 67.

ευρέως διαδεδομένο και αποτελεί ουσιαστικά έναν εναλλακτικό τρόπο λειτουργίας ενός ιδιόκτητου κέντρου δεδομένων. [644] Σε σύγκριση με τα παραδοσιακά κέντρα δεδομένων, το ιδιωτικό νέφος προσφέρει σημαντικά πλεονεκτήματα. Ανάμεσα σε αυτά είναι η ενοποίηση και εικονικότητα των εξυπηρετητών, η κοινή «δεξαμενή» πόρων υπολογιστικής, αποθήκευσης και δικτύου, ο κεντρικός έλεγχος και ορατότητα, οι ενσωματωμένες πλατφόρμες ανάπτυξης λογισμικού, η αυτοματοποιημένη τροφοδότηση και συντονισμός, η μέτρηση και χρέωση ανάλογα με τη χρήση και τέλος οι πιθανές διεπαφές σε πόρους δημοσίων νεφών.[645] Για συστήματα υψηλής ασφαλείας ή κρίσιμα συστήματα, όπως τα συστήματα των οργανισμών άμυνας, προτείνεται η εγκατάσταση συστημάτων ιδιωτικού νέφους.

Η κύρια διαφορά ανάμεσα στα ιδιωτικά και τα δημόσια νέφη είναι ότι τα πρώτα βασίζονται σε μια σχέση ένα προς ένα με τον καταναλωτή, ενώ το δημόσιο νέφος διατηρεί μια σχέση ένα προς πολλά. Αυτό υποδεικνύει ότι οι πόροι ενός ιδιωτικού νέφους παραμένουν αποκλειστικοί για έναν οργανισμό και δεν μπορούν να διαμοιραστούν. Επομένως, τα χαρακτηριστικά της πολλαπλής μίσθωσης δεν εφαρμόζονται στο ιδιωτικό νέφος, όπως συμβαίνει στο δημόσιο νέφος. Αυτή η απομόνωση όμως διασφαλίζει την ιδιωτικότητα και δημιουργεί ένα πιο ασφαλές υπολογιστικό περιβάλλον. Αυτό παράλληλα δεν σημαίνει ότι το δημόσιο νέφος δεν είναι αρκετά ασφαλές. Το άλλο σημείο διαφοροποίησης αφορά την ικανότητα των καταναλωτών να ελέγξουν το νέφος. Οι καταναλωτές δεν έχουν έλεγχο επί του περιβάλλοντος του δημοσίου νέφους. Αλλά στην περίπτωση του ιδιωτικού νέφους, οι καταναλωτές μπορούν να επωφεληθούν από τα περισσότερα από τα πλεονεκτήματα της υπολογιστικής νέφους και να διατηρούν παράλληλα τον έλεγχο επί του περιβάλλοντος. Για τους καταναλωτές, το κόστος της αξιοποίησης του ιδιωτικού νέφους είναι υψηλότερο σε σχέση με το αντίστοιχο του δημοσίου καθώς οι πόροι παραμένουν αποκλειστικά σε έναν συγκεκριμένο οργανισμό.[646]

Το μοντέλο ανάπτυξης κοινοτικού νέφους (**community cloud deployment model**) επιτρέπει την πρόσβαση σε μια σειρά οργανισμών ή καταναλωτών που ανήκουν σε μια κοινότητα και είναι δομημένο ώστε να εξυπηρετεί κάποιον κοινό και συγκεκριμένο σκοπό. Προορίζεται για χρήση από μια κοινότητα ανθρώπων ή οργανισμών που μοιράζονται κοινές ανησυχίες αναφορικά με επιχειρηματικές λειτουργίες, απαιτήσεις ασφαλείας κ.λπ. Το μοντέλο αυτό επιτρέπει τον διαμοιρασμό υποδομών και πόρων ανάμεσα σε πολλαπλούς καταναλωτές που ανήκουν σε μια ενιαία κοινότητα και επομένως καταλήγει να έχει λιγότερο κόστος σε σχέση με το ιδιωτικό νέφος. Η ανάπτυξη του κοινοτικού νέφους μπορεί να συντελείται στις εγκαταστάσεις ή εκτός αυτών. Σε φυσικό επίπεδο μπορεί να τοποθετείται στις εγκαταστάσεις οποιουδήποτε μέλους της κοινότητας, ή να τοποθετείται σε κάποια εξωτερική τοποθεσία. Όπως το ιδιωτικό νέφος, αυτό το νέφος μπορεί επίσης να διακυβερνάται από κάποιον από τους συμμετέχοντες οργανισμούς (στην κοινότητα) ή μπορεί να ανατεθεί εξωτερικά σε κάποιον πωλητή.

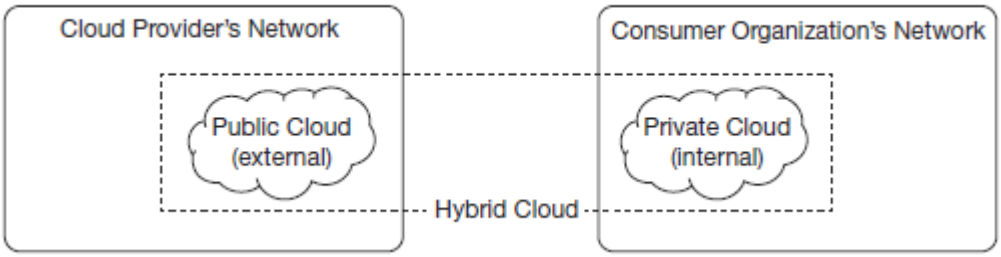
Η μορφή αυτή ανάπτυξης του υπολογιστικού νέφους μπορεί να θεωρηθεί και ως μια γενικευμένη μορφή ιδιωτικού νέφους. Ενώ το ιδιωτικό νέφος είναι προσβάσιμο μόνο σε έναν καταναλωτή, ένα κοινοτικό νέφος χρησιμοποιείται από πολλαπλούς καταναλωτές μιας κοινότητας. Επομένως,

---

[644] Anders Lisdorf, *Cloud Computing Basics: A Non-Technical Introduction*, 1st ed. (repr., Berkeley, CA: Apress, 2021), 9.
[645] Bernardo Nicoletti, *Cloud Computing in Financial Services*, 1st ed. (repr., Basingstoke: Palgrave Macmillan, 2013), 36.
[646] Sandeep Bhowmik, *Cloud Computing*, 1st ed. (repr., Cambridge, UK: Cambridge University Press, 2017), 68.

αυτό το μοντέλο ανάπτυξης υποστηρίζει την πολλαπλή μίσθωση αλλά όχι στον ίδιο βαθμό με το δημόσιο νέφος που επιτρέπει την ύπαρξη πολλαπλών μισθωτών που δεν σχετίζονται ο ένας με τον άλλο. Επομένως, το μισθωτικό μοντέλο του κοινοτικού νέφους τοποθετείται ανάμεσα στα αντίστοιχα των ιδιωτικών και δημοσίων νεφών. Ο στόχος της ανάπτυξης του κοινοτικού μοντέλου είναι να παρέχει τα οφέλη του δημοσίου νέφους, όπως αυτά της πολλαπλής μίσθωσης, της χρέωσης ανά την χρήση κ.λπ. στους καταναλωτές, παράλληλα με ένα πρόσθετο επίπεδο ιδιωτικότητας και ασφαλείας όπως το ιδιωτικό νέφος. Ένα γνώριμο παράδειγμα κοινοτικού νέφους είναι οι υπηρεσίες που λανσάρονται από την κυβέρνηση μιας χώρας με στόχο την παροχή υπηρεσιών νέφους σε εθνικές υπηρεσίες. Οι υπηρεσίες είναι οι καταναλωτές σε αυτήν την περίπτωση και ανήκουν σε μια κοινότητα (αυτήν της κυβέρνησης).[647]

Το υβριδικό νέφος με τη σειρά του γενικά δημιουργείται μέσω του συνδυασμού της ανάπτυξης του ιδιωτικού ή του κοινοτικού νέφους μαζί με την ανάπτυξη του δημοσίου νέφους. Αυτό το μοντέλο ανάπτυξης βοηθά τις επιχειρήσεις να εκμεταλλευτούν τα ιδιωτικά ή κοινοτικά νέφη μέσω της αποθήκευσης κρίσιμων εφαρμογών και δεδομένων. Παράλληλα, παρέχει το όφελος του μειωμένου κόστους, διατηρώντας τα διαμοιρασμένα δεδομένα και τις εφαρμογές στο δημόσιο νέφος. Σε πρακτικό επίπεδο, το υβριδικό νέφος μπορεί να σχηματιστεί μέσω του συνδυασμού δύο στοιχείων από ένα σετ πέντε διαφορετικών μοντέλων ανάπτυξης νέφους ως ιδιωτικό νέφος στις εγκαταστάσεις, ιδιωτικό νέφος εκτός εγκαταστάσεων, κοινοτικό νέφος εντός των εγκαταστάσεων, κοινοτικό νέφος εκτός των εγκαταστάσεων και δημόσιο νέφος, όπου ένα από τα πρώτα μοντέλα ανάπτυξης συνδυάζεται με το τελευταίο (δημόσιο νέφος).



Εικόνα 6. Μοντέλο ανάπτυξης υβριδικού υπολογιστικού νέφους

7.3.2 Η επιλογή του κατάλληλου μοντέλου ανάπτυξης υπολογιστικού νέφους

Η επιλογή του κατάλληλου μοντέλου ανάπτυξης υπολογιστικού νέφους εξαρτάται από πολλούς παράγοντες. Εξαρτάται κυρίως από τα επιχειρηματικά μοντέλα αλλά και από το μέγεθος και την ωριμότητα του πληροφορικού επιπέδου του εκάστοτε οργανισμού. Οι καταναλωτές θα πρέπει να αναλύουν τα υπέρ και τα κατά των επιλογών ανάπτυξης εντός και εκτός των εγκαταστάσεών τους και θα πρέπει να είναι προσεκτικοί πριν προβούν σε επιλογή ενός μοντέλου ανάπτυξης καθώς οι διαφορετικές επιλογές ανάπτυξης εξυπηρετούν διαφορετικές απαιτήσεις. Οι επιχειρηματικές ανάγκες και οι ανάγκες ασφαλείας (ειδικά των δεδομένων), αποτελούν δύο σημαντικούς παράγοντες που διαδραματίζουν σημαντικό ρόλο στην λήψη των σχετικών αποφάσεων.

[647] Ibid., 69.

Για τους γενικούς χρήστες, οποιαδήποτε υπηρεσία νέφους με καλή φήμη αποτελεί καλή επιλογή. Το ζήτημα της κατάλληλης επιλογής ανάπτυξης νέφους αφορά κυρίως τους οργανισμούς αλλά και τις κοινότητες. Και στην περίπτωσή τους οποιαδήποτε υπηρεσία δημοσίου νέφους με καλή φήμη μπορεί να αποτελέσει επιλογή για αυτούς, αλλά ιδιωτική (ή κοινοτική) ανάπτυξη νέφους θα πρέπει να είναι η πρώτη τους επιλογή όταν εγείρονται ζητήματα διαφύλαξης της ιδιωτικότητας των ευαίσθητων ή των ζωτικών για την επιχείρηση δεδομένων. Ακόμα και κατά την εγκατάσταση ενός ιδιόκτητου νέφους, ένας οργανισμός (ή κοινότητα) θα πρέπει να λάβει υπόψιν την ικανότητα της τεχνικής ομάδας που διαθέτει. Εναλλακτικά έχουν την επιλογή της εξωτερικής ανάθεσης της υπηρεσίας νέφους. Κατά την εξωτερική αυτή ανάθεση, η ειδημοσύνη και η φήμη του παρόχου υπηρεσιών θα πρέπει να εξακριβωθούν. Ο προϋπολογισμός επίσης αποτελεί ζήτημα κατά την επιλογή των υπηρεσιών νέφους. Το κόστος της μετάβασης σε κάποια δομή νέφους και το συνολικό κόστος της ιδιοκτησίας θα πρέπει να εξεταστούν προτού γίνει επιλογή του μοντέλου ανάπτυξης. Γενικότερα, για μια κρίσιμη εφαρμογή που εμφανίζει προβλήματα ασφαλείας, ένα ιδιωτικό ή υβριδικό μοντέλο νέφους θα αποτελεί καλή επιλογή. Αντιθέτως, για μια γενική εφαρμογή, το δημόσιο νέφος μπορεί να εξυπηρετεί τον σκοπό αυτό καλύτερα. Είναι επίσης σημαντικό να γίνουν κατανοητοί οι επιχειρηματικοί στόχοι του οργανισμού βάσει των λειτουργικών και άλλων μη λειτουργικών απαιτήσεων. Για παράδειγμα, ο έλεγχος του καταναλωτή επί του υπολογιστικού περιβάλλοντος μεταβάλλεται άμεσα ανάλογα με το μοντέλο ανάπτυξης.[648]

7.4 Η υιοθέτηση του υπολογιστικού νέφους από τα χρηματοπιστωτικά ιδρύματα

Οι χρηματοπιστωτικές υπηρεσίες αποτελούν τους προπομπούς αναφορικά με την υιοθέτηση νέων τεχνολογιών και τεχνολογιών υπολογιστικής νέφους. Μπορούν να επωφεληθούν σε μεγάλο βαθμό από τις δυνατότητες του υπολογιστικού νέφους, ως αποτέλεσμα των χαρακτηριστικών του. Συγκεκριμένα, τα υπολογιστικά νέφη προσφέρουν στα χρηματοπιστωτικά ιδρύματα τη δυνατότητα να επεξεργαστούν τεράστιες ποσότητες πληροφοριών από διάφορες πηγές ενώ διευκολύνουν την αυτοματοποίηση των επιχειρηματικών τους διεργασιών. Παράλληλα, αναβαθμίζουν την διατερματική και αυτοματοποιημένη διεκπεραίωση των συναλλαγών (**Straight Through Processing – STP**), ενώ επιτρέπουν την ανάπτυξη ενός ώριμου και λειτουργικού χαρτοφυλακίου. Τα οφέλη αυτά προκύπτουν από τη φύση της επιχείρησης και την εξάρτησή της από την τεχνολογία, από το μέγεθος των επενδύσεων σε τεχνολογίες πληροφορικής και επικοινωνιών και από την έκθεση αυτής στις μεταβολές της αγοράς και τις οικονομικές συνθήκες.

Η χρήση υποδομών πληροφορικής και επικοινωνιών (Internet and Communication Technologies – ICT) από τα χρηματοπιστωτικά ιδρύματα μεταβάλλεται ανάλογα με το μέγεθος του οργανισμού. Στο πλαίσιο αυτό, τα χρηματοπιστωτικά ιδρύματα μπορούν να κατηγοριοποιηθούν σε τρεις ομάδες ανάλογα με το μέγεθός τους. Η πρώτη ομάδα αφορά τα ιδρύματα μεγάλου μεγέθους, η δεύτερη τα ιδρύματα μεσαίου μεγέθους και η τρίτη τα ιδρύματα μικρού μεγέθους. Στην πρώτη ομάδα εντάσσονται τα ιδρύματα που έχουν μεγάλο αριθμό υποκαταστημάτων. Παραδείγματα αποτελούν η Citigroup, η HSBC, η BNP, η Deutsche Bank, η Santander, η BBVA, η ιταλική Intesa

[648] Sandeep Bhowmik, *Cloud Computing*, 1st ed. (repr., Cambridge, UK: Cambridge University Press, 2017), 71.

Sanpaolo, η Unicredit Group κ.λπ. Η διαχείριση των υποδομών ICT διενεργείται εντός της επιχείρησης. Οι μεσαίου μεγέθους χρηματοπιστωτικοί θεσμοί, οι οποίοι απαριθμούν περισσότερα από πεντακόσια υποκαταστήματα, ακολουθούν ένα τύπο κυρίως εσωτερικής διοίκησης των τεχνολογιών επικοινωνίας και πληροφορίας. Ωστόσο, η διαχείριση των διεργασιών που αφορά την διοίκηση των εγκαταστάσεων καθώς και αρκετών εφαρμογών (όπως της διαχείρισης καρτών) ανατίθενται σε εξωτερικούς συνεργάτες. Τέλος, οι χρηματοπιστωτικοί θεσμοί μικρού μεγέθους, δηλαδή όσοι απαριθμούν λιγότερα από πεντακόσια υποκαταστήματα, ακολουθούν ένα μοντέλο πλήρους εξωτερικής ανάθεσης για την διαχείριση των εφαρμογών και των υποδομών που αφορούν τις τεχνολογίες πληροφορικής και επικοινωνιών. Έχουν επίσης μια τάση να εφαρμόζουν την εξωτερική ανάθεση των επιχειρηματικών διεργασιών (***Business Process Outsourcing - BPO***) για κάποιες από τις δραστηριότητές τους, όπως την μισθοδοσία ή την είσπραξη. Αυτή η προσέγγιση τα τελευταία χρόνια εξαπλώνεται και στα άλλα γκρουπ χρηματοπιστωτικών θεσμών.[649]

Σε γενικές γραμμές, σε πολλές χώρες, ένα μεγάλο μέρος των παρόχων χρηματοοικονομικών υπηρεσιών ήδη αναθέτουν τα πληροφοριακά τους συστήματα σε εξωτερικούς συνεργάτες. Η βιομηχανία των χρηματοπιστωτικών υπηρεσιών αποτελεί συνεπώς ένα από τα πιο εξελιγμένα παραδείγματα εξωτερικής ανάθεσης πληροφοριακών συστημάτων. Η διάδοση του μοντέλου της πλήρους εξωτερικής ανάθεσης εξαρτάται σε μεγάλο βαθμό από την οικονομική απόδοση, καθώς προσφέρει στους χρήστες την δυνατότητα ουσιώδους εξοικονόμησης και πλήρους συμμόρφωσης με τους αυστηρούς και μεταβαλλόμενους κανονισμούς.[650]

Ο κύριος λόγος για τον οποίο τα χρηματοπιστωτικά ιδρύματα εξετάζουν την υιοθέτηση υπηρεσιών νέφους, έγκειται στο γεγονός ότι οι πιο εξελιγμένες οικονομικές υπηρεσίες έχουν καινοτόμα και ευέλικτα επιχειρηματικά μοντέλα. Η υπολογιστική νέφους αποτελεί μια δυνητικά διαταρακτική καινοτομία και οι χρηματοπιστωτικοί οργανισμοί ενδιαφέρονται να εξετάσουν τις αλλαγές που αυτή επιφέρει. Εκμεταλλευόμενοι την υπολογιστική νέφους, θα μεταφέρουν τις εσωτερικές επιχειρηματικές και τεχνολογικές διεργασίες σε μια σειρά ολοκληρωμένων, ευέλικτων, παραμετροποίησιμων και κλιμακούμενων πλατφορμών οι οποίες καλύπτουν τρεις κύριες διαστάσεις της τεχνολογικής ανάπτυξης. Η πρώτη αφορά τις κεντρικές υπηρεσίες και τα προϊόντα, η δεύτερη τις προσανατολισμένες προς τους πελάτες λειτουργίες για τις πολυκαναλικές υπηρεσίες και τις υπηρεσίες ένταξης (**multichannel and integration services**) και η τρίτη αφορά τις διεργασίες που επιτρέπουν την επιχειρηματική δράση όπως αυτές που αφορούν το ανθρώπινο δυναμικό, τις νομικές υπηρεσίες και το μάρκετινγκ.

Οι χρηματοπιστωτικοί θεσμοί αντιμετωπίζουν την υπολογιστική νέφους ως μια εξέλιξη (και σε ορισμένες περιπτώσεις ως επανάσταση) των παραδοσιακών μοντέλων παροχής υπηρεσιών. Εξετάζουν στο πλαίσιο αυτό ποιους τύπους υπολογιστικών φορτίων θα μεταφέρουν ενώ παράλληλα εστιάζουν στο να διασφαλίσουν ότι οι επιχειρηματικές εφαρμογές βρίσκονται σε συμμόρφωση με τις εσωτερικές και τις εξωτερικά επιβαλλόμενες πολιτικές ασφαλείας. Η προσοχή των χρηματοπιστωτικών υπηρεσιών είναι ιδιαιτέρως στραμμένη προς πεδία στα οποία τέτοιου είδους προσεγγίσεις φαίνεται να καθιστούν δυνατή την απόδοση οφέλους σε μικρό χρονικό

[649] Bernardo Nicoletti, *Cloud Computing in Financial Services*, 1st ed. (repr., Basingstoke: Palgrave Macmillan, 2013), 65-66.
[650] Ibid., 66.

διάστημα. Αυτό μπορεί να επιτευχθεί μέσω ευρέως κατανεμημένων τεχνολογικών εγκαταστάσεων και της δυνατότητας να αποσυνδεθούν από την κοινή λογική της απόκτησης λογισμικού, ώστε να μεταβούν σε ένα μοντέλο των τεχνολογιών πληροφορικής και επικοινωνιών ως υπηρεσία.

Οι μεγάλου μεγέθους χρηματοπιστωτικοί οργανισμοί έχουν επιδείξει ενδιαφέρον για την ανάπτυξη μιας προσέγγισης που βασίζεται στην υπολογιστική ιδιωτικού νέφους εντός των δικών τους πληροφοριακών οργανισμών, στοχεύοντας έτσι στην βελτιστοποίηση της χρήσης των εσωτερικών πόρων που είναι ήδη διαθέσιμοι σε αυτούς. Στους χρηματοπιστωτικούς θεσμούς, παρατηρούνται υψηλά συναλλακτικά φορτία, καθιστώντας απαραίτητη την αξιολόγηση της υιοθέτησης τεχνολογιών και αρχιτεκτονικών πληροφορικής, οι οποίες είναι εξειδικευμένες ανάλογα με το φορτίο που καλούνται να διαχειριστούν. Το επόμενο βήμα είναι η εξέλιξη των συστημάτων προς υβριδικές αρχιτεκτονικές νέφους (**Cloud Arcs**), ακόμα και αν αυτό θα δημιουργήσει προκλήσεις ως προς την ενσωμάτωση των λειτουργικών διαδικασιών. Επιπροσθέτως, η αρχιτεκτονική η οποία έχει ως γνώμονα την εξυπηρέτηση των υπηρεσιών (**Service-Oriented Architecture - SOA**) θα διαδραματίσει σημαντικό ρόλο ως πρωτεύον μηχανισμός αλληλεπίδρασης με τις υπηρεσίες νέφους. Η διεπαφή ανάμεσα σε δύο υπολογιστικά νέφη (ιδιωτικά και δημόσια) θα απαιτεί έναν υπηρεσιακό δίαυλο και ένα ασφαλές πρωτόκολλο δικτύωσης (**Internet Protocol Security - IPsec**).[651]

7.4.1 Οι προσδοκίες από την υιοθέτηση λύσεων υπολογιστικού νέφους

Οι χρηματοπιστωτικοί θεσμοί ακολουθούν ένα συνεχώς εξελισσόμενο και ευέλικτο τεχνολογικό μοτίβο. Ο στόχος είναι να ανταποκριθούν στις διαφοροποιημένες και μεταβαλλόμενες επιχειρηματικές και πελατειακές ανάγκες. Προσπαθούν επομένως να εκμεταλλευτούν τους τεχνολογικούς πόρους και την λειτουργικότητα που παρέχονται ως υπηρεσίες και κατά παραγγελία. Κατά αυτόν τον τρόπο, μπορούν να έχουν ότι χρειάζονται και όποτε το χρειάζονται, αντί να εκπονούν εκ των προτέρων σχέδια που αφορούν λύσεις, χωρητικότητες και διαθεσιμότητα. Επιπροσθέτως, προσπαθούν να επιτύχουν αποδοτικότητα σε κόστος και να κάνουν χρήση κλιμακούμενων υπηρεσιών μέσω της χρήσης βελτιστοποιημένων και εικονικών υποδομών. Μέσω των υπηρεσιών νέφους, τα χρηματοπιστωτικά ιδρύματα μπορούν να αξιοποιήσουν τα κατάλληλα εξαρτήματα υλισμικού και να διαχειριστούν τις υπολογιστικές απαιτήσεις ως λειτουργία που βασίζεται στην πραγματική χρήση και όχι στον σχεδιασμό, αλλά και να διεκπεραιώνουν τις διεργασίες τους στο μέγιστο της χωρητικότητας, με εφεδρείες και με πρόσθετη ανθεκτικότητα προκαταβολικά. Τέλος, εξίσου σημαντική κρίνεται η μείωση των λειτουργικών κινδύνων. Η υπολογιστική νέφους συμπεριλαμβάνει την ριζική αναδιοργάνωση, αποφεύγοντας παράλληλα τους κινδύνους εκτέλεσης που συνδέονται με τα εσωτερικά τμήματα των υπηρεσιών πληροφορικής.

Η υιοθέτηση των επιχειρηματικών λύσεων που βασίζονται στις υπηρεσίες νέφους θα μπορούσε να επιταχυνθεί εντός των χρηματοπιστωτικών υπηρεσιών εάν ληφθεί υπόψιν ότι υπόσχονται επιχειρηματική ευκινησία, μέσω της ικανότητας να κλιμακώνονται και να ανταποκρίνονται στις

---

[651] Bernardo Nicoletti, *Cloud Computing in Financial Services*, 1st ed. (repr., Basingstoke: Palgrave Macmillan, 2013), 70.

επιχειρηματικές διαφοροποιήσεις ανάλογα με τις ανάγκες, αντί να δημιουργούνται εφεδρικές υποδομές. Επιπροσθέτως, η αρχική επιτυχία των τεχνολογιών νέφους στο πεδίο της εικονικότητας και των κατά παραγγελία λύσεων στο χώρο υποδομών, προσφέρει πολλαπλά πλεονεκτήματα για τους χρηματοπιστωτικούς οργανισμούς οι οποίοι σήμερα επιδιώκουν να συγχωνεύσουν τους εξυπηρετητές τους και τα κέντρα δεδομένων τους. Οι χρηματοπιστωτικοί οργανισμοί εφαρμόζουν σήμερα εικονικές λύσεις σε όλη την έκταση των οργανωτικών τους δομών, παρουσιάζοντας εξαιρετικές αποδόσεις στις επενδύσεις τους (***Return on Investment - ROI***).

Η ανάλυση των χρηματοπιστωτικών οργανισμών και των επιχειρηματικών τους δραστηριοτήτων δείχνει ωστόσο ότι δεν υπάρχει ένα συγκεκριμένο μοντέλο νέφους που να ανταποκρίνεται σε όλες τις απαιτήσεις τους. Αντιθέτως, οι οργανισμοί αυτοί δημιουργούν και διαχειρίζονται ένα ομόσπονδο οικοσύστημα υπηρεσιών που βασίζονται στην υπολογιστική νέφους αλλά και σε άλλες υπηρεσίες που δεν βασίζονται στην υπολογιστική νέφους. Σε κάποιες εκφάνσεις της λειτουργικότητας, οι υπηρεσίες νέφους αξιοποιούν την αφαίρεση του ελέγχου που παρέχεται από την ανάπτυξη μοντέλων δημοσίων, ιδιωτικών και κοινοτικών νεφών. Ένα ομόσπονδο οικοσύστημα δύναται να αξιοποιήσει πολλαπλούς τύπους εφαρμογών αλλά και να παρέχει ευέλικτη χωρητικότητα για να ανταποκρίνεται στις επιχειρηματικές απαιτήσεις. Επιπροσθέτως, παρέχει ένα βαθμιαίο μονοπάτι υιοθέτησης, χτίζοντας πάνω στην επιτυχία του ακριβώς προηγούμενου βήματος.

Όσο οι χρηματοπιστωτικοί θεσμοί εξελίσσονται προς ένα μοντέλο που βασίζεται στην υπολογιστική νέφους, οι εσωτερικές επιχειρηματικές διεργασίες θα οργανωθούν με βάση πέντε συγκεκριμένες κατηγορίες. Ειδικότερα, η πρώτη κατηγορία θα αφορά την ανάπτυξη υπηρεσιών, που συμπεριλαμβάνει την λειτουργική, τεχνική και επιχειρησιακή ανάπτυξη. Εδώ εντάσσονται όλες οι υπηρεσίες πληροφορικής ανάπτυξης εντός του οργανισμού και καλύπτεται η ανάπτυξη εφαρμογών και υποδομών αλλά και η ανάπτυξη και συντήρηση υπηρεσιών. Παρά το γεγονός ότι υπάρχει σημαντική ποικιλομορφία στις τεχνολογίες και τα εργαλεία που χρησιμοποιούνται εντός του οργανισμού, υπάρχει μια τάση προς την χρήση εμπορικών πακέτων λογισμικού αντί να αναπτύσσονται λύσεις λογισμικού εντός αυτού. Η δεύτερη κατηγορία αφορά τις υπηρεσίες εξυπηρέτησης πελατών και αναφέρεται σε όλες τις πλευρές της ενασχόλησης με τους πελάτες αλλά και τις πωλήσεις, την παροχή υπηρεσιών και τις αλληλεπιδράσεις. Επίσης συμπεριλαμβάνει τις λειτουργίες που αφορούν τους εργαζόμενους με βάση τις οποίες διενεργούνται οι δραστηριότητες που εστιάζουν στους πελάτες. Οι περισσότεροι χρηματοπιστωτικοί οργανισμοί αναπτύσσουν και προσφέρουν υπηρεσίες που βασίζονται στην κινητή τηλεφωνία και οι υπηρεσίες νέφους διευκολύνουν σε μεγάλο βαθμό τη λειτουργία αυτών των υπηρεσιών. Η τρίτη κατηγορία αφορά τις κεντρικές επιχειρηματικές υπηρεσίες, οι οποίες αφορούν τις διεργασίες που καλύπτουν τις χρηματοοικονομικές υπηρεσίες λιανικής, τις εμπορικές χρηματοοικονομικές υπηρεσίες, τις πληρωμές, τις επενδυτικές υπηρεσίες, την διαχείριση χαρτοφυλακίου και άλλες λειτουργίες όπως αυτές που αφορούν τις κάρτες και τις πληρωμές, την διακυβέρνηση, την διαχείριση κινδύνων και τις υπηρεσίες συμμόρφωσης. Το υπολογιστικό νέφος καλύπτει αρκετές πλευρές των διεργασιών αυτών.

Η τέταρτη κατηγορία αφορά τις υπηρεσίες που επιτρέπουν την επιχειρηματική δράση, στις οποίες συμπεριλαμβάνεται ένα σύνολο επιχειρηματικών λειτουργιών που κρίνονται απαραίτητες για την ολοκλήρωση της επιχειρηματικής επεξεργασίας. Αρχικά, οι λειτουργίες αυτές ήταν ενσωματωμένες στις κεντρικές λειτουργίες αλλά με την πάροδο του χρόνου οι περισσότεροι

θεσμοί τις αφαίρεσαν και τις παραδίδουν ως διαμοιραζόμενες υπηρεσίες κατά μήκος διαφορετικών επιχειρηματικών τομέων. Οι υπηρεσίες αυτές παρέχουν αληθινές και πρακτικές ευκαιρίες για την αξιοποίηση των πλεονεκτημάτων των υπηρεσιών νέφους. Τέλος, η πέμπτη κατηγορία αφορά τις λειτουργίες των εταιρικών υπηρεσιών, που συμπεριλαμβάνουν λειτουργίες που επιτρέπουν την επιχειρηματική ύπαρξη και τις κάθε είδους εργασίες που έχουν νομική φύση. Οι περισσότερες από αυτές τις λειτουργίες, ενσωματωμένες διεργασίες και τεχνολογικές πλατφόρμες, έχουν τυποποιηθεί σε αποσπαστεί σε καλά καθορισμένες γραμμές υπηρεσιών. Οι περισσότεροι χρηματοπιστωτικοί θεσμοί έχουν ήδη αναθέσει σε εξωτερικούς συνεργάτες σημαντικά τμήματα των πλατφορμών αυτών. Οι συνεργάτες αυτοί προσφέρουν τις πλατφόρμες τους με τη μορφή λογισμικού ως υπηρεσία, βασιζόμενες δηλαδή στις τεχνολογίες υπολογιστικής νέφους.

Χαρακτηριστικό παράδειγμα χρηματοπιστωτικού ιδρύματος που επωφελήθηκε από την χρήση τεχνολογιών δημοσίου νέφους είναι η LPL Financial, η οποία αποτελεί τον μεγαλύτερο πάροχο επενδυτικών υπηρεσιών στις Η.Π.Α. Το Νοέμβριο του 2010, η διοίκηση της εταιρείας προέβη σε σημαντικές επενδύσεις στα εσωτερικά συστήματα, συμπεριλαμβανομένων των συστημάτων ανθρώπινου δυναμικού και λογιστικής. Η επενδυτική αυτή κίνηση πραγματοποιήθηκε καθώς η χωρητικότητα των συστημάτων υποστήριξης ήταν περιορισμένη και η διοίκηση έπρεπε να εξετάσει πως θα αναπτύξει και θα συντηρήσει τα συστήματα αυτά αποτελεσματικά σε βάθος χρόνου. Οι εξωτερικοί πωλητές λύσεων πληροφορικής παρείχαν σημαντική υποστήριξη στα συστήματα ασφαλείας της LPL καθώς και τεχνική ειδημοσύνη. Επίσης, έδωσαν στην εταιρεία τη δυνατότητα να διαχειρίζεται τα συστήματά της αποτελεσματικά μέσω του υπολογιστικού νέφους. Η διοίκηση υπολογίζει ότι η μεταφορά των οικονομικών εφαρμογών της εταιρείας στο νέφος, έδωσε στην οικονομική οργάνωση της LPL τη δυνατότητα να ασκεί μεγαλύτερο έλεγχο ως προς την χρήση των συστημάτων της. Επί του παρόντος μεγιστοποιούν την χρήση των συστημάτων αυτών. [652]

7.4.2 Η προσέγγιση του υπολογιστικού νέφους από τις ευρωπαϊκές τράπεζες

Οι ευρωπαϊκές τράπεζες έχουν ξεκινήσει να χρησιμοποιούν το υπολογιστικό νέφος με τρεις διαφορετικούς τρόπους. Ο πρώτος αφορά το σκιώδες υπολογιστικό νέφος (**shadow cloud**), ο δεύτερος το νέφος μανιταριών (**mushrooming cloud**) και ο τρίτος την υιοθέτηση μιας επίσημης στρατηγικής νέφους (**formal cloud strategy**), που εφαρμόζεται από το τμήμα πληροφορικής της εκάστοτε επιχείρησης.

Ένας από τους τρόπους μέσω των οποίων οι τράπεζες κάνουν χρήση του υπολογιστικού νέφους είναι το «σκιώδες νέφος», στο οποίο οι εργαζόμενοι εγγράφονται απευθείας στις υπηρεσίες νέφους χωρίς να έχουν γνώση του γεγονότος αυτού τα τμήματα πληροφορικής ή τα νομικά τμήματα των τραπεζών, ή εναλλακτικά τα τμήματα πληροφορικής αποκτούν τις υπηρεσίες αυτές χωρίς να συμβουλεύονται προηγουμένως τα νομικά τμήματα ή τα τμήματα συμμόρφωσης. Ενώ το κίνητρο πίσω από την χρήση του σκιώδους νέφους ήταν συνήθως καλόβουλο, ώστε για παράδειγμα να βελτιωθεί η παραγωγικότητα, το αποτέλεσμα είναι ότι πολλές υπηρεσίες νέφους

[652] Bernardo Nicoletti, *Cloud Computing in Financial Services*, 1st ed. (repr., Basingstoke: Palgrave Macmillan, 2013), 72-73.

χρησιμοποιούνται χωρίς να το γνωρίζει η τράπεζα, ειδικά στην περίπτωση των δωρεάν υπηρεσιών όπως το αποθηκευτικό Dropbox και η υπηρεσία ηλεκτρονικού ταχυδρομείου της Google (**G-mail**). Κάποιες από τις μεγαλύτερες τράπεζες ωστόσο έχουν επιληφθεί του ρίσκου της χρήσης υπηρεσιών σκιώδους νέφους. Μια από αυτές τις τράπεζες δήλωσε ότι αστυνομεύει την χρήση του σκιώδους νέφους, μέσω σημείων ελέγχου σε διαφορετικά επίπεδα σχετικά με την πρόσβαση σε ορισμένους εξωτερικούς ιστοτόπους, αλλά και μέσω διαδικασιών έγκρισης και αξιολόγησης. Έτσι κατάφερε να εντοπίσει και να απενεργοποιήσει περιπτώσεις χρήσεως του σκιώδους υπολογιστικού νέφους. Σε άλλες περιπτώσεις, οι τράπεζες μπορεί χωρίς την θέλησή τους να βασίζονται στις υπηρεσίες νέφους μέσω των ενεργειών του πωλητή υπηρεσιών με τον οποίο συνεργάζονται. Κάποιοι παραδοσιακοί πωλητές λογισμικού, όπως ορισμένες πλατφόρμες δεδομένων με τη μορφή CRM, έχουν μεταβεί σε ένα μοντέλο SaaS, το οποίο με τη σειρά του βασίζεται σε πλατφόρμες IaaS/PaaS. Ακόμα και αν οι τράπεζες συνεργάζονται με αυτούς τους πωλητές, ανακαλύπτουν συχνά ότι έχουν άθελά τους μεταβεί στο νέφος μέσω των ενεργειών του πωλητή, καθώς οι προτιμώμενοι από αυτές πάροχοι μεταβιβάζουν αυτές σε μια λύση υπολογιστικού νέφους που έχει ακριβώς την ίδια λειτουργικότητα με την υπάρχουσα υποδομή τους.[653]

Ένας από τους λόγους για τους οποίους οι τράπεζες υιοθετούν λύσεις υπολογιστικών νεφών μανιταριών είναι η ίδια η διαδικασία εντός αυτών. Συνήθως υπάρχει ένα οικονομικό κατώτατο όριο κάτω από το οποίο οι συναλλαγές μπορούν να περάσουν απαρατήρητες. Το τμήμα προμηθειών συγκρίνει προσφορές και επιλέγει όσες περνούν το οικονομικό όριο. Οι συναλλαγές που εγκρίνονται από το τμήμα προμηθειών συνήθως είναι συμβατές με τους συνήθεις όρους των τραπεζών. Είναι επίσης σημαντικό να αναφερθεί ότι οι συμφωνίες με ενδιάμεσους μικρότερους παρόχους συνήθως κάτω από το οικονομικό όριο που θέτουν οι τράπεζες. Στο πλαίσιο αυτό εντάσσονται και οι δοκιμαστικές ενέργειες των τμημάτων πληροφορικής των τραπεζών, οι οποίες συνήθως αφορούν μοντέλα νέφους IaaS/PaaS και βασίζονται σε συμφωνίες απόκτησης που δεν ξεπερνούν το οικονομικό όριο, πέραν του οποίου κρίνεται απαραίτητο να ληφθεί η σύμφωνη γνώμη του νομικού τμήματος.

Με αυτόν τον τρόπο κινούνται και οι τράπεζες ως προς την υιοθέτηση λύσεων υπολογιστικού νέφους. Συγκεκριμένα, ξεκινούν με την χρήση των υπηρεσιών αυτών σε μικρή κλίμακα, για λόγους εσωτερικής παραγωγικότητας και στη συνέχεια επεκτείνουν τη χρήση σε μεγαλύτερη κλίμακα καλύπτοντας περισσότερα τμήματα του οργανισμού. Η διαδικασία αυτή για τις τράπεζες μπορεί να διαρκέσει έως και πέντε χρόνια, καθώς αυτές ανακαλύπτουν στην πορεία πολλές μικρότερες προσφορές που αφορούν τις υπηρεσίες νέφους IaaS, προτού μεταβούν σε ένα μοντέλο δομημένης διακυβέρνησης υπολογιστικού νέφους. Το «νέφος μανιταριών» αποτελεί γενικότερα ένα ρίσκο για τις τράπεζες. Η χρήση του νέφους κλιμακώνεται ταχύτατα από συγκεκριμένες χρήσεις, στις οποίες δοκιμάζεται σε μικρή κλίμακα χωρίς τη χρήση ευαίσθητων δεδομένων, σε μεγαλύτερου μεγέθους χρήσεις οι οποίες συμπεριλαμβάνουν εντελώς διαφορετικές κατηγορίες ρίσκου, καθιστώντας αναγκαία από τις τράπεζες την εφαρμογή ειδοποιήσεων όταν ξεπερνώνται

[653] W. Kuan Hon and Christopher Millard, "Banking in The Cloud: Part 1 – Banks' Use of Cloud Services", *Computer Law & Security Review* 34, no. 1 (2018): 13, doi: 10.1016/j.clsr.2017.11.005.

συγκεκριμένα όρια ή μέτρων που αποτρέπουν την υπερβολική χρήση σε συγκεκριμένες περιπτώσεις.[654]

Αναφορικά με την επίσημη και οργανωμένη χρήση του υπολογιστικού νέφους, οι τράπεζες συχνά ξεκινούν με την δοκιμή των υπηρεσιών νέφους, συνήθως σε συγκεκριμένες επιχειρηματικές μονάδες ή χώρες στις οποίες δραστηριοποιούνται. Οι χρήστες που λαμβάνουν μέρος στις δοκιμές αυτές επιλέγονται προσεκτικά και αποφεύγεται η επιλογή προσωπικού που διαδραματίζει ευαίσθητο ρόλο εντός της επιχείρησης. Παράλληλα, ο σχεδιασμός, η εφαρμογή, η δημοσίευση, η επιβολή και η συχνή ενημέρωση του εσωτερικού κανονισμού του υπολογιστικού νέφους είναι ύψιστης σημασίας ώστε να διασφαλίζεται η ασφάλεια των δεδομένων που διακινούνται μέσω του νέφους και είναι σύνηθες φαινόμενο στην πολιτική που ακολουθούν τα χρηματοπιστωτικά ιδρύματα. Ο κανονισμός αυτός μπορεί για παράδειγμα να απαγορεύει την χρήση του σκιώδους νέφους από τους εργαζόμενους. Παράλληλα, αποτελεί συχνό φαινόμενο για τις πολιτικές των τραπεζών που αφορούν το νέφος να απαγορεύουν τη χρήση δημοσίων νεφών για κρίσιμες και σημαντικές λειτουργίες, αλλά ακόμα και αν ο κανονισμός δίνει προτεραιότητα στην χρήση ιδιωτικών νεφών, μπορεί κάποια διαδικασία να επιτρέπει εξαιρέσεις. Κάποιες χρήσεις του νέφους μπορεί να ξεκίνησαν προτού εκδοθεί ο κανονισμός, ειδικά σε περιπτώσεις τραπεζών που ανέλαβαν πρωτοβουλίες διακυβέρνησης του νέφους αφού ανακάλυψαν τη χρήση σκιωδών νεφών.

Οι περισσότερες τράπεζες ξεκινούν τη χρήση των υπολογιστικών νεφών μέσω της εικονικότητας, χωρίς να χρησιμοποιούν το νέφος σε οποιαδήποτε κλίμακα, παρά μόνο σε κάποιες συγκεκριμένες περιπτώσεις. Αυτό συμβαίνει λόγω της οργάνωσης τους, κάνοντας διαχείριση των παρόχων υπηρεσιών βάσει κόστους και όχι με βάση το σύνολο των χαρακτηριστικών των συστημάτων. Αυτό το είδος οργάνωσης όμως δεν επέτρεπε την εύκολη δημιουργία υποδομών ως υπηρεσία λόγω του κόστους επένδυσης και του κόστους λειτουργίας. Ωστόσο, κατά καιρούς πολλές τράπεζες αυξάνουν την χρήση της τεχνολογίας νέφους, κυρίως για να επεκτείνουν την εικονικότητα, μέσω κάποιας χρήσης του ιδιωτικού νέφους. Άλλες τράπεζες επιλέγουν να χρησιμοποιήσουν ένα συνδυασμό δημοσίου νέφους με ένα ιδιωτικό νέφος που βρίσκεται εντός των εγκαταστάσεών τους. Στο ιδιωτικό νέφος φιλοξενούν τις κρίσιμες για τη λειτουργία τους εφαρμογές.[655]

7.4.3 Τα πλεονεκτήματα της χρήσης των υπηρεσιών του υπολογιστικού νέφους για τις τράπεζες

Όπως προαναφέρθηκε, τα τραπεζικά ιδρύματα χρησιμοποιούν κυρίως ιδιωτικά υπολογιστικά νέφη για να φιλοξενούν τις κρίσιμες επιχειρηματικές εφαρμογές τους και να διασφαλίζουν ότι τα ευαίσθητα δεδομένα των πελατών διατηρούνται ασφαλή. Το ιδιωτικό νέφος αναδεικνύεται ως ισχυρότερη επιλογή για τις τράπεζες σε σχέση με το δημόσιο νέφος, καθώς παρέχει σε αυτές έλεγχο επί των πληροφοριακών συστημάτων τους ενώ παράλληλα παρουσιάζει μειωμένη πολυπλοκότητα, αυξημένη ευελιξία και άλλα πλεονεκτήματα που σχετίζονται με την υπολογιστική νέφους. Παράλληλα, τα ιδιωτικά νέφη προτιμώνται στην τραπεζική βιομηχανία καθώς σε ένα οικονομικό περιβάλλον στο οποίο οι εφαρμογές είναι κρίσιμες και εντάσσονται σε έναν πλαίσιο αυστηρής κανονιστικής συμμόρφωσης, μπορούν να προσφέρουν υψηλή ασφάλεια. Διασφαλίζουν ότι τα δεδομένα δεν θα χαθούν ή θα βρεθούν σε λάθος σημεία και επίσης παρέχουν

[654] Ibid.
[655] Ibid., 14.

ευελιξία αναφορικά με τον έλεγχο με στόχο την τροποποίηση της ρύθμισης των πόρων σύμφωνα με την ζήτηση. Τα ιδιωτικά νέφη επιτρέπουν σε περισσότερα συστήματα να λειτουργήσουν στο πλαίσιο υψηλού όγκου συναλλαγών χωρίς να υπερφορτώνουν το δίκτυο ή να καθυστερούν τις διαδικασίες, διασφαλίζοντας με αυτόν τον τρόπο ότι θα παρέχεται η καλύτερη δυνατή εμπειρία στους πελάτες. Από τη στιγμή που οι πόροι μισθώνονται αντί να αγοράζονται, τα ιδιωτικά νέφη συμβάλλουν στην μετατροπή των εξόδων κεφαλαίου σε λειτουργικά έξοδα, μειώνοντας το συνολικό κόστος της ιδιοκτησίας. Για να πετύχουν σε βάθος χρόνου, οι τράπεζες θα πρέπει να κατανοήσουν πλήρως τον τρόπο με τον οποίο λειτουργούν τα νέφη και να προχωρήσουν στην ανάπτυξη νέων εφαρμογών που θα ωφελούν τους πελάτες.

Όταν ένας οργανισμός μετατρέπει τις υποδομές του σε υποδομές υπολογιστικού νέφους, αυτό θα πρέπει να λάβει χώρα σε πραγματικό χρόνο ώστε να μειωθεί η σπατάλη αχρησιμοποίητων πόρων. Τεχνολογίες όπως τα ενοποιημένα υπολογιστικά συστήματα της Cisco (**Unified Computing Systems - UCS**[656]), βοηθούν στην παρακολούθηση των εξυπηρετητών, των χώρων αποθήκευσης, της μνήμης και της χωρητικότητας του δικτύου. Μπορούν να υπολογίσουν, με υψηλά ποσοστά ακριβείας, ποιοι εξυπηρετητές απαιτούν περισσότερους πόρους και αυτομάτως δίνουν προτεραιότητα σε αυτούς. Μια καλά σχεδιασμένη πλατφόρμα ιδιωτικού υπολογιστικού νέφους επίσης κοστίζει λιγότερο σε σχέση με έναν αποκλειστικό εξυπηρετητή. Οι συνεργατικές πλατφόρμες νέφους μπορούν επίσης να παρέχουν μια πλατφόρμα για την ανάπτυξη εφαρμογών, μείωσης του κόστους αλλά και να βοηθήσουν τις τράπεζες να επικοινωνούν με τους πελάτες τους πιο αποτελεσματικά. Πέραν του κόστους, μπορούν να δημιουργήσουν σημαντικές ευκαιρίες για να μπορέσουν οι τράπεζες να αναπτύξουν νέα επιχειρηματικά μοντέλα που είναι πελατοκεντρικά, οδηγώντας έτσι σε περαιτέρω ανάπτυξη και κερδοφορία.[657]

Γενικότερα τα μεγαλύτερα οφέλη που προσφέρουν οι τεχνολογίες υπολογιστικού νέφους στα χρηματοπιστωτικά ιδρύματα είναι τα εξής:

Α) <u>*Μείωση του κόστους*</u>: Η χρήση τεχνολογιών υπολογιστικής νέφους συνεπάγεται ότι οι τράπεζες δεν θα πρέπει να επενδύσουν μαζικά σε εξειδικευμένο υλισμικό, λογισμικό και το απαιτούμενο προσωπικό. Είναι πολύ πιο εύκολο για αυτές να αναβαθμίσουν τις πληροφορικές τους υποδομές και το αρθρωτό, κατά παραγγελία μοντέλο νέφους συνεπάγεται ότι θα πρέπει αυτές να πληρώνουν για το υλισμικό και το λογισμικό που χρειάζονται κάθε φορά.

Β) <u>*Βελτίωση της ευελιξίας και της κλιμακωσιμότητας*</u>: Το υπολογιστικό νέφος δίνει στα τραπεζικά ιδρύματα τη δυνατότητα να ανταποκρίνονται άμεσα στην μεταβαλλόμενη αγορά αλλά και στις ανάγκες των πελατών και της τεχνολογίας. Η δυνατότητα αυτή να ανταποκρίνονται άμεσα παρέχει σε αυτές ένα ανταγωνιστικό πλεονέκτημα σε μια εποχή που καλούνται να ανταγωνιστούν τις νεοφυείς εταιρείες χρηματοπιστωτικής τεχνολογίας (**fintech companies**). Μέσω των τεχνολογιών υπολογιστικού νέφους μπορούν να κλιμακώνουν από πάνω προς τα κάτω την διαθέσιμη σε αυτά τεχνολογία ανάλογα με τις εκάστοτε απαιτήσεις.

Γ) <u>*Αύξηση της αποδοτικότητας*</u>: Τα τραπεζικά ιδρύματα κάνοντας χρήση των τεχνολογιών νέφους θα οδηγηθούν σε αυξημένα ποσοστά αποδοτικότητας και λειτουργικής μόχλευσης. Η

---

[656]Products Services, "Cisco Servers – Unified Computing System (UCS)", Cisco, 2022, https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html.

[657] Nancy Awadallah, "Usage of Cloud Computing in Banking System", *International Journal of Computer Science Issues* 13, no. 1 (2016): 51, doi:10.20943/ijcsi-201602-4952.

τυποποιημένη μορφή των μοντέλων νέφους διευκολύνει την ενσωμάτωση νέων τεχνολογιών και εφαρμογών από τα χρηματοπιστωτικά ιδρύματα. Καθώς οι επιχειρηματικές και τεχνολογικές λειτουργίες μπορούν να ευθυγραμμιστούν περαιτέρω, το υπολογιστικό νέφος αποτελεί μια χρυσή ευκαιρία για τις τράπεζες ώστε να απαλλαχθούν από την πολυπλοκότητα.

Δ) *Ταχύτερη εξυπηρέτηση των πελατών*: Η υπολογιστική νέφους καθιστά πιο εύκολη την ανάπτυξη και προσφορά νέων πακέτων προϊόντων και υπηρεσιών, είτε σε ατομική βάση είτε συνεργατικά. Πρακτικά εξαλείφει τις καθυστερήσεις απόκτησης υλισμικού και λογισμικού. Οι τράπεζες δύνανται έτσι να ενισχύσουν την υπολογιστική τους ισχύ για να ανταποκριθούν στις αιχμές της ζήτησης και να παρέχουν τις πιο πρόσφατες ταμειακές λύσεις χωρίς να ανησυχούν για το αν η τεχνολογία που χρησιμοποιούν είναι ενημερωμένη. Οι επιχειρήσεις συνεπώς θα επωφεληθούν σε μεγάλο βαθμό καθώς θα μπορούν να αποκτήσουν πρόσβαση στα τραπεζικά συστήματα κάνοντας χρήση προγραμμάτων περιήγησης από οποιοδήποτε μέρος και οποιαδήποτε στιγμή.

Ε) *Ενίσχυση των σχέσεων με τους πελάτες*: Ο συνδυασμός των μεγάλων δεδομένων και της δυνητικά απεριόριστης υπολογιστικής ισχύος θα επιτρέψει στις τράπεζες να αναπτύξουν συστήματα που θα έχουν την ικανότητα να παρέχουν περισσότερες και πιο ακριβείς γνώσεις σε σχέση με τους πελάτες τους και να οδηγηθούν έτσι στην λήψη καλύτερων αποφάσεων εκ μέρους τους. Επιπροσθέτως, θα μπορέσουν να εξατομικεύσουν περαιτέρω τις υπηρεσίες τους και να δημιουργούν αναλυτικά προφίλ των πελατών μέσω τεχνικών μηχανικής μάθησης που φιλοξενούνται στις υποδομές νέφους (**Machine Learning as a Service**).

ΣΤ) *Ευκολία διεκπεραίωσης τραπεζικών συναλλαγών*: Οι συναλλαγές που διενεργούνται μέσω του τραπεζικού συστήματος διευκολύνει την πραγματοποίηση πληρωμών ανάμεσα σε πωλητές και αγοραστές. Επί του παρόντος, οι δραστηριότητες που απαιτούνται για την επεξεργασία των πληρωμών είναι εγγενώς μη αποδοτικές καθώς κάνουν χρήση διαφορετικών τεχνολογιών. Ωστόσο, οι αγοραστές και οι πωλητές μπορούν να διευκολυνθούν και να συγκεντρωθούν μέσω της χρήσης κοινών εφαρμογών που φιλοξενούνται στο υπολογιστικό νέφος.[658]

7.5 Ζητήματα ασφαλείας και ιδιωτικότητας στο υπολογιστικό νέφος

Οι συνεχείς πρόοδοι στις τεχνολογίες της πληροφορίας επεκτείνουν τον πολλαπλασιασμό του υπολογιστικού νέφους σε νέα πεδία. Η ανάδυση των μεγάλων δεδομένων και οι πρόσφατες εξελίξεις σε πεδία όπως του διαδικτύου των πραγμάτων έχουν αυξήσει μαζικά τους όγκους των δεδομένων που παράγονται από τους περισσότερους οργανισμούς, οδηγώντας σε μια αυξημένη ανάγκη για εξωτερική ανάθεση της αποθήκευσης των δεδομένων σε παρόχους υπηρεσιών υπολογιστικού νέφους.[659] Στο επίπεδο του καταναλωτή, η δημοτικότητα αλλά και ο αριθμός των εφαρμογών κινητής τηλεφωνίας που μεταφορτώνονται από τους χρήστες έχει επίσης οδηγήσει σε μια εξάρτηση από το υπολογιστικό νέφος ώστε να επιλυθούν τα προβλήματα χωρητικότητας. Η τάση αυτή αναφέρεται και ως κινητή – υπολογιστική νέφους (**mobile - cloud computing**). Η μεγάλη αυτή εξάρτηση από τις τεχνολογίες νέφους επιδεινώνει σημαντικά τον κίνδυνο να

[658] Ibid., 51.
[659] Paul Benjamin Lowry, Tamara Dinev and Robert Willison, "Why Security and Privacy Research Lies at The Centre of The Information Systems (IS) Artefact: Proposing A Bold Research Agenda", *European Journal of Information Systems* 26, no. 6 (2017): 547, doi:10.1057/s41303-017-0066-x.

συμβούν περιστατικά που απειλούν την ασφάλεια και την ιδιωτικότητα ενώ παράλληλα αυξάνει περαιτέρω τους κινδύνους που σχετίζονται με τα παραδοσιακά τρωτά σημεία ασφαλείας. Η ιδιωτικότητα και η ασφάλεια αποτελούν σημαντικές προκλήσεις και πιθανά εμπόδια, τόσο για τους οργανισμούς που εξετάζουν την υιοθέτηση αλλά και για όσους ήδη βασίζονται στις υπηρεσίες υπολογιστικού νέφους και τους παρόχους υπηρεσιών νέφους. Πράγματι, τα ζητήματα που αφορούν την ασφάλεια και την ιδιωτικότητα εντός του πεδίου της υπολογιστικής νέφους είναι πολύ μεγαλύτερα σε σχέση με αυτά που είναι παρόντα όταν τα δεδομένα είναι αποθηκευμένα σε μια συγκεκριμένη τοποθεσία.[660]Αυτό οφείλεται εν μέρει στο γεγονός ότι τα δεδομένα που είναι αποθηκευμένα στο νέφος είναι συχνά σε μη κρυπτογραφημένη μορφή και επομένως είναι ευάλωτα σε πολλές ευπάθειες.[661] Επιπροσθέτως, η χρήση της υπολογιστικής νέφους συχνά συμπεριλαμβάνει την μετακίνηση των δεδομένων πέρα από τα όρια των διεθνών συνόρων απαιτώντας έτσι την εξέταση των νομικών απαιτήσεων των διαφορετικών δικαιοδοσιών, καθιστώντας παράλληλα πιο πολύπλοκη την ικανότητα των οργανισμών να παρατηρούν και να διαχειρίζονται τις ροές δεδομένων και να διατηρούν την ιδιωτικότητα των καταναλωτών.[662]

Γενικότερα, η ασφάλεια των πληροφοριών αναφέρεται στην διατήρηση των τριών αρχών της ασφάλειας. Οι αρχές αυτές είναι η εμπιστευτικότητα (**confidentiality**), η ακεραιότητα (**integrity**) και η διαθεσιμότητα (**availability**) των πληροφοριών, ενώ θα πρέπει παράλληλα να ληφθούν υπόψιν άλλοι κίνδυνοι που σχετίζονται με την αξιοπιστία, την αυθεντικότητα και την λογοδοσία.[663] Στο πλαίσιο της υπολογιστικής νέφους, οι κύριες ευπάθειες ασφαλείας στις οποίες θα πρέπει να δοθεί προσοχή είναι η εμπιστοσύνη, η κρυπτογράφηση, η κοινόχρηστη φύση (multi – tenancy) και η αξιοπιστία. Επιπροσθέτως, οι ευπάθειες αυτές οδηγούν σε σοβαρούς κινδύνους για την ασφάλεια που σχετίζονται με την ακεραιότητα, την εμπιστευτικότητα των δεδομένων, την απώλεια των δεδομένων και την αυθεντικοποίηση των δεδομένων. Οι ερευνητικές προσπάθειες που αφορούν τα ζητήματα αυτά έχουν υποστηρίξει μέσω των ευρημάτων τους την σχετικότητα των κινδύνων αυτών. Επί παραδείγματι, στην έρευνά της σχετικά με τους παράγοντες που επηρεάζουν την υιοθέτηση του υπολογιστικού νέφους στον δημόσιο τομέα στην Νότια Αφρική, η Scholtz ανακάλυψε ότι η προσβασιμότητα στα δεδομένα αποτελούσε παράγοντα ανησυχίας για το ενενήντα τοις εκατό των συμμετεχόντων και οι κυβερνοεπιθέσεις αποτελούσαν παράγοντα ανησυχίας για το εβδομήντα έξι τοις εκατό των συμμετεχόντων.[664] Η ασφάλεια και η ιδιωτικότητα είναι άρρηκτα συνδεδεμένες καθώς κάθε περιστατικό ασφαλείας θέτει την ιδιωτικότητα των δεδομένων των υποκειμένων σε κίνδυνο. Επιπροσθέτως, αυτά τα ζητήματα ασφαλείας μπορεί να

---

[660] Ramireddy, Srilakshmi, Chakraborthy, Rajarshi, Raghu, T.S. and Rao, H. Raghav, "Privacy and Security Practices in the Arena of Cloud Computing - A Research in Progress" (2010). *AMCIS 2010 Proceedings*. 574. https://aisel.aisnet.org/amcis2010/574

[661] Ishan Senarathna et al., "Security and Privacy Concerns for Australian Smes Cloud Adoption: Empirical Study of Metropolitan Vs Regional SMEs", *Australasian Journal of Information Systems* 20 (2016): 2, doi:10.3127/ajis.v20i0.1193.

[662] Paul Benjamin Lowry, Tamara Dinev and Robert Willison, "Why Security and Privacy Research Lies at The Centre of The Information Systems (IS) Artefact: Proposing A Bold Research Agenda", *European Journal of Information Systems* 26, no. 6 (2017): 547, doi:10.1057/s41303-017-0066-x.

[663] Siani Pearson and Azzedine Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing", *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, 2010, 695, doi:10.1109/cloudcom.2010.66.

[664] Scholtz, Brenda; Govender, Judian; and Gomez, Jorge Marx, "Technical and Environmental Factors Affecting Cloud Computing Adoption in the South African Public Sector" (2016). *CONF-IRM 2016 Proceedings*. 16. https://aisel.aisnet.org/confirm2016/16

οδηγήσουν σε ασαφείς κινδύνους ή ανησυχίες όπως η απώλεια της εμπιστοσύνης στην αξιοπιστία του νέφους αλλά και σε φόβους σχετικά με την πρόσβαση στα προσωπικά δεδομένα.[665]

Στο πλαίσιο της υπολογιστικής νέφους, υπάρχουν πολλά ζητήματα ιδιωτικότητας τα οποία οι οργανισμοί θα πρέπει να εξετάσουν και να επιλύσουν, συμπεριλαμβανομένων των ζητημάτων που άπτονται του ελέγχου, της μη εξουσιοδοτημένης δευτερεύουσας χρήσης των δεδομένων και της μη ορθής πρόσβασης. Ωστόσο, η πλειοψηφία των υφιστάμενων ερευνών που αφορούν την ιδιωτικότητα στο υπολογιστικό νέφος, έχει εστιάσει στις τεχνικές λύσεις ώστε να τεθούν τα δεδομένα σε καθεστώς ασφαλείας τόσο από το σχεδιασμό όσο και σε σχέση με τις αρχιτεκτονικές πλευρές του νέφους.[666] Οι ανησυχίες των ατόμων σχετικά με την απώλεια της ιδιωτικότητάς τους κατά τη χρήση των υπολογιστικών νεφών αφορούν κυρίως την συλλογή και την αποθήκευση μεγάλων όγκων προσωπικών δεδομένων από τους οργανισμούς. Οι καταναλωτές συχνά παρουσιάζουν άγνοια σχετικά με τον τρόπο με τον οποίο αποθηκεύονται και διασπείρονται τα δεδομένα τους στο νέφος, ενώ συχνά δεν γνωρίζουν αν αυτά χρησιμοποιούνται για σκοπούς διαφορετικούς σε σχέση με αυτούς για τους οποίους συνελέγησαν. Για παράδειγμα, σε περιπτώσεις που αφορούν αποθηκευτικές υπηρεσίες όπως το Google Drive ή το Dropbox, η αποθήκευση των προσωπικών πληροφοριών στο νέφος αποτελεί τον κύριο σκοπό της υπηρεσίας και επομένως η χρήση είναι διαφανής. Στις περιπτώσεις όμως εφαρμογών όπως αυτών που χρησιμοποιούνται από τις συσκευές του διαδικτύου των πραγμάτων, οι χρήσεις και οι σκοποί δεν είναι πάντα σαφείς και διαφανείς. Τα δεδομένα μπορεί να αποθηκεύονται στην συσκευή, σε τοπικό επίπεδο, ή στο νέφος, ή μέσω του συνδυασμού κάποιων από αυτών. Οι καταναλωτές μπορεί να μην έχουν καν επίγνωση για το που αποθηκεύονται τα δεδομένα τους.[667] Σε άλλες περιπτώσεις, όπως αυτές που αφορούν την χρήση νέφους από τα τραπεζικά ιδρύματα, οι ανησυχίες των καταναλωτών μπορεί να αφορούν την έλλειψη γνώσης σχετικά με το πώς ο οργανισμός χρησιμοποιεί και προστατεύει τα προσωπικά τους δεδομένα.[668]

Η εμπιστευτικότητα και η ιδιωτικότητα αποτελούν ζωτικές απαιτήσεις με τις οποίες οι πάροχοι υπηρεσιών νέφους θα πρέπει να συμμορφώνονται εφόσον τα ευαίσθητα δεδομένα των πελατών των τραπεζών μεταφέρονται στο νέφος. Η τράπεζα της Ελβετίας για παράδειγμα, τα τελευταία χρόνια έχει αποκτήσει καλή φήμη και χαίρει σεβασμού για την προστασία της ιδιωτικότητας των πελατών της. Παρομοίως, οι πάροχοι υπηρεσιών υπολογιστικής νέφους θα πρέπει να διασφαλίζουν ότι οι πολιτικές τους που σχετίζονται με την διατήρηση της ιδιωτικότητας των δεδομένων πείθει τους υφιστάμενους αλλά και τους μελλοντικούς πελάτες τους. Τα δεδομένα ενός οργανισμού αποτελούν σημαντικό κεφάλαιο για αυτόν και επομένως θα πρέπει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα ώστε να αποτρέπει τις παραβιάσεις που μπορεί να θέσουν σε κίνδυνο τα δεδομένα αυτά.[669]

---

[665] Theo Lynn et al., *Data Privacy and Trust in Cloud Computing*, 1st ed. (repr., Cham: Springer, 2021), 62.
[666] Ibid., 63
[667] Ibid., 65.
[668] Ibid., 66.
[669] Ranjit Bose, Xin (Robert) Luo and Yuan Liu, "The Roles of Security and Trust: Comparing Cloud Computing and Banking", *Procedia - Social and Behavioral Sciences* 73 (2013): 33, doi: 10.1016/j.sbspro.2013.02.015.

7.5.1 Οι κυριότερες απειλές για την ασφάλεια των προσωπικών δεδομένων στο σύννεφο

Σύμφωνα με το ISO 27001, μια απειλή αποτελεί ένα πιθανό γεγονός. Όταν η απειλή μετατρέπεται σε πραγματικό γεγονός, μπορεί να προκαλέσει ένα ανεπιθύμητο περιστατικό. Είναι ανεπιθύμητο διότι το περιστατικό μπορεί να βλάψει έναν οργανισμό ή ένα σύστημα, προκαλώντας ένα περιστατικό ασφαλείας ή ακόμα και παραβίαση της ιδιωτικότητας των χρηστών. Οι τρέχουσες προσπάθειες να ταξινομηθούν οι απειλές που αναγνωρίζονται στα περιβάλλοντα υπολογιστικού νέφους βασίζονται είτε στις εξαρτήσεις του νέφους (όπως το δίκτυο ή η κοινή μνήμη των εικονικών μηχανών) είτε στη χρήση διαφόρων εργαλείων αξιολόγησης, όπως το CRAMM[670] και το Octave. Η μέθοδος ταξινόμησης που παρουσιάζεται στην παρούσα ενότητα κάνει χρήση τριών διακριτών κατηγοριών: των απειλών που σχετίζονται με την υποδομή, των απειλών που σχετίζονται με τον πάροχο υπηρεσιών και των γενικών απειλών. Ο κύριος στόχος της προτεινόμενης ταξινόμησης είναι να μειώσει το φόρτο των διαχειριστών νέφους σε θέματα που σχετίζονται με την ασφάλεια, υποδεικνύοντας τα σημαντικά προβλήματα που αναδύονται και εξοικονομώντας έτσι χρόνο και χρήματα.

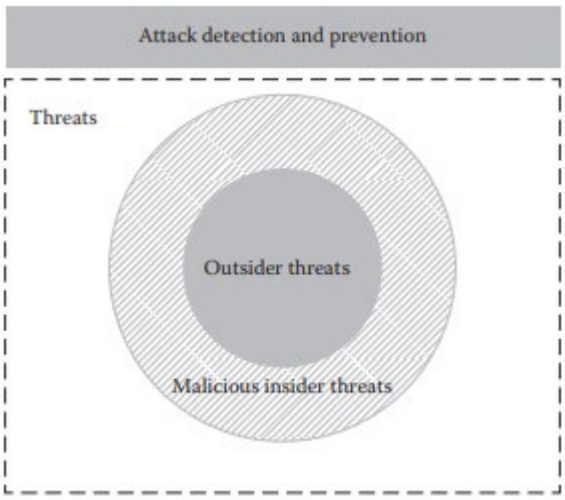
Πριν από μερικά χρόνια η ENISA παρουσίασε μια έρευνα που είχε τον τίτλο «Ασφάλεια στα συστήματα υπολογιστικής νέφους» («**Security in cloud computing systems**»).[671]Η έρευνα αυτή ξεκινά με την ανάλυση των πλεονεκτημάτων που προσφέρουν τα συστήματα υπολογιστικής νέφους. Ωστόσο, παρόλο που υπάρχουν πλεονεκτήματα σε σχέση με την κλίμακα και τους πόρους, όσον αφορά τις κύριες απειλές ασφαλείας, καθίσταται προφανές ότι τα πλεονεκτήματα υστερούν σε αριθμό. Η ίδια έρευνα κατηγοριοποιεί τις απειλές, διαχωρίζοντας αυτές σε απειλές πολιτικής και οργάνωσης, τεχνικές απειλές, νομικές απειλές και απειλές που δεν αφορούν αποκλειστικά το νέφος. Κάθε απειλή λαμβάνει μια βαθμολογία που ποικίλει ανάλογα με την πιθανότητα να συμβεί, την επίδρασή της, τις ευπάθειες που προκαλεί και τα στοιχεία που επηρεάζει. Καθίσταται επομένως σαφές ότι η εμφάνιση των συστημάτων υπολογιστικού νέφους έχει δημιουργήσει έναν νέο κόσμο απειλών ασφαλείας που ήταν άγνωστες στο παρελθόν. Καλά αντιπροσωπευτικά παραδείγματα αποτελούν η αποτυχία απομόνωσης (**isolation failure**), που αναφέρεται στην έλλειψη λογικής απομόνωσης και η οικονομική επίθεση άρνησης υπηρεσίας (**economic denial of service – EdoS**), που αναφέρεται στην εξάντληση των υπολογιστικών πόρων ενός συστήματος νέφους εκ προθέσεως από έναν πελάτη ώστε να παρεμποδιστεί ο πάροχος υπηρεσιών νέφους να παρέχει την υπηρεσία σε άλλους πελάτες. Ένα άλλο παράδειγμα αποτελεί η δράση του κακόβουλου εσωτερικού παράγοντα (**malicious insider**), που ως έννοια επαναπροσδιορίστηκε στο πλαίσιο των συστημάτων νέφους.

Η Συμμαχία Ασφαλείας του υπολογιστικού νέφους (***Cloud Security Alliance***) υποστηρίζει με τη σειρά της ότι, παρά τις ομοιότητες στους ελέγχους ασφαλείας ανάμεσα στα συστήματα πληροφορικής και τα συστήματα νέφους, υπάρχουν αρκετές διαφορές στις απειλές στις οποίες μπορεί να εκτεθεί ένας οργανισμός. Οι υπηρεσίες νέφους χρησιμοποιούν λειτουργικά μοντέλα και οι τεχνολογίες πίσω από αυτά είναι οι πηγές των νέων απειλών. Περαιτέρω, υπάρχουν διαφορές ως προς τις υποχρεώσεις ασφαλείας ανάμεσα στον πάροχο και τον καταναλωτή ανάμεσα στα μοντέλα υπηρεσιών νέφους. Επιπροσθέτως, καθώς οι πάροχοι υπηρεσιών νέφους στοχεύουν στην

[670]https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_cramm.html
[671] https://www.enisa.europa.eu/publications/security-and-resilience-in-governmental-clouds

αποδοτικότητα κόστους, επιτυγχάνοντας έτσι την κλίμακα, την επανάχρηση και την τυποποίηση, φτάνουν σε ένα σημείο στο οποίο οι μηχανισμοί ασφαλείας χάνουν την ελαστικότητά τους. Τόσο η ENISA όσο και η Συμμαχία, αναφέρονται στους πελάτες και στους απλούς χρήστες συστημάτων νέφους, οι οποίοι μπορούν να καταστούν μια από τις μεγαλύτερες απειλές μαζί με τους χρήστες που έχουν διαβαθμισμένα προνόμια. Σε σχέση με τις παραδοσιακές υπηρεσίες πληροφορικής, η επιφάνεια επίθεσης στο υπολογιστικό νέφος έχει διευρυνθεί, όχι μόνο εξαιτίας των διαμοιραζόμενων πόρων αλλά και εξαιτίας των επιπρόσθετων φορέων επίθεσης που ο επιτιθέμενος μπορεί να χρησιμοποιήσει για να εκμεταλλευτεί μια πιθανή ευπάθεια στην εικονική μηχανή (**Virtual Machine – VM**), στην πλατφόρμα διαχείρισης του νέφους, ή σε κάθε άλλο συστατικό στοιχείο της υποδομής νέφους. Ως αποτέλεσμα η απειλή του εσωτερικού κακόβουλου παράγοντα έχει εξελιχθεί σε μια από τις μεγαλύτερες προκλήσεις ασφαλείας στα περιβάλλοντα υπολογιστικής νέφους.[672]

Σύμφωνα με τον Xiao, ο όρος κάτοχος εμπιστευτικών πληροφοριών (**insider**), για ένα σύστημα πληροφορικής, εφαρμόζεται σε οποιονδήποτε έχει εγκεκριμένη πρόσβαση, προνόμια, ή γνώση του πληροφορικού συστήματος και των υπηρεσιών και αποστολών του. Ένας κακόβουλος τέτοιος παράγοντας είναι κάποιος που έχει κίνητρο να επηρεάσει αρνητικά την αποστολή ενός οργανισμού μέσα από μια σειρά δράσεων που θέτουν σε κίνδυνο την εμπιστευτικότητα των πληροφοριών, την ακεραιότητα και την διαθεσιμότητα, εκμεταλλευόμενος τα προνόμιά του/της. Για τα συστήματα υπολογιστικής νέφους, ένας τέτοιος παράγοντας μπορεί να είναι μια οντότητα που εργάζεται για τον πάροχο φιλοξενίας του νέφους, έχει προνομιακή πρόσβαση στους πόρους νέφους και χρησιμοποιεί τις υπηρεσίες νέφους. Οι δράσεις των προσώπων αυτών μπορεί να έχουν ως αποτέλεσμα την προσωρινή διακοπή, την παραβίαση της ιδιωτικότητας των χρηστών, ή ακόμα και την μόνιμη διακοπή των παρεχόμενων υπηρεσιών, ανάλογα με τα προνόμιά τους.[673]



Εικόνα 7. Οι απειλές των κακόβουλων εσωτερικών παραγόντων

[672] John R Vacca, *Cloud Computing Security: Foundations and Challenges*, 1st ed. (repr., Boca Raton, FL: CRC Press, Taylor & Francis Group, 2017), 47-48.
[673] Zhifeng Xiao and Yang Xiao, "Security and Privacy in Cloud Computing", *IEEE Communications Surveys & Tutorials* 15, no. 2 (2013): 848, doi:10.1109/surv.2012.060912.00182.

7.5.2 Ταξινόμηση των απειλών κατά των συστημάτων υπολογιστικού νέφους και αντίμετρα

Με στόχο τη διευκόλυνση της ανάλυσης των απειλών που αντιμετωπίζονται στα συστήματα υπολογιστικού νέφους, είναι απαραίτητο να ταξινομηθούν οι αναγνωρισμένες απειλές σε διακριτές κατηγορίες. Η ταξινόμηση αυτή μπορεί να χρησιμοποιεί τρεις κύριες κατηγορίες: α) τις απειλές που σχετίζονται με τις υποδομές, οι οποίες επηρεάζουν συνολικά τη δομή του νέφους, β) τις απειλές που αφορούν τους παρόχους υπηρεσιών, οι οποίες μπορεί να επηρεάσουν τους πελάτες που αναζητούν μια υπηρεσία στο νέφος και γ) τις γενικές απειλές που μπορεί να επηρεάσουν τόσο τις υποδομές όσο και τους παρόχους υπηρεσιών και τους πελάτες.

7.5.2.1 Απειλές που σχετίζονται με τις υποδομές νέφους

Η πλειοψηφία των απειλών στα συστήματα νέφους σχετίζονται με την συνολική υποδομή αυτών. Αυτές είτε κληρονομούνται από τις παραδοσιακές δομές πληροφορικής είτε σχετίζονται αποκλειστικά με το νέφος. Σεισμοί, πλημμύρες, τυφώνες, φωτιές και άλλες φυσικές καταστροφές μπορούν να έχουν καταστροφικές επιπτώσεις στα συστήματα και σε υπό άλλες περιστάσεις στην ανθρώπινη ζωή. Συστήματα αξιολόγησης του ρίσκου, όπως το CRAMM και το Octave, μπορούν να ελαχιστοποιήσουν τις συνέπειες των φυσικών καταστροφών. Επιπροσθέτως, στην κατηγορία αυτή εντάσσονται οι περιπτώσεις μη εξουσιοδοτημένης πρόσβασης στις εγκαταστάσεις των συστημάτων νέφους. Αυτή η φυσική πρόσβαση μπορεί να απειλήσει τις συσκευές και τον εξοπλισμό των συστημάτων και να οδηγήσει σε επιθέσεις αρνήσεως πρόσβασης (**denial of service – DoS**) για μακρά χρονικά διαστήματα.

Σε πολλές περιπτώσεις, οι εργαζόμενοι μπορεί να θέσουν σε σοβαρό κίνδυνο το σύστημα του νέφους. Η έλλειψη ορθής εκπαίδευσης ή η αμέλεια είναι στενά συνδεδεμένες με τις απρόσεκτες και απρόβλεπτες ενέργειες του μέσου εργαζομένου. Οι ενέργειες αυτές μπορούν να οδηγήσουν στην τυχαία απώλεια ή την διαγραφή εφεδρικών δεδομένων και αρχείων καταγραφής ασφαλείας ή λειτουργίας. Ένα σχέδιο διαχείρισης κινδύνου σε συνδυασμό με την ανάπτυξη μιας πλήρους πολιτικής ασφαλείας μπορούν να συμβάλλουν στην αποφυγή παρόμοιων περιστατικών. Τα μέτρα αυτά βοηθούν τους υπαλλήλους να ακολουθήσουν ένα πρωτόκολλο διαδικασιών, μειώνοντας σημαντικά την πιθανότητα να κάνουν κρίσιμα και μη αναστρέψιμα λάθη.

Το φαινόμενο του «dumpster diving» αποτελεί επίσης ένα ρίσκο στο οποίο εκτίθενται οι οργανισμοί ή τα άτομα μέσω της απόρριψης πληροφοριών που μπορεί τελικά αποδειχθούν χρήσιμες. Δεν υπάρχει όριο στην εκμετάλλευση των πληροφοριών που ανευρίσκοντα στα απορρίμματα. Αυτές οι απορριφθείσες πληροφορίες μπορεί να συμπεριλαμβάνουν κωδικούς πρόσβασης, τηλεφωνικούς αριθμούς, αριθμούς πιστωτικών καρτών κ.α. Πολλές φορές σε αυτές μπορεί να συμπεριλαμβάνονται χρήσιμες πληροφορίες για πιθανούς επιτιθέμενους στα συστήματα νέφους. Οι διαρροές πληροφοριών μπορούν επίσης να αποτελέσουν αντικείμενο εκμετάλλευσης από κακόβουλους χρήστες που επιχειρούν να εκκινήσουν επιθέσεις κοινωνικής μηχανικής (**social engineering**), ή να θέσουν σε ισχύ πιο επικίνδυνα σενάρια. Κάθε οργανισμός πρέπει να υιοθετήσει/εγκαθιδρύσει πολιτικές σχετικές με τον κύκλο ζωής και την προστασία των ευαίσθητων πληροφοριών και θα πρέπει να διασφαλίσει ότι οι πολιτικές ακολουθούνται από τους εργαζομένους χωρίς εξαιρέσεις.

Μέσω της χρήσης τεχνικών κοινωνικής μηχανικής και άλλων εργαλείων, όπως το «Social Engineering Toolkit» και το «TrustedSec», οι κακόβουλοι χρήστες μπορούν να μαντέψουν τους κωδικούς που χρησιμοποιούνται. Αυτό το είδος επιθέσεως απαιτεί πολλές προσπάθειες (**brute force attack**) και επομένως είναι εύκολο να αποτραπεί θέτοντας ένα όριο λανθασμένων κωδικών πρόσβασης.

Περαιτέρω, η μη εξουσιοδοτημένη πρόσβαση μπορεί να επιτευχθεί μέσω επιθέσεων πειρατείας (hacking) ή κοινωνικής μηχανικής (**social engineering**). Μέσω των επιθέσεων αυτών ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση, αποκτώντας τα στοιχεία εισόδου του χρήστη. Ένα παράδειγμα αντίστοιχου προβλήματος αποτελεί το πρόγραμμα εκμετάλλευσης ευπάθειας SYSRET, στο οποίο κακόβουλα τρίτα μέρη εκμεταλλεύονται στο σύνολο οδηγιών (**instruction set**) της AMD, SYSRET, εφαρμόζοντας αυτό σε πλατφόρμες της Intel. Για να αποφευχθούν τέτοια σενάρια, είναι απαραίτητο να χρησιμοποιούνται τα κατάλληλα και ενημερωμένα αντίμετρα ασφαλείας και να εφαρμόζεται ο αυστηρός έλεγχος πρόσβασης.[674]

Επιπροσθέτως, κάθε ενέργεια σε ένα μεγάλης κλίμακας πληροφοριακό σύστημα, παρακολουθείται και αποθηκεύεται σε λεπτομερή αρχεία καταγραφής. Αυτά τα αρχεία, που χρησιμοποιούνται κυρίως από τους διαχειριστές συστημάτων και τους ελεγκτές, παρέχουν κρίσιμα τμήματα πληροφοριών που μπορούν να χρησιμοποιηθούν από κακόβουλα τρίτα μέρη για να επιτεθούν. Επιπροσθέτως, τα αρχεία αυτά μπορούν να εκθέσουν την ταυτότητα των χρηστών καθώς συμπεριλαμβάνουν ευαίσθητα και ιδιωτικά δεδομένα. Η προστασία των αρχείων αυτών θα πρέπει να έχει υψηλή προτεραιότητα, εφόσον η διακινδύνευσή τους μπορεί να επηρεάσει ολόκληρα τα συστήματα ή τους χρήστες τους.

Τα κακόβουλα τρίτα μέρη, με στόχο την απόκτηση πληροφοριών που αφορούν το σύστημα υπολογιστικού νέφους, χρησιμοποιούν εργαλεία διερεύνησης του δικτύου όπως το «hping», το «Nmap» και το «Wget» για να παρακολουθήσουν το δίκτυο της υποδομής νέφους. Συχνά εγκαθιστούν κακόβουλο λογισμικό (malware) που συλλέγει πληροφορίες για να χαρτογραφήσουν το σύστημα νέφους. Όταν ένας χρήστης γνωρίζει την τρέχουσα θέση του είτε εντός του δικτύου είτε στη φυσική μηχανή της υποδομής νέφους, μπορεί να χρησιμοποιήσει αυτήν για να κλιμακώσει τα προνόμιά του και να αποκτήσει πρόσβαση σε άλλες εικονικές μηχανές. Σε τέτοιες περιπτώσεις, ο κακόβουλος χρήστης μπορεί να αποκτήσει παρανόμως πληροφορίες στις οποίες εναλλακτικά δεν θα είχε δικαίωμα να αποκτήσει πρόσβαση.

Περαιτέρω, η πρόοδος στην κρυπτανάλυση μπορεί να καταστήσει έναν μηχανισμό κρυπτογράφησης ή έναν αλγόριθμο μη ασφαλή. Από την άλλη μεριά, αποτελεί συχνό φαινόμενο τα συστήματα νέφους να μην εφαρμόζουν με ακρίβεια τα πρωτόκολλα κρυπτογράφησης, ενώ στη χειρότερη περίπτωση δεν υπάρχει καν κρυπτογράφηση. Επομένως, η εξαντλητική εφαρμογή σύγχρονων τεχνικών κρυπτογράφησης θα πρέπει να αποτελεί προτεραιότητα καθώς μπορεί να προστατεύσει το σύστημα από πολλαπλές κακόβουλες ενέργειες.

Επίσης θα πρέπει να γίνει αναφορά στην απειλή που συνιστούν οι επιθέσεις οικονομικής αρνήσεως εξυπηρέτησης (Economic denial of service – EDoS). Αποτελεί ένα νέο είδος απειλής

---

[674] John R Vacca, *Cloud Computing Security: Foundations and Challenges*, 1st ed. (repr., Boca Raton, FL: CRC Press, Taylor & Francis Group, 2017), 49.

που έχει εμφανιστεί στα περιβάλλοντα υπολογιστικής νέφους. Τα πιο πιθανά σενάρια αφορούν την κλοπή ταυτότητας, στα οποία ένας επιτιθέμενος μπορεί να κλέψει τον λογαριασμό και τους πόρους ενός πελάτη ώστε να τα χρησιμοποιήσει προς όφελός του. Στις περιπτώσεις αυτές, ο επιτιθέμενος αποκτά ελεύθερη πρόσβαση σε υπηρεσίες ενώ ο λογαριασμός του θύματος χρεώνεται για τις υπηρεσίες αυτές. Επιπροσθέτως, ο επιτιθέμενος μπορεί να κάνει χρήση της κλεμμένης ταυτότητας και δρώντας κακόβουλα, να απειλήσει την φήμη του θύματος. Στα σενάρια αυτά, οι υπηρεσίες μπορεί να μην είναι διαθέσιμες στους πελάτες και ο έλεγχος πρόσβασης μπορεί να έχει διακυβευθεί. Πέρα από αυτό, η αξιοπιστία του παρόχου νέφους μπορεί να απειληθεί. Οι επιθέσεις αυτές έχουν ως κύριο στόχο τον πάροχο υπηρεσιών και ως δευτερεύον στόχο τους πελάτες αυτών.[675] Οι Kalinski και Pauley προτείνουν την αξιολόγηση ρίσκου (***risk assessment***) ως ένα τρόπο να αποφευχθούν οι επιθέσεις αυτές.[676]

Παράλληλα με τις επιθέσεις άρνησης υπηρεσίας που μπορούν να καταστήσουν τις υπηρεσίες νέφους μη διαθέσιμες για μικρά χρονικά διαστήματα, είναι επίσης πιθανό να συμβεί ένα σφάλμα ή ένας τερματισμός της υπηρεσίας, σηματοδοτώντας μια μόνιμη ή μια προσωρινή ανικανότητα της υποδομής νέφους να παρέχει τις υπηρεσίες της. Αυτό μπορεί να επέλθει ως αποτέλεσμα λόγων κακόβουλων ενεργειών χρηστών που έχουν καταφέρει να αποκτήσουν διαβαθμισμένα προνόμια εντός των υποδομών και να αποκτήσουν κατά αυτόν τον τρόπο πρόσβαση σε μηχανισμούς που μπορούν να διαταράξουν την λειτουργικότητα των παρεχόμενων υπηρεσιών. Η εγκατάσταση συστημάτων αποδοτικού εντοπισμού εισβολών (**Efficient Intrusion Detection System - IDS**) σε πολλαπλές εικονικές μηχανές, μπορεί αποτελεσματικά να μειώσει τον κίνδυνο τέτοιων απειλών.[677]

Πολλά προβλήματα προκύπτουν επίσης όταν οι υποδομές νέφους αλλάζουν κυριότητα και πολιτικές, ενώ οι παλαιοί χρήστες παραμένουν ως πελάτες. Μια δυσκολία που κρίνεται σημαντική εμφανίζεται όταν οι πελάτες δεν μπορούν εύκολα να μεταφέρουν είτε τις υπηρεσίες τους είτε τα δεδομένα τους από έναν πάροχο υπηρεσιών νέφους σε έναν άλλο. Στις περιπτώσεις αυτές έχουμε πολλαπλά προβλήματα κλειδώματος (lock – in) που εξαρτώνται από την αρχιτεκτονική του συστήματος νέφους. Και στις τρεις αρχιτεκτονικές (SaaS, PaaS, IaaS), το πρόβλημα του κλειδώματος των δεδομένων είναι εμφανές. Είναι εξαιρετικά δύσκολο να αφαιρεθούν τα δεδομένα κάθε ξεχωριστού πελάτη εξαιτίας τεχνικών ή νομικών δυσκολιών. Στην περίπτωση της αρχιτεκτονικής SaaS, το πρόβλημα του κλειδώματος των δεδομένων μπορεί επίσης να αναδυθεί. Αυτό σημαίνει ότι κάθε πάροχος υπηρεσιών νέφους χρησιμοποιεί διαφορετικά εργαλεία για τον έλεγχο και την παρακολούθηση όπως το openQRM, το Cobbler, το Crowbar και το Spacewalk. Στην αρχιτεκτονική PaaS, το πρόβλημα εντοπίζεται στο επίπεδο της διεπαφής καθώς οι πάροχοι υπηρεσιών δεν χρησιμοποιούν την ίδια πλατφόρμα εικονικότητας. Το πρόβλημα του κλειδώματος στην αρχιτεκτονική IaaS εξαρτάται από την υποδομή που χρησιμοποιεί κάθε πελάτης. Για να αποφευχθούν τέτοια προβλήματα, η επιλογή του κατάλληλου παρόχου υπηρεσιών θα πρέπει να

---

[675] John R Vacca, *Cloud Computing Security: Foundations and Challenges*, 1st ed. (repr., Boca Raton, FL: CRC Press, Taylor & Francis Group, 2017), 50.

[676]Burton S. Kaliski Jr and Wayne Pauley, "Toward Risk Assessment as a Service in Cloud Environments", *Proceedings of the 2nd USENIX Conference on Hot Topics in Cloud Computing*, 2010, 13.

[677] Sebastian Roschke, Feng Cheng and Christoph Meinel, "An Advanced IDS Management Architecture", *Journal of Information Assurance and Security* 5 (2010): 246.

αποφασιστεί έπειτα από ενδελεχή έρευνα, ενώ ιδιαίτερη προσοχή θα πρέπει να δοθεί σε κάθε αλλαγή που συντελείται στο υπολογιστικό νέφος.[678]

7.5.2.1.1 Προέλευση των δεδομένων στο υπολογιστικό νέφος, διαχείριση μεταδεδομένων και δικαιοδοσία

Τα ζητήματα που σχετίζονται με την προέλευση των δεδομένων αποτελούν ανοιχτά ζητήματα που ουσιαστικά κληρονομούνται από τις παραδοσιακές πληροφορικές δομές μεγάλης κλίμακας. Καθώς τα συστήματα νέφους έχουν ποικίλα στοιχεία της υποδομής τους κατανεμημένα σε διαφορετικές χώρες, οι απειλές για τα δεδομένα πολλαπλασιάζονται. Ειδικότερα, στην κατηγορία αυτή εντάσσονται τα ζητήματα που αφορούν την προέλευση των δεδομένων που βρίσκονται στο νέφος, την δυναμική των δεδομένων και των ροών δεδομένων, τις τοποθεσίες των αρχείων αλλά και τις πληροφορίες που αφορούν τις πηγές εισόδου και εξόδου των εφαρμογών (input/output information). Επίσης, εδώ εντάσσονται και τα ζητήματα που αφορούν την προέλευση των ροών εργασίας στο νέφος (**cloud workflow provenance**), την δομή, τη μορφή και την εξέλιξη της ίδιας της ροής εργασίας. Λαμβάνοντας υπόψιν τις παραμέτρους αυτές και τις προκλήσεις που εμφανίζονται, κάθε πάροχος υπηρεσιών θα πρέπει να δημιουργεί το δικό του σύστημα προέλευσης, ώστε να εγγυάται την ποιότητα των παρεχόμενων υπηρεσιών και να προστατεύει την εμπιστευτικότητα των δεδομένων και την ιδιωτικότητα των πελατών του. Εάν αυτές οι απαιτήσεις παραμείνουν ανικανοποίητες, μπορεί να προκύψουν προβλήματα δικαιοδοσίας σχετικά με τα δεδομένα και την αποθήκευσή τους.

Παράλληλα με την προέλευση των δεδομένων, ένα άλλο σοβαρό ζήτημα στην υπολογιστική νέφους είναι η επεξεργασία των δεδομένων. Ένας πελάτης δεν μπορεί να είναι σίγουρος για τον τρόπο με τον οποίο γίνεται διαχείριση των δεδομένων του από το σύστημα νέφους και εάν η επεξεργασία αυτή συμμορφώνεται με το νομικό πλαίσιο της χώρας στην οποία κατοικεί. Κάποιοι πάροχοι υπηρεσιών νέφους περιγράφουν τις διαδικασίες που ακολουθούν και τις πιστοποιήσεις που έχουν λάβει, αλλά ακόμα και αν τα δεδομένα είναι προστατευμένα από κακόβουλες ενέργειες, δεν μπορεί να διασφαλιστεί ότι τα αποθηκευμένα δεδομένα των χρηστών έχουν αποκτηθεί με νόμιμο τρόπο ή όχι. Για να μπορούν να αξιολογηθούν τα δεδομένα με όρους νομιμότητας και να προστατεύονται από πιθανή αποκάλυψή τους χωρίς να παραβιάζεται η ιδιωτικότητα των χρηστών, προτείνεται η επίσημη συμφωνία σε επίπεδο υπηρεσιών (service level agreement – SLA) ανάμεσα σε πάροχο και χρήστη, ώστε να διατυπώνονται με σαφήνεια οι υποχρεώσεις των δύο πλευρών. Παράλληλα θα πρέπει να εφαρμόζεται από τον πάροχο υπηρεσιών ένα μοντέλο εμπιστοσύνης που θα καθορίζει τις ελάχιστες απαιτήσεις για να επιτευχθεί ένα αποδεκτό επίπεδο ασφάλειας των δεδομένων.

Σε περίπτωση που ο πάροχος αλλάξει διοικητικό προσωπικό ή πωληθεί το σύστημά του σε άλλη εταιρεία, θα πρέπει να διατηρούνται τα προισχύοντα μέτρα ασφαλείας για ένα χρονικό διάστημα μέχρι η νέα διοίκηση αποφασίσει να αλλάξει αυτά. Με αυτόν τον τρόπο θα διασφαλιστεί η εμπιστευτικότητα, ακεραιότητα και η διαθεσιμότητα των δεδομένων των χρηστών.[679]

---

[678] John R Vacca, *Cloud Computing Security: Foundations and Challenges*, 1st ed. (repr., Boca Raton, FL: CRC Press, Taylor & Francis Group, 2017), 51.
[679] Ibid., 52.

7.5.2.2 Απειλές που σχετίζονται με τους παρόχους υπηρεσιών νέφους

Μια άλλη κατηγορία που έχει εμφανιστεί στα συστήματα νέφους αφορά τις απειλές που σχετίζονται με τους παρόχους υπηρεσιών. Οι απειλές αυτές διαφοροποιούνται από τις άλλες δύο κατηγορίες καθώς επηρεάζουν τους πελάτες που αναζητούν μια υπηρεσία νέφους. Παρά το γεγονός ότι μακροπρόθεσμα οι απειλές αυτές μπορούν να βλάψουν ολόκληρη την υποδομή νέφους, οι πελάτες αντιμετωπίζουν τις αρχικές επιπτώσεις.

Σημαντικές στην κατηγορία αυτή είναι οι επιθέσεις επανάληψης (**replay attacks**) που είναι παραπλήσιες με τις επιθέσεις «man in the middle». Στην περίπτωση αυτή, ο επιτιθέμενος υποκλέπτει και αποθηκεύει τα μεταδιδόμενα μηνύματα. Αφού τα τροποποιήσει με δόλιο σκοπό (**spoofing**), ο επιτιθέμενος τα αποστέλλει εκ νέου στην υπηρεσία, υποδυόμενος έναν από τους συμμετέχοντες που επικοινωνούν. Η χρήση νέων και τυχαίως παραγόμενων συμβολοσειρών (**alphanumeric strings / nonces**) στα μηνύματα μπορεί να αντιμετωπίσει τα προβλήματα αυτά επιτυχώς. Άλλα αντίμετρα συμπεριλαμβάνουν μια χρονοσφραγίδα, που υποδεικνύει τον χρόνο κατά τον οποίο απεστάλη το μήνυμα.

Στη συνέχεια, οι μέθοδοι υποκλοπής και αναχαίτησης μηνυμάτων αποτελούν μια ομάδα επιθέσεων που αρχικά έκαναν την εμφάνισή τους στις παραδοσιακές υποδομές πληροφορικής. Εδώ εντάσσονται οι επιθέσεις «man in the middle», η λαθρακρόαση (**eavesdropping**), και η επιθέσεις μέσω πλάγιων καναλιών (**side channel attacks**). Στον πρώτο τρόπο επίθεσης, ο επιτιθέμενος μπορεί να υποδυθεί το θύμα αλλάζοντας το δημόσιο κλειδί ή τον συσχετισμό χρήστη. Ως αποτέλεσμα, ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του επιτιθέμενου. Επομένως, ο τελευταίος μπορεί να λάβει, να αποκρυπτογραφήσει και να τροποποιήσει το μήνυμα. Τέλος, ο επιτιθέμενος κρυπτογραφεί το πλαστογραφημένο μήνυμα με το αληθινό δημόσιο κλειδί του θύματος και το προωθεί στο θύμα. Η λαθρακρόαση (**eavesdropping**) μπορεί να πραγματοποιηθεί μέσω κοινωνικής μηχανικής, περισυλλογής δεδομένων (**data scavenging**), οικονομικής ή πολιτικής κατασκοπίας, παρακολούθησης της πληκτρολόγησης και μέσω τακτικών «**sniffing**» και «**shoulder surfing**». Ο στόχος είναι να αποκτηθούν πληροφορίες ή να τεθούν τα θεμέλια για μετέπειτα επιθέσεις. Η επίθεση πλαγίου καναλιού πραγματοποιείται μέσω της χρήσης πλάγιων καναλιών σε κοινόχρηστο υλισμικό που επιτρέπει στους επιτιθέμενους να διεισδύσουν σε ευαίσθητα δεδομένα, εντός εικονικών μηχανών στην υποδομή νέφους.

Περαιτέρω, οι επιθέσεις «XML Signature Element Wrapping» αποτελούν επιθέσεις στα πρωτόκολλα που χρησιμοποιούν υπογραφές XML (**extensible markup language**) για την αυθεντικοποίηση και την προστασία της ακεραιότητας και εφαρμόζεται σε δικτυακές υπηρεσίες και συστήματα νέφους. Αποτελούσαν απλά θεωρία μέχρι το 2008, όταν ανακαλύφθηκε ότι οι υπηρεσίες EC2 της Amazon ήταν ευάλωτες σε τέτοιου είδους επιθέσεις. Η συγκεκριμένη ευπάθεια ήταν ουσιαστικά μια εκμετάλλευση της αρχιτεκτονικής SOAP (**simple object access protocol**) που χρησιμοποιήθηκε σε συνδυασμό με την τεχνική αυτή. Αυτές οι ομάδες επιθέσεων δεν μπορούν να εντοπιστούν με ευκολία και αποτελούν μεγάλη απειλή για το υπολογιστικό νέφος.

Σοβαρές θεωρούνται επίσης οι ευπάθειες που οφείλονται σε επιθέσεις έγχυσης SQL (**SQL injection attacks**), οι οποίες εκμεταλλεύονται τις καταχωρίσεις στις υπηρεσίες ή στις εφαρμογές. Τέτοιου είδους εκμετάλλευση μπορεί να εξαναγκάσει την μετάφραση και στη συνέχεια την εκτέλεση ενός παράνομου κώδικα. Εφόσον οι επιθέσεις αυτές είναι αρκετά δημοφιλείς και στις περισσότερες περιπτώσεις εκμεταλλεύσιμες, οι πάροχοι υπηρεσιών νέφους θα πρέπει νε

εξετάσουν το ενδεχόμενο εφαρμογής αντιμέτρων και σχεδίων προστασίας ήδη από τα πρώτα στάδια εγκαθίδρυσης των υπηρεσιών τους.[680]

Περαιτέρω, τα κακόβουλα μέρη μπορούν να εκμεταλλευτούν ευπάθειες που τα προγράμματα περιήγησης αλλά και την απομακρυσμένη πρόσβαση ώστε να αποκτήσουν πρόσβαση σε πολλαπλές διεπαφές ελέγχου του συστήματος νέφους. Σε αυτές συμπεριλαμβάνονται οι διεπαφές των πελατών που ελέγχουν μια σειρά εικονικών μηχανών και την λειτουργία του συνόλου του συστήματος νέφους. Για την αντιμετώπιση τέτοιων ευπαθειών προτείνεται η συχνή ενημέρωση των προγραμμάτων περιήγησης και η εγκατάσταση συστημάτων εντοπισμού παραβιάσεων σε πολλαπλές εικονικές μηχανές.

Τέλος, όπως προαναφέρθηκε, οι μέθοδοι ασφαλείας που χρησιμοποιούνται από τους πελάτες των υπηρεσιών νέφους αποκλίνουν σε μεγάλο βαθμό από τις οδηγίες των παρόχων νέφους. Τέτοιες αντιφάσεις μπορεί να οδηγήσουν σε απώλεια της διακυβέρνησης και του ελέγχου που μπορεί με τη σειρά τους να οδηγήσουν σε καθοριστικές επιπτώσεις για το σύστημα νέφους και τα δεδομένα του. Για το λόγο αυτό, κάθε πάροχος υπηρεσιών νέφους θα πρέπει να κρατά ενήμερους τους πελάτες του με σαφείς και αυστηρές διαδικασίες ασφαλείας και οδηγίες, ενώ στις περιπτώσεις εξωτερικής ανάθεσης, η υπηρεσία των συνεργατών θα πρέπει να είναι συμβατή με αυτές τις οδηγίες/πολιτικές.[681]

7.5.2.3 Γενικότερες απειλές που σχετίζονται με τις υπηρεσίες νέφους

Στην τελευταία αυτή κατηγορία εντάσσονται οι απειλές που μπορεί να επηρεάσουν τόσο τις υποδομές όσο και τις υπηρεσίες των παρόχων νέφους και των πελατών τους. Σε περίπτωση παραβιάσεως της ασφάλειας, το περιβάλλον του υπολογιστικού νέφους αντιμετωπίζει σοβαρές επιπτώσεις.

Τα ταξινομημένα δεδομένα και οι άλλες κρίσιμες πληροφορίες μπορούν να αποκαλυφθούν από τους χρήστες ή τους εργαζόμενους εξαιτίας της πλημμελούς εκπαίδευσης, της αμέλειάς τους ή της κοινωνικής πίεσης. Ένας επιτιθέμενος μπορεί μέσω τηλεφωνημάτων ή μηνυμάτων ηλεκτρονικού ταχυδρομείου να υποδυθεί έναν επιβλέποντα, έναν ειδικευμένο τεχνικό ή άλλες σημαίνουσες οντότητες ώστε να συγκεντρώσει εμπιστευτικά δεδομένα που μπορούν να χρησιμοποιηθούν για άμεσες ή έμμεσες επιθέσεις στο σύστημα. Τέτοιες πληροφορίες μπορεί να είναι κωδικοί πρόσβασης, τοπολογίες δικτύων, χρησιμοποιούμενο λογισμικό κ.α., οι οποίες μπορούν να παρέχουν στον επιτιθέμενο τις απαραίτητες γνώσεις ώστε να εξαπολύσει μια επίθεση. Όλα αυτά υποδεικνύουν ότι στις περιπτώσεις αυτές οι άνθρωποι αποτελούν τους πιο αδύναμους κρίκους σε σχέση με την ασφάλεια. Η κοινωνική μηχανική μπορεί να αντιμετωπιστεί μέσω αυστηρών διαδικασιών και μέσω αξιολογήσεων ασφαλείας, που διαδραματίζουν σημαντικό ρόλο στην αποφυγή τέτοιων επιθέσεων.

Σημαντικές είναι επίσης οι επιθέσεις κατανεμημένης αρνήσεως υπηρεσιών (Distributed Denial of Service Attack) που αποτελούν εξελιγμένη μορφή των επιθέσεων αρνήσεως υπηρεσιών (Denial of Service Attack. Η διαφορά της από άλλου είδους επιθέσεις είναι αρχικά η ικανότητά της να παρατάσσει τα όπλα της με τρόπο «κατανεμημένο» μέσω του Διαδικτύου και να συγκεντρώνει τις

---

[680] John R Vacca, *Cloud Computing Security: Foundations and Challenges*, 1st ed. (repr., Boca Raton, FL: CRC Press, Taylor & Francis Group, 2017), 52-53.
[681] Ibid., 53.

δυνάμεις αυτές (υπολογιστικά συστήματα) για να δημιουργήσει συντριπτική διαδικτυακή κίνηση. Ο κύριος στόχος των επιθέσεων DDoS είναι να προκαλέσει ζημιές σε ένα θύμα είτε για προσωπικούς λόγους είτε για την επίτευξη υλικού κέρδους, ή για δημοτικότητα. Οι επιθέσεις αυτές έχουν καταστεί πιο ισχυρές διότι εκμεταλλεύονται την αρχιτεκτονική νέφους που έχει «κληρονομήσει» τα πλεονεκτήματα και τα μειονεκτήματα των κατανεμημένων συστημάτων. Ωστόσο, μια λύση που έχει προταθεί για την αντιμετώπισή τους είναι η εφαρμογή συστημάτων εντοπισμού εισβολών εντός των εικονικών μηχανών.

Πολύ συχνές είναι και οι επιθέσεις που βασίζονται στη χρήση κακόβουλου λογισμικού (**malware**). Τα κακόβουλα αυτά λογισμικά αποτελούν κακόβουλους κώδικες, που πιθανότατα είναι κρυμμένοι εντός χρήσιμων προγραμμάτων και επιτίθενται στους σταθμούς εργασίας, στους εξυπηρετητές ή στα δίκτυα, ή επιτρέπουν την μη εξουσιοδοτημένη πρόσβαση σε συσκευές. Ο κακόβουλος κώδικας μπορεί να μεταφερθεί μέσω κίνησης του δικτύου, όπως συμβαίνει στην περίπτωση των μεταφορτώσεων μέσω του πρωτοκόλλου μεταφοράς αρχείων (File Transfer Protocol – FTP) ή μέσω εφαρμογών που μεταφορτώνονται από ιστοσελίδες ή μπορεί να διανεμηθεί μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου. Κάποιοι τύποι malware προγραμματίζονται να ανοίγουν συγκεκριμένες θύρες για να επιτρέψουν την παράνομη πρόσβαση των επιτιθέμενων ή για να εκμεταλλευτούν τις ευπάθειες ενός συστήματος. Η εγκατάσταση προγραμμάτων anti-malware ή συστημάτων εντοπισμού παραβιάσεων στις εικονικές μηχανές συνδεόμενες μέσω ενός διαχειριστή συμβάντων, μπορεί να αποτελεί ένα αποδοτικό αντίμετρο.

Τέλος, σε περιβάλλον υπολογιστικού νέφους, αύξηση παρατηρείται στις επιθέσεις που αφορούν την έκθεση ή την απώλεια των κλειδιών κρυπτογράφησης. Στις περιπτώσεις αυτές, η αμέλεια των εργαζομένων ή η έλλειψη πολιτικών ασφαλείας καθιστούν τα μυστικά κλειδιά (κρυπτογράφησης αρχείων, SSL, ιδιωτικά κλειδιά πελατών) ευάλωτα σε κακόβουλους χρήστες που είτε δεν έχουν εξουσιοδότηση ή δεν έχουν αυθεντικοποίηση για να τα χρησιμοποιήσουν. Τέτοια αμέλεια μπορεί να επιτρέψει την πρόσβαση σε μη εξουσιοδοτημένους χρήστες που μπορεί να εξαπολύσουν επιθέσεις ενάντια στις υποδομές νέφους ή ενάντια άλλων πελατών.

7.5.3 Ο έλεγχος ρίσκου του υπολογιστικού νέφους από τα χρηματοπιστωτικά ιδρύματα

Οι χρηματοπιστωτικές υπηρεσίες κατέχουν κρίσιμες και εμπιστευτικές επιχειρηματικές πληροφορίες. Θα πρέπει επομένως να εξεταστεί ενδελεχώς το σενάριο της πιθανής απώλειας του ελέγχου, τουλάχιστον εν μέρει, επί των δεδομένων, αλλά και κάθε συναφές ρίσκο. Οι χρηματοπιστωτικοί οργανισμοί σήμερα θα πρέπει να βρίσκονται σε διαρκή επαγρύπνηση σχετικά με την βελτιστοποίηση των οργανωτικών διαδικασιών και την εισαγωγή συγκεκριμένων λύσεων, στη βάση της αποτελεσματικότητας, της αποδοτικότητας και των οικονομικών τους. Ειδικότερα, ο αντιπρόεδρος των οικονομικών υπηρεσιών της Capgemini, Schiaffonati, τόνισε ότι: «Η διαχείριση ρίσκου αφορά την απόκτηση ενός κεντρικού ρόλου στην διαδικασία της διαχείρισης. Ένας διαχειριστής ρίσκου δεν είναι πλέον ένας απλός ελεγκτής των επιπέδων ρίσκου ή ένας παραγωγός πληροφοριών, προς όφελος της διοίκησης, αλλά καθίσταται ένας διαπιστευμένος συνεργάτης που συμμετέχει ενεργά στην διαδικασία της στρατηγικής λήψης αποφάσεων».[682]

---

[682] Bernardo Nicoletti, *Cloud Computing in Financial Services*, 1st ed. (repr., Basingstoke: Palgrave Macmillan, 2013), 101.

Συνεπώς, πριν υπογράψει μια σύμβαση με έναν πάροχο υπολογιστικής νέφους, ένας χρηματοπιστωτικός οργανισμός θα πρέπει να αναγνωρίσει τα πιθανά ρίσκα, να εγγυηθεί ότι τα πιθανά προβλήματα θα επιλυθούν το συντομότερο δυνατόν, να εξειδικεύσει τις ενέργειες που θα μειώσουν την πιθανότητα να υλοποιηθούν τα ρίσκα ή να εξαλείψει τα αίτια και επομένως την πιθανότητα ότι αυτά θα αποτελέσουν προβλήματα κατά την εφαρμογή και χρήση των υπηρεσιών νέφους και να αναπτύξει σχέδια δράσης, τόσο προληπτικά όσο και έκτακτα ώστε να μειωθεί η επίδραση της πραγματοποίησης του ρίσκου. Όλα αυτά τα μέτρα αποτελούν μέρος μιας συνολικής στρατηγικής αξιολόγησης του ρίσκου.

Περαιτέρω, κατά την αξιολόγηση ενός παρόχου υπηρεσιών νέφους, είναι σημαντικό να αναγνωρίζονται οι πιστοποιήσεις του, συντομεύοντας έτσι τη φάση κατά την οποία οι έλεγχοι και οι αξιολογήσεις ανατίθενται. Τα χαρακτηριστικά των υπηρεσιών που προσφέρονται από τους παρόχους των υπηρεσιών νέφους, ο τύπος των αγορών στις οποίες απευθύνονται και το μέγεθος των οργανισμών δείχνουν τη χρησιμότητα των πιστοποιήσεων οι οποίες διασφαλίζουν την βεβαιότητα της ορθότητας των διαδικασιών που χρησιμοποιεί ο πάροχος, ανεξαρτήτως των γνώσεων ή της εμπειρίας του προσωπικού και τον έλεγχο ότι οι μέθοδοι δεν είναι μόνο ορθοί αλλά εφαρμόζονται πάντα προσεκτικά. Κάποιες από τις πιο σημαντικές πιστοποιήσεις στο πλαίσιο αυτό είναι: α) τα ευρωπαϊκά πρότυπα EN ISO 9001/2008, που εκδίδονται από τα διαπιστευμένα σώματα υπό τους κανόνες που θέτει το ευρωπαικό πρότυπο EN 45000 EA33 «τεχνολογία των πληροφοριών», β) το πρότυπο ISO/IEC 27001:2005, το οποίο θεωρείται σημαντικό υπό την σκοπιά της ασφάλειας, γ) το πρότυπο ISO/IEC 42010, το οποίο σχετίζεται με την μηχανική των συστημάτων και του λογισμικού, δ) το πρότυπο ISO 27001 το οποίο αφορά τους πόρους προσωπικού. Περαιτέρω, κρίσιμη είναι η συμμετοχή προσωπικού που έχει διαπιστευθεί από τους παρόχους υλισμικού και λογισμικού. Περαιτέρω, οι υπηρεσίες νέφους θα πρέπει να συμπεριλαμβάνουν την πρόβλεψη διαφόρων τύπων ψηφιακών πιστοποιητικών που αφορούν την υπογραφή εγγράφων, την διενέργεια επιγραμμικών συναλλαγών, την κρυπτογράφηση, την διαχείριση πιστοποιημένων μηνυμάτων ηλεκτρονικού ταχυδρομείου και ψηφιακών υπογραφών και την πιστοποίηση των εξυπηρετητών.[683]

7.5.3.1 Οι συμβάσεις παροχής υπηρεσιών υπολογιστικού νέφους ως στοιχείο διακυβέρνησης ενός παρόχου υπηρεσιών νέφους

Ένα θεμελιώδες εργαλείο για την διακυβέρνηση των παρόχων υπηρεσιών νέφους είναι η σύμβαση. Για να διασφαλιστεί ότι η σύμβαση παροχής υπηρεσιών νέφους είναι σαφής και ικανή να επιτύχει τους στόχους που οδήγησαν στην επιλογή των δραστηριοτήτων και των διεργασιών που έχουν ανατεθεί υπεργολαβικώς, όλες οι παράμετροι θα πρέπει να αντιμετωπίζονται λεπτομερώς και ανεξαρτήτως. Με αυτόν τον τρόπο, είναι πιθανό να αποφευχθούν οι ασαφείς και αντιφατικές καταστάσεις. Το πιο σημαντικό στοιχείο κατά τον καθορισμό ενός συμβολαίου με έναν πάροχο υπηρεσιών νέφους είναι να έχουν ήδη καθοριστεί οι επιχειρηματικοί στόχοι για την πρωτοβουλία υιοθέτησης υποδομών και υπηρεσιών νέφους.

[683] Bernardo Nicoletti, *Cloud Computing in Financial Services*, 1st ed. (repr., Basingstoke: Palgrave Macmillan, 2013), 102-103.

Η διαχείριση της ασφάλειας απαιτεί σε κάθε περίπτωση ένα σχέδιο και ένα σύστημα ελέγχου. Αυτά έχουν ως στόχο να αντιμετωπίσουν τις πιθανές ευπάθειες του κύριου παρόχου και να αναγνωρίσουν και να επιλέξουν εναλλακτικές τοποθεσίες και εναλλακτικούς παρόχους ώστε να επαναλειτουργήσουν οι υπηρεσίες σε περίπτωση διακοπής τους. Περαιτέρω, το σχέδιο και το σύστημα ελέγχου αμβλύνουν την εξάρτηση από έναν μοναδικό πάροχο καθώς ένας ξεχωριστός πάροχος μπορεί να επιλεγεί για παροχή υπηρεσιών αποκατάστασης από καταστροφές (Disaster Recovery Services).

Η διαπραγμάτευση των συμφωνιών σε επίπεδο υπηρεσιών (Service Level Agreements – SLA) με τους παρόχους αποτελεί επίσης σημαντικό στοιχείο για τον έλεγχο των υπηρεσιών νέφους. Πολλοί οργανισμοί αφήνουν τους παρόχους να γράψουν τις σχετικές συμβάσεις, αλλά αυτό μπορεί να οδηγήσει στη διαχείριση πολύπλοκων συμφωνιών παροχής μέσω απλοποιημένων και ανεπαρκών όρων, που ευνοούν τον πάροχο. Οι συμβατικές διαρρυθμίσεις με τους παρόχους θα πρέπει να εστιάζουν στο εύρος και στην περίμετρο της υπηρεσίας. Αλλά αυτές σπανίως καθορίζουν με σαφήνεια τους ρόλους και τις ευθύνες, ενώ άλλες φορές δεν καλύπτουν θέματα όπως την συμφωνία σε επίπεδο υπηρεσιών. Ακόμα χειρότερα, δεν συμπεριλαμβάνουν κοστολόγηση των μοντέλων παροχής υπηρεσιών ή περιγραφές της διαχείρισης των πιθανών αλλαγών της υπηρεσίας. Όσον αφορά τα ζητήματα διαχείρισης στα συμβατικά έγγραφα, η προσέγγιση που εγγυάται τα καλύτερα αποτελέσματα είναι πυραμιδοειδής. Ο θεμέλιος λίθος είναι μια κύρια/βασική συμφωνία παροχής (**Master Services Agreement – MSA**), που αντιπροσωπεύει την νομική αρχιτεκτονική στην οποία αναφέρονται κατά τον κύκλο ζωής της σχέσης τους. Στην συμφωνία αυτή περιλαμβάνονται όροι που αφορούν τους στόχους, την διάρκεια, τους λόγους τερματισμού των συμβάσεων και τις συνέπειες αυτών για τον πελάτη, την διακυβέρνηση, την εμπιστευτικότητα, τις υποχρεώσεις του παρόχου και του πελάτη, τις νομικές ρήτρες, τους περιορισμούς στις αμοιβαίες αλλαγές των συμβάσεων και όροι που αφορούν την κυριότητα των συστημάτων που χρησιμοποιούνται. Η Συμφωνία αυτή δεν θα πρέπει να αφορά διαδικαστικές και λειτουργικές πτυχές. Αυτές καθορίζονται στα παραρτήματα. Θα πρέπει, ωστόσο, να συμπεριλαμβάνει μια αναλυτική περιγραφή των στοιχείων και των φάσεων του κύκλου ζωής των υπηρεσιών νέφους υπό μια οπτική λειτουργική και διαδικαστική.

7.6 Σύνοψη

Η υπολογιστική νέφους αποτελεί μια από τις πιο δημοφιλείς και ταχέως αναπτυσσόμενες τεχνολογίες στον τομέα των πληροφοριών και των επικοινωνιών τα τελευταία χρόνια. Η μετάβαση των χρηματοπιστωτικών ιδρυμάτων στις τεχνολογίες υπολογιστικού νέφους αποτελεί μια σημαντική τάση, όχι μόνο από μια τεχνολογική σκοπιά, αλλά καθίσταται ολοένα και πιο σημαντική από μια επιχειρηματική σκοπιά. Ωστόσο, ένα από τα μεγαλύτερα εμπόδια για την υιοθέτηση της υπολογιστικής νέφους είναι το αίσθημα ανασφάλειας και παραβίασης της ιδιωτικότητας. Το αίσθημα αυτό οφείλεται κυρίως στις ποικίλες απειλές ασφαλείας που αντιμετωπίζουν τα συστήματα νέφους, οι οποίες απειλούν τόσο τις υποδομές νέφους όσο και τα δεδομένα των πελατών των χρηματοπιστωτικών συστημάτων. Λόγω των περιορισμών των υπαρχουσών ταξινομήσεων των απειλών ασφαλείας για τα συστήματα νέφους, το κεφάλαιο αυτό παρουσιάζει μια εναλλακτική ταξινόμηση που διαχωρίζει τους κινδύνους σε τρεις κατηγορίες. Ο στόχος της προτεινόμενης ταξινόμησης είναι να δημιουργηθεί ένας αποδοτικός κατάλογος ασφαλείας για τα συστήματα νέφους που θα φανεί χρήσιμος σε όποιον είναι πρόθυμος να δομήσει

ή να χρησιμοποιήσει μια υποδομή ή μια υπηρεσία υπολογιστικού νέφους. Επιπροσθέτως, η διακυβέρνηση των συστημάτων νέφους είναι απαραίτητη και απαιτεί προσπάθειες τόσο από την μεριά του παρόχου όσο και από την μεριά των πελατών τους, να δημιουργήσουν μια σχέση συνεργασίας. Λόγω της αύξησης της τεχνικής και οργανωτικής πολυπλοκότητας και των εσωτερικών και εξωτερικών απειλών στο μέλλον, θα παρουσιαστούν μεγαλύτερες απαιτήσεις για μια βελτιωμένη διακυβέρνηση των υπηρεσιών νέφους. Η διακυβέρνηση αυτή μπορεί να συντελεστεί αποτελεσματικά μέσω των εξειδικευμένων και αναλυτικών συμβάσεων παροχής υπηρεσιών υπολογιστικού νέφους.

ΣΥΜΠΕΡΑΣΜΑΤΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ – ΕΠΙΛΟΓΟΣ

Με βάση την ανάλυση που προηγήθηκε, κατέστη σαφές ότι τα χρηματοπιστωτικά ιδρύματα, κατά την άσκηση των συναλλακτικών και των επιχειρηματικών τους δραστηριοτήτων, καθίστανται αποδέκτες μεγάλου όγκου προσωπικών δεδομένων των πελατών τους. Τα χρηματοπιστωτικά ιδρύματα επομένως, έχουν υποχρέωση να προστατεύουν και να προχωρούν στη σύννομη επεξεργασία των δεδομένων αυτών βάσει του ειδικού νομοθετικού και κανονιστικού πλαισίου για την προστασία των προσωπικών δεδομένων καθαυτών (Ν. 4624/2019 και Κανονισμός (ΕΕ) 2016/679) και βάσει της ειδικής σχέσης εμπιστοσύνης που αναπτύσσεται μεταξύ των χρηματοπιστωτικών ιδρυμάτων και των πελατών τους.

Η προστασία των δεδομένων προσωπικού χαρακτήρα των πελατών των πιστωτικών ιδρυμάτων αποκτά ολοένα και μεγαλύτερο ενδιαφέρον ενόψει της υιοθέτησης των νέων τεχνολογιών από τα πιστωτικά ιδρύματα. Η εισαγωγή των νέων αυτών τεχνολογιών καθιστά πιο επιτακτική την ανάγκη για την προστασία των δεδομένων των πελατών, τα οποία βρίσκονται αρχειοθετημένα είτε σε φυσικές υποδομές των καταστημάτων, είτε σε δομές υπολογιστικών νεφών. Παράλληλα, η εισαγωγή των εφαρμογών ηλεκτρονικής τραπεζικής, που οδηγεί σε μείωση της φυσικής παρουσίας των πελατών στα καταστήματα των πιστωτικών ιδρυμάτων, σε συνδυασμό με την αύξηση των ηλεκτρονικών συναλλαγών και των συναλλαγών μέσω καρτών και εφαρμογών e-banking, καθιστά την σχέση ανάμεσα σε τράπεζες και πελάτες πιο απρόσωπη, με αποτέλεσμα τα προσωπικά δεδομένα των πελατών να αποτελούν συχνά τα μόνα κριτήρια για τη λήψη αποφάσεων που τους αφορούν εκ μέρους των πιστωτικών ιδρυμάτων.

Στις προηγούμενες σκέψεις θα πρέπει να προστεθεί και η άποψη ότι στην εποχή μας η τεχνολογία και το δίκαιο βρίσκονται σε μια διαρκή σχέση έντασης. Η τεχνολογική εξέλιξη πάντοτε ηγείται της χάραξης κανόνων τεχνο-κοινωνικής συμβίωσης. Το δίκαιο συνήθως έρχεται εκ των υστέρων να τιθασεύσει τα αρνητικά αποτελέσματα της τεχνολογίας. Τα χαρακτηριστικά αυτά είναι έκδηλα στην τεταμένη σχέση μεταξύ των σύγχρονων τεχνολογιών πληροφορικής και επικοινωνιών και του δικαίου προστασίας των προσωπικών δεδομένων. Χαρακτηριστικό παράδειγμα τέτοιας έντασης είναι και οι τεχνολογίες υπολογιστικής νέφους (cloud computing technologies). Οι τεχνολογίες αυτές οδηγούν σε υπερσυσσώρευση της πληροφορίας μέσω δημοφιλών εφαρμογών λογισμικού από τους προσωπικούς μας ηλεκτρονικούς υπολογιστές στους εταιρικούς πυλώνες του διαδικτύου, αλλάζοντας τους συσχετισμούς της δύναμης στην κοινωνία της πληροφορίας και εγείροντας ανησυχίες για την ασφάλεια και την εμπιστευτικότητα των δεδομένων. Στο πλαίσιο αυτό, οι τραπεζικοί οργανισμοί που υιοθετούν τις λύσεις τελευταίας τεχνολογίας με στόχο την βελτίωση των υπηρεσιών τους και το επιχειρηματικό κέρδος, θα πρέπει να συμμορφώνονται με

τις επιταγές του δικαίου προστασίας προσωπικών δεδομένων, το οποίο πλαισιώνει την παροχή υπηρεσιών υπολογιστικής νέφους με σκοπό την προστασία των θεμελιωδών δικαιωμάτων της ιδιωτικής ζωής και του πληροφοριακού αυτοκαθορισμού.

Καταλήγουμε επομένως στο συμπέρασμα ότι η προστασία της ιδιωτικότητας των πελατών των χρηματοπιστωτικών ιδρυμάτων καθίσταται πιο αναγκαία από ποτέ. Για να προστατευτούν αποτελεσματικά τα δικαιώματα των υποκειμένων, αφενός θα πρέπει το νομοθετικό και κανονιστικό πλαίσιο να προσαρμόζεται διαρκώς στις μεταβαλλόμενες κοινωνικές και τεχνολογικές συνθήκες, αφετέρου τα χρηματοπιστωτικά ιδρύματα να μεριμνούν για την προστασία της ασφάλειας των δεδομένων των πελατών τους αλλά και για την διασφάλιση της ιδιωτικότητάς τους, η οποία δύναται στο μέλλον να αποτελέσει ανταγωνιστικό πλεονέκτημα και εχέγγυο αξιοπιστίας για αυτά.

Επιπροσθέτως, η χρηματοπιστωτική βιομηχανία θα πρέπει να συνεχίσει να διερευνά τις τεχνικές εφαρμογές των δικαιωμάτων ώστε να συνδράμει τα υποκείμενα των δεδομένων στην άσκηση ελέγχου. Ενώ πράττει αυτό θα πρέπει όμως να λάβει υπόψιν ότι πολλές ρυθμίσεις ελέγχου μπορεί να αποδειχθούν παραπλανητικές, καθώς υπόσχονται περισσότερα από όσα μπορούν να προσφέρουν, δημιουργώντας έτσι ένα ψευδές αίσθημα εμπιστοσύνης και αυτονομίας. Επίσης, ο υπερβολικός έλεγχος και ο χείμαρρος επιλογών μπορούν να οδηγήσουν σε σύγχυση των υποκειμένων. Οι ρυθμιστικές αρχές θα πρέπει σε κάθε περίπτωση να αναγνωρίσουν τη σημασία της τεχνολογίας για την ενίσχυση του ελέγχου από τη μεριά των υποκειμένων αλλά παράλληλα να έχουν επίγνωση των μειονεκτημάτων της. Οι τεχνολογικές λύσεις θα πρέπει να ελέγχονται και να αναθεωρούνται συνεχώς ώστε να εξακριβωθεί εάν ανταποκρίνονται στα κανονιστικά πρότυπα.

Κατά την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων, οι παράγοντες της χρηματοπιστωτικής βιομηχανίας θα πρέπει να αναζητούν συνεχώς καλύτερες διασυνδέσεις ανάμεσα στα καθήκοντα προστασίας δεδομένων και τα μέτρα ελέγχου των δεδομένων των υποκειμένων, λαμβάνοντας υπόψιν ότι για να είναι αποτελεσματικά, τα δικαιώματα ελέγχου θα πρέπει να συμπληρώνονται από τα καθήκοντα του υπευθύνου επεξεργασίας των δεδομένων. Οι ρυθμιστικές αρχές που επιβλέπουν τους παράγοντες που συμμετέχουν στην οικονομία των δεδομένων θα πρέπει να έχουν επίγνωση των αλληλεπιδράσεων αυτών και να εξετάζουν τα δικαιώματα των υποκειμένων των δεδομένων υπό το πρίσμα των καθηκόντων του υπευθύνου επεξεργασίας, όπως για παράδειγμα του καθήκοντος διενέργειας εκτιμήσεων αντικτύπου για την προστασία της ιδιωτικής ζωής.[684]

[684] Helena U Vrabec, *Data Subject Rights Under The GDPR*, 1st ed. (repr., Oxford, United Kingdom: Oxford University Press, 2021), 235.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ι. ΒΙΒΛΙΑ

Α) Ξενόγλωσσα

Arora, Anu. *Banking Law*. 1st ed. Reprint, London, UK: Pearson Education Limited, 2014.

Ausloos, Jef. *The Right to Erasure in EU Data Protection Law*. 1st ed. Reprint, Oxford University Press, 2020.

Bennett., Colin J. *Regulating Privacy: Data Protection and Public Policy in Europe and The United States*. 1st ed. Reprint, Ithaca, N.Y.: Cornell University Press, 1992.

Bhowmik, Sandeep. *Cloud Computing*. 1st ed. Reprint, Cambridge: Cambridge University Press, 2017.

Bing, Jon. *Comparative Law Yearbook 2*. 1st ed. Reprint, Den Haag: Kluwer Law International, 1978.

Blokdijk, Gerard, and Ivanka Menken. *Cloud Computing - The Complete Cornerstone Guide to Cloud Computing Best Practices*. 2nd ed. Reprint, London, United Kingdom: Emereo Pty Ltd, 2009.

Büllesbach, Alfred, and Serge Gijrath. *Concise European IT Law*. 2nd ed. Reprint, Alphen aan den Rijn: Kluwer Law International, 2010.

Carey, Peter. *Data Protection: A Practical Guide to UK And EU Law*. 5th ed. Reprint, Oxford, UK: Oxford University Press, 2018.

Claes, Erik, Antony Duff, and Serge Gutwirth. *Privacy And the Criminal Law*. 1st ed. Reprint, Oxford: Intersentia, 2006.

Flaherty, David H. *Protecting Privacy in Surveillance Societies*. 1st ed. Reprint, Chapel Hill and London: The University of North Carolina Press, 2014.

Ghezzi, Alessia, Ângela Guimarães Pereira, and Lucia Vesnić-Alujević. *The Ethics of Memory in A Digital Age*. 1st ed. Reprint, Palgrave Macmillan, 2014.

Gola, Peter. *BDSG, Bundesdatenschutzgesetz: Kommentar*. 10th ed. Reprint, München: Beck, 2010.

González Fuster, Gloria. *The Emergence of Personal Data Protection as A Fundamental Right of the EU*. 1st ed. Reprint, Cham: Springer, 2016.

Haentjens, Matthias, and Pierre De Gioia-Carabellese. *European Banking and Financial Law*. 2nd ed. Reprint, London: Routledge, 2020.

Hondius, Frits W. *Emerging Data Protection in Europe*. 1st ed. Reprint, Amsterdam: American Elsevier Pub. Co, 1975.

Kahin, Brian, and Charles R Nesson. *Borders In Cyberspace*. 1st ed. Reprint, Boulder, Colorado: The MIT Press, 1999.

Kalpokas, Ignas. *Algorithmic Governance: Politics and Law in The Post-Human Era*. 1st ed. Reprint, Cham, Switzerland: Palgrave Pivot, 2019.

Kelleher, John D, and Brendan Tierney. *Data Science*. 1st ed. Reprint, Cambridge, Massachusetts: MIT Press, 2018.

Kosta, Eleni. *Consent In European Data Protection Law*. 1st ed. Reprint, Leiden: Martinus Nijhoff Publishers, 2013.

Kuner, Christopher, Lee A Bygrave, and Christopher Docksey. *The EU General Data Protection Regulation (GDPR). A Commentary*. 1st ed. Reprint, Kettering: Oxford University Press, 2019.

Lee Andrew Bygrave, *Data Privacy Law*, 1st ed. (repr., New York: Oxford, 2013).

Lisdorf, Anders. *Cloud Computing Basics: A Non-Technical Introduction*. 1st ed. Reprint, Berkeley, CA, Apress, 2021.

Lynn, Theo, John G Mooney, Lisa van der Werff, and Grace Fox. *Data Privacy and Trust in Cloud Computing*. 1st ed. Reprint, Cham: Springer, 2021.

Millard, Christopher. *Cloud Computing Law*. 2nd ed. Reprint, Oxford, United Kingdom: Oxford University Press, 2021.

Miller, Michael. *Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online*. 1st ed. Reprint, Indianapolis, Ind.: Que Publishing, 2009.

Moerel, Lokke. *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*. 1st ed. Reprint, Oxford: Oxford University Press, 2012.

Nicoletti, Bernardo. *Cloud Computing in Financial Services*. 1st ed. Reprint, Basingstoke: Palgrave Macmillan, 2013.

Nissenbaum, Helen. *Privacy In Context: Technology, Policy, And the Integrity of Social Life*. 1st ed. Reprint, Stanford, CA, United States: Stanford University Press, 2009.

Peers, Steve, Tamara Hervey, Jeff Kenner, and Angela Ward. *The EU Charter of Fundamental Rights*. 2nd ed. Reprint, Oxford: Hart Publishing, 2022.

Politou, Eugenia, Efthimios Alepis, Maria Virvou, and Constantinos Patsakis. *Privacy And Data Protection Challenges in The Distributed Era*. 1st ed. Reprint, Cham, Switzerland: Springer Nature, 2022.

Reese, George. *Web Architecture and Programming in The Cloud*. 1st ed. Reprint, Sebastopol, California: O'Reilly Media, Inc., 2009.

Ristol, Santi, Katarina Stanoevska-Slabeva, and Thomas Wozniak. *Grid And Cloud Computing*. 1st ed. Reprint, Heidelberg: Springer, 2010.

Sharma, Sanjay, and Pranav Menon. *Data Privacy and GDPR Handbook*. 1st ed. Reprint, Hoboken, New Jersey: John Wiley and Sons, Inc., 2019.

Vacca, John R. *Cloud Computing Security: Foundations and Challenges*. 1st ed. Reprint, Boca Raton, FL: CRC Press, Taylor & Francis Group, 2017.

Van Alsenoy, Brendan. *Data Protection Law in the EU*. 1st ed. Reprint, Cambridge: Intersentia, 2019.

Voigt, Paul, and Axel Von dem Bussche. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. 1st ed. Reprint, New York: Springer, 2017.

Vrabec, Helena U. *Data Subject Rights Under The GDPR*. 1st ed. Reprint, Croydon: Oxford University Press, 2021.

Walden, Ian, Chris Edwards, and Nigel Savage. *Information Technology & The Law*. 1st ed. Reprint, New York: Palgrave Macmillan, 1990.

Β) Ελληνόγλωσσα

Αλεξανδροπούλου-Αιγυπτιάδου Ευγενία. *Προσωπικά Δεδομένα*, 1η εκδ. ,Θεσσαλονίκη: Νομική Βιβλιοθήκη, 2016.

Γεωργιάδης, Απόστολος Σ., and Μιχάλης Π. Σταθόπουλος. *Αστικός Κώδικας, Ερμηνεία Κατ' Άρθρο, Τόμος Ιβ, Γενικές Αρχές / Άρθρα 127-286*. 2η εκδ. Reprint, Αθήνα: Π. Ν. Σάκκουλας, 2016.

Γιαννόπουλος Γεώργιος. *Εισαγωγή Στη Νομική Πληροφορική*. 1η εκδ. repr., Αθήνα: Νομική Βιβλιοθήκη, 2018.

Γραμματίκας Αθ. Γεώργιος. *Το Τραπεζικό Απόρρητο*, 1η εκδ. repr., Αθήνα: Εκδόσεις Σάκκουλα, 1991.

Ιγγλεζάκης Ιωάννης, *Ευαίσθητα Προσωπικά Δεδομένα*, 1η εκδ. repr., Θεσσαλονίκη: Εκδόσεις Σάκκουλα, 2003.

Ιγγλεζάκης Ιωάννης. *Δίκαιο Πληροφορικής*, 4η εκδ. repr., Θεσσαλονίκη: Εκδόσεις Σάκκουλα, 2021.

Καλαμίτσης Σωτήριος. *Το Απόρρητο Των Τραπεζικών Καταθέσεων*, 1η εκδ. repr., Αθήνα: Εκδόσεις Π. Χιωτέλλη, 1993.

Καλλιμόπουλος, Γεώργιος Δ., Ζαφείριος Ν. Τσολακίδης, και Κωνσταντίνος Γ. Καραγιάννης. *Δίκαιο Τραπεζικών Συναλλαγών*. 1η εκδ Reprint, Αθήνα: Π. Ν. Σάκκουλας, 2019.

Κοντιάδης Ξενοφών. Πανδημία, Βιοπολιτική Και Δικαιώματα, 1η εκδ., Αθήνα: Εκδόσεις Καστανιώτη, 2020.

Κοτσαλής, Λεωνίδας Γ. *Προσωπικά Δεδομένα, Ανάλυση - Σχόλια - Εφαρμογή*. 1η εκδ. Reprint, Αθήνα: Νομική Βιβλιοθήκη, 2016.

Κουτσούκης Δημήτριος Β. *Τραπεζικό Απόρρητο (Νομοθεσία-Νομολογία)*, 1η εκδ. repr., Αθήνα: Αντ. Ν. Σάκκουλας, 1998.

Μήτρου Λίλιαν. *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*, 1η εκδ. (repr., Αθήνα: Εκδόσεις Σάκκουλα, 2017.

Ντόστας Μιχαήλ Θ. *Γενικό Τραπεζικό Απόρρητο Και Απόρρητο Των Καταθέσεων. Κατάσχεση Των Καταθέσεων*, 1η εκδ. repr., Αθήνα: Εκδόσεις Αντ. Ν. Σάκκουλα Ε.Ε, 2000.

Παπαθεωδόρου Θεόδορος. *Επιτηρούμενη Δημοκρατία*, 1η εκδ. ,Αθήνα: Βιβλιόραμα, 2009.

Πατινιώτης Μανώλης. *Εισαγωγή Στις Ψηφιακές Σπουδές*, 1η εκδ. ,Θεσσαλονίκη: Εκδόσεις Ροπή, 2020.

Πελλένη-Παπαγεωργίου Ανθή. *Ζητήματα Από Τις Νέες Ρυθμίσεις Για Τις Συμβάσεις Καταναλωτικής Πίστης*, 1η εκδ. repr., Αθήνα: Αντ. Ν. Σάκκουλα, 2012.

Περάκης, Μανώλης και Βασίλειος Α. Χριστιανός. *Νομοθεσία Της Ευρωπαϊκής Ένωσης Μετά Της Συνθήκη Της Λισαβόνας*. 1η εκδ. Reprint, Αθήνα: Νομική Βιβλιοθήκη, 2010.

Πλατής, Ειρηνικός. *Προσωπικά Δεδομένα-Προστασία GDPR*. 1η εκδ. Reprint, Αθήνα: Εκδόσεις Παπαδόπουλος, 2018.

Πλιαβέσης Ε. Γεώργιος. *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας-Πελάτη*, 1η εκδ. repr., Αθήνα: Νομική Βιβλιοθήκη, 2019.

Ρόκας, Νικόλαος Κ., Χρήστος Βλ. Γκόρτσος, Αλεξάνδρα Π. Μικρουλέα, and Χριστίνα Κ. Λιβαδά. *Στοιχεία Τραπεζικού Δικαίου*. 3η εκδ. Reprint, Αθήνα: Νομική Βιβλιοθήκη, 2016.

Σταθόπουλος Μιχαήλ. *Γενικό Ενοχικό Δίκαιο*, 4η εκδ. repr., Αθήνα-Κομοτηνή: Εκδόσεις Σάκκουλα, 2004.

Συλλογικό Έργο. *Τιμητικός Τόμος Γεωργίου Δ. Καλλιμόπουλου*. 1η εκδ. Reprint, Αθήνα: Σάκκουλας Αντ. Ν., 2010.

Συλλογικό Έργο. *Τιμητικός Τόμος Νικολάου Θ. Νίκα*. 1η εκδ. Reprint, Αθήνα: Εκδόσεις Σάκκουλα, 2018.

Χριστοδούλου, Κωνσταντίνος. *Δίκαιο Προσωπικών Δεδομένων*. 2η εκδ. Reprint, Αθήνα: Νομική Βιβλιοθήκη, 2020.

Ψυχομάνης Σπυρίδων Δ. *Τραπεζικό Δίκαιο, δίκαιο τραπεζικών συμβάσεων Ι:Γενικό Μέρος*, 6η εκδ. repr., Αθήνα, Θεσσαλονίκη: Εκδόσεις Σάκκουλα, 2008.

Ψυχομάνης Σπυρίδων. *Εγχειρίδιο Τραπεζικού Δικαίου*, 2η εκδ. repr., Αθήνα, Θεσσαλονίκη: Εκδόσεις Σάκκουλα, 2016.

ΙΙ. ΑΚΑΔΗΜΑΙΚΑ ΑΡΘΡΑ

Α) Ξενόγλωσσα

Abdul, Temilola. "The Concept of Privacy: Is Privacy Still a Useful Concept?". SSRN Electronic Journal, 2020. doi:10.2139/ssrn.3668520.

Badger, M., Grance, T., Patt-Corner, R. and Voas, J. (2012), Cloud Computing Synopsis and Recommendations, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-146 (Accessed January 5, 2022)

Bennett, Colin J. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Cornell University Press, 1992. http://www.jstor.org/stable/10.7591/j.ctv2n7hxs.

Bose, Ranjit, Xin (Robert) Luo, and Yuan Liu. "The Roles of Security and Trust: Comparing Cloud Computing and Banking". Procedia - Social and Behavioral Sciences 73 (2013): 30-34. doi:10.1016/j.sbspro.2013.02.015.

Burton S. Kaliski and Wayne Pauley. 2010. Toward risk assessment as a service in cloud environments. In Proceedings of the 2nd USENIX conference on Hot topics in cloud computing (HotCloud'10). USENIX Association, USA, 13.

Cavoukian, Ann. "Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices". Privacy.Ucsc.Edu, 2011. https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf.

Cockfield, Arthur J. "Protecting Taxpayer Privacy Rights Under Enhanced Cross-Border Tax Information Exchange: Toward A Multilateral Taxpayer Bill of Rights". SSRN Electronic Journal, 2008. doi:10.2139/ssrn.1356841.

Coyle, Erin K. "E. L. Godkin's Criticism of The Penny Press: Antecedents to A Legal Right to Privacy". American Journalism 31, no. 2 (2014): 262-282. doi:10.1080/08821127.2014.905362.

De Simone, Lisa, Rebecca Lester, and Kevin Markle. "Transparency And Tax Evasion: Evidence from The Foreign Account Tax Compliance Act (FATCA)". Journal Of Accounting Research 58, no. 1 (2020): 105-153. doi:10.1111/1475-679x.12293.

Diakopoulos, Nicholas. "Accountability In Algorithmic Decision Making". Communications Of the ACM 59, no. 2 (2016): 56-62. doi:10.1145/2844110.

Einav, Liran, and Jonathan Levin. "The Data Revolution and Economic Analysis". Innovation Policy and The Economy 14 (2014): 1-24. doi:10.1086/674019.

Foster, Ian, Yong Zhao, Ioan Raicu, and Shiyong Lu. "Cloud Computing and Grid Computing 360-Degree Compared". 2008 Grid Computing Environments Workshop, 2008. doi:10.1109/gce.2008.4738445.

Gellert, Raphaël. "Understanding The Notion of Risk in The General Data Protection Regulation". Computer Law & Security Review 34, no. 2 (2018): 279-288. doi: 10.1016/j.clsr.2017.12.003.

Hatfield, Michael. "Taxation And Surveillance: An Agenda". SSRN Electronic Journal 319 (2014). doi:10.2139/ssrn.2539835.

HJI Panayi, Christiana. "Current Trends on Automatic Exchange of Information". SSRN Electronic Journal 2016--43 (2016). doi:10.2139/ssrn.2748659.

Holleaux, André. “La Loi Du 6 Janvier 1978 Sur l’informatique et Les Libertés -I-.” La Revue Administrative 31, no. 181 (1978): 31–40. http://www.jstor.org/stable/40767795.

Hon, W. Kuan, and Christopher Millard. "Banking In the Cloud: Part 1 – Banks' Use of Cloud Services". Computer Law & Security Review 34, no. 1 (2018): 4-24. doi:10.1016/j.clsr.2017.11.005.

Houser, Kimberly and Sanders, Debra, The Use of Big Data Analytics by the IRS: Efficient Solution or the End of Privacy as We Know it? (March 29, 2017). Vanderbilt Journal of Entertainment & Technology Law, Vol. 19, No. 4, 2017, Available at SSRN: https://ssrn.com/abstract=2943002

Ilshammar, Lars. "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960S". Human IT 9, no. 1 (2007): 6-57.

Kirby, Michael D. "Transborder Data Flows and The Basic Rules of Data Privacy". Stanford Journal of International Studies 16, no. 27 (1980): 1-59.

Kirby, Michael D. "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy". International Data Privacy Law 1, no. 1 (2010): 6-14. doi:10.1093/idpl/ipq002.

Kosinski, M., D. Stillwell, and T. Graepel. "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior". Proceedings Of the National Academy of Sciences 110, no. 15 (2013): 5802-5805. doi:10.1073/pnas.1218772110.

Kuner, Christopher, Lee A. Bygrave, Chris Docksey, Laura Drechsler, and Luca Tosoni. "The EU General Data Protection Regulation: A Commentary/Update of Selected Articles". SSRN Electronic Journal, 2021. doi:10.2139/ssrn.3839645.

Lowry, Paul Benjamin, Tamara Dinev, and Robert Willison. "Why Security and Privacy Research Lies at The Centre of The Information Systems (IS) Artefact: Proposing A Bold Research Agenda". European Journal of Information Systems 26, no. 6 (2017): 546-563. doi:10.1057/s41303-017-0066-x.

Lynskey, Orla. "Deconstructing Data Protection: The "Added-Value" Of A Right to Data Protection in The EU Legal Order". International And Comparative Law Quarterly 63, no. 3 (2014): 569-597. doi:10.1017/s0020589314000244.

Pagano, Robert. "Panorama Of Personal Data Protection Laws". Council Of Europe, Legislation and Data Protection. Proceedings Of the Rome Conference on Problems Relating to The Development and Application of Legislation on Data Protection, 1983.

Pearson, Siani, and Azzedine Benameur. "Privacy, Security and Trust Issues Arising from Cloud Computing". 2010 IEEE Second International Conference on Cloud Computing Technology and Science, 2010, 693-702. doi:10.1109/cloudcom.2010.66.

Porat, Ariel, and Lior Strahilevitz. "Personalizing Default Rules and Disclosure with Big Data". SSRN Electronic Journal, 2013. doi:10.2139/ssrn.2217064.

Post, Robert C. "Three Concepts of Privacy". The Georgetown Law Journal 89, no. 2087 (2001). https://openyls.law.yale.edu/bitstream/handle/20.500.13051/1114/Three_Concepts_of_Privacy.pdf?sequence=2.

Ramireddy, Srilakshmi, Rajarshi Chakraborthy, T.S Raghu, and H. Raghav Rao. "Privacy And Security Practices in The Arena of Cloud Computing - A Research in Progress". AMCIS 2010 Proceedings 574 (2010).

Roschke, Sebastian, Feng Cheng, and Christoph Meinel. "An Advanced IDS Management Architecture". Journal Of Information Assurance and Security 5 (2010): 246-255.

Scholtz, Brenda, Judian Govender, and Jorge Marx Gomez. "Technical And Environmental Factors Affecting Cloud Computing Adoption in The South African Public Sector". CONF-IRM 2016 Proceedings 16 (2016). https://aisel.aisnet.org/confirm2016/16.

Senarathna, Ishan, William Yeoh, Matthew Warren, and Scott Salzman. 2016. "Security and Privacy Concerns for Australian SMEs Cloud Adoption: Empirical Study of Metropolitan

Vs Regional SMEs". Australasian Journal of Information Systems 20 (March). Australia. https://doi.org/10.3127/ajis.v20i0.1193.

Sharman, J.C. "Privacy as Roguery: Personal Financial Information in An Age of Transparency". Public Administration 87, no. 4 (2009): 717-731. doi:10.1111/j.1467-9299.2009.01785.x.

Simitis, Spiros. "Revisiting Sensitive Data". Review Of the Answers to The Questionnaire of The Consultative Committee of The Convention for The Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS 108), 1999.

Solove, Daniel J. "A Taxonomy of Privacy." University of Pennsylvania Law Review 154, no. 3 (2006): 477–564. https://doi.org/10.2307/40041279.

Taylor, Linnet, Ralph Schroeder, and Eric Meyer. "Emerging Practices and Perspectives on Big Data Analysis in Economics: Bigger and Better or More of The Same?". Big Data & Society 1, no. 2 (2014): 205395171453687. doi:10.1177/2053951714536877.

van Duijvenvoorde, Gera. "Transborder Flow of Personal Data within the EC, A Comparative Analysis of the Privacy Statutes of the Federal Republic of Germany, France, the United Kingdom and the Netherlands and Their Impact on the Private Sector; A.C.M. Nugter; Kluwer Law and Taxation Publishers, Deventer 1990; 434" Leiden Journal of International Law 4, no. 1 (1991): 155–63. doi:10.1017/S0922156500001904.

Veale, Michael, Max Van Kleek, and Reuben Binns. "Fairness And Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision-Making". Proceedings Of The 2018 CHI Conference on Human Factors in Computing Systems, 2018. doi:10.1145/3173574.3174014.

Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. "Why A Right to Explanation of Automated Decision-Making Does Not Exist in The General Data Protection Regulation". SSRN Electronic Journal, 2016. doi:10.2139/ssrn.2903469.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4, no. 5 (1890): 193–220. https://doi.org/10.2307/1321160.

Xiao, Zhifeng, and Yang Xiao. "Security And Privacy in Cloud Computing". IEEE Communications Surveys & Tutorials 15, no. 2 (2013): 843-859. doi:10.1109/surv.2012.060912.00182.

Youseff, Lamia, Maria Butrico, and Dilma Da Silva. "Toward A Unified Ontology of Cloud Computing". 2008 Grid Computing Environments Workshop, 2008, 1-10. doi:10.1109/gce.2008.4738443.

B) Ελληνόγλωσσα

Δουβλής, Βασίλης Α. "Τραπεζικό Απόρρητο, Προστασία Προσωπικών Δεδομένων και Νομιμοποίηση Παράνομων Εσόδων κατά τη Διεξαγωγή Φορολογικών Ελέγχων". *Δίκαιο Επιχειρήσεων Και Εταιρειών*, no. 12 (2012): 1093-1108.

Κοτσίρης, Λάμπρος. "Τραπεζικό Απόρρητο και Κατάσχεση Τραπεζικών Καταθέσεων", 2002. http://www.dsanet.gr/ekpaideush/seminaria/KOTSIRIS.htm.

Μυλώση, Μαρία και Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου. "Προσωπικά Δεδομένα Οικονομικής Συμπεριφοράς και Ηλεκτρονική Επεξεργασία τους από την ΤΕΙΡΕΣΙΑΣ Α.Ε". *Δίκαιο Μέσων Μαζικής Ενημέρωσης* 1, no. 45 (2015): 25-37.

ΙΙΙ. ΠΙΝΑΚΑΣ ΑΝΑΦΟΡΩΝ ΝΟΜΟΛΟΓΙΑΣ

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ

ΑΠΟΦΑΣΕΙΣ ΑΠΔΠΧ: 24/2004, 25/2004 αποφάσεις για τον περιορισμό του χρόνου διατήρησης των δεδομένων αρχείων της ΤΕΙΡΕΣΙΑΣ Α.Ε.

ΑΠΟΦΑΣΕΙΣ ΕΘΝΙΚΩΝ ΔΙΚΑΣΤΗΡΙΩΝ:
United States v. Jones, No. 10–1259, 615 F. 3d 544 (Supreme Court of the United States, 2012). https://www.law.cornell.edu/supct/pdf/10-1259.pdf

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ

ΑΠΟΦΑΣΕΙΣ ΑΠΔΠΧ: 83/2009, 59/2011, 26/2014, 134/2014, 175/2014, 22/2015, 95/2014, 24/2004, 25/2004, 185/2014, 98/2013, 13/2003, 74/2010, 100/2000, 3/2009, 8/2010, 38/2005, 86/2013, 55/2010. 38/2010, Ολ ΑΠΔ 29/2012, 44/2009, 52/2003, υπ'αριθ. 109/31.3.2009 απόφαση, 26/2002, 73/2012, 76/2012, 55/2007, 46/2007,12/2016, 15/2016, 16/2016

ΓΝΩΜΟΔΟΤΗΣΕΙΣ ΑΠΔΠΧ: 1/2013, 1/2017, 4/2017

ΟΔΗΓΙΕΣ ΑΠΔΠΧ: 2/2011

ΑΠΟΦΑΣΕΙΣ ΕΘΝΙΚΩΝ ΔΙΚΑΣΤΗΡΙΩΝ: ΣτΕ 3542/2002, ΟλΑΠ 6/2009, ΑΠ 163/2007, 634/2007, 769/2007, 1255/2007

ΑΠΟΦΑΣΕΙΣ ΕΔΔΑ: *K.H. and Others v. Slovakia*, No. 32881/04, 28 April 2009.

ΑΠΟΦΑΣΗ CNIL: 1/2019

ΑΠΟΦΑΣΕΙΣ ΔΕΕ: C-131/2012, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN

Case C-101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* para. 37. ECLI:EU:C: 2003:596. https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:62001CJ0101.

Joined Cases C-465/00, C-138/01 and C-139/01, Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk

Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy

Case C-201/14, Smaranda Bara κ.λπ. κατά Casa Naţională de Asigurări de Sănătate

Case C-524/06, Heinz Huber v Bundesrepublik Deutschland,
https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62006CJ0524.

Case C-291/12, Michael Schwarz κατά Stadt Bochum,
https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:62012CJ0291.

Case C-434/16, Peter Nowak v Data Protection Commissioner.
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62016CJ0434&from=en

Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN,

Case C-582/ 14, Patrick Breyer κατά Bundesrepublik Deutschland
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62014CJ0582&from=el

Case C-212/ 13, František Ryneš v Úřad pro ochranu osobních údajů
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62013CJ0212&from=EN

Case C-345/17, Sergejs Buivids
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62017CJ0345&from=en.

Joined Cases C-141/12 and C-372/12. Opinion of Advocate General Sharpston delivered on 12 December 2013.
https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:62012CC0141&from=EN

Case C-434/16, Peter Nowak v Data Protection Commissioner.
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62016CJ0434&from=en

Joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0141&from=en.

Joined Cases C-141/ 12 and C-372/ 12, *YS* (Προτάσεις ΓΕ).
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62012CC0141&from=en

Joined Cases C-92/ 09 and 93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen,
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62009CJ0092&from=en.

C-419/14, WebMindLicenses kft v Nemzeti Adó- és Vámhivatal Kiemelt Adó-és Vám Főigazgatóság, https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62014CJ0419&from=en

Case C-620/19, Land Nordrhein-Westfalen v D.-H. T. as liquidator of J & S Service UG.
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62019CJ0620&from=en.

C-136/17, *G.C., A.F., B.H., E.D* (Προτάσεις ΓΕ), 23. ECLI:EU:C: 2019:14.
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62017CC0136&from=el.

ΔΕΕ Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk..
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62000CJ0465&from=en

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ

ΑΠΟΦΑΣΗ ΥΠΟΙΚ: ΠΟΛ 1156/11.5.2010

ΑΠΟΦΑΣΕΙΣ ΕΘΝΙΚΩΝ ΔΙΚΑΣΤΗΡΙΩΝ: ΑΠ 939/2004, ΑΠ 589/2001, ΑΠ 1352/2011, ΕφΑθ 1403/2015, ΕφΛαμ 27/2013, ΑΠ 1717/2012, ΕφΘεσ 76/2009, ΠΠρΑθ 437/2012 , ΑΠ 1352/2011, ΠΠρΑθ 2087/2004, ΕφΑθ 1403/2015, ΑΠ 244/2016, ΑΠ 1738/2013, ΑΠ 1727/2008, ΑΠ 820/2002, ΕφΠειρ 329/2021, ΑΠ 244/2016, ΑΠ 2212/2014, ΑΠ 1350/2018

ΑΠΟΦΑΣΕΙΣ ΕΤΠΘ (Επιτροπής Τραπεζικών και Πιστωτικών Θεμάτων) :
Υπ' αριθμ. 234/11.12.2006 απόφαση και υπ' αριθμ. 178/3/19.07.2004 απόφαση, αποφ. 178/3/2004, Απόφαση ΕΤΠΘ 231/4/13.10.2006

ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ

ΑΠΟΦΑΣΕΙΣ ΑΠΔΠΧ: 98/2017, 24/2004, 193/2012, 116/2004, 38/2013, ΟλΑΠΔΠΧ 59/2009, 98/2017, 20/2001, 39/2015, 65/2010 , 72/2013, 26/2004, 58/2015, 91/2014, 66/2018, 20/2001, 59/2009, 49/2011, 98/2017, 194/2012

ΓΝΩΜΟΔΟΤΗΣΕΙΣ ΑΠΔΠΧ: Γνωμοδότηση 5/2013, Γνωμοδότηση 1/2009

ΕΚΘΕΣΕΙΣ ΑΠΔΠΧ:
Ετήσια έκθεση ΑΠΔΠΧ 2014
https://www.dpa.gr/sites/default/files/2020-12/ARXH%20PROSTASIAS_APOLOGISMOS%202013.PDF.

Ετήσια Έκθεση ΑΠΔΠΧ 2007,
https://www.dpa.gr/sites/default/files/2019-09/DPA_ANNUAL_REPORT_2007.PDF.

Ετήσια Έκθεση ΑΠΔΠΧ 2009.
https://www.dpa.gr/sites/default/files/2020-12/DPA_ANNUAL_REPORT_2009.PDF

Ετήσια έκθεση ΑΠΔΠΧ 2015.
https://www.dpa.gr/sites/default/files/2020-12/ANNUAL%202015%20V2.0%20WEB%20VIEW2.PDF.

Ετήσια έκθεση ΑΠΔΠΧ 2018.
https://www.dpa.gr/sites/default/files/2020-02/ANNUAL2018V30WEBPAGE_01.PDF.

Ετήσια έκθεση ΑΠΔΠΧ 2001, 41.
https://www.dpa.gr/sites/default/files/2019-09/DPA_ANNUAL_REPORT_2001.PDF.

ΑΠΟΦΑΣΕΙΣ ΕΘΝΙΚΩΝ ΔΙΚΑΣΤΗΡΙΩΝ: ΣτΕ 150/2017, ΕφΑθ 2887/2010, ΑΠ 1740/2013, ΕφΑθ 1437/2014, ΕιρΑθ 273/2016, ΑΠ 1923/2006, ΕφΑθ. 5717/2008, ΠΠρΑθ. 3944/2009, ΑΠ 820/2002, ΑΠ 1352/2011, ΕιρΠειρ 92/2018

ΑΠΟΦΑΣΕΙΣ ΕΔΔΑ: Copland v United Kingdom [2007] ECHR 253

ΑΠΟΦΑΣΕΙΣ ΔΕΕ: C-673/17, Planet49 GmbH κατά Bundesverband der Verbraucherzentralen und Verbraucherverbänd
https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:62017CC0673&from=GA

C-40/17, Fashion ID GmbH & Co.KG κατά Verbraucherzentrale NRW Ev,
https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=el&mode=lst&dir=&occ=first&part=1&cid=4408645

ΚΕΦΑΛΑΙΟ ΠΕΜΠΤΟ

ΑΠΟΦΑΣΕΙΣ ΑΠΔΠΧ: 26/2003, 1/2007, 18/2007, 22/2007, 33/2008, 66/2008, 54/2010, 122/2011 και 27/2012, 122/2011, 50/2011, 113/2001

ΓΝΩΜΟΔΟΤΗΣΕΙΣ ΑΠΔΠΧ: 3/2009

ΑΠΟΦΑΣΕΙΣ ΕΘΝΙΚΩΝ ΔΙΚΑΣΤΗΡΙΩΝ: ΕφΑθ 2257/1985, ΑΠ 1225/1975, ΕφΠατρ 14/2011, ΕφΘες 1013/2011, ΕφΑθ. 1597/2007, ΕφΘες 702/2005, ΕφΑθ 1664/2001, ΠΠρΘες 6657/2010, ΜΠρΑθ 1654/2010, ΕφΑθ 1597/2007, ΑΠ 1923/2006, ΕφΑθ. 3727/2007, ΕφΑθ 1664/2001, ΕφΑθ 7277/2003

ΚΕΦΑΛΑΙΟ ΕΚΤΟ

ΑΠΟΦΑΣΕΙΣ ΑΠΔΠΧ: 98/2017, 75/2009, 87/2017

ΚΑΝΟΝΙΣΤΙΚΕΣ ΠΡΑΞΕΙΣ ΑΠΔΠΧ: 1/1999, 408/1998

ΑΠΟΦΑΣΕΙΣ ΕΘΝΙΚΩΝ ΔΙΚΑΣΤΗΡΙΩΝ: ΕιρΑθ 273/2016, ΜΠρΑθ 3428/2016, ΕιρΑθ 3277/2014, ΕιρΑθ 415/2016, ΜΕφΑθ 1437/2014, ΑΠ 1923/2006, ΕφΑθ 3833/2003, ΜΠρΑθ 2828/2014

IV. ΚΕΙΜΕΝΑ ΟΜΑΔΑΣ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29

Opinion 1/2010 On the Concepts of "Controller" and "Processor"", *ec.europa.eu*,2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

Opinion 4/2007 on the concept of personal data, https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf

Opinion No. 7/2004 on the Inclusion of Biometric Elements in Residence Permits and Visas Taking Account of the Establishment of the European Information System on visas (VIS)' (WP 96, 11 August 2004),

Opinion 3/2005 on Implementing Council Resolution (EC) No. 2252/ 2004 of 13 December 2004 on Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States' (WP 112, 30 September 2005),

Opinion 3/2012 on Developments in Biometric Technologies' (WP 193, 27 April 2012). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec7

Opinion 03/2013 on purpose limitation (2 April 2013), available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Working Document on The Processing of Personal Data by Means of Video Surveillance", Article 29 Data Protection Working Party, *ec.Europa.eu*, 2002, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp67_en.pdf.

Article 29 Working Party, 'Advice Paper on Special Categories of Data' (4 April 2011), available at https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_ artwp_ mme_ le_ bail_ directive_ 9546ec_ annex1_ en.pdf.

Article 29 Working Party, 'Working Document on Biometrics' (WP 80, 1 August 2003)

Article 29 Working Party, 'Working Document on Genetic Data' (WP 91, 17 March 2004). https://www.statewatch.org/media/documents/news/2004/mar/wp91.pdf.

Article 29 Working Party, "Opinion 03/2013 On Purpose Limitation", Ec.Europa.Eu, 2013 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Article 29 Working Party, 'Guidelines on Individual Automated Decision- Making and Profiling for the Purposes of Regulation 2016/ 679' (WP251.rev01, as last revised and adopted on 6 February 2018).

Ομάδα άρθρου 29, Γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_el.pdf

Ομάδα άρθρου 29, Γνώμη 4/2007 σχετικά με την έννοια του όρου «δεδομένα προσωπικού χαρακτήρα», https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_el.pdf

Ομάδα εργασίας του άρθρου 29, «Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679», 17/EL WP260 rev.01, (29 Νοεμβρίου 2017).

Ομάδα εργασίας του άρθρου 29, «Κατευθυντήριες γραμμές σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679», 17/EL WP259 αναθ.01, (28 Νοεμβρίου 2017).

V. ΝΟΜΟΘΕΣΙΑ ΚΑΙ ΑΛΛΑ ΚΕΙΜΕΝΑ

Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση της οδηγίας 95/46/ΕΚ (General Data Protection Regulation), OJ L 119/1-88, 4.5.2016

Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, OJ L 281/31-50, 23.11.1995.

Charter of Fundamental Rights of the European Union, Charter of Fundamental Rights of the European Union, 2012/C 326/02 (2012)

"European Convention on Human Rights, Convention for The Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, As Amended) (ECHR) (1950)", Echr.Coe. Int, 2021, https://www.echr.coe.int/documents/convention_ell.pdf.

"Το κείμενο Της Διακήρυξης Είναι Διαθέσιμο Στην Ιστοσελίδα", Ohchr.Org, accessed 15 November 2021, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/grk.pdf.

Organisation for Economic Co-operation and Development (OECD), "Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data", 23 September 1980.

Commission Informatique et Libertes, *Rapport de la Commission Informatique et libertes*, La Documentation Francaise, Paris, 1975, 7. https://www.cnil.fr/sites/default/files/atoms/files/rapport_tricot_1975_vd.pdf.

Assemble Nationale, *Projet de loi relatif a l'informatique et aux libertes*, Enregistre a la Presidence de l'Assemblee national le 9 aout 1976, Annexe au proces-verbal de la seance du 2 Octobre 1976, Document Parl. no. 2516, 1–18. https://www.senat.fr/leg/pjl76-2516.pdf

Law no. 78–17 of 6 January 1978 concerning informatics, files and liberties [«*Loi n° 78-17 du 6 Janvier 1978 relative a l'informatique, aux fichiers et aux libertes*»], Official Journal of the French Republic 7 January 1978, 227–231. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000886460

Gesetz zum Schutz vor Miβbrauch personenbezogener Daten bei der Datenverarbeitung of 27 January 1977, *Bundesgesetblatt* 1 February 1977, I, No. 7, 201.
http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl177007.pdf

The Data Protection Registrar, "The Data Protection Act of 1984,
https://www.legislation.gov.uk/ukpga/1984/35/enacted

Recommendation No. R (87) 15 Of The Committee Of Ministers To Member States Regulating The Use Of Personal Data In The Police Sector", Rm.Coe.Int, 2021, https://rm.coe.int/168062dfd4

Οδηγία για τα δικαιώματα των καταναλωτών (Οδηγία 2011/83/ΕΕ διαθέσιμη στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32011L0083&from=EN)

Κανονισμός (ΕΕ) 2018/1807 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Νοεμβρίου 2018, σχετικά με ένα πλαίσιο για την ελεύθερη ροή των δεδομένων μη προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση.

Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (OJ 2005 C 181 p.20).
https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=OJ:C:2005:181:TOC.

Information Commissioner's Office, 'Investigation into the use of Data Analytics in Political Campaigns (6 November 2018), 36. https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

European Data Protection Board, 'Guidelines 3/ 2019 on the processing of personal data through video devices (version for public consultation)' (10 July 2019) https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

Commission expert group on the Regulation (EU) 2016/ 679 and Directive (EU) 2016/ 680, 'Minutes of the Second Meeting'
https://ec.europa.eu/transparency/expert-groups-register/core/api/front/document/9290/download.

Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών.
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_el.pdf.

Council of Europe, 'Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data' (10 October 2018 available at
https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

Committee of Ministers of the Council of Europe, 'Recommendation Concerning the Protection of Personal Data Collected and Processed for Statistical Purposes' (Rec (1997)18, 30 September 1997)

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

F.T. Commission et al., big data: a tool for inclusion or exclusion? Understanding the issues. FTC Report, (2016, January).
https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

ΠΔ/ΤΕ 2622/2009, ΠΔ/ΤΕ 2501/2002, ΠΔ/ΤΕ 2577/9.3.2006

Ελληνική Ένωση Τραπεζών, "Πρόληψη Της Χρησιμοποίησης Του Χρηματοπιστωτικού Συστήματος Για Τη Νομιμοποίηση Εσόδων Από Εγκληματικές Δραστηριότητες Και Την Καταπολέμηση Της Τρομοκρατίας" https://www.hba.gr/5Ekdosis/UplPDFs/deltia/4_2006/4-41.pdf.

Ελληνική Ένωση Τραπεζών, "Κώδικας Δεοντολογίας Για Την Επεξεργασία Προσωπικών Δεδομένων Στο Τραπεζικό Σύστημα" (repr., Σχέδιο 16.1.2019).
https://www.hba.gr/UplDocs/GDPR/%CE%9A%CE%A9%CE%94%CE%99%CE%9A%CE%91%CE%A3%20%CE%94%CE%95%CE%9F%CE%9D%CE%A4%CE%9F%CE%9B%CE%9F%CE%93%CE%99%CE%91%CE%A3.pdf

Ενημερωτικό Δελτίο ΑΠΔΠΧ - Τεύχος 12 Ιούλιος 2015", (2015). Διαθέσιμο στην ιστοσελίδα: https://www.dpa.gr/sites/default/files/2020-12/JULY2015.PDF.

VI. ΙΣΤΟΣΕΛΙΔΕΣ

"Ξεκινούν Οι Επενδύσεις Στα Data Center Νέας Γενιάς – Κόμβος Δεδομένων Η Ελλάδα", Capital.Gr, 2021, https://www.capital.gr/epixeiriseis/3559124/xekinoun-oi-ependuseis-sta-data-center-neas-genias-kombos-dedomenon-i-ellada.

"Embracing The Internet of Everything to Capture Your Share Of $14.4 Trillion". Cisco.Com, 2013. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf.

"Semayne's Case Definition", Duhaime.Org, 2021,
Διαθέσιμο στο: http://www.duhaime.org/LegalDictionary/S/SemaynesCase.aspx.

Katz v. United States." Oyez. Accessed July 15, 2021. https://www.oyez.org/cases/1967/35.

Katz Κατά Ηνωμένων Πολιτειών: Ανώτατο Δικαστήριο, Επιχειρήματα, Επιπτώσεις, Greelane.Com, 2020, https://www.greelane.com/el/%CE%BA%CE%BB%CE%B1%CF%83%CF%83%CE%B9%CE%BA%CE%AD%C

F%82-%CE%BC%CE%B5%CE%BB%CE%AD%CF%84%CE%B5%CF%82/%CE%B8%CE%AD%CE%BC%CE%B1%CF%84%CE%B1/katz-v-united-states-supreme-court-case-arguments-impact-4797888/.

Julia Angwin, Terry Jr. Parris and Surya Mattu, "Facebook Is Quietly Buying Information from Data Brokers About Its Users' Offline Lives", Business Insider, 2016, https://www.businessinsider.com/facebook-data-brokers-2016-12#:~:text=Facebook%20is%20quietly%20buying%20information,about%20its%20users'%20offline%20lives&text=Nor%20does%20Facebook%20show%20users,the%20Center%20for%20Digital%20Democracy

"ING And the Use of Customer Data". ING.Com, 2022. https://www.ing.com/about-us/ing-and-the-use-of-customer-data.htm#:~:text=Apart%20from%20the%20transactions%2C%20ING,tailored%20information%20and%20special%20offers.

Βασίλης Σωτηρόπουλος, "Προστασία Προσωπικών Δεδομένων", Digestaonline.Gr, 2005, http://www.digestaonline.gr/pdfs/Digesta%202005/DIGESTA%201-2005/5%20SOTOU.pdf.

Flexera, 'State of the Cloud Report 2020' (2020) <https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020> accessed 10 January 2022.

Gartner, 'Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019' (2019) https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwidepublic-cloud-revenue-to-g, accessed 7 October 2020.

IBM, 'How you're Charged' https://cloud.ibm.com/docs/billing-usage?topic=billing-usage-charges.

Products Services, "Cisco Servers – Unified Computing System (UCS)", Cisco, 2022, https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html.

"Threat And Risk Management-CRAMM", 2005. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_cramm.html. https://www.enisa.europa.eu/publications/security-and-resilience-in-governmental-clouds

"Standard For Automatic Exchange of Financial Account Information in Tax Matters | En | OECD". Oecd.Org, 2014. https://www.oecd.org/ctp/exchange-of-tax-information/standard-for-automatic-exchange-of-financial-account-information-for-tax-matters-9789264216525-en.htm.

"Financial Action Task Force (FATF)". Fatf-Gafi.Org. Accessed 30 January 2022. https://www.fatf-gafi.org/countries/.

"The 5 Biggest Threats to A Bank's Cyber Security". SQN Banking Systems. Accessed 5 January 2022. https://sqnbankingsystems.com/blog/the-5-biggest-threats-to-a-banks-cyber-security/.

"The Equifax Breach: What You Should Know – Krebs on Security". Krebsonsecurity.Com, 2017. https://krebsonsecurity.com/2017/09/the-equifax-breach-what-you-should-know/.

Tunggal, Abi Tyas. "The 62 Biggest Data Breaches (Updated for January 2022) | Upguard". Upguard.Com, 2022. https://www.upguard.com/blog/biggest-data-breaches.

"'Εντυπο ενημέρωσης για την επεξεργασία προσωπικών δεδομένων της τράπεζας eurobank α.ε. σύμφωνα με τον Κανονισμό (ΕΕ) 2016/679 και τη σχετική ελληνική και ενωσιακή νομοθεσία". Eurobank.Gr. Accessed 30 January 2022. https://www.eurobank.gr/el/gdpr-prosopika-dedomena/.

Piraeus Group, "Ενημέρωση Επενδυτών-Μετοχολόγιο", Piraeusholdings.Gr, 2022, https://www.piraeusholdings.gr/el/investors/metochologio.

"Νομιμότητα Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα Από Εταιρείες Ενημέρωσης Οφειλετών". *Hellenicparliament.Gr*, 2013. https://www.hellenicparliament.gr/UserFiles/67715b2c-ec81-4f0c-ad6a-476a34d732bd/7970809.pdf.

"Νομιμότητα Επεξεργασίας Δεδομένων Τρίτων Προσώπων – Μη Οφειλετών Στο Πλαίσιο Ενημέρωσης Οφειλετών Για Ληξιπρόθεσμες Απαιτήσεις". Dpa.Gr, 2013. https://www.dpa.gr/sites/default/files/2020-05/ENIMEROSI%20OFEILETON%20-%20KATAGRAFI%20SYNOMILION%20ME%20TRITOYS_FINAL.PDF.

ΠΑΡΑΡΤΗΜΑ