ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2022-2023

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της Μαρίας Ρουμελιώτη (Α.Μ.: 2143)

«ΕΠΙΘΕΣΕΙΣ PHISHING, ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΧΡΗΣΤΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΡΑΠΕΖΙΚΗΣ»

Επιβλέπουσα:

Λίλιαν Μήτρου

Πειραιάς, Δεκέμβριος 2023

Αφιέρωση

Στους γονείς μου

Δημήτρη και Χριστίνα

Ευχαριστίες

Με την παρούσα Διπλωματική Εργασία ολοκληρώνεται ο κύκλος σπουδών μου στο Πρόγραμμα Μεταπτυχιακών Σπουδών «ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ» του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς.

Η φοίτηση παράλληλα με την άσκηση δικηγορίας αποτέλεσε ένα μονοπάτι δύσβατο προς την αναζήτηση νέων πνευματικών οριζόντων, όμως ο τελικός προορισμός άξιζε τις οποιεσδήποτε θυσίες, αφού εν τέλει αποτέλεσε φαρέτρα για την προσωπική και την επαγγελματική μου ανέλιξη.

Αρχικά, θα ήθελα να ευχαριστήσω τις συμφοιτήτριες και τους συμφοιτητές μου για την ανταλλαγή επιστημονικών απόψεων καθώς και το σύνολο των καθηγητριών και των καθηγητών μου που μας μεταλαμπάδευσαν την εμπειρία και την τεχνογνωσία στους τομείς όπου εξειδικεύονται. Ιδιαίτερα θα ήθελα να απευθύνω θερμές ευχαριστίες στον εμπνευστή και υπεύθυνο του εν λόγω Π.Μ.Σ., στον κο Στέφανο Γκρίτσαλη και κυρίως στην καθηγήτρια και επιβλέπουσα, στην κα Λίλιαν Μήτρου για τη συνεισφορά της τόσο στην εκπόνηση της παρούσας εργασίας, αλλά και για την μαθητοκεντρική διδασκαλία της, την πολύτιμη καθοδήγησή της και την εν γένει συνεισφορά της στον τομέα του Δικαίου και των ΤΠΕ.

Τέλος, ευχαριστώ όσους και όσες με δίδαξαν να μην εγκαταλείπω τους στόχους μου μέχρι να κατακτήσω τα όνειρά μου. Πάνω από όλα ευχαριστώ εγκαρδίως την οικογένεια μου και όλους τους κοντινούς μου ανθρώπους που αποτέλεσαν το στήριγμά μου για να φτάσω έως εδώ.

Περιεχόμενα

Συντομογραφίες

Ελληνικές

❖ αιτ. σκ.	αιτιολογική σκέψη
❖ Α.Ε.	Ανώνυμη Εταιρεία
❖ ΑΚ	Αστικός Κώδικας
❖ ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
❖ αρθ.	άρθρο
❖ βλ.	βλέπε
❖ ΓΕΜΗ	Γενικό Εμπορικό Μητρώο
❖ ΓΚΠΔ	Γενικός Κανονισμός για την Προστασία των Δεδομένων
❖ ΔΕΕ	Δικαστήριο Ευρωπαϊκής Ένωσης
❖ ΔΙΑΣ	Διατραπεζικά Συστήματα
❖ ΕΛΣΤΑΤ	Ελληνική Στατιστική Αρχή
❖ Ε.Ο.Χ.	Ευρωπαϊκός Οικονομικός Χώρος
❖ ΕΣΠΔ	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
❖ κλπ.	και λοιπά
❖ επ.	επόμενα
❖ ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
❖ Ν.	Νόμος
❖ Οδ.	Οδηγία
❖ ό.π	όπως και προηγουμένως
❖ παρ.	παράγραφος
❖ ΠΕΕ	Πράξη Εκτελεστικής Επιτροπής
❖ περ.	περίπτωση
❖ ΠΚ	Ποινικός Κώδικας
❖ ΠΥΠ	Πάροχος Υπηρεσιών Πληρωμών

- στοιχ. — στοιχείο
- ΤΠΕ — Τεχνολογίες Πληροφορικής και Επικοινωνιών
- ΤτΕ — Τράπεζα της Ελλάδος
- ΦΕΚ — Φύλλα Εφημερίδας της Κυβέρνησης
- ΧΘΔΕΕ — Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

Ξενόγλωσσες

- Art. 29 WP — Article 29 Working Party
- B2B — Business to Business
- B2C — Business to Consumer
- CSIRT — Computer Security Incident Response Team
- DNS — Domain Name System
- DORA — Digital Operational Resilience Act
- DPIA — Data Protection Impact Assessment
- ENISA — European Union Agency for Cybersecurity
- GDPR — General Data Protection Regulation
- FA — Factor Authentication
- IP address — Internet Protocol address
- ISO — International Organization for Standardization
- MiFID — Markets in Financial Instruments Directive
- NIS — Network and Information Security
- OTP — One Time Password
- PSD — Payment Services Directive

Περίληψη

Ο ψηφιακός μετασχηματισμός της κοινωνίας και κατ' επέκταση της οικονομίας έχει διεισδύσει στην καθημερινότητά μας και στον τραπεζικό τομέα. Η εκτεταμένη χρήση υπηρεσιών ηλεκτρονικής τραπεζικής μπορεί να παρέχει αρκετά προνόμια στο πλαίσιο συνεργασίας των τραπεζών με τους πελάτες της, ανοίγει όμως ένα νέο παράθυρο δράσης στους κυβερνοεγκληματίες για τη διάπραξη ηλεκτρονικών τραπεζικών απατών, θέτοντας στο στόχαστρο το άδειασμα των τραπεζικών λογαριασμών ανυποψίαστων θυμάτων, την παρακώλυση των ψηφιακών συστημάτων των τραπεζών και την παραβίαση των προσωπικών δεδομένων των χρηστών ηλεκτρονικής τραπεζικής.

Στο πρώτο κεφάλαιο επιχειρείται η προσέγγιση του φαινομένου επιθέσεων ηλεκτρονικού ψαρέματος (phishing) στον τομέα της ηλεκτρονικής τραπεζικής. Κατόπιν διενέργειας αυθαίρετων συναλλαγών και απώλειας των χρημάτων, το θύμα έρχεται συχνά αντιμέτωπο με την αδυναμία ανεύρεσης του δράστη καθώς και με την απέκδυση ευθυνών της τράπεζας. Έτσι, κρίνεται σκόπιμη η νομική προστασία του, η οποία εξετάζεται εν προκειμένω τόσο σε επίπεδο ποινικών κυρώσεων όσο και σε επίπεδο αστικών αξιώσεων, οι οποίες απορρέουν από την ενδοσυμβατική και αδικοπρακτική ευθύνη της τράπεζας. Παράλληλα εξετάζεται το επίπεδο ευθύνης του πληρωτή από μη εγκεκριμένες συναλλαγές και το πλαίσιο κυβερνοασφάλειας που οφείλει να τηρεί η τράπεζα για την διασφάλιση ενός ασφαλούς περιβάλλοντος διενέργειας τραπεζικών συναλλαγών εξ αποστάσεως.

Στο δεύτερο κεφάλαιο αναπτύσσεται το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων των χρηστών ηλεκτρονικής τραπεζικής σύμφωνα με τις επιταγές του GDPR. Αρχικά, επιχειρείται η χαρτογράφηση μέσω της καταγραφής των κατηγοριών προσωπικών δεδομένων των χρηστών και έπειτα των γενικών αρχών και των βάσεων για τη σύννομη επεξεργασία των τραπεζικών δεδομένων τους. Εν συνεχεία, καταγράφονται τα δικαιώματα του υποκειμένου – χρήστη υπηρεσιών ηλεκτρονικής τραπεζικής και οι λοιπές υποχρεώσεις κανονιστικής συμμόρφωσης της τράπεζας. Τέλος, θίγεται το

ζήτημα παραβίασης ασφαλείας των δεδομένων των χρηστών ηλεκτρονικής τραπεζικής, η οποία ενδέχεται να λάβει χώρα κατόπιν μιας επίθεσης phishing και υποκλοπής των τραπεζικών στοιχείων τους.

Λέξεις κλειδιά: ηλεκτρονική τραπεζική απάτη, επιθέσεις phishing, ισχυρή ταυτοποίηση, συναλλαγή, γνήσια, εγκεκριμένη, ευθύνη τράπεζας για phishing, ευθύνη πληρωτή, μέτρα δέουσας επιμέλειας, κυβερνοασφάλεια συστημάτων τράπεζας, κυβερνοανθεκτικότητα, διαχείριση κινδύνων ΤΠΕ, προστασία προσωπικών δεδομένων χρηστών ηλεκτρονικής τραπεζικής, τεχνικά και οργανωτικά μέτρα, παραβίαση ασφαλείας

1. Εισαγωγή στην ηλεκτρονική τραπεζική

Στις αρχές της νέας χιλιετίας, η άνοδος του Διαδικτύου και η εκτεταμένη χρήση προσωπικών ηλεκτρονικών υπολογιστών, συντέλεσε στην εμφάνιση νέων επιχειρηματικών μοντέλων και στη μετάβαση από τα παραδοσιακά φυσικά καταστήματα, αποκαλούμενα ως brick and mortar stores, με χαρακτηριστικό την αυτοπρόσωπη παρουσία πωλητή και καταναλωτή, στις πλατφόρμες ηλεκτρονικού εμπορίου και στις εξ αποστάσεως ηλεκτρονικές συναλλαγές[1]. Επιπροσθέτως, η εμφάνιση των έξυπνων συσκευών στα τέλη της δεκαετίας του 2000 δημιούργησε το υπόβαθρο για την ανάδυση νέων καναλιών σύνδεσης και επικοινωνίας με τους καταναλωτές, όπως τα μέσα κοινωνικής δικτύωσης. Τη δεκαετία (2010-2020) η αύξηση της χρήσης των έξυπνων συσκευών και των χρηστών των μέσων κοινωνικής δικτύωσης, δημιούργησε ένα «οικοσύστημα» από έξυπνες συσκευές που «αλληλεπιδρούν» και προσπαθούν να «προλάβουν» ή και να δημιουργήσουν την επιθυμία του καταναλωτή[2]. Μετά το ξέσπασμα της Τέταρτης Βιομηχανικής Επανάστασης, ο ψηφιακός μετασχηματισμός των επιχειρήσεων φαίνεται να είναι κρίσιμος παράγοντας για τη βιωσιμότητα τους καθώς όσες επιχειρήσεις έχουν εντονότερο ψηφιακό αποτύπωμα διαθέτουν συγκριτικό πλεονέκτημα έναντι όσων δεν είναι έτοιμες ψηφιακά.

Η εισδοχή της τεχνολογικής και κυρίως της εξελιγμένης ψηφιακής οικονομίας με την ανάπτυξη νέων μορφών ψηφιακού εμπορίου, δεν αφήνει ανεπηρέαστο και τον τραπεζικό τομέα. Σύμφωνα με την ανακοίνωση της Ευρωπαϊκής Επιτροπής αναφορικά με μια στρατηγική ψηφιακών χρηματοοικονομικών υπηρεσιών[3], το μέλλον προβλέπεται ψηφιακό. Τα τελευταία χρόνια σημειώθηκε αλματώδης αύξηση της ψηφιακής οικονομίας, η

---

[1] *Ελληνική Συνομοσπονδία Εμπορίας & Επιχειρηματικότητας, (2021), Η Λευκή Βίβλος του Λιανικού Εμπορίου 2040, Προβληματισμοί και εκτιμήσεις για τον μετασχηματισμό του λιανικού εμπορίου σελ.7*

[2] *Βλ. Ελληνική Συνομοσπονδία Εμπορίας & Επιχειρηματικότητας, 2021, Η Λευκή Βίβλος του Λιανικού Εμπορίου 2040, ό.π.*

[3] *Ανακοίνωση της Ευρωπαϊκής Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή οικονομική και κοινωνική Επιτροπή και την Επιτροπή Περιφερειών σχετικά με μια στρατηγική ψηφιακών χρηματοοικονομικών υπηρεσιών για την ΕΕ της 24ης Σεπτεμβρίου 2020, COM (2020) 591, Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:52020DC0591*

πρωτοφανής δε κατάσταση που επικράτησε μετά την πανδημία του COVID-19 συντέλεσε στο να αξιοποιήσουν σε μεγαλύτερο βαθμό τις ψηφιακές τεχνολογίες τόσο οι τράπεζες όσο και οι καταναλωτές και να μεταβληθούν κατά αυτό τον τρόπο τα επιχειρηματικά μοντέλα. Λόγου χάρη, μέσω της ηλεκτρονικής ταυτοποίησης χρήστη, πολλοί καταναλωτές προέβησαν σε άνοιγμα τραπεζικού λογαριασμού, απέκτησαν ευκολότερη πρόσβαση σε αιτήσεις για δανειοδότηση και αυξήθηκαν σημαντικά οι ηλεκτρονικές πληρωμές μέσω της ηλεκτρονικής τραπεζικής.

Σύμφωνα με την Ένωση Ελληνικών Τραπεζών[4], ως **ηλεκτρονική τραπεζική (e-banking)** ορίζεται «οποιαδήποτε εμπορική συναλλαγή που διεξάγεται μεταξύ της τράπεζας και των πελατών της διαμέσου ηλεκτρονικών δικτύων και βοηθάει στην πώληση τραπεζικών υπηρεσιών/ προϊόντων». Οι συναλλαγές αυτές μπορεί να λαμβάνουν χώρα είτε ανάμεσα στην τράπεζα και στους ιδιώτες πελάτες - καταναλωτές, οπότε πρόκειται για retail banking (B2C), είτε ανάμεσα στις τράπεζες και τις επιχειρήσεις (B2B). Πρόκειται για έναν ευρύτερο ορισμό στον οποίο εντάσσονται διαφορετικοί τρόποι διενέργειας συναλλαγών εξ αποστάσεως, όπως: μέσω του παγκόσμιου διαδικτύου (internet banking), μέσω σταθερού τηλεφώνου (phone banking), μέσω κινητού τηλεφώνου (mobile banking) είτε μέσω αυτόματης ταμειολογιστικής μηχανής (ATM).

Επιπροσθέτως, κατά την Ένωση Ελληνικών Τραπεζών αναφορικά με τις **τραπεζικές υπηρεσίες e-banking**, αυτές περιλαμβάνουν τόσο πληροφοριακές όσο και οικονομικές συναλλαγές. Στις πληροφοριακές συναλλαγές ενδεικτικά μπορεί να συγκαταλέγονται πληροφορίες λογαριασμών, πληροφορίες για κινήσεις και υπόλοιπα λογαριασμών, πληροφορίες δανείων, υπόλοιπα πιστωτικών καρτών, αιτήσεις για τραπεζικά προϊόντα, παρακολούθηση της εξέλιξης εντολών πληρωμών, αλλαγή προσωπικών στοιχείων όπως κωδικών πρόσβασης, παρακολούθηση και ανάκληση/ ακύρωση επιταγών, αποστολή προσωπικών μηνυμάτων, συναλλαγματικές ισοτιμίες, υπολογισμός δανείων.

[4] *Γιαννόπουλος Γ., Internet Banking: Νομικά ζητήματα από τη διεξαγωγή τραπεζικών συναλλαγών στο διαδίκτυο, Ελληνική Ένωση Τραπεζών, Διαθέσιμο στο:* https://www.hba.gr/5Ekdosis/UplPDFs/deltia/3_2003/97-108.pdf

Στις δε οικονομικές συναλλαγές, ενδεικτικά συγκαταλέγονται μεταφορές κεφαλαίων είτε μεταξύ προσωπικών λογαριασμών εντός της τράπεζας, είτε σε λογαριασμούς τρίτων εντός τράπεζας, είτε σε άλλη τράπεζα της Ελλάδας ή του εξωτερικού, καθώς και πληρωμές: δημοσίου, λογαριασμών ΔΕΚΟ, ασφαλιστικών εισφορών, συνδρομών, πιστωτικής κάρτας, δόσης δανείου και αποστολή αρχείου μισθοδοσίας, αποστολή αρχείου μαζικών πληρωμών τρίτων εντός τραπέζης και σε άλλες τράπεζες και ακύρωση εντολών.

Στην Ελλάδα, βάσει στατιστικών στοιχείων της ΔΙΑΣ Α.Ε. για το έτος 2022, σημειώθηκε διψήφιο ποσοστό αύξησης των συναλλαγών που διενεργήθηκαν μέσω διατραπεζικών συστημάτων για δεύτερη συνεχόμενη χρονιά. Η εκρηκτική άνοδος των ηλεκτρονικών συναλλαγών δικαιολογείται ένεκα των πολλαπλών ωφελειών που παρέχει η διενέργεια τους τόσο για το τραπεζικό ίδρυμα όσο και για τους πελάτες. Πρώτα απ' όλα, οι χρήστες μπορούν να χρησιμοποιούν τις υπηρεσίες e-banking με ευκολία από την άνεση του σπιτιού τους οποιαδήποτε ημέρα και σε οποιαδήποτε από τις 24 ώρες της ημέρας επιθυμούν, καταρρίπτοντας χωρικούς και χρονικούς περιορισμούς και εξοικονομώντας χρόνο από το να περιμένουν στην ουρά ενός φυσικού καταστήματος, όπου τηρείται συγκεκριμένο ωράριο εξυπηρέτησης. Το προνόμιο αυτό απέκτησε ιδιαίτερη αξία στην περίοδο της καραντίνας εξαιτίας της πανδημίας Covid-19, όπου ο πελάτης μπορούσε να χρησιμοποιεί κανονικά τις ηλεκτρονικές υπηρεσίες από την ασφάλεια του σπιτιού του τη στιγμή που δεν ήταν εύκολο να έχει πρόσβαση σε ένα φυσικό υποκατάστημα τράπεζας. Επιπλέον, μέσω της χρήσης e- banking, παρέχεται ταχύτητα στη διενέργεια των συναλλαγών, καθώς το τραπεζικό σύστημα μπορεί να εκτελέσει τις εντολές μεταφορές εμβασμάτων με την ίδια ταχύτητα ή ακόμα πιο γρήγορα και από το ΑΤΜ. Ένα ακόμα πλεονέκτημα αποτελεί ότι ο χρήστης μπορεί ανά πάσα στιγμή να έχει ενημέρωση και τον έλεγχο του τραπεζικού του λογαριασμού, λόγου χάρη για το εάν μια συναλλαγή εκτελέστηκε επιτυχώς, για την ημερομηνία και ώρα εκτέλεσής της, να οργανώσει με πάγιες εντολές την ακριβή ημερομηνία που επιθυμεί να πληρωθεί ένας λογαριασμός αλλά και να ενημερωθεί άμεσα για νέα προϊόντα και υπηρεσίες. Ο πελάτης έχοντας αυξημένες δυνατότητες

επιλογής τραπεζικών υπηρεσιών «στα χέρια της συσκευής που χρησιμοποιεί», μπορεί έτσι να εξοικονομεί δαπάνες από χρήση υπηρεσιών που θα ενείχαν κόστος, εάν τις πραγματοποιούσε στο γκισέ ενός υποκαταστήματος. Παράλληλα, η τράπεζα εξοικονομεί λειτουργικά έξοδα σε σχέση με τη διατήρηση ενός φυσικού υποκαταστήματος, ελαχιστοποιώντας το κόστος παραγωγής αλλά και αυξάνοντας τις δυνατότητες παγκόσμιας δράσης με την ανάπτυξη του πελατολογίου και των εργασιών της, τη συλλογή πληροφοριών και παροχή εξειδικευμένων υπηρεσιών για τους πελάτες της και τη βελτιωμένη ανταγωνιστικότητα.

Όπως κάθε νόμισμα έχει δύο όψεις, έτσι και ο ψηφιακός μετασχηματισμός στον τραπεζικό τομέα μπορεί να παρείχε πολλαπλά οφέλη για τη διενέργεια συναλλαγών εξ αποστάσεως, συντέλεσε όμως στο να κερδίσουν έδαφος για δράση οι κυβερνοεγκληματίες, καθώς αυξήθηκαν επίσης οι δυνατότητες τέλεσης ηλεκτρονικής τραπεζικής απάτης με τη μέθοδο phishing. Ειδικότερα, οι δράστες εκμεταλλευόμενοι την εκτεταμένη χρήση του διαδικτύου και ιδίως της χρήσης των κινητών τηλεφώνων από τους χρήστες των υπηρεσιών ηλεκτρονικής τραπεζικής -η οποία αυξήθηκε έτι περαιτέρω κατόπιν των μέτρων για τον περιορισμό της διάδοσης του COVID-19- αποκτούν πρόσβαση σε δεδομένα προσωπικού χαρακτήρα προκειμένου να αποκομίσουν ιδίως οικονομικό όφελος. Επιπλέον, οι δράστες χρησιμοποιώντας τα κατάλληλα εργαλεία, αποκρύπτουν την πραγματική τους ταυτότητα και τοποθεσία, ενώ η επιλογή των θυμάτων είναι κατά βάση τυχαία αφού γίνεται με αυτοματοποιημένα μαζικά μηνύματα ή κλήσεις σειριακά σε όλους τους αριθμούς.

Αξιοσημείωτο είναι το γεγονός ότι για τους πρώτους εννέα μήνες του έτος 2021 συνεπεία και του lockdown, σύμφωνα με σύσκεψη που πραγματοποιήθηκε στο Υπουργείο Προστασίας του Πολίτη, σημειώθηκε ότι στη χώρα μας υπήρξε **αύξηση κατά 200 % στις ηλεκτρονικές απάτες με τη μέθοδο «phishing»,** με τους επιτήδειους να έχουν αφαιρέσει παράνομα συνολικά το ποσό των 40 εκατομμυρίων ευρώ από ανυποψίαστους πολίτες, χρησιμοποιώντας εκατό διαφορετικούς τρόπους ηλεκτρονικής απάτης.

Επιπροσθέτως, σύμφωνα με στατιστικά στοιχεία της Έκθεσης Χρηματοπιστωτικής Σταθερότητας της Ελλάδος[5], αναφορικά με τα περιστατικά απάτης στις συναλλαγές εξ αποστάσεως, οι περισσότερες εξ αυτών αφορούν διαδικτυακές συναλλαγές κυρίως με επιχειρήσεις του εξωτερικού. Οι οικονομικές ζημίες από τις ηλεκτρονικές απάτες κρούουν τον κινδύνου, καθώς βάσει στοιχείων της Ευρωπαϊκής Τραπεζικής Αρχής, **το ετήσιο κόστος από τις ηλεκτρονικές απάτες στην Ελλάδα ξεπερνάει τα 22 εκατομμύρια Ευρώ**, δηλαδή ποσοστό τριπλάσιο από το τον ευρωπαϊκό μέσο όρο[6]. Τα χρήματα των ανυποψίαστων θυμάτων «κάνουν φτερά» από τους τραπεζικούς λογαριασμούς τους είτε κατόπιν αγορών που πραγματοποιούνται με κάρτες στο διαδίκτυο είτε κατόπιν μεταφοράς πιστώσεων στις online πληρωμές/μεταφορές κεφαλαίων μέσω της χρήσης υπηρεσιών ηλεκτρονικής τραπεζικής μέσω διαδικτύου και μέσω κινητού τηλεφώνου.

Παρά τις οικονομικές ζημίες, το φαινόμενο phishing συνεχώς δεν εκλείπει με τους πολίτες να βρίσκονται εκτεθειμένοι ενώπιον των τεχνασμάτων που ευρίσκουν ανελλιπώς οι δράστες. Στις 15 Ιουλίου του έτους που διανύουμε (2023), η Εθνική Αρχή Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης, εξέδωσε Δελτίο Τύπου, κατόπιν αυξημένων αναφορών για αποστολή παραπλανητικών μηνυμάτων ηλεκτρονικού ψαρέματος είτε μέσω ηλεκτρονικής αλληλογραφίας, είτε μέσω γραπτών μηνυμάτων αλλά και μέσω των μέσων κοινωνικής δικτύωσης. Η εν λόγω Αρχή με σκοπό την ενημέρωση και προστασία των πολιτών από τις επιθέσεις phishing, δημοσίευσε μάλιστα μια τυπική μορφή ψευδούς μηνύματος email, που είχε ως σκοπό την εξαπάτηση του θύματος και το οποίο προσομοίωνε αίτημα από την υπηρεσία eGov- KYC, με το οποίο οι δράστες ζητούσαν στοιχεία επικοινωνίας από ανυποψίαστα θύματα[7].

---

[5] *Τράπεζα της Ελλάδος, (2023), Έκθεση Χρηματοπιστωτικής Σταθερότητας, Διαθέσιμο στο: https://www.bankofgreece.gr/Publications/FINANCIAL_STABILITY_REVIEW_MAY_2023_EL.pdf, σελ.118*

[6] *Newsroom, Emea Business Voice, Ξεπερνούν τα 22 εκατ. ευρώ οι ηλεκτρονικές απάτες στην Ελλάδα, Διαθέσιμο στο: https://emea.gr/kyrio-thema/653181/xepernoun-ta-22-ekat-evro-oi-ilektronikes-apates-stin-ellada/*

[7] *Ελληνική Δημοκρατία, Υπουργείο Ψηφιακής Διακυβέρνησης, Ανακοίνωσης της 15ης Ιουλίου 2023 της Εθνικής Αρχής Κυβερνοασφάλειας, Διαθέσιμο στο: https://mindigital.gr/archives/5310*

2. Κεφάλαιο Α': Επιθέσεις phishing και κυβερνοασφάλεια στον τομέα της ηλεκτρονικής τραπεζικής

2.1. Ορισμός ηλεκτρονικού ψαρέματος (phishing) στον τραπεζικό τομέα

Αναφορικά με την έννοια του «phishing», αποδιδόμενου στα ελληνικά ως «ηλεκτρονικό ψάρεμα», θεωρείται: *η απόκτηση πληροφοριών προσωπικού και οικονομικού χαρακτήρα (όνομα χρήστη, κωδικοί πρόσβασης, κλπ) μέσω δολίων μέσων, όπως παραπλανητικών τηλε –μηνυμάτων ή αντιγράφων γνήσιων νόμιμων ιστοτόπων*[8]. Σύμφωνα με έναν ακόμη ορισμό που συναντούμε στην αιτ. σκ. 13 της Οδ. 2019/73 σχετικά με την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών, ως **ηλεκτρονικό ψάρεμα** νοείται *«η αντιγραφή δεδομένων κάρτας ή κατεύθυνσης ή ανακατεύθυνσης των χρηστών υπηρεσιών πληρωμής σε ψευδεπίγραφους ιστότοπους και η διανομή τους»*. Περαιτέρω, σύμφωνα με τον ορισμό της αιτιολογικής έκθεσης για το άρθ.20 του σχέδιο Νόμου για την Ενσωμάτωση της Οδ.2020/1828, γίνεται αναφορά στο phishing ως «*πρακτική εξαπάτησης (με πλαστές ιστοσελίδες, ηλεκτρονικά μηνύματα ή ειδοποιήσεις), με τις οποίες οι δράστες πληροφορούνται ή υφαρπάζουν τους μυστικούς κωδικούς («PIN», «TAN») των καταναλωτών για διαδικτυακές συναλλαγές και μεταφορές χρημάτων*».

Εκ των ανωτέρω συνάγεται ότι, το ηλεκτρονικό ψάρεμα αποτελεί μια μορφή επίθεσης της κοινωνικής μηχανικής, ομόηχη της λέξης fishing, δηλαδή της αλιείας – δολώματος καθώς αναφέρεται στη μέθοδο των δραστών να αλιεύουν απόρρητα προσωπικά και οικονομικά δεδομένα των ανυποψίαστων «δολωμάτων», χρηστών των υπηρεσιών της ηλεκτρονικής τραπεζικής. Ειδικότερα, ο δράστης προσποιούμενος μια έμπιστη οντότητα, εν προκειμένω μια τράπεζα, προσπαθεί να πείσει το ανυποψίαστο θύμα να προβεί σε αποκάλυψη τραπεζικών δεδομένων του όπως το username και το password για τη σύνδεση σε υπηρεσίες ηλεκτρονικής τραπεζικής, ή/και τα στοιχεία της πιστωτικής/χρεωστικής κάρτας, μέσω μιας ψεύτικης φόρμας η οποία ομοιάζει με

[8] *Jougleux, P. (2016) «Ευρωπαϊκό δίκαιο του διαδικτύου, Νομικές πτυχές του διαδικτύου στην Ευρώπη», Αθήνα – Θεσσαλονίκη, σελ.133 επ.*

την αυθεντική.[9] Η μέθοδος αυτή στηρίζεται στη ψυχολογική/συναισθηματική χειραγώγηση του θύματος καθώς και την έλλειψη γνώσεων και έλλειψης προσοχής που έχει ως αποτέλεσμα το θύμα να προβεί στην κοινολόγηση εμπιστευτικών πληροφοριών στο δράστη ή να προχωρήσει το ίδιο το θύμα σε ενέργειες ενάντια στη (συνειδητή) βούλησή του, η οποία εν τέλει θα οδηγήσει στην περιουσιακή ζημία του.

2.2. Συνηθέστερες μορφές επιθέσεων phishing κατά τη χρήση υπηρεσιών ηλεκτρονικής τραπεζικής

Αναφορικά με τους μεθόδους που χρησιμοποιούν οι phishers στις ηλεκτρονικές τραπεζικές απάτες, αυτές συνεχώς εξελίσσονται και είναι μη προβλέψιμες ακολουθώντας τη ροή των τεχνολογικών εξελίξεων. Οι πιο συνηθισμένες επιθέσεις τελούνται κυρίως είτε μέσω **μηνυμάτων ηλεκτρονικής αλληλογραφίας,** με την αποστολή μαζικών παραπλανητικών spam bot μηνυμάτων, τα οποία αποστέλλονται προς το υποψήφιο θύμα με τρόπο που να φαίνονται εξατομικευμένα και σαν να έχουν αποσταλεί από την τράπεζα[10], είτε μέσω **μεταμφιεσμένων «πλαστών» ιστοσελίδων** στις οποίες μπορεί να ανακατευθυνθεί ο δράστης ύστερα από την αναζήτηση του για σύνδεση στο σύστημα ηλεκτρονικής τραπεζικής, είτε μέσω υπερσυνδέσμου που θα έχει λάβει προηγουμένως από το δράστη.

Οι μέθοδοι που χρησιμοποιούνται για επιθέσεις με ηλεκτρονικό ταχυδρομείο μπορεί να περιλαμβάνουν[11]: χρήση αλληλογραφίας που φαίνεται να έχει αποσταλεί από έμπιστη πηγή όπως εν προκειμένω το τραπεζικό ίδρυμα με το οποίο ο παραλήπτης διενεργεί τις συναλλαγές τους, χρήση εξατομικευμένης αλληλογραφίας, χρήση αντιγράφων ηλεκτρονικής αλληλογραφίας στα οποία έχουν γίνει αλλαγές στα περιεχόμενα URLs και hyperlinks, χρήση ιών (viruses) και σκουληκιών (worms) συνημμένων σε

---

[9] *Γέρμανος Γ., Γεωργίου Ν., (2021) «Κυβερνοέγκλημα, Πρόληψη-Διερεύνηση-Αντιμετώπιση», Αθήνα, ISBN 978-618-00-2651-1, σελ.115 επ.*

[10] *Βλ. Γέρμανος Γ., Γεωργίου Ν., (2021), ό.π.*

[11] *Παπαδόπουλος Μ, (2005), Phishing: Η νέα μέθοδος εξαπάτησης στο Διαδίκτυο, 3ο Πανελλήνιο Συνέδριο Ηλεκτρονικό Έγκλημα 2005, Δικτυοπειρατεία & Τηλεπικοινωνιακή απάτη, Πρόληψη – Αντιμετώπιση – Λύσεις - Εφαρμογές, σελ. 8 επ.*

ηλεκτρονική αλληλογραφία καθώς και χρήση ηλεκτρονικής αλληλογραφίας, όπου έχει τροποποιηθεί η ένδειξη αποστολέα. Τα spoofed μηνύματα ηλεκτρονικού ταχυδρομείου, προκαλούν ως συνήθως τον ανυποψίαστο παραλήπτη να λάβει δράση κατόπιν συγκεκριμένων οδηγιών που παρέχονται με το απατηλό ηλεκτρονικό μήνυμα, όπως με το να παρέχει στοιχεία της πιστωτικής κάρτας, με σκοπό να πληροφορηθούν έτσι σημαντικά τραπεζικά δεδομένα και να αποσπάσουν χρηματικά ποσά.

Παρά τη σταδιακή επιμόρφωση των χρηστών και την αυξημένη αποτελεσματικότητα της τεχνητής νοημοσύνης στο φιλτράρισμα μηνυμάτων ηλεκτρονικών μηνυμάτων, αυτή η μέθοδος διαδικτυακής απάτης δεν εκλείπει έως σήμερα. Το γεγονός αυτός εξηγείται καθώς η αποστολή ενός μηνύματος δεν κοστίζει τίποτα στο δράστη και επιπλέον επειδή, εάν υποθέσουμε ότι η πιθανότητα επιτυχίας ενός απλού μηνύματος ηλεκτρονικού μηνύματος είναι περίπου 0,1 %, αυτό σημαίνει ότι με την αποστολή 10.000 μηνυμάτων, ο δράστης εξασφαλίζει δυνητικά συμμετοχή 10 θυμάτων[12]. Μάλιστα πολλές φορές οι δράστες ενσυνείδητα θα προσθέσουν ορθογραφικά και συντακτικά λάθη στα μηνύματά τους, ώστε να απευθυνθούν πιο εύκολα σε πιο ευάλωτα κοινωνικά στρώματα.

Πέραν των μηνυμάτων ηλεκτρονικής αλληλογραφίας, από το 2000 και μετά εμφανίστηκαν και οι μέθοδοι που χρησιμοποιούν οι δράστες με τους **πλαστούς διαδικτυακούς τόπους**[13]. μπορεί να περιλαμβάνουν εισαγωγή παραπλανητικών υπερσυνδέσμων σε δημοφιλείς διαδικτυακούς τόπους, χρήση παραπλανητικών γραφικών/ διαφημιστικών πινακίδων ώστε να προσελκύσουν πελάτες του αυθεντικού διαδικτυακού τόπου, χρήση αναδυόμενων παραθύρων (pop-us ή frameless windows) για τη μεταμφίεση της πραγματικής προέλευσης του μηνύματος του δράστη καθώς και ενσωμάτωση κακόβουλου λογισμικού κώδικα σε ιστοσελίδα που εκμεταλλεύεται γνωστή αδυναμία των browsers των χρηστών – καταναλωτών.

Ειδικότερα, σε μία επίθεση **brand phishing** δημοφιλούς επωνυμίας μιας

[12] *Βλ. Jougleux, P., (2016), ό.π. σελ. 133*
[13] *Βλ. Παπαδόπουλος Μ,(2005), ό.π., σελ.8*

τράπεζας, ο επιτήδειος θα προσπαθήσει να καταστήσει έναν κακόβουλο ιστότοπο πανομοιότυπο με τον επίσημο ιστότοπο της συγκεκριμένης τράπεζας με την οποία συνεργάζεται το θύμα είτε χρησιμοποιώντας παρόμοιο domain name ή παρόμοια διεύθυνση URL και σχεδιασμό ιστοσελίδας με τον γνήσιο ιστότοπο. Ο σύνδεσμος για ανακατεύθυνση στον εν λόγω ιστότοπο μπορεί να αποσταλεί είτε μέσω μηνύματος ηλεκτρονικού ταχυδρομείου είτε γραπτού μηνύματος στο κινητό του θύματος. Συχνά ο ιστότοπος – κλώνος της αυθεντικής ιστοσελίδας της τράπεζας περιέχει μια φόρμα συμπλήρωσης στοιχείων, η οποία αποσκοπεί στην κλοπή προσωπικών δεδομένων των χρηστών ηλεκτρονικής τραπεζικής όπως διαπιστευτήρια, στοιχεία πληρωμής, κωδικοί πρόσβασης κτλ.

2.3. Ποινική αντιμετώπιση του φαινομένου ηλεκτρονικής τραπεζικής απάτης με τη μέθοδο phishing

Όπως αναπτύχθηκε και ανωτέρω, ο δράστης κατά την επίθεση με μορφή phishing, μιμείται μια αξιόπιστη οντότητα και εν προκειμένω ένα τραπεζικό ίδρυμα, ζητώντας από το θύμα να του αποκαλύψει προσωπικά στοιχεία, όπως στοιχεία ταυτότητας, τραπεζικά δεδομένα, στοιχεία καρτών, επιτυγχάνοντας την περιουσιακή μετάθεση ή/ και κλοπή ταυτότητας του θύματος και την προσβολή του εννόμου αγαθού της περιουσίας του.

Κατά μια άποψη, το φαινόμενο του phishing αντιμετωπίζεται ποινικά με τη διάταξη του άρθ. **386 του ΠΚ,** όπου τυποποιείται η απλή απάτη, σε περίπτωση που το θύμα πειστεί να καταβάλλει κατευθείαν ποσά στον δράστη εξαιτίας της παραπλάνησης του[14]. Για τη στοιχειοθέτηση του εγκλήματος της απάτης απαιτούνται[15]:

- *ο σκοπός του δράστη να περιποιήσει στον εαυτό του ή και σε άλλον (τρίτον) παράνομο περιουσιακό όφελος, χωρίς να είναι αναγκαία η πραγματοποίηση του οφέλους αυτού*

[14] *Βαϊτσούδης , Ι., (2020) Απάτη μέσω υπολογιστή και απάτη με υπολογιστή (Άρθρα 386, 386 Α ΠΚ), Θεσσαλονίκη, σελ. 70 επ.*

[15] *Ερμηνεία του άρθρου 386 ΠΚ., Διαθέσιμο στην τράπεζα νομικών πληροφοριών «Τετράβιβλος»*

- *εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή αθέμιτη απόκρυψη ή παρασιώπηση αληθινών, από την οποία ως παραγωγό αιτία, παραπλανήθηκε κάποιος και προέβη στην επιζήμια για τον ίδιο ή άλλον πράξη, παράλειψη ή ανοχή.*
- *βλάβη ξένης περιουσίας, η οποία να τελεί σε αιτιώδη συνάφεια με τις παραπλανητικές ενέργειες του δράστη.*

Σύμφωνα με έτερη άποψη, η επίθεση phishing διώκεται σύμφωνα με τη διάταξη του άρθ. **386 Α του ΠΚ**, όπου προβλέπεται το αδίκημα της απάτης με υπολογιστή. Κατά την εισηγητική έκθεση του Ν.1805/1988, η απάτη με υπολογιστή θεσπίστηκε για να καλύψει τα κενά του νόμου που υπήρχαν και εμπόδιζαν την εφαρμογή της διάταξης της απάτης, κατά το πρότυπο της παρ. 263 του γερμανικού ΠΚ. Πιο συγκεκριμένα, η πρόθεση του νομοθέτη ήταν να παρέχει προστασία από τις προσβολές του εννόμου αγαθού της περιουσίας, οι οποίες τελούνται με τη χρήση των ΤΠΕ, ως υποκατάστατο της ανθρώπινης δραστηριότητας[16].

Η απάτη με υπολογιστή αποτελεί ένα πολύτροπο ή υπαλλακτικώς μικτό έγκλημα (ΑΠ 1087/2019). Επισημαίνεται ότι αποτελεί ιδιώνυμο έγκλημα σε σχέση με την απάτη καθώς ακολουθεί την πρόβλεψη της διάταξης του άρθ. 386 του ΠΚ, **ωστόσο η διαφορά έγκειται ότι δεν αναφέρεται στην πράξη της εξαπάτησης, αλλά σε μορφές συμπεριφοράς που κατευθύνουν στον «επηρεασμό «των στοιχείων του υπολογιστή που συνεπάγεται τη μη ορθή επεξεργασία δεδομένων**[17].Για την αντικειμενική υπόσταση του εγκλήματος της διάταξης του άρθ. 386 Α του ΠΚ προβλέπονται οι εξής τρόποι τέλεσης:

- *είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή, όπως για παράδειγμα η προσθήκη ή αλλοίωση των λογικών βημάτων ενός προγράμματος αλλά και κάθε μεταβολή του προγράμματος αλλά και διαγραφή ή και εισαγωγή νέων στοιχείων,*

[16] *Ιγγλεζάκης, Ι., (2021) Δίκαιο Πληροφορικής, Δ΄ Έκδοση, Αθήνα – Θεσσαλονίκη, Εκδόσεις Σάκκουλα, σελ. 405 και επ.*
[17] *Μυλωνόπουλος, Χ. (1991), Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο. Συμβολή στην ερμηνεία των άρθρων 13γ, 370 Β, 370 Γ και 386 Α Π.Κ. (άρθρ. 2-5 ν. 1805/88)*

- *είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα*
- *είτε με τη χρησιμοποίηση μη ορθών ή ελλιπών ψηφιακών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας,*
- *είτε με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή, μετάδοση ή εξάλειψη ορθών ψηφιακών δεδομένων υπολογιστή, ιδίως ψηφιακών δεδομένων αναγνώρισης της ταυτότητας και*
- *είτε με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων ή νομισματικής αξίας, η οποία τιμωρείται με φυλάκιση, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή.*

Σημειωτέον ότι σύμφωνα με την αιτιολογική έκθεση του Ν. 4411/2016, τιμωρείται και η χρήση ορθών δεδομένων που γίνεται χωρίς δικαίωμα**,** όπως π.χ. στην περίπτωση που ο δράστης έχει αποκτήσει όνομα/κωδικό χρήστη. Έτσι , η αντικειμενική υπόσταση του άρθ. 386 Α του ΠΚ **πληρούται όταν οποιαδήποτε μεταφορά χρημάτων γίνεται με την υποκλοπή και χρήση ξένων ορθών κωδικών ή με παράνομη διείσδυση δράστη στα πληροφοριακά συστήματα μίας τράπεζας.** Επιπροσθέτως, ειδικά ως προς το στοιχείο της χωρίς δικαιώματος χρήσης ψηφιακών δεδομένων, αυτή νοείται ως τη χωρίς τη συναίνεση του δικαιούχου και χωρίς να συντρέχει άλλος νομιμοποιητικός λόγος, ακόμη κι αν το PIN έχει αποκτηθεί σύννομα αλλά χρησιμοποιείται χωρίς δικαίωμα.

Σύμφωνα με την απόφαση του ΣυμβΠλημΘεσ 828/2022, **άμεσο αποτέλεσμα της ως άνω εγκληματικής συμπεριφοράς του δράστη αποτελεί ο «επηρεασμός» των στοιχείων του υπολογιστή (κατ' αντιστοιχία προς την «πλάνη» της κοινής απάτης) η έναρξη του οποίου συνιστά αρχή εκτέλεσης του εγκλήματος και ο οποίος με τη σειρά του πρέπει να οδηγήσει άμεσα στη βλάβη ξένης περιουσίας, προς όφελος του δράστη ή τρίτου (ΑΠ 1087/2019).** Βλάβη ξένης, κατά το αστικό δίκαιο, περιουσίας, η οποία να τελεί σε αιτιώδη σύνδεσμο με τις ενέργειες του δράστη, υπάρχει και σε περίπτωση μείωσης ή χειροτέρευσης της περιουσίας του παθόντα, έστω και αν αυτός έχει ενεργό αξίωση προς αποκατάστασή της.

Για την **υποκειμενική υπόσταση** του εγκλήματος αρκεί δόλος ως προς όλα τα στοιχεία της αντικειμενικής υπόστασής του, χωρίς να απαιτείται ειδικότερα (όπως στην κοινή απάτη) γνώση του δράστη για την αναλήθεια των στοιχείων που χρησιμοποιεί. Η απάτη με υπολογιστή αποτελεί περαιτέρω έγκλημα σκοπού (υπερχειλούς υποκειμενικής υπόστασης) διότι ο δράστης πρέπει να έχει σκοπό παράνομου περιουσιακού οφέλους για τον εαυτό του ή τρίτον (ΑΠ 1087/2019), χωρίς να είναι αναγκαία η πραγμάτωση του οφέλους αυτού (βλ. για το αδίκημα της απάτης ΟλΑΠ 1/2020, ΑΠ 13/2020, ΑΠ 1354/2011, ΑΠ 546/2009). Περιουσιακό όφελος συνιστά η αύξηση της περιουσίας του ίδιου του δράστη ή άλλου, καθώς και η ευνοϊκότερη διαμόρφωση της περιουσιακής κατάστασης οιουδήποτε από αυτούς (βλ. για το αδίκημα της απάτης ΟλΑΠ 1/2020, ΑΠ 13/2020).

Σε μια πιο σύνθετη μορφή επίθεσης phishing κατά την οποία ο δράστης έχει αποστείλει μήνυμα ηλεκτρονικού ταχυδρομείου προς το ανυποψίαστο θύμα, στο οποίο εμφανίζεται δήθεν ως αποστολέας η τράπεζα και εμφανίζεται το αυθεντικό λογότυπο του τραπεζικού ιδρύματος, είναι πιθανόν να αναφέρεται στο επίμαχο μήνυμα ότι υφίσταται κάποιο τεχνικό πρόβλημα, όπως παραδείγματος χάριν ότι έχει κλειδωθεί η κάρτα και να ζητείται από το θύμα να προβεί άμεσα στην επίλυση του εν λόγω ζητήματος «κάνοντας κλικ» σε έναν σύνδεσμο[18]. Αφού το θύμα πείθεται και επιλέγει τον υπερσύνδεσμο, ανακατευθύνεται σε μια ιστοσελίδα κλώνο της αυθεντικής της τράπεζας και εν συνεχεία πιστεύοντας ότι πλοηγείται στο web banking της τράπεζας του, εισάγει τα προσωπικά του στοιχεία όπως το όνομα χρήστη και τον κωδικό πρόσβασης προκειμένου να συνδεθεί στον τραπεζικό του λογαριασμό. Εισάγοντας αυτά τα στοιχεία, τα εν λόγω δεδομένα περιέρχονται στην κατοχή του δράστη και εν συνεχεία αυτός τα χρησιμοποιεί στην αυθεντική σελίδα e- banking της τράπεζας με σκοπό να πραγματοποιήσει αυθαίρετες μεταφορές εμβασμάτων και να αποκτήσει περιουσιακό όφελος. Μάλιστα σε περίπτωση που ζητείται κωδικός μιας χρήσης για την επιβεβαίωση της επίμαχης συναλλαγής, είναι πιθανό η πλαστή ιστοσελίδα που έχει κατασκευαστεί από το δράστη, να απαιτεί και αυτό

[18] *Βλ. Βαϊτσούδης , Ι., (2020), ό.π. σελ. 72*

το στοιχείο από το θύμα. Πληρούται δηλαδή η αντικειμενική υπόσταση του εγκλήματος της απάτης με υπολογιστή του άρθ. 386 Α του ΠΚ, παρ. 1., εδ. ε' «*με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων*». Στην περίπτωση που ο phisher χρησιμοποιεί τεχνικές ανακατεύθυνσης στην πλαστή ιστοσελίδα με τροποποίηση του τοπικού διακομιστή DNS, τότε είναι πιθανόν το phishing να συνδυάζεται με το pharmimg. **Η μέθοδος pharming[19] συνίσταται στην εγκατάσταση κακόβουλου κώδικα σε διακομιστή DNS, ο οποίος ανακατευθύνει το πρόγραμμα περιήγησης του θύματος σε ψεύτικες ιστοσελίδες χωρίς τη συναίνεσή του**. Στη μέθοδο αυτή επειδή η επίθεση με τη μορφή pharming, προκαλεί τη μόλυνση της κρυφής μνήμης του διακομιστή, πληρούται η αντικειμενική υπόσταση της διάταξης του άρθ. 370 Β του ΠΚ, ήτοι της παράνομης πρόσβασης σε σύστημα πληροφοριών.

Στη διάταξη της απλής απάτης του 386 ΠΚ, η περιουσιακή βλάβη είναι αποτέλεσμα της πρόκλησης πλάνης σε φυσικό πρόσωπο «πείθοντας κάποιον», ενώ στη διάταξη του 386 Α ΠΚ η απάτη εμφανίζεται ως αποτέλεσμα της επέμβασης στα δεδομένα του υπολογιστή[20]. Όπως επισημαίνει η Βασιλάκη[21], σε μια επίθεση phishing, πληρούται η αντικειμενική υπόσταση της κοινής απάτης του άρθ. 386 του ΠΚ καθώς ο δράστης έχει γνώση και θέληση σχετικά με την παράνομη δραστηριότητά του, αλλά και σκοπό να αποκομίσει ο ίδιος παράνομο περιουσιακό όφελος από αυτήν και στην πραγματικότητα ουδέποτε μετανιώνει και χρησιμοποιεί τα προσωπικά τραπεζικά δεδομένα που έχει προηγουμένως υποκλέψει, αφού τα έχει λάβει από το θύμα με σκοπό να προβεί στην περιουσιακή μετάθεση και έτσι σε κάθε περίπτωση ο κίνδυνος της περιουσιακής βλάβης είναι αντικειμενικός και όχι υποκειμενικός. Υποστηρίζεται εντούτοις και η αντίθετη άποψη ότι η μέθοδος phishing δεν μπορεί να υπαχθεί στην κοινή απάτη και συγκεκριμένα ως **προς το στοιχείο της αμεσότητας**, που είναι

---

[19] Saloni, M., Swapnesh T, Dilbag S., (2019) ,Detection of pharming Attack on Websites using SVM Classifier, International Journal of Scientific & Technology Research,Volume 1, Issue 1

[20] Παπαδαμάκης, Α., (2020) Τα περιουσιακά εγκλήματα, Αθήνα – Θεσσαλονίκη, Εκδόσεις Σάκκουλα, , σελ. 153

[21] Βασιλάκη Ε., Τα φαινόμενα «Phishing», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ ΝΖ/2007, σελ. 860-863

απαραίτητο στοιχείο για τη θεμελίωση της κοινής απάτης ως έγκλημα αυτοβλάβης, καθώς: α) η κοινοποίηση των προσωπικών στοιχείων μπορεί να μην οδηγήσει στην περιουσιακή βλάβη εάν ο δράστης εν τέλει δεν τα χρησιμοποιήσει, β) η χρήση των στοιχείων που έχει υποκλέψει ο δράστης συνιστά μια αυτόνομη ενέργεια και η αποδοχή της αποδοχής των αποστολής των τραπεζικών στοιχείων από το ίδιο ως περιουσιακή διάθεση θα μπορούσε να αποτελεί μια διεύρυνση του αξιοποίνου και γ) ένα η πλάνη του θύματος ληφθεί ως άμεση περιουσιακή διάθεση, ενδέχεται το έγκλημα της απάτης να μεταβληθεί από έγκλημα αποτελέσματος σε έγκλημα διακινδύνευσης.[22]

Τέλος, αναφορικά με τις διαδικτυακές απάτες, υπάρχει πρόβλεψη στο **άρθ. 7 της Σύμβασης της Βουδαπέστης** για το έγκλημα στον κυβερνοχώρο για το αδίκημα της πλαστογραφίας σχετιζόμενης με ηλεκτρονικό υπολογιστή και στο άρθρ. 8 αντίστοιχα για το αδίκημα της απάτης σχετικής με υπολογιστή .Από την αιτιολογική σκέψη του εν λόγω άρθρου προκύπτει η βούληση του νομοθέτη να συμπεριλάβει στις περιπτώσεις επέμβασης στη λειτουργία ενός συστήματος υπολογιστή, με την εισαγωγή ανακριβών δεδομένων ή με την επέμβαση στη λειτουργία ενός προγράμματος ή με άλλες παρεμβάσεις, με σκοπό την επίτευξη παράνομης περιουσιακής βλάβης και σε περιουσιακά αγαθά που τηρούνται ηλεκτρονικά, μέσω ηλεκτρονικής τραπεζικής[23].

2.4. Νομικό πλαίσιο θεμελίωσης ευθύνης της Τράπεζας από απάτες phishing

2.4.1. Ενδοσυμβατική ευθύνη

Κατόπιν της τέλεσης της εξαπάτησης του θύματος με τη μέθοδο phishing, το θύμα αφού συνδεθεί στον ηλεκτρονικό λογαριασμό του και συνειδητοποιήσει ότι τα χρήματα του έχουν χαθεί, επικοινωνεί με την Τράπεζα η οποία συχνά αποποιείται των ευθυνών της. Τίθεται επί τάπητος λοιπόν εάν ορθώς απεκδύεται των ευθυνών της η τράπεζα ή εάν έχει και ο πελάτης ευθύνη για την παραβίαση του ηλεκτρονικού του λογαριασμού, εφόσον ο ίδιος έχει προηγουμένως προβεί σε αποκάλυψη των προσωπικών του δεδομένων, όπως του

[22] *Βλ. Βαϊτσούδης , Ι., (2020), ό.π. σελ. 73*
[23] *Βλ. Ιγγλεζάκης. Ι.,ό.π., σελ. 406*

username και του password.

Αρχικά, η κατάθεση χρημάτων σε Τράπεζα φέρει το χαρακτήρα ανώμαλης παρακαταθήκης. Σύμφωνα με **το άρθ. 830 παρ. 1 του ΑΚ,** εφαρμόζονται αφενός η περί δανείου διάταξη του άρθ. 806 του ΑΚ, κατά την οποία η τράπεζα αποκτά την κυριότητα κατατιθεμένων χρημάτων, αφετέρου δε η διάταξη του άρθ. 827 του ΑΚ, που ορίζει ότι ο θεματοφύλακας, αν ο παρακαταθέτης απαιτεί το πράγμα, οφείλει να το αποδώσει, και αν ακόμη δεν έχει περάσει η προθεσμία που ορίστηκε για τη φύλαξη του. Επομένως, αν ο τρίτος μετήλθε αξιόποινη πράξη και συνεπεία αυτής πέτυχε την απόδοση σ' αυτόν του ποσού της κατάθεσης, η αδικοπραξία τελείται εις βάρος της τράπεζας, η οποία είναι κυρία των χρημάτων και της οποίας η περιουσία βλάπτεται από την παράνομη και υπαίτια συμπεριφορά του τρίτου, ενώ η εναντίον της ενοχική αξίωση του καταθέτη από τη σύμβαση της ανώμαλης παρακαταθήκης παραμένει άθικτη **(***ΑΠ 830/ 2003 Δ 45. 176, ΑΠ 1083/1991*), εφόσον δεν συντρέχει περίπτωση απαλλαγής της, κατά το άρθρο 3 του Ν.Δ.. 17.7/13.8. 1923 «περί ειδικών διατάξεων επί ανωνύμων εταιριών».

Επιπροσθέτως, σύμφωνα με το άρθ. 824 του ΑΚ, η τράπεζα ως θεματοφύλακας δεν έχει το δικαίωμα να μεταχειρίζεται το πράγμα, δηλαδή τα χρήματα χωρίς την άδεια του παρακαταθέτη, εν προκειμένω δηλαδή του πελάτη. Επιπροσθέτως, η τράπεζα δεν έχει το δικαίωμα να καταθέσει το πράγμα σε τρίτον, εκτός αν εξουσιοδοτήθηκε γι' αυτό από τον παρακαταθέτη, ή αν εξαναγκάστηκε από τις περιστάσεις, ή αν συνηθίζεται η περαιτέρω κατάθεση. Βάσει του άρθ. 825 του ΑΚ, η τράπεζα η οποία ως θεματοφύλακας προέβη σε κατάθεση χρημάτων **χωρίς δικαίωμα, δηλαδή χωρίς τη συναίνεση,** σύμφωνα με το άρθ. 236 του ΑΚ ή χωρίς την έγκριση, σύμφωνα με το άρθ. 238 του ΑΚ, φέρει ευθύνη για κάθε πταίσμα έναντι του πελάτη της και θεωρείται ότι έχει παραβιάσει και τις διατάξεις του άρθ. 713 επ. του ΑΚ περί εντολής.

Η σύμβαση παροχής υπηρεσιών ηλεκτρονικής τραπεζικής ανάμεσα στον πελάτη και στην τράπεζα, αποτελεί μικτή σύμβαση καθώς εμφανίζει στοιχεία τόσο εντολής όσο και σύμβασης έργου, κατά τις προβλέψεις του **άρθ. 681 επ. του ΑΚ**, διότι η τράπεζα φέρει την υποχρέωση να φυλάει τα χρήματα του πελάτη της και να εκτελεί εντολές που δίνονται από τον πελάτη για μεταφορές εμβασμάτων, κατόπιν

συμφωνημένης αμοιβής είτε με τη μορφή συνδρομής είτε/ και με την προμήθεια κατά την εκτέλεση της μεταφοράς χρημάτων. Κατά την εκτέλεση της εν λόγω σύμβασης, η τράπεζα έχει την υποχρέωση να ενεργεί σύμφωνα με την καλή πίστη και τα συναλλακτικά ήθη, κατά τις διατάξεις των άρθ. 200 και 288 του ΑΚ.

Σε περιπτώσεις που ο χρήστης ηλεκτρονικής τραπεζικής έχει πέσει θύμα ηλεκτρονικής απάτης με τη μορφή phishing, είναι σημαντικό να εξεταστεί ιδιαιτέρως το ενδεχόμενο της αυθαίρετης μεταφοράς των χρημάτων σε άγνωστο δικαιούχο **χωρίς την εντολή και τη συναίνεση του πελάτη,** λόγω πλημμελούς εκτέλεσης της παροχής υπηρεσιών από την τράπεζα και της βαριάς αμέλειας που επέδειξε ως προς την ασφάλεια των συναλλαγών.

Πρώτα από όλα, είναι σημαντικό να τηρούνται τα προβλεπόμενα μέτρα από την τράπεζα αναφορικά με την **ταυτοποίηση** και δη την **ισχυρή ταυτοποίηση** του δράστη καθώς και να διασφαλίζεται ότι έχει δοθεί η **συγκατάθεση** του χρήστη για την εκτέλεση της συναλλαγής που διενεργείται μέσω ηλεκτρονικής τραπεζικής, ώστε να θεωρείται εγκεκριμένη από τον πραγματικό δικαιούχο του τραπεζικού λογαριασμού που τηρείται στο σύστημα ηλεκτρονικής τραπεζικής.

Στο άρθρο **4 του Ν. 4537/2018** σε αντιστοιχία με τις προβλέψεις του άρθ. 4 της Οδ. 2015/2366 και συγκεκριμένα στην **περ.29** δίνεται ο ορισμός της ταυτοποίησης, η οποία νοείται ως: «*η διαδικασία που επιτρέπει στον πάροχο υπηρεσιών πληρωμών να επαληθεύει την ταυτότητα χρήστη υπηρεσιών πληρωμών ή την εγκυρότητα χρήσης συγκεκριμένου μέσου πληρωμών, συμπεριλαμβανομένης της χρήσης των εξατομικευμένων διαπιστευτηρίων ασφάλειας του χρήστη*». Περαιτέρω, στην **περ. 30 δίνεται ο ορισμός για την ισχυρή ταυτοποίηση πελάτη, η οποία νοείται ως:** «*η ταυτοποίηση με βάση τη χρήση δύο ή περισσότερων στοιχείων που αφορούν* ***γνώση*** *(στοιχείο το οποίο μόνο ο χρήστης υπηρεσίας πληρωμών γνωρίζει),* ***κατοχή*** *(στοιχείο το οποίο μόνο ο χρήστης κατέχει) και κάποιο* ***μοναδικό εγγενές χαρακτηριστικό του*** *(στοιχείο το οποίο ο χρήστης είναι), στοιχεία τα οποία είναι ανεξάρτητα μεταξύ τους, ως προς το ότι η παραβίαση του ενός δεν θέτει σε κίνδυνο την αξιοπιστία των υπολοίπων και η διαδικασία της οποίας είναι σχεδιασμένη κατά τρόπο που να προστατεύεται η εμπιστευτικότητα των δεδομένων ταυτοποίησης*».

Συνεπώς, η έννοια της «**αυστηρής ταυτοποίησης του πελάτη**» σημαίνει

ότι η ταυτοποίηση του πελάτη γίνεται με βάση τη χρήση δύο ή περισσότερων στοιχείων που αφορούν **γνώση,** όπως για παράδειγμα το PIN ή ο κωδικός ασφαλείας, **κατοχή,** όπως για παράδειγμα μια πιστωτική ή χρεωστική κάρτα και κάποιο μοναδικό εγγενές χαρακτηριστικό του, όπως για παράδειγμα ένα βιομετρικό στοιχείο, όπως το δακτυλικό αποτύπωμα ή αναγνώριση φωνής του κατόχου[24].

Εξαιρέσεις από την υποχρέωση για της αυστηρή εξακρίβωση της ταυτότητας του πελάτη από τους παρόχους υπηρεσιών πληρωμών, προβλέπονται **στο άρθ. 18 του Κανονισμού 389/2018,** σε περίπτωση που ο πληρωτής διενεργεί ηλεκτρονικά την έναρξη πράξης πληρωμής εξ αποστάσεως η οποία κρίνεται ως έχουσα κίνδυνο χαμηλού επιπέδου, σύμφωνα με τους μηχανισμούς παρακολούθησης συναλλαγών, οι οποίοι προβλέπονται στο άρθ. 2 και παρ.2 και στοιχ. γ' του εν λόγω άρθρου.

Επιπροσθέτως, ως προς το κρίσιμο στοιχείο για το εάν μια συναλλαγή θεωρείται **εγκεκριμένη**: Κατά **το αρθ. 64 του Ν. 4537/2018:** *«1. Μια πράξη πληρωμής θεωρείται ως **εγκεκριμένη**, μόνον εφόσον ο πληρωτής έχει δώσει τη **συγκατάθεσή** του στην εκτέλεσή της. Μια πράξη πληρωμής μπορεί να εγκρίνεται από τον πληρωτή είτε πριν, είτε εφόσον υπάρχει συμφωνία του πληρωτή με τον οικείο πάροχο υπηρεσιών πληρωμών μετά την εκτέλεσή της. 2. Η συγκατάθεση για την εκτέλεση μιας πράξης πληρωμής ή σειράς πράξεων πληρωμής παρέχεται με τον τύπο που έχει συμφωνηθεί μεταξύ του πληρωτή και του οικείου παρόχου υπηρεσιών πληρωμών. Η συγκατάθεση για την εκτέλεση μιας πράξης πληρωμής μπορεί, επίσης, να παρέχεται μέσω του δικαιούχου ή του παρόχου υπηρεσίας εκκίνησης πληρωμής**. **Αν δεν έχει παρασχεθεί συγκατάθεση, η πράξη πληρωμής θεωρείται ως μη εγκεκριμένη».***

Έτσι, μια πράξη πληρωμής θεωρείται **γνήσια κ**αι κατ' επέκταση εγκεκριμένη μόνο εφόσον ο πληρωτής έχει δώσει τη συγκατάθεσή του για την εκτέλεσή της. Στο άρθ. **72 του Ν**. **του Ν.4537/2018,** προβλέπονται τα στοιχεία που τεκμηριώνουν **τη γνησιότητα και την εκτέλεση των πράξεων πληρωμής.** Με

[24] *Μήτσου,Α.-Ο.,2021, Η προστασία του πληρωτή από την απατηλή χρήση των μέσων πληρωμής στθς συναλλαγές του ηλεκτρονικού εμπορίου, ΤΝΠ Qualex, ΔΕΕ, σελ. 606-619*

τον όρο «γνησιότητα της πράξης πληρωμής» νοείται η πράξη που ενεργήθηκε με την πραγματική συναίνεση του χρήστη υπηρεσιών πληρωμής, δηλαδή είτε από τον ίδιο, είτε εν γνώσει του από τρίτο πρόσωπο, στο οποίο είχε παράσχει σχετική άδεια. Δεν υφίσταται γνήσια συναλλαγή, όταν ο χρήστης αγνοεί αυτήν και ενεργήθηκε αθέμιτα από τρίτο πρόσωπο χωρίς δικαίωμα, ακόμη και αν η συγκατάθεσή του φέρεται να δόθηκε με τη μορφή που συμφωνήθηκε μεταξύ των μερών. Σε περίπτωση λοιπόν, μη εγκεκριμένης πράξης πληρωμής κατά τα προαναφερόμενα και έγκαιρη χωρίς υπαίτια καθυστέρηση του τραπεζικού ιδρύματος, ο χρήστης υπηρεσιών ηλεκτρονικής τραπεζικής μπορεί να αξιώσει αποζημίωση από τον πάροχο πληρωμών , βάσει του άρθ. 71 του Ν. 4537/2018.

Σχετικά με τις προαναφερόμενες διατάξεις, αξιοσημείωτη είναι η απόφαση του **ΕιρΜυτ24/2023**[25]**,** που έκρινε το ζήτημα της υποχρέωσης της τράπεζας προς αποζημίωση σε περίπτωση θύματος ηλεκτρονικής τραπεζικής απάτης. Εν προκειμένω, το Ειρηνοδικείο Μυτιλήνης έκρινε ότι στην υπό κρίση περίπτωση δεν είχε αποδειχθεί η γνησιότητα της επίδικης συναλλαγής, καθώς ουδείς από τους δικαιούχους του επίδικου τραπεζικού λογαριασμού δεν είχε δώσει τη συγκατάθεσή του για την έγκριση της εκτέλεσης της πράξης πληρωμής. Εξάλλου, ό ένας εκ των δικαιούχων (σύζυγος της ενάγουσας) δεν έλαβε κωδικό μιας χρήσης OTP ούτε μέσω γραπτού μηνύματος στο κινητό τηλέφωνο ούτε μέσω της εφαρμογής Viber, προκειμένου να τον πληκτρολογήσει και να εγκρίνει την επίμαχη συναλλαγή. Έτσι, το δικαστήριο απέρριψε τους ισχυρισμούς της εναγόμενης τράπεζας περί αποποίησης της ευθύνης της σύμφωνα με το πλαίσιο συνεργασίας και γενικών όρων διενέργειας τραπεζικών συναλλαγών που επικαλέστηκε και την υποχρέωσε στην καταβολή αποζημίωσης στο θύμα της ηλεκτρονικής τραπεζικής απάτης.

---

[25] *Απόφαση ΕιρΜυτ 24/2023, Sakkoulas-online, Διαθέσιμο στο:* ***https://www.sakkoulas-online.gr/reader/d27b6c02fa3398d81c33/?utm_source=%CE%95%CE%BA%CE%B4%CF%8C%CF%83%CE%B5%CE%B9%CF%82+%CE%A3%CE%AC%CE%BA%CE%BA%CE%BF%CF%85%CE%BB%CE%B1+%CE%91%CE%95&utm_campaign=a19b562d52-e-info-18.7.2023&utm_medium=email&utm_term=0_7bee924d9b-a19b562d52-146922345&ct=t(e-info-18.7.2023)&mc_cid=a19b562d52&mc_eid=5bd0876ef5***

2.4.2. Αδικοπρακτική ευθύνη

Αναφορικά με τη θεμελίωση ευθύνης της τράπεζας από αδικοπραξία, λεκτέα τα ακόλουθα: Στη διάταξη του άρθρου **914 του ΑΚ**, προβλέπεται ότι «***όποιος ζημιώσει άλλον παράνομα και υπαίτια έχει υποχρέωση να τον αποζημιώσει***». Εκ τούτου, συνάγεται ότι απαιτείται για τη στοιχειοθέτηση της αδικοπρακτικής ευθύνης και της εξ αυτής υποχρέωσης του δράστη σε αποζημίωση του παθόντος να συντρέχουν οι εξής προϋποθέσεις: α) η ζημία αυτή να προξενηθεί από το δράστη παρανόμως, συγχρόνως δε και υπαιτίως, δηλαδή από δόλο ή αμέλεια (ΑΚ 330 εδ. β'), β) η παράνομη συμπεριφορά του υπαιτίου να οφείλεται σε πράξη ή παράλειψή του και τέλος, γ) να υφίσταται πρόσφορη αιτιώδης συνάφεια μεταξύ της ζημιογόνου πράξεως ή παραλείψεως και της επελθούσης ζημίας *(ΑΠ 263/1996 ΕλλΔνη 37.1453, ΑΠ 574/1994 Ελλ.Δνη 36.828).* Παρανομία συνιστά και η παράβαση της γενικής υποχρεώσεως πρόνοιας και ασφάλειας στο πλαίσιο της συναλλακτικής και γενικότερα της κοινωνικής δραστηριότητας των ατόμων, δηλαδή η παράβαση της κοινωνικά επιβεβλημένης, απορρέουσας από τις διατάξεις των άρθρων **281 και 288** Α.Κ. και εκ της θεμελιώδους δικαιϊκής αρχής της συνεπούς συμπεριφοράς υποχρεώσεως λήψεως ορισμένων μέτρων επιμέλειας για την αποφυγή προκλήσεως ζημίας σε έννομα αγαθά τρίτων προσώπων.

Στην περίπτωση των τραπεζικών ιδρυμάτων στο πλαίσιο της σχέσης εμπιστοσύνης με τους πελάτες τους, έχουν την υποχρέωση να διαθέτουν σωστή εσωτερική οργάνωση και να μεριμνούν για την προστασία των συμφερόντων των πελατών τους. Ειδικότερες εκφάνσεις της **πρόνοιας και της ασφάλειας** στο πλαίσιο της συναλλακτικής σχέσεως με τους πελάτες αποτελούν οι **υποχρεώσεις διαφώτισης, ενημέρωσης και τήρησης των κανόνων ασφαλείας** για τη θωράκιση του εννόμου αγαθού της περιουσίας καθώς και των προσωπικών δεδομένων των χρηστών ηλεκτρονικής τραπεζικής. Η λήψη των απαραίτητων μέτρων τεχνικής φύσης, εκ μέρους των προμηθευτών από απόσταση τραπεζικών υπηρεσιών, ώστε να εξαλείψουν η έστω να περιορίσουν τον κίνδυνο παράνομων και παραπλανητικών ενεργειών απόσπασης προσωπικών στοιχείων και κωδικών των πελατών, μπορούν να περιλαμβάνουν

τη διπλή ταυτοποίηση, την αποστολή κωδικού διέλευσης μιας χρήσης μέσω κινητού τηλεφώνου για την ολοκλήρωση μιας συναλλαγής[26]. Η παράλειψη μάλιστα εκπλήρωσης των προαναφερόμενων υποχρεώσεων της τράπεζας, ώστε να μην είναι σε θέση να διαφυλάσσει με ασφάλεια τα κεφάλαια των πελατών της, θεμελιώνει την αδικοπρακτική της ευθύνη.

Προμετωπίδα στη θωράκιση των συμφερόντων των πελατών θεωρείται η **υποχρέωση πληροφόρησης** ή άλλως **ενημέρωση**, η οποία καθιερώνεται σε όλα τα στάδια της συναλλακτικής επαφής της τράπεζας με τον πελάτη. Ιδιαίτερα, στις περιπτώσεις διενέργειας αυθαίρετων συναλλαγών, είναι ιδιαίτερο σημαντικό εάν τηρήθηκε προηγουμένως η υποχρέωση της τράπεζας για έλεγχο ύποπτης συναλλαγής, η οποία δεν συνάδει με το συναλλακτικό προφίλ του πελάη της καθώς και τηλεφωνική επιβεβαίωση συναλλαγής/έγκαιρη ενημέρωση του πελάτη για ενδεχόμενη αυθαίρετη μεταφορά χρημάτων η οποία, απορρέει σύμφωνα με τις υποχρεώσεις ενημέρωσης των συναλλασσομένων και διαφάνειας των συναλλαγών του **Κώδικα Τραπεζικής Δεοντολογίας** αλλά και από τις προβλέψεις του **Ν. 4457/2018**. Παράλληλα, το τραπεζικό ίδρυμα έχει την υποχρέωση να αξιολογεί και να συλλέγει πληροφορίες για το **αντικείμενο** και το **σκοπό** της υποτιθέμενης συναλλακτικής σχέσης, με την οποία σχετίζεται μια ύποπτη συναλλαγή.

Η Τράπεζα της Ελλάδος έχει καθορίσει με την ΠΕΕ 190/2/16.06.2021[27], απαιτήσεις και υποχρεώσεις των πιστωτικών ιδρυμάτων αναφορικά με τη διαχείριση κινδύνων ΤΠΕ και ασφαλείας και ειδικότερα στο κεφάλαιο VIII, όπου γίνεται αναφορά στη διαχείριση των σχέσεων με τους χρήστες υπηρεσιών πληρωμών. Αξιοσημείωτη είναι η υποχρέωση των ιδρυμάτων να εφαρμόζουν διαδικασίες για την πρόληψη εμφάνισης ζητημάτων ασφαλείας στα συστήματα ασφαλείας τους, να εντοπίζουν ευπάθειες και να τις αποκαθιστούν. Δηλαδή, σε περίπτωση που όπως προαναφέρθηκε υφίσταται ιστοσελίδα πανομοιότυπη με

---

[26] *Τζίβα, Ε., 2021, Εφαρμογές της ψηφιακής τεχνολογίας στις τραπεζικές συναλλαγές, ΤΝΠ Qualex, ΔΕΕ, σελ. 316-325*

[27] *ΠΕΕ, Αριθμ. απόφ. 190/2/16.06.2021, «Υιοθέτηση των κατευθυντήριων γραμμών της Ευρωπαϊκής Αρχής Τραπεζών (EBA/GL/2019/04) σχετικά με τη διαχείριση κινδύνων Τεχνολογίας Πληροφορικής και & Επικοινωνιών (ΤΠΕ) και Ασφαλείας»*

την αυθεντική ιστοσελίδα της τράπεζας, η τράπεζα θα πρέπει να μεριμνήσει να ενημερώσει τους πελάτες της και να τους προφυλάξει από τυχόν κακόβουλες ενέργειες λαμβάνοντας μέτρα υψηλού επιπέδου για την προστασία των συστημάτων της.

Επιπροσθέτως από το **άρθ. 13 του Ν. 4557/2018**, τα πιστωτικά ιδρύματα οφείλουν να εφαρμόζουν καθορισμένα **μέτρα συνήθους δέουσας επιμέλειας** ως προς τους πελάτες τους, προς τον σκοπό πρόληψης και καταστολής της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, με την επαλήθευση των στοιχείων ταυτότητας του πελάτη και του πραγματικού δικαιούχου πριν από τη σύναψη επιχειρηματικής σχέσης ή επαγγελματικής συναλλαγής. Η παράλειψη εφαρμογής των προβλεπόμενων αυτών μέτρων εκ μέρους της τραπεζικής εταιρείας αποτελεί παράνομη πράξη, η οποία αντιτίθεται προς την **Οδ. 849/2015, τον Ν. 4557/2018** και τον Κώδικα Τραπεζικής Δεοντολογίας.

Αξιοσημείωτη είναι η απόφαση του ΕιρΘεσ 232/2023[28] με την οποία κρίθηκε ότι η εναγόμενη τράπεζα έφερε ευθύνη για την πλημμελή θωράκιση των συστημάτων ασφαλείας τη απέναντι στις διαρκώς εξελισσόμενες μεθόδους εξαπάτησης με απότοκο την περιουσιακή ζημία του πελάτη που την εμπιστεύτηκε και κλήθηκε να καταβάλλει το ποσό των 2.500,00 Ευρώ ως αποζημίωση. Στην προκειμένη περίπτωση, το δικαστήριο έκρινε ότι συντρέχει και η προσωπική ευθύνη του ενάγοντα ο οποίος δε διαφύλαξε ως όφειλε τα προσωπικά τραπεζικά του στοιχεία και τα γνωστοποίησε στο δράστη.

Στο σημείο αυτό λοιπόν κρίνεται σκόπιμη και η εξέταση της προστασίας του χρήστη της ηλεκτρονικής τραπεζικής από τις πρακτικές εξαπάτησης phishing, η οποία ακολουθεί κατωτέρω.

---

[28] *Lawspot.gr, (2023), Διαδικτυακές απάτες, τήρηση μέτρων ασφαλείας και ευθύνη τράπεζας (ΕιρΘεσ 232/2023), Διαθέσιμο στο: https://www.lawspot.gr/nomika-nea/diadiktyakes-apates-tirisi-metron-asfaleias-kai-eythyni-trapezas-eirthes-232-2023*

2.5. Νομικό πλαίσιο ευθύνης πληρωτή από μη εγκεκριμένες πράξεις πληρωμής

Σύμφωνα με το προηγούμενο νομοθετικό καθεστώς του **άρθ. 74 του Ν.4537/2018**, ο πληρωτής έφερε ευθύνη για όλες τις ζημίες που προέρχονταν από πρακτικές εξαπάτησης phishing, εάν αυτές οφείλονταν σε δόλο ή βαριά αμέλειά του. Στην εθνική νομοθεσία εισήχθησαν με τον **Ν. 5019/2023** νέοι κανόνες με αρχή ισχύος από 1η Σεπτεμβρίου του έτους που διανύουμε (2023) και σε εναρμόνιση με την Οδηγία 2020/1828. Οι νέοι κανόνες θέτουν ως στόχο την προστασία του καταναλωτή από τις πρακτικές εξαπάτησης με μορφή **phishing**, οι οποίες λαμβάνουν χώρα είτε μέσω πλαστών ιστοσελίδων είτε ηλεκτρονικών μηνυμάτων είτε μέσω ειδοποιήσεων, εκ των οποίων οι δράστες αποσκοπούν να λάβουν γνώση και να υφαρπάξουν προσωπικούς κωδικούς (PIN, TAN) των χρηστών της ηλεκτρονικής τραπεζικής και εν συνεχεία να προβούν σε αυθαίρετες μεταφορές χρημάτων[29].

Αξιοσημείωτη είναι η πρόβλεψη **του άρθ. 22 του Ν. 5019/2023,** αναφορικά με τον περιορισμό της ευθύνης του πληρωτή για μη εγκεκριμένες πράξεις πληρωμής, και την τροποποίηση της σχετική παρ. 1 του αρ. 74 του Ν. 4537/2018. Σύμφωνα με την εν λόγω νομοθετική ρύθμιση, κατά παρέκκλιση από το άρθρο 73, στο οποίο θεμελιώνεται η ευθύνη του παρόχου υπηρεσιών πληρωμών για μη εγκεκριμένες πράξεις πληρωμής**: «*Ο πληρωτής ευθύνεται μέχρι του ανώτατου ποσού των πενήντα (50) ευρώ για τις ζημίες από τη διενέργεια μη εγκεκριμένων πράξεων πληρωμής,* *οι οποίες προκύπτουν είτε από τη χρήση απολεσθέντος ή κλαπέντος μέσου πληρωμών είτε από υπεξαίρεσή του*». Περαιτέρω:

- *Ο πληρωτής δεν ευθύνεται για ζημίες από phishing, εφόσον η απώλεια, κλοπή ή υπεξαίρεση του μέσου πληρωμών δεν ήταν δυνατό να εντοπιστεί από τον πληρωτή πριν από τη διενέργεια πράξης πληρωμής ή η ζημία προκλήθηκε από πράξεις ή παραλείψεις ιδίως υπαλλήλου ή* υποκαταστήματος ενός παρόχου υπηρεσιών πληρωμών (π.χ. πιστωτικού ιδρύματος)

[29] *Lawspot.gr, 2023, Δημοσιεύτηκε ο Νόμος για τις αντιπροσωπευτικές αγωγές και την προστασία των καταναλωτών (Ν. 5019/2023), Διαθέσιμο στο: https://www.lawspot.gr/nomika-nea/dimosieythike-o-nomos-gia-tis-antiprosopeytikes-agoges-kai-tin-prostasia-ton-katanaloton*

- *Ο πληρωτής που είναι καταναλωτής, ευθύνεται μέχρι του ποσού των 1.000,00 Ευρώ, εφόσον οι ζημίες οφείλονται σε βαριά αμέλεια.*

Ειδικότερα, για την περίπτωση όπου αντισυμβαλλόμενος του τραπεζικού ιδρύματος είναι **καταναλωτής**, εφαρμογή βρίσκουν και οι διατάξεις του **άρθρου 8 του Ν. 2251/1994 περί προστασίας του καταναλωτή**, κατά τις οποίες:*«1.Ο παρέχων υπηρεσίες ευθύνεται για κάθε περιουσιακή ζημία ή ηθική βλάβη που προκάλεσε παράνομα και υπαίτια, με πράξη ή παράλειψή του, κατά την παροχή αυτών στον καταναλωτή*, συνάγεται ότι η Τράπεζα, ως προμηθευτής, ευθύνεται για κάθε περιουσιακή ζημία ή ηθική βλάβη που προκάλεσε παράνομα και υπαίτια με πράξη ή παράλειψή της κατά την παροχή των υπηρεσιών της στον καταναλωτή.

- *Ο πληρωτής* ***ευθύνεται για όλες τις ζημίες, εάν ο πάροχος υπηρεσιών εφαρμόζει υπέρτερα από τα απαιτούμενα για την ισχυρή ταυτοποίηση των συναλλαγών μέτρα,*** *όπως ιδίως μηχανισμούς που αξιοποιούν τεχνολογίες της τεχνητής νοημοσύνης ή επιπλέον κωδικό ή βιομετρική ταυτοποίηση ή τηλεφωνική επιβεβαίωση σε συναλλαγές που ενδέχεται να προκαλέσουν ζημία άνω των 1.000, 00 Ευρώ*
- *Ο πληρωτής* ***ευθύνεται για όλες τις ζημίες, εφόσον προκλήθηκαν από δόλο του***
- *Ο πληρωτής ευθύνεται* ***για όλες τις ζημίες, εφόσον αυτός αθέτησε από δόλο τις υποχρεώσεις του, όπως η άμεση ενημέρωση του πιστωτικού ιδρύματος***

Ως προς τις νέες ρυθμίσεις, θα πρέπει θα επισημανθεί ότι η ρύθμιση περί ευθύνης του πληρωτή για όλες τις ζημίες, σε περίπτωση που το τραπεζικό ίδρυμα αποδείξει ότι διαθέτει και εφαρμόζει πρόσθετους, αποτελεσματικούς και πιο εξελιγμένους μηχανισμούς ελέγχου των συναλλαγών, από αυτούς που εφαρμόζει για την ισχυρή ταυτοποίηση των συναλλαγών, για συναλλαγές που μπορούν να προκαλέσουν ζημία άνω των χιλίων (1.000) ευρώ, προστέθηκε κατόπιν αντιδράσεων των τραπεζών.

Εντούτοις, η εν λόγω τροποποίηση του τελευταίου εδαφίου του άρθ. 22

του Ν. 5019/2023, κατακρίθηκε από ενώσεις καταναλωτών[30] καθώς θεωρήθηκε ότι δε συνάδει σύμφωνα με το πνεύμα αναθεώρησης του Ν. 4537/2018, ο οποίος ενσωμάτωσε την Οδ. 2015/2366 για την ευθύνη του πληρωτή για μη εγκεκριμένες πράξεις πληρωμών με την οποία οι εθνικές αρχές κλήθηκαν να υιοθετήσουν μια συντονισμένη προσέγγιση για τη ρύθμιση της ευθύνης και της κατανομής ζημιών. Η ρύθμιση κατακρίθηκε επιπλέον ως επαχθής για την προστασία των εννόμων συμφερόντων των καταναλωτών που θεωρείται το αδύναμο μέρος με αντισυμβαλλόμενη την Τράπεζα και είναι πιθανό να επωμίζονται την ευθύνη για ζημίες που ξεπερνούν τα 1.000,00 Ευρώ. Σε κάθε περίπτωση, αξιολογείται θετικά ότι τι βάρος απόδειξης σχετικά με την απόδειξη των εξελιγμένων μηχανισμών βαρύνει τα τραπεζικά ιδρύματα και κρίνεται σημαντικός ο ενεργός ρόλος της ΤτΕ[31].

---

[30] *Ε.Κ.ΠΟΙ.ΖΩ, (2023), Αναποτελεσματική η προστασία καταναλωτών από τις ηλεκτρονικές απάτες στο νομοσχέδιο προς συζήτηση στη Βουλή, Διαθέσιμο στο:* *https://www.ekpizo.gr/%CE%BF%CE%B9-%CE%B4%CF%81%CE%AC%CF%83%CE%B5%CE%B9%CF%82-%CE%BC%CE%B1%CF%82/%CF%87%CF%81%CE%B7%CE%BC%CE%B1%CF%84%CE%BF%CE%BF%CE%B9%CE%BA%CE%BF%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CE%AC/%CE%B1%CE%BD%CE%B1%CF%80%CE%BF%CF%84%CE%B5%CE%BB%CE%B5%CF%83%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE-%CE%B7-%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1-%CF%84%CF%89%CE%BD-%CE%BA%CE%B1%CF%84%CE%B1%CE%BD%CE%B1%CE%BB%CF%89%CF%84%CF%8E%CE%BD-%CE%B1%CF%80%CF%8C-%CF%84%CE%B9%CF%82-%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CE%AD%CF%82*

[31] *Βλ. Βαϊτσούδης , Ι., (2020), ό.π. σελ. 87*

2.6. Ορισμός κυβερνοασφάλειας και σχετικών εννοιών

Σύμφωνα με στοιχεία του Ευρωπαϊκού Κοινοβουλίου[32], επιτήδειοι απατεώνες χρησιμοποιούν ιστοσελίδες και email ηλεκτρονικού ψαρέματος, τα οποία περιλαμβάνουν κακόβουλους συνδέσμους και συνημμένα αρχεία, έχοντας ως σκοπό είτε να υποκλέψουν τραπεζικά δεδομένα χρηστών είτε να εκβιάσουν οργανισμούς αφού έχουν προηγουμένως παρακωλύσει τη λειτουργία των πληροφοριακών τους συστημάτων. Το γεγονός αυτό έχει οικονομικό αντίκτυπο για την τράπεζα της οποίας η φήμη διακυβεύεται και σε περίπτωση που πέσει θύμα κυβερνοεπίθεσης καθίσταται όμηρος των hackers και καλείται να πληρώσει τα λύτρα που της ζητούν. Επιπροσθέτως, σε περίπτωση μη συμμόρφωσης με τη λήψη των κατάλληλων μέτρων θωράκισης των ψηφιακών συστημάτων της και διασφάλισης ασφαλούς ψηφιακού περιβάλλοντος για τη διενέργεια των συναλλαγών στο πλαίσιο παροχής υπηρεσιών ηλεκτρονικής τραπεζικής, η τράπεζα βρίσκεται αντιμέτωπη με τον κίνδυνο επιβολής υψηλών προστίμων. Παράλληλα, οικονομικές απώλειες ενδέχεται να προκληθούν για τους πελάτες με την προσβολή του εννόμου αγαθού της περιουσίας τους και της ιδιωτικότητας των τραπεζικών δεδομένων τους.

Σύμφωνα με εκτιμήσεις της Ευρωπαϊκής Επιτροπής υπολογίζεται ότι το **2020 το κόστος του κυβερνοεγκλήματος για την παγκόσμια οικονομία έφτασε τα 5,5 τρις ευρώ, ποσό διπλάσιο σε σύγκριση με εκείνο του 2015.** Πέραν των οικονομικών επιπτώσεων, το κόστος είναι και κοινωνικό καθώς η ζημία που προκαλείται από τις κυβερνοεπιθέσεις μπορεί να αποτελέσει απειλή για τη λειτουργία της δημοκρατίας και της προστασίας ανθρωπίνων δικαιωμάτων όπως η ιδιωτικότητα αλλά και να κλονίσει τη σχέση εμπιστοσύνης μεταξύ της τράπεζας και των πελατών. Εκ των ανωτέρω, ανακύπτει ότι για την αποτελεσματική προστασία από τις κυβερνοεπιθέσεις ειδικότερα στον τραπεζικό τομέα καθώς και μια συνδεδεμένη κοινωνία και οικονομία, τίθεται στο επίκεντρο η λήψη μέτρων κυβερνοασφάλειας από τις τράπεζες.

---

[32] *Ευρωπαϊκό Κοινοβούλιο, (2021),Γιατί η κυβερνοασφάλεια είναι τόσο σημαντική για την ΕΕ; Διαθέσιμο στο: https://www.europarl.europa.eu/news/el/headlines/society/20211008STO14521/giati-i-kuvernoasfaleia-einai-toso-simantiki-gia-tin-ee*

Αρχικά, αναφορικά με τις επιθέσεις κατά των πληροφοριακών συστημάτων των τραπεζών κατόπιν ηλεκτρονικού ψαρέματος, κρίνεται σημαντική η αναφορά στην Οδ. 2013/40. Έτσι, κατά τον ορισμό του άρθ. 2 της εν λόγω Οδηγίας, ως «**χωρίς δικαίωμα**» εκλαμβάνεται η συμπεριφορά συμπεριλαμβανομένης της πρόσβασης, παρεμβολής ή υποκλοπής, μη εξουσιοδοτημένη από τον ιδιοκτήτη ή από άλλο νόμιμο δικαιούχο του συστήματος ή μέρους του ή μη επιτρεπόμενη δυνάμει του εθνικού δικαίου», ενώ η παράνομη πρόσβαση σε συστήματα πληροφοριών, παράνομη παρεμβολή σε σύστημα και παράνομη παρεμβολή σε δεδομένα, ρυθμίζεται υπό τις προβλέψεις των άρθ. 3,4, και 5 αντίστοιχα.

Στη συνέχεια, αναφορικά με την κυβερνοασφάλεια, σύμφωνα με τον ορισμό που δίνεται στο άρθ. 2, περ.1 του Κανονισμού 2019/881 σχετικά με τον ENISA και την πιστοποίηση της κυβερνοασφάλειας στον τομέα των ΤΠΕ, ως **κυβερνοαφάλεια** νοείται *«το σύνολο των δραστηριοτήτων που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων»*. Κατά το Ευρωπαϊκό Κοινοβούλιο[33], η κυβερνοασφάλεια αφορά την ασφάλεια πληροφοριών και επικοινωνιών, τις λειτουργικές τεχνολογίες και τις πλατφόρμες πληροφορικής που είναι αναγκαίες για τη διασφάλιση των ψηφιακών συστημάτων. Επιπροσθέτως, σε εθνικό επίπεδο, βάσει του ορισμού που δίνεται στο άρθ. 3 του Ν. 4577/2018, σε εναρμόνιση με την Οδ. 2016/1148, δε δίδεται ορισμός της έννοιας της κυβερνοασφάλειας αλλά αναφορικά με την **ασφάλεια συστημάτων δικτύου και πληροφοριών,** εκλαμβάνεται ως η «*ικανότητα συστημάτων δικτύου και πληροφοριών να ανθίστανται με δεδομένο βαθμό αξιοπιστία, σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών"*. Επισημαίνεται ότι ως προς την έννοια της **ασφάλεια**

[33] *Βλ. Ευρωπαϊκό Κοινοβούλιο, (2021) Γιατί η κυβερνοασφάλεια είναι τόσο σημαντική για την ΕΕ, ό.π.*

πληροφορίας/ δεδομένων αυτή συγκροτείται από το τρίπτυχο της **εμπιστευτικότητας,** της **ακεραιότητας** και της **διαθεσιμότητας.** Με βάση την εμπιστευτικότητα (confidentiality)[34], οι πληροφορίες δεν θα πρέπει να κοινολογούνται σε μη εξουσιοδοτημένα άτομα. Με γνώμονα την ακεραιότητα (integrity), τα δεδομένα θα πρέπει να είναι ακριβή, ακέραια και γνήσια και τέλος με γνώμονα τη διαθεσιμότητα (availability), οι πληροφορίες θα πρέπει να είναι στη διάθεση των χρηστών όποτε είναι απαραίτητη η χρήση τους.

Εκ των ανωτέρω ορισμών, προκύπτει ότι βασική έννοια, η οποία σχετίζεται με την κυβερνοασφάλεια είναι η η κυβερνοαπειλή. Αναφορικά με την έννοια της **κυβερνοαπειλής,** στη διάταξη του άρθ. 2, περ.7 του Κανονισμού 2019/881, αυτή ορίζεται ως «*κάθε πιθανή περίσταση, πιθανό συμβάν ή πιθανή ενέργεια που θα μπορούσε να καταστρέψει, να διαταράξει ή να επιδράσει κατ' άλλον τρόπο δυσμενώς στα συστήματα δικτύου και πληροφοριών, στους χρήστες των εν λόγω συστημάτων και σε άλλα πρόσωπα*». Δέον όπως επισημανθεί ότι σύμφωνα με έρευνα του ENISA, η οποία έλαβε χώρα στο χρονικό διάστημα ανάμεσα από το μήνα Απρίλιο του έτους 2020 έως το μήνα Ιούνιο του έτους 2021, ο τραπεζικός τομέας ανήκει στους πέντε τομείς που αντιμετωπίζουν τις περισσότερες απειλές στον τομέα της κυβερνοασφάλειας[35], με το λυτρισμικό (ransomware) να αποτελεί τη μεγαλύτερη απειλή που χρησιμοποιούν οι κυβερνοεγκληματίες, οι οποίες κρυπτογραφούν τα δεδομένα μιας οντότητας και εν συνεχεία ζητούν λύτρα για να αποκαταστήσουν την πρόσβαση σε αυτά.

Εν συνεχεία, αναφορικά με τον ορισμό του συμβάντος, για το οποίο γίνεται λόγος στον προαναφερόμενο ορισμό της κυβερνοαπειλής, σύμφωνα με το άρθ.4 , περ. 7. της Οδ. 2016/1148, ως **συμβάν** ορίζεται: «*κάθε γεγονός που έχει στην πραγματικότητα μια δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών*», *ενώ* σύμφωνα με το άρθ.4 , περ. 8 της Οδ. 2016/1148, ως **χειρισμός συμβάντων** ορίζεται: «*το σύνολο των διαδικασιών που υποστηρίζουν*

---

[34] *Αρχή Προστασίας Δεδομένων, Ασφάλεια προσωπικών δεδομένων, Διαθέσιμο στο:* https://dpa.gr/el/enimerwtiko/thematikes_enotites/asfaleia

[35] *Lawspot.gr, (2022), Κυβερνοασφάλεια: οι μεγαλύτερες απειλές για το 2021 (γράφημα), Διαθέσιμο στο:* https://www.lawspot.gr/nomika-nea/kyvernoasfaleia-oi-megalyteres-apeiles-gia-2021-grafima

τον εντοπισμό, την ανάλυση και την ανάσχεση ενός συμβάντος, καθώς και την παρέμβαση για την αντιμετώπισή του». Ακόμη, ως **κίνδυνος** σύμφωνα με το άρθ.4 της Οδ. 2016/1148 και της αντίστοιχης ενσωμάτωσης στην εθνική νομοθεσία με το άρθ. 3 του Ν. 4577/2018, περ. 9, θεωρείται: «*κάθε εύλογα διαπιστώσιμη περίσταση ή γεγονός με ενδεχομένως δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών».*

Επιπροσθέτως, με την Οδ. NIS 2 προστέθηκαν στις προβλέψεις του άρθ. 6 ορισμένοι νέοι ορισμοί όπως η έννοια του **περιστατικού κυβερνοασφαλείας μεγάλης κλίμακας,** το οποίο ορίζεται ως περιστατικό με σημαντικό αντίκτυπο σε τουλάχιστον δύο κράτη μέλη ή το οποίο προκαλεί διατάραξη που υπερβαίνει την ικανότητα ενός κράτους μέλους να ανταπεξέλθει. Προστέθηκε ακόμη στην ίδια διάταξη η έννοια της «**σημαντικής κυβερνοαπειλής»,** η οποία με βάση τα τεχνικά χαρακτηριστικά της μπορεί να θεωρηθεί ότι «*έχει τη δυνατότητα να επηρεάσει σοβαρά τα συστήματα δικτύου και πληροφοριών μιας οντότητας ή τους χρήστες της, προκαλώντας σημαντικές υλικές ή μη υλικές ζημίες*» **καθώς και η έννοια «παρ' ολίγον περιστατικό**» ως «συμβάν το οποίο θα μπορούσε δυνητικά να προκαλέσει βλάβη στα συστήματα δικτύου και πληροφοριών μιας οντότητας ή των χρηστών της, αλλά το οποίο εμποδίστηκε ή δεν υλοποιήθηκε επιτυχώς.

2.7. Ψηφιακή επιχειρησιακή ανθεκτικότητα - πλαίσιο διαχείρισης κινδύνων σχετικά με τις ΤΠΕ στον τομέα της ηλεκτρονικής τραπεζικής

Οι τράπεζες θεωρούνται πιστωτικά ιδρύματα, τα οποία ανήκουν στους φορείς εκμετάλλευσης βασικών υπηρεσιών, όπως αναφέρονται στο άρθ. 4 του Ν. 4577/2018, στο άρθ. 5 και στο Παράρτημα Ι της Οδ. 2022/2555 (NIS 2). Ως είδος των οντοτήτων ανήκουν στους **τομείς υψηλής κρισιμότητας/ ζωτικής σημασίας για βασικές κοινωνικές και οικονομικές δραστηριότητες στην οικονομική αγορά**. Όπως υποστηρίζεται και στην αιτ. σκ. 82 της NIS 2 .τα μέτρα διαχείρισης των κινδύνων στον τομέα της κυβερνοαφάλειας των τραπεζών οφείλουν να είναι επαυξημένα, αναλογικά με το βαθμό έκθεσης τους ως

σημαντικών οντοτήτων σε κινδύνους και με τον οικονομικό και κοινωνικό αντίκτυπο που θα είχε ένα περιστατικό. Σύμφωνα και με την ΑΠΔΠΧ[36], στους τρεις βασικούς στόχους της ασφάλειας των δεδομένων, ήτοι την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα, ο GDPR προσθέτει και την **αξιοπιστία** των συστημάτων. Στην εποχή μάλιστα της αυξημένης ψηφιοποίησης και στον τραπεζικό τομέα, η τράπεζα ως κρίσιμη υποδομή για την οικονομία και την κοινωνία, οφείλει να εξασφαλίζει ότι τα συστήματα και οι εφαρμογές της θα συνεχίζουν να λειτουργούν υπό δυσμενείς συνθήκες όπως ένα περιστατικό τεχνικής φύσεως και ότι θα είναι σε θέση να τα επαναφέρει σε λειτουργία.

Στις 27 Δεκεμβρίου 2022 δημοσιεύτηκε στην επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης **ο Κανονισμός 2022/2554** σύμφωνα με τη δέσμη μέτρων του Συμβουλίου της ΕΕ για τον ψηφιακό χρηματοοικονομικό τομέα και πιο συγκεκριμένα σχετικά με **την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα «DORA»**. Με τον εν λόγω κανονισμό θεσπίστηκαν απαιτήσεις σχετικά με τη διαχείριση κινδύνων ΤΠΕ και την αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ, οι οποίες είναι αυστηρότερες σε σύγκριση με τις λοιπές νομοθετικές ρυθμίσεις της Ένωσης σχετικά με την παροχή χρηματοοικονομικών υπηρεσιών.

Ως «ψηφιακή επιχειρησιακή ανθεκτικότητα» κατά το άρθ. 3 του Κανονισμού 2022/2554 εκλαμβάνεται: «*η ικανότητα μιας χρηματοοικονομικής οντότητας να διαμορφώνει, να εξασφαλίζει και να επανεξετάζει την επιχειρησιακή ακεραιότητα και αξιοπιστία της, διασφαλίζοντας, άμεσα ή έμμεσα μέσω της χρήσης υπηρεσιών που προσφέρονται από τρίτους παρόχους υπηρεσιών ΤΠΕ, το πλήρες φάσμα των ικανοτήτων ΤΠΕ που απαιτούνται, ώστε να ανταποκρίνεται στην ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιεί η χρηματοοικονομική οντότητα και τα οποία υποστηρίζουν τη συνεχή παροχή χρηματοοικονομικών υπηρεσιών και την ποιότητά τους, μεταξύ άλλων καθ'* όλη τη διάρκεια διαταραχών».

[36] *Αρχή Προστασίας Δεδομένων, Ασφάλεια προσωπικών δεδομένων, ό.π.*

Η τράπεζα στο πλαίσιο παροχής υπηρεσιών ηλεκτρονικής τραπεζικής προς τους πελάτες θα πρέπει να διασφαλίζει ένα ασφαλές ψηφιακό περιβάλλον διενέργειας συναλλαγών ανιχνεύοντας ενδεχόμενες απειλές για τα συστήματα της και καταστρώνοντας ένα **πλάνο διαχείρισης κινδύνων**. Βασικό συστατικό ενός πλαισίου διαχείρισης κινδύνου αποτελεί η αξιολόγηση του κινδύνου (risk assessment)[37]. Το πλαίσιο διαχείρισης κινδύνων για τις χρηματοοικονομικές οντότητες βάσει του άρθ. 6 επ. του Κανονισμού 2022/2554 θα πρέπει να περιλαμβάνει τουλάχιστον στρατηγικές, πολιτικές, διαδικασίες, πρωτόκολλα ΤΠΕ και εργαλεία για την επαρκή προστασία των πληροφοριακών πόρων, *συμπεριλαμβανομένου του λογισμικού, του υλισμικού, των διακομιστών, καθώς και για την προστασία όλων των σχετικών υλικών συνιστωσών και υποδομών, όπως εγκαταστάσεων, κέντρων δεδομένων και ευαίσθητων οριοθετημένων χώρων, ώστε να διασφαλίζεται ότι όλοι αυτοί οι πληροφοριακοί πόροι και πόροι ΤΠΕ προστατεύονται επαρκώς από κινδύνους, συμπεριλαμβανομένων τυχόν βλάβης και μη εξουσιοδοτημένης πρόσβασης ή χρήσης*».

Αναλυτικότερα, για την επίτευξη της κυβερνοασφάλειας στον τομέα της ηλεκτρονικής τραπεζικής, οι τράπεζες θα πρέπει να διατηρούν **επικαιροποιημένα συστήματα και πρωτόκολλα, τα οποία να είναι ανθεκτικά και αξιόπιστα.** Επιπροσθέτως, θα πρέπει να προσδιορίζουν σε συνεχή βάση τις πηγές κινδύνου, να αξιολογούν τις κυβερνοαπειλές και τις ευπάθειες των συστημάτων τους. Στο άρθ. 9 του άνωθεν Κανονισμού επισημαίνεται **η σημασία της προστασίας** και της **πρόληψης** της έλλειψης διαθεσιμότητας, της υποβάθμισης της γνησιότητας και της ακεραιότητας και των παραβιάσεων της εμπιστευτικότητας και απώλειας δεδομένων. Επιπλέον, οι τράπεζες έχουν την υποχρέωση να διαθέτουν μηχανισμούς με πολυεπίπεδες δικλείδες ασφαλείας για τον **άμεσο εντοπισμό ασυνήθιστων**

---

[37] *Ελληνική Δημοκρατία, Υπουργείο Ψηφιακής Διακυβέρνησης,(2021), Εγχειρίδιο Κυβερνοασφάλειας, Διαθέσιμο στο :* https://mindigital.gr/wp-content/uploads/2021/06/%CE%95%CE%B3%CF%87%CE%B5%CE%B9%CF%81%CE%AF%CE%B4%CE%B9%CE%BF-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf, σελ. 9

δραστηριοτήτων, να υποβάλλουν περιοδικά σε δοκιμή κατάλληλα σχέδια αντιμετώπισης, ανάκαμψης και επιχειρηματικής συνέχειας. Συνάμα, με σκοπό τη **διασφάλιση και αποκατάσταση των συστημάτων**, οι τράπεζες πρέπει να καταρτίζουν και να τεκμηριώνουν πολιτικές και διαδικασίες δημιουργίας εφεδρικών δεδομένων και συστημάτων. Σημαντική είναι επίσης η **εκπαίδευση και ευαισθητοποίηση του προσωπικού** αναφορικά με τις κυβερνοεπιθέσεις και την ανάλυση των συνεπειών τους καθώς και η επανεξέταση κατόπιν συμβάντων. Τέλος, οι τράπεζες θα πρέπει να διαθέτουν και **σχέδια επικοινωνίας** σε καταστάσεις κρίσης όπου είναι εφικτή η γνωστοποίηση μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ ή ευπαθειών σε πελάτες και αντισυμβαλλομένους τους.

Η **διαδικασία διαχείρισης και ταξινόμησης συμβάντων** που σχετίζονται με τις ΤΠΕ και τις κυβερνοαπειλές λαμβάνει χώρα σύμφωνα με τα προβλεπόμενα κριτήρια στο άθρ. 18 επ. του Κανονισμού 2022/2554, όπως: ο αριθμός ή / και η συνάφεια των επηρεαζόμενων πελατών**,** η διάρκεια του συμβάντος, οι γεωγραφικά επηρεαζόμενες περιοχές, ιδίως εάν το συμβάν επηρεάζει περισσότερα από δύο κράτη μέλη, οι απώλειες δεδομένων σχετικά με τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων, η σημαντικότητα των υπηρεσιών που επηρεάστηκαν, συμπεριλαμβανομένων των συναλλαγών και οι οικονομικές επιπτώσεις. Σχετικά με τα μείζονα περιστατικά που σχετίζονται με τις ΤΠΕ θα πρέπει να γίνεται αναφορά στην αρμόδια αρχή, ενώ η κοινοποίηση σημαντικών κυβερνοαπειλών είναι προαιρετική κατά το άρθ. 19 του Κανονισμού 2022/2554.

Περαιτέρω, σύμφωνα με την αιτ. σκ. 60 της Οδ. NIS 2, τα κράτη μέλη σε συνεργασία με τον ENISA οφείλουν να λαμβάνουν μέτρα ώστε να διευκολύνουν τη συντονισμένη γνωστοποίηση των τρωτοτήτων με τη θέσπιση σχετικής εθνικής πολιτικής. Κάθε κράτος μέλος θα πρέπει να θεσπίζει εθνική στρατηγική με σκοπό τη διατήρηση υψηλού επιπέδου αναφορικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών έτσι ώστε να καλύπτονται τουλάχιστον τομείς που αφορούν βασικές υπηρεσίες, υποδομές ζωτικής σημασίας ή κρίσιμες υποδομές όπως οι τράπεζες και υπηρεσίες που αφορούν την επιγραμμική αγορά

όπως οι υπηρεσίες ηλεκτρονικής τραπεζικής. Στην Ελλάδα, η Εθνική Στρατηγική Κυβερνοασφάλειας έθεσε ως ένα εκ των στρατηγικών της στόχων τη **θωράκιση κρίσιμων υποδομών, ασφάλειας και νέων τεχνολογιών**, ο οποίος αντιστοιχεί στο στόχο του ENISA για προστασία της υποδομής των κρίσιμων πληροφοριών, θέσπιση βασικών μέτρων ασφαλείας και εξισορρόπηση της ασφάλειας με την προστασία της ιδιωτικής ζωής[38]. Σύμφωνα με την Εθνική Στρατηγική για την κυβερνοασφάλεια στις κρίσιμες υποδομές θα πρέπει να κατανοηθεί ο τρόπος που οι τεχνολογικές εξελίξεις επηρεάζουν την ψηφιακή διακυβέρνηση, να γίνει αναβάθμιση της προστασίας και να θωρακιστούν τα συστήματα και οι εφαρμογές μέσω ενισχυμένων απαιτήσεων ασφαλείας. Αναφορικά δε με την αντιμετώπιση συμβάντων που κρίνονται ως σοβαρές διαταράξεις για τις παρεχομένες από τους φορείς υπηρεσίες οδηγό αποτελεί η εκπόνηση του **Εθνικού Σχεδίου Έκτακτης Ανάγκης** το οποίο περιλαμβάνει κριτήρια για το πότε ένα συμβάν θεωρείται ως κρίση, τα σενάρια, τους ρόλους και τις αρμοδιότητες των ενδιαφερομένων μερών, τα σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές, την εκτίμηση, αναγνώριση και ανάλυση των ευπαθειών/ κινδύνων, την αναγνώριση της επικείμενης κρίσης, την επικοινωνία της κρίσης και τις επιλογές ασκήσεων. Τελικά, σπουδαία είναι και η ενδυνάμωση των συνεργασιών κατά το άρθ.9 της NIS, σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο με την ανάπτυξη του κλάδου της κυβερνοδιπλωματίας και την υποχρέωση προσδιορισμού των εθνικών αρχών που θα είναι επιφορτισμένες με την τήρηση της εφαρμογής του κανονιστικού πλαισίου της κυβερνοασφάλειας, την υποχρέωση ορισμού ενός εθνικού ενιαίου κέντρου επαφής για την ασφάλεια των συστημάτων δικτύου και πληροφοριών και την υποχρέωση ορισμού μίας ή περισσότερων ομάδων απόκρισης για συμβάντα που αφορούν στην ασφάλεια των υπολογιστών (CSIRT). Προκειμένου να αποδεικνύεται η συμμόρφωση με τα

---

[38] *Ελληνική Δημοκρατία, Υπουργείο Ψηφιακής Διακυβέρνησης, Εθνική Αρχή Κυβερνοασφάλειας, 2020, Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025, Διαθέσιμο στο: https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7%CC%81-%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7%CC%81-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf, σελ. 20 επ.*

μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, τα κράτη μέλη μπορούν να απαιτούν από βασικές και σημαντικές οντότητες να χρησιμοποιούν **συστήματα πιστοποίησης, σύμφωνα με το άρθ. 49 του Κανονισμού 2019/881.** Ένα τέτοιο πρότυπο πιστοποίησης αποτελεί το ISO/IEC 27001:2019, αναφορικά με τη διαχείριση της ασφάλειας των πληροφοριών και κατ' επέκταση την κανονιστική συμμόρφωση με τον GDPR.

Η μη συμμόρφωση προς τις επιταγές της κυβερνοσφάλειας για παράλειψη ή καθυστέρηση κοινοποοίησης συμβάντος με σοβαρό αντίκτυπο στη συνέχεια βασικών υπηρεσιών ή παράλειψης λήψης κατάλληλων τεχνικών και οργανωτικών, προληπτικών μέτρων καθώς και η παροχή ή καθυστερημένη παροχή πληροφοριών για διενέργεια ελέγχου ή διερεύνηση συμβάντος, συνεπάγεται κυρώσεις, οι οποίες θα πρέπει να είναι αποτελεσματικές, αναλογικές και αποτρεπτικές λαμβάνοντας υπόψη κάθε μεμονωμένη περίπτωση , σύμφωνα με τις προβλέψεις του άρθ. 32 της Οδ. NIS 2.

2.7.1. Μέτρα ασφάλειας πληρωμών κατά τη χρήση υπηρεσιών ηλεκτρονικής τραπεζικής

Εν συνεχεία, αναφορικά με τις ελάχιστες απαιτήσεις στον τομέα της ασφάλειας πληρωμών μέσω ηλεκτρονικής τραπεζικής, ενδιαφέρον παρουσιάζουν οι κατευθυντήριες γραμμές της Ευρωπαϊκής Αρχής Τραπεζών[39], οι οποίες αφορούν την παροχή υπηρεσιών πληρωμών που προσφέρονται μέσω διαδικτύου από Παρόχους Υπηρεσιών Πληρωμών, ήτοι από χρηματοοικονομικά ιδρύματα όπως οι τράπεζες. Πιο συγκεκριμένα, οι τράπεζες ως ΠΥΠ, θα πρέπει να προβαίνουν στις ακόλουθες ενέργειες, ώστε να εξασφαλίζουν ένα ασφαλές ψηφιακό περιβάλλον διενέργειας συναλλαγών:

Αρχικά, να διασφαλίζουν ένα **γενικό περιβάλλον ελέγχου και ασφαλείας**, το οποίο θα περιλαμβάνει τα ακόλουθα:

Σχετικά με τη **διακυβέρνηση:** Να εφαρμόζουν και επανεξετάζουν σε

[39] *Ευρωπαϊκή Αρχή Τραπεζών, (2014), Τελικές κατευθυντήριες γραμμές σχετικά με την ασφάλεια πληρωμών μέσω διαδικτύου, Διαθέσιμο στο:* https://www.eba.europa.eu/sites/default/files/documents/10180/1004450/b636aaaa-fdf9-47ef-a100-e03a75448bb0/EBA-GL-2014-12_EL_rev1%20GL%20on%20Internet%20Payments.pdf

τακτική βάση μια πολιτική ασφαλείας συμπεριλαμβανομένης της διαχείρισης κινδύνου με απευθείας αναφορά στο Διοικητικό Συμβούλιο, καθώς και τις υπηρεσίες πληρωμών που παρέχουν μέσω διαδικτύου, περιλαμβανόμενης της διαχείρισης ευαίσθητων δεδομένων.

Σχετικά με την **αξιολόγηση κινδύνου για την ασφάλεια των πληρωμών:** να διενεργούν λεπτομερείς αξιολογήσεις ελέγχου για τις πληρωμές μέσω διαδικτύου, να εξετάζουν τα αποτελέσματα των απειλών, να καθορίζουν κατά πόσο απαιτούνται αλλαγές στα υπάρχοντα μέτρα ασφαλείας, στις διαδικασίες ή στις υπηρεσίες που προσφέρονται, να επανεξετάζουν τα σενάρια κινδύνου τουλάχιστον μία φορά ετησίως.

Σχετικά με την **παρακολούθηση και αναφορά περιστατικών ασφαλείας:** να εφαρμόζουν διαδικασία για τον έλεγχο και τον χειρισμό καταγγελιών πελατών, να ενημερώνουν άμεσα τις εποπτικές αρχές και αρχές προστασίας των δεδομένων, να συνεργάζονται με τις διωκτικές αρχές, να απαιτούν από τις επιχειρήσεις ηλεκτρονικού εμπορίου που αποθηκεύουν, επεξεργάζονται ή διαβιβάζουν ευαίσθητα δεδομένα πληρωμών να συνεργάζονται σε περιπτώσεις σημαντικών περιστατικών ασφαλείας πληρωμών.

Σχετικά με τ**ον έλεγχο και μετριασμό των κινδύνων**: να εφαρμόζουν μέτρα ασφαλείας μέσω των οποίων επιτυγχάνεται μια «εις βάθος άμυνα» τηρώντας την αρχή των «ελάχιστων προνομίων» για τη χρηστή διαχείριση της ταυτότητας και της πρόσβασης. Προκειμένου να περιορίζουν τη χρήση «πλαστών – κλώνων» διαδικτυακών τόπων, οι οποίοι μιμούνται τις αυθεντικές ιστοσελίδες των τραπεζών, θα πρέπει να διαθέτουν πιστοποιητικά εκτεταμένης επικύρωσης που εκδίδονται στο όνομα της τράπεζας ή να μεριμνούν για την εφαρμογή άλλων παρόμοιων μεθόδων ταυτοποίησης. Επιπλέον, θα πρέπει να εφαρμόζουν κατάλληλες διαδικασίες παρακολούθησης και περιορισμού της πρόσβασης σε ευαίσθητα δεδομένα και κρίσιμους φυσικούς πόρους. Κατά το σχεδιασμό, πρέπει να διασφαλίζεται η ελαχιστοποίηση των δεδομένων και η απεικόνιση των ευαίσθητων δεδομένων πληρωμών πρέπει να τηρείται στα απολύτως αναγκαία επίπεδα. Τα μέτρα ασφαλείας πρέπει να υποβάλλονται σε

δοκιμές ώστε να διασφαλίζεται η ανθεκτικότητα και η αποτελεσματικότητά τους και οι έλεγχοι να διενεργούνται από αξιόπιστους πραγματογνώμονες. Σε περιπτώσεις αποδοχής συναλλαγών με κάρτα πρέπει να απαιτούν από τις επιχειρήσεις ηλεκτρονικού εμπορίου που χειρίζονται ευαίσθητα δεδομένα πληρωμών να εφαρμόζουν ομοίως μέτρα ασφαλείας στις υποδομές πληροφορικής τους.

Σχετικά με την **ιχνηλασιμότητα,** οι τράπεζες πρέπει να εφαρμόζουν διαδικασίες που εξασφαλίζουν ότι το σύνολο των συναλλαγών και της ροής επεξεργασίας της ηλεκτρονικής εξουσιοδότησης ιχνηλατούνται δεόντως.

Στη συνέχεια, οι τράπεζες θα πρέπει να τηρούν πέραν των προαναφερόμενων γενικών και **ειδικά μέτρα ελέγχου και ασφάλειας των πληρωμών μέσω διαδικτύου,** όπως:

Η **αρχική εξακρίβωση της ταυτότητας του πελάτη** σύμφωνα με τις επιταγές της νομοθεσίας για την καταπολέμηση της νομιμοποίησης των εσόδων από παράνομες δραστηριότητες με την παροχή επαρκών εγγράφων ταυτότητας (όπως διαβατήριο, αστυνομική ταυτότητα ή προηγμένη ψηφιακή υπογραφή), η επιβεβαίωση της βούλησης των πελατών να προβούν σε πληρωμές και η προηγούμενη **ενημέρωση** του πελάτη ειδικά για την παροχή υπηρεσιών πληρωμών μέσω διαδικτύου (απαιτήσεις για τον εξοπλισμό, λογισμικό ή άλλα απαραίτητα εργαλεία, ορθή και ασφαλή χρήση εξατομικευμένων διαπιστευτηρίων ασφαλείας, περιγραφή των σταδίων για υποβολή και έγκριση πράξεως πληρωμών, ασφαλή χρήση υλισμικού και λογισμικού που παρέχεται στον πελάτη, διαδικασίες σε περίπτωση απώλειας ή κλοπής των εξατομικευμένων διαπιστευτηρίων ασφαλείας ή του υλισμικού ή του λογισμικού για την είσοδο στο σύστημα ηλεκτρονικής τραπεζικής ή για την εκτέλεση των πράξεων πληρωμής, διαδικασίες σε περίπτωση υπόνοιας κατάχρησης, περιγραφή αρμοδιοτήτων και ευθυνών της τράπεζας και του πελάτη αντιστοίχως κατά τη χρήση υπηρεσιών ηλεκτρονικής τραπεζικής. Στη σύμβαση πλαίσιο που αφορά την παροχή υπηρεσιών ηλεκτρονικής τραπεζικής και καταρτίζεται ανάμεσα στην τράπεζα και τον πελάτη θα πρέπει να διευκρινίζεται ότι ο ΠΥΠ μπορεί να αναστείλει την εκτέλεση συγκεκριμένης πράξης πληρωμής

ή τη χρήση μέσου πληρωμής για λόγους ασφαλείας.

Η **ισχυρή ταυτοποίηση του πελάτη για την έγκριση, σύμφωνα με τις προβλέψεις του άρθ. 4, περ. 30, του Ν. 4537/2018,** όπως αναπτύχθηκε και ανωτέρω στο πλαίσιο θεμελίωσης της ενδοσυμβατικής ευθύνης της τράπεζας κατόπιν επιθέσεων ηλεκτρονικού ψαρέματος. Περαιτέρω, οι ΠΥΠ θα πρέπει να διασφαλίζουν ότι η **εγγραφή του πελάτη σε εργαλεία ταυτοποίησης** που απαιτούνται για τη χρήση των υπηρεσιών ηλεκτρονικής τραπεζικής και η παράδοση σχετικού λογισμικού με τις πληρωμές διεξάγεται **με ασφαλή τρόπο** καθώς και να περιορίζουν τον αριθμό προσπαθειών σύνδεσης ή ταυτοποίησης θέτοντας χρονικό όριο σύνδεσης στις υπηρεσίες και της διάρκειας ισχύος της ταυτοποίησης.

Η **παρακολούθηση των συναλλαγών** για την πρόληψη, τον εντοπισμό ύποπτων συναλλαγών και την αναστολή εκτέλεσης παράνομων πράξεων πληρωμής η οποία μπορεί να επιτευχθεί με τη χρήση παραμετροποιημένων κανόνων, όπως οι μαύρες λίστες με στοιχεία καρτών που έχουν διαρρεύσει η κλαπεί, η παρακολούθηση της συσκευής πρόσβασης του πελάτη, όπως η αλλαγή διεύθυνσης IP, ασυνήθεις επιχειρήσεις ηλεκτρονικού εμπορίου για έναν συγκεκριμένο πελάτη ή ασυνήθιστα δεδομένα συναλλαγών. Επίσης, τα πληροφοριακά συστήματα των τραπεζών θα πρέπει να είναι σε θέση να εντοπίζουν ενδείξεις κακόβουλου λογισμικού. Έχουν υποχρέωση να θέτουν **όρια για τις υπηρεσίες πληρωμών και να παρέχουν επιλογές στους πελάτες για τον περιορισμό του κινδύνου** (όπως το μέγιστο ποσό για κάθε πληρωμή ή συγκεντρωτικό ποσό για καθορισμένη χρονική περίοδο), παρέχοντας υπηρεσίες προειδοποίησης και διαχείρισης του προφίλ των πελατών καθώς και να **επιβεβαιώνουν στους πελάτες τους την έναρξη πληρωμής και να τους παρέχουν εγκαίρως τις απαραίτητες πληροφορίες ώστε να ελέγχουν την ορθή έναρξη και/ ή εκτέλεση της πράξης πληρωμής.**

Στο σημείο αυτό αναφορικά με την ταυτοποίηση και την ασφάλεια των συναλλαγών άξια αναφοράς είναι η προσθήκη μιας δικλείδας ασφαλείας κατά την παροχή υπηρεσιών ηλεκτρονικής τραπεζικής από της τράπεζες και συγκεκριμένα αυτή της **τριπλής ταυτοποίησης (3 Factor Authentication-3 FA**).

Το πρώτο βήμα ταυτοποίησης του χρήστη ηλεκτρονικής τραπεζικής διεξάγεται με την εισαγωγή των στοιχείων εισόδου (username και password) και επιβεβαίωσής τους μέσω βιομετρικών στοιχείων, εάν υπάρχει αυτή η λειτουργικότητα στη συσκευή από την οποία συνδέεται. Το δεύτερο βήμα περιλαμβάνει τον κωδικό μιας χρήσης **(OTP),** τον οποίο λαμβάνει ο χρήστης, εάν δεν είναι συνδεδεμένος στο διαδίκτυο μέσω γραπτού μηνύματος sms, ή αν είναι συνδεδεμένος στο διαδίκτυο μέσω της εφαρμογής viber ή push notification, σε περίπτωση που έχει ενεργοποιήσει τη σχετική δυνατότητα. Ο εν λόγω κωδικός αποστέλλεται στον χρήστη κάθε φορά που πραγματοποιεί μια συναλλαγή από τον υπολογιστή ή το κινητό του προς επιβεβαίωσή της εκτέλεσης της σχετικής εντολής μεταφοράς χρημάτων. Στα παραπάνω προστέθηκε το τρίτο βήμα που αφορά την επιβεβαίωση ολοκλήρωσης συναλλαγής που εκλαμβάνεται ως ύποπτη, όταν οι συναλλαγές ξεπερνούν αθροιστικά τα 1.000 Ευρώ/ημέρα και θα πρέπει να επιβεβαιωθεί είτε μέσω τηλεφωνικής κλήσης από την τράπεζα είτε μέσω ενός επιπλέον κωδικού μιας χρήσης στο viber είτε μέσω sms.

Επιπροσθέτως, αναφορικά με τα ειδικά μέτρα ελέγχου και ασφαλείας των πληρωμών που πρέπει να τηρούν οι τράπεζες, περιλαμβάνονται και η **προστασία των ευαίσθητων δεδομένων πληρωμής**, όπως δεδομένα που χρησιμοποιούνται για την αναγνώριση και την ταυτοποίηση των πελατών κατά την αποθήκευση, επεξεργασία ή τη διαβίβασή τους.

Τελευταίο αλλά εξίσου σημαντικό είναι το μέτρο της **ευαισθητοποίησης, εκπαίδευσης** και **επικοινωνίας της τράπεζας με τους πελάτες αναφορικά με την ασφαλή χρήση υπηρεσιών ηλεκτρονικής τραπεζικής.** Θα πρέπει να αναπτύσσεται ένας δίαυλος επικοινωνίας αναφορικά με τη διαδικασία που θα πρέπει να ακολουθούν οι πελάτες για την αναφορά υπονοιών για παράνομες πληρωμές, ύποπτα περιστατικά, ανωμαλίες κατά τη διάρκεια σύνδεσης στις υπηρεσίες ηλεκτρονικής τραπεζικής, πιθανές απόπειρες ηλεκτρονικού ψάρεματος μέσω της κοινωνικής μηχανικής. Παράλληλα, το τραπεζικό ίδρυμα πρέπει να ενημερώνει τον πελάτη για πιθανές παράνομες συναλλαγές, να τον προειδοποιεί για εκδηλώσεις επιθέσεων με μορφή phishing, να παρέχει υπηρεσίες εξυπηρέτησης σε όλα τα παράπονα, αιτήματα στήριξης

και γνωστοποιήσεις σχετικά με τις δυσλειτουργίες κατά την παροχή υπηρεσιών πληρωμών. Θα πρέπει να διασφαλίζεται από την τράπεζα ότι οι πελάτες κατανοούν την ανάγκη για προστασία των κωδικών πρόσβασης και εμπιστευτικών τους δεδομένων, την ανάγκη για ορθή διαχείριση της ασφάλειας των συσκευών μέσω των οποίων συνδέονται στις υπηρεσίες ηλεκτρονικής τραπεζικής καθώς και την ανάγκη για εξακρίβωση της χρήσης του γνήσιου διαδικτυακού τόπου πληρωμών. Τέλος, τα τραπεζικά ιδρύματα θα πρέπει να απαιτούν από τις επιχειρήσεις ηλεκτρονικού εμπορίου το σαφή διαχωρισμό της διαδικασίας πληρωμής από το περιβάλλον του ηλεκτρονικού καταστήματος ώστε οι πελάτες να αναγνωρίζουν πότε επικοινωνούν με την τράπεζα και όχι με τον δικαιούχο πληρωμής.

3. Κεφάλαιο Β': Νομική προστασία προσωπικών δεδομένων χρηστών ηλεκτρονικής τραπεζικής

3.1. Η σημασία συμμόρφωσης με τις απαιτήσεις του GDPR κατά την παροχή υπηρεσιών ηλεκτρονικής τραπεζικής

Σε περιπτώσεις επιθέσεων με μορφή phishing όπως αναπτύχθηκε και στο προηγούμενο κεφάλαιο το θύμα πέραν της περιουσιακής βλάβης που υφίσταται, συχνά έρχεται αντιμέτωπο και με την παραβίαση των προσωπικών δεδομένων των οποίων τηρεί και επεξεργάζεται η τράπεζα στο πλαίσιο συνεργασίας τους για την παροχή υπηρεσιών ηλεκτρονικής τραπεζικής, καθώς ενέχει ο κίνδυνος να αποκτήθηκε πρόσβαση από τρίτο μη εξουσιοδοτημένο πρόσωπο στα τραπεζικά του δεδομένα.

Οι Τράπεζες επεξεργάζονται μεγάλο όγκο δεδομένων των πελατών τους σε καθημερινή βάση και ήταν ήδη εξοικειωμένες με ζητήματα που άπτονται του GDPR, πριν την εφαρμογή του στις 25 Μαΐου του 2018, διότι έχουν μια μεγάλη ιστορία σε θέματα αυστηρής συμμόρφωσης που απαιτούνται από τις εποπτικές αρχές αναφορικά με την προστασία της ιδιωτικότητας και των κανόνων προστασίας προσωπικών δεδομένων[40]. Εντούτοις, το ζήτημα της πλήρους εναρμόνισης, απασχόλησε και τον τραπεζικό χώρο και απαιτήθηκαν αλλαγές επιχειρηματικής κουλτούρας, υπό το πρίσμα της επιβολής υψηλών προστίμων για τις επιχειρήσεις βάσει του άρθ. 83 του ΓΚΠΔ, που ανέρχονται έως το 2% του συνολικού παγκόσμιου ετήσιου τζίρου του προηγούμενου οικονομικού έτους,. Πέραν των οικονομικών κυρώσεων, μια γνωστοποίηση περιστατικού παραβίασης της προστασίας προσωπικών δεδομένων πελάτη της τράπεζας, μπορεί να αποβεί επιζήμια και να κλονίσει τη φήμη της, η οποία είναι αρκετά σημαντική στη σχέση εμπιστοσύνης που έχει χτίσει με τον πελάτη.

Εξαιτίας λοιπόν του τεράστιου όγκου των δεδομένων που συλλέγει και επεξεργάζεται το τραπεζικό ίδρυμα εγείρονται προκλήσεις αναφορικά με το σεβασμό της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων του

[40] *Deloitte, 2019, After the dust settles, How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on.*

χρήστη ηλεκτρονικής τραπεζικής. Η ανάγκη προσαρμογής των τραπεζών με κανονιστικές απαιτήσεις έρχεται πολλές φορές αντιμέτωπη με την καινοτομία και την αξιοποίηση των δυνατοτήτων της ψηφιακής τεχνολογίας και δημιουργείται έτσι η ανάγκη για εξισορρόπηση κατά την παροχή ηλεκτρονικών τραπεζικών υπηρεσιών χωρίς να διακυβεύεται ο σεβασμός της ιδιωτικότητας.[41] Προς την κατεύθυνση αυτή, το ΕΣΠΔ εξέδωσε κατευθυντήριες γραμμές σχετικά με την αρμονική συνύπαρξη της PSD2 και του GDPR, βάσει των οποίων οι υπεύθυνοι επεξεργασίας που δραστηριοποιούνται στον τραπεζικό τομέα πρέπει να διασφαλίζουν τις απαιτήσεις με τη συμμόρφωση της προστασίας των προσωπικών δεδομένων συμπεριλαμβανομένων των αρχών που διέπουν την επεξεργασία δεδομένων και καταγράφονται στο άρθ. 5 του GDPR καθώς και τις προβλέψεις της Οδ. 2002/58 αναφορικά με την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες[42].

Συνεπώς, είναι απαραίτητο να ακολουθούνται όλα τα απαιτούμενα βήματα κανονιστικής συμμόρφωσης με τον GDPR και στον τομέα της ηλεκτρονικής τραπεζικής, τα οποία εκκινούν από τη χαρτογράφηση των τραπεζικών δεδομένων (data mapping), την ανάλυση ελλείψεων (gap analysis), τη σύνταξη πολιτικών και διαδικασιών, μέχρι και την ενημέρωση των υποκειμένων-χρηστών ηλεκτρονικής τραπεζικής, τη λήψη συγκατάθεσής τους όπου απαιτείται καθώς και την εκπαίδευση του προσωπικού της τράπεζας και τη συνεχή παρακολούθηση αναφορικά με τη συμμόρφωση.

3.2. Χαρτογράφηση προσωπικών δεδομένων υποκειμένων - χρηστών ηλεκτρονικής τραπεζικής

Το κρισιμότερο βήμα για να εκκινήσει η διαδικασία συμμόρφωσης των τραπεζών σύμφωνα με το κανονιστικό πλαίσιο του ΓΚΠΔ, είναι η

[41] *Cambridge University Press, (2021), Know your customer: Balancing innovation and regulation for financial inclusion*

[42] *Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, (2020) Κατευθυντήριες γραμμές 06/2020 σχετικά με την αλληλεπίδραση μεταξύ της δεύτερης οδηγίας για τις υπηρεσίες πληρωμών και του ΓΚΠΔ, Διαθέσιμο στο: https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202006_psd2_afterpublicconsultation_el.pdf,*

χαρτογράφηση των δεδομένων (data mapping/ data flow mapping), προκειμένου να καταγραφούν τι είδους δεδομένα συλλέγει και επεξεργάζεται το τραπεζικό ίδρυμα, για ποιο σκοπό, πού υπάρχουν, ποιος έχει πρόσβαση σε αυτά, για πόσο χρονικό διάστημα τα διατηρεί και περαιτέρω ποια είναι τα στοιχεία του υπεύθυνου επεξεργασίας και ποια μέτρα ασφαλείας έχει λάβει. Στην πράξη αυτό καταγράφεται με ένα αρχείο με την περιγραφή των δραστηριοτήτων επεξεργασίας, στη μορφή χάρτη για το οποίο γίνεται λόγος στο **άρθ. 30 του ΓΚΠΔ**. Στο εν λόγω αρχείο καταγράφεται αναλυτικά ο κύκλος της ζωής των δεδομένων εντός των υπηρεσιών των τραπεζικών ιδρυμάτων, όπως των καταστημάτων και των διοικητικών υπηρεσιών[43]. Προκειμένου να υλοποιηθεί η διαδικασία της χαρτογράφησης, θα πρέπει να πραγματοποιηθούν «συνεντεύξεις» με τα στελέχη και το υπόλοιπο προσωπικό ώστε να γίνει πλήρης και αναλυτική καταγραφή της ροής των δεδομένων που επεξεργάζεται η Τράπεζα.

Η τήρηση του αρχείου αυτού αποτελεί υποχρέωση του Υπεύθυνου/ Εκτελούντος την επεξεργασία στο πλαίσιο της **αρχής της λογοδοσίας** αλλά και γιατί συντελεί στην ορθή οργάνωση των διαδικασιών χειρισμού των προσωπικών δεδομένων που τηρούνται. Τα στοιχεία που πρέπει να περιλαμβάνει το αρχείο δραστηριοτήτων αναφορικά με τους υπεύθυνους επεξεργασίας καταγράφονται στο άρθ. 30 παρ. 1 του ΓΚΠΔ, ενώ αναφορικά με τους εκτελούντες την επεξεργασίας στο άρθ. 30 παρ. 2 του ΓΚΠΔ. Εξαίρεση από την εν λόγω υποχρέωση προβλέπεται στις περιπτώσεις των επιχειρήσεων/ οργανισμών που απασχολούν λιγότερα από 250 άτομα, εκτός αν συντρέχουν ιδιαίτεροι κίνδυνοι. Η Τράπεζα θα πρέπει να τηρεί αρχείο δραστηριοτήτων όπου αποτυπώνεται η υφιστάμενη κατάσταση, αλλά και να το διαθέτει πάντοτε **επικαιροποιημένο**, να το τροποποιεί/συμπληρώνει όποτε απαιτείται καθώς ως προκύπτει και από **το** άρθ. 9 του Κώδικα Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα αναφορικά με την ακρίβεια των δεδομένων, τα πιστωτικά ιδρύματα λαμβάνουν όλα τα απαραίτητα μέτρα,

[43] *Ξυγκάκη, Α. (2020), Η προσαρμογή των τραπεζών στο νέο κανονισμό για την προστασία των προσωπικών δεδομένων, Πειραιάς, σελ.33*

προκειμένου τα δεδομένα των υποκειμένων – πελατών τους να είναι ακριβή και να επικαιροποιούνται**.** Δεδομένου ότι ο χάρτης δεδομένων αποτελεί βασικό αποδεικτικό στοιχείο της συμμόρφωσης της με τις κανονιστικές επιταγές του ΓΚΠΔ και σε περίπτωση ελέγχου ή περιστατικού παραβίασης προσωπικών δεδομένων η Τράπεζα μπορεί να το επικαλεστεί ώστε να αποδείξει ότι είχε προβεί σε όλες τις απαιτούμενες ενέργειες αναφορικά με την καταγραφή των δραστηριοτήτων επεξεργασίας.

3.2.1. Κατηγορίες προσωπικών δεδομένων υποκειμένων - χρηστών ηλεκτρονικής τραπεζικής

Μία εκ των σημαντικότερων ενεργειών που θα πρέπει να υλοποιηθούν στο πλαίσιο της τήρησης του αρχείου δραστηριοτήτων είναι η καταγραφή **των κατηγοριών των δεδομένων προσωπικού χαρακτήρα** που τηρεί το τραπεζικό ίδρυμα ως υπεύθυνος επεξεργασίας, κατά το άρθ. 30 παρ. 1 στοιχ. γ' στο πλαίσιο συνεργασίας με τους πελάτες που χρησιμοποιούν τις υπηρεσίες ηλεκτρονικής τραπεζικής.

Αρχικά, σύμφωνα με τον ορισμό **του άρθ. 4. στοιχ.1 του ΓΚΠΔ**, στα «δεδομένα προσωπικού χαρακτήρα», συγκαταλέγεται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (υποκείμενο των δεδομένων). Ως ταυτοποιήσιμο θεωρείται το φυσικό πρόσωπο, του οποίου η ταυτότητα μπορεί να εξακριβωθεί με άμεσο ή έμμεσο τρόπο και ειδικότερα μέσω αναφοράς σε αναγνωριστικό στοιχείο της ταυτότητας, όπως *το όνομα, ο αριθμός ταυτότητας, τα δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.*

Συνάγεται εκ του παραπάνω ορισμού ότι η ταυτότητα ενός φυσικού προσώπου μπορεί να εξακριβωθεί και με την αναφορά σε **δεδομένα θέσης,** τα οποία σύμφωνα με τον ορισμό του άρθ.2, στοιχ.4 του **Ν. 3471/2006** αποτελούν «*τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών*

και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μίας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών». Αποτελεί καινοτομία του ΓΚΠΔ, ότι ρητώς εντάσσονται τα επιγραμμικά αναγνωριστικά ταυτότητας **(online indentifier)**[44], ως στοιχείο ταυτοποίησης. Τα online **αναγνωριστικά ταυτότητας,** παρέχονται από τις συσκευές, τις εφαρμογές, τα εργαλεία και τα πρωτόκολλά τους, όπως για παράδειγμα οι διευθύνσεις διαδικτυακού πρωτοκόλλου (διευθύνσεις IP), τα αναγνωριστικά cookies ή άλλα αναγνωριστικά στοιχεία όπως ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων. Καθοριστική υπήρξε η απόφαση του ΔΕΕ *Scarlet/Sabam*[45], αναφορικά με τις διευθύνσεις IP, *όπου αναγνωρίστηκε ότι* «συνιστούν δεδομένα προσωπικού χαρακτήρα καθόσον καθιστούν δυνατή την πλήρη αναγνώριση των εν λόγω χρηστών».

Τα προσωπικά δεδομένα αφορούν αποκλειστικώς ζώντα πρόσωπα, ενώ η επεξεργασία δεδομένων που αφορούν αποβιώσαντα πρόσωπα ρυθμίζεται μόνο εφόσον και στον βαθμό που αφορούν και ζώντα φυσικά πρόσωπα. Επιπροσθέτως, στο προστατευτικό πεδίο εφαρμογής του ορισμού περί των προσωπικών δεδομένων του ΓΚΠΔ υπάρχει διχογνωμία για το εάν εμπίπτουν τόσο «αντικειμενικές» πληροφορίες όσο και «υποκειμενικές» πληροφορίες, γνώμες ή εκτιμήσεις. Αυτό το είδος των δηλώσεων αποτελεί σημαντικό κομμάτι της επεξεργασίας δεδομένων σε τομείς όπως ο τραπεζικός τομέας για την αξιολόγηση περί φερεγγυότητας ή μη ενός πελάτη[46].

Οι Τράπεζες στην Ελλάδα στο πλαίσιο ανάπτυξης της ελληνικής οικονομίας και του τραπεζικού συστήματος, εντόπισαν την ανάγκη για πρόσβαση σε ακριβή **δεδομένα οικονομικής συμπεριφοράς,** αφού η διάχυση

---

[44] *Ροϊδου, Α. (2021), Η προστασία των προσωπικών δεδομένων στον τραπεζικό χώρο και η χρήση νέων τεχνολογιών, Θεσσαλονίκη, σελ. 36*

[45] *ΔΕΕC-70/10 Scarlet v. Extended SA Societe belge des auteurs, compositeurs et Editeurs SCRL (SABAM), απόφαση της 24ης Νοεμβρίου 2011, Διαθέσιμο στο: https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&lgrec=en&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-70%252F10&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=el&avg=&cid=3771539*

[46] *Βλ. Ροϊδου, ό.π., σελ.35*

αυτών των πληροφοριών συμβάλλουν στην προστασία της πίστης και στη μείωση επισφαλειών προς όφελος του τραπεζικού συστήματος, των συναλλασσομένων πελατών αλλά και εν γένει της εθνικής οικονομίας[47]. Για το λόγο αυτό, το 1997 ιδρύθηκε από τις Τράπεζες που δραστηριοποιούνται στην Ελλάδα, η «ΤΕΙΡΕΣΙΑΣ Α.Ε.» στην οποία ανατέθηκε η τήρηση ενός Αρχείου Δεδομένων Οικονομικής Συμπεριφοράς[48], το οποίο περιλαμβάνει αρχείο δεδομένων αθέτησης υποχρεώσεων – υποθηκών και προσημειώσεων, αρχείο δεδομένων συγκέντρωσης χορηγήσεων, αρχείο δεδομένων ελέγχου κινδύνων, αρχείο αναφοράς, αρχείο απολεσθέντων κλεμμένων δελτίων ταυτοτήτων και διαβατηρίων, αρχείο δεδομένων καταγγελθεισών συμβάσεων επιχειρήσεων, αρχείο δεδομένων εκχωρημένων απαιτήσεων από συμβάσεις/ πιστοποιήσεις εκτέλεσης δημοσίων έργων, αρχείο δεδομένων εταιρειών από ΦΕΚ και ΓΕΜΗ και σύστημα βαθμολόγησης πιστοληπτικής ικανότητας.

Ειδικότερα, **στο χώρο της ηλεκτρονικής τραπεζικής**, η Τράπεζα ενδέχεται να εκτελεί μια από τις οποιαδήποτε πράξεις επεξεργασίας, όπως ενδεικτικά αυτές καταγράφονται στο άρθ. 4 του ΓΚΠΔ, οι οποίες αφορούν προσωπικά δεδομένα είτε υποψήφιων είτε υφιστάμενων πελατών και γενικότερα συναλλασσόμενων σε όλα τα στάδια της συναλλακτικής σχέσης, το προσυμβατικό στάδιο έως και κατά την εκτέλεση της σύμβασης συνεργασίας. Τα δεδομένα αυτά παρέχονται είτε απευθείας από το υποκείμενο το δεδομένων είτε από τρίτο φυσικό πρόσωπο είτε νομικό πρόσωπο είτε από δημόσια προσβάσιμες πηγές όπως Δικαστήρια, υποθηκοφυλακεία, κτηματολογικά γραφεία, φορολογικές αρχές, εμπορικά μητρώα κλπ.

Πιο συγκεκριμένα, με γνώμονα τις προβλέψεις **του άρθ.6 του Κώδικα Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα**, το πιστωτικό ίδρυμα ενδέχεται να συλλέγει και επεξεργάζεται τα κάτωθι είδη δεδομένων:

---

[47] *Μήτια, (Α), (2021), Εκτέλεση τραπεζικών εργασιών και προσωπικά δεδομένα στον ελληνικό τραπεζικό τομέα, Θεσσαλονίκη, σελ.39*

[48] *ΤΕΙΡΕΣΙΑΣ Α.Ε., Ποια δεδομένα τηρούνται, Διαθέσιμο στο: https://www.tiresias.gr/el/idiotes/poia-dedomena-tirountai/*

- **Δεδομένα ταυτοποίησης:** όπως το ονοματεπώνυμο, ο αριθμός δελτίου αστυνομικής ταυτότητας ή ο αριθμός του διαβατηρίου, ο αριθμός φορολογικού μητρώου (ΑΦΜ), η Δημόσια Οικονομική Υπηρεσία (ΔΟΥ) όπου ανήκει ο πελάτης, ο Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ), το φύλο, η υπηκοότητα, δείγμα υπογραφής (φυσικής ή ψηφιακής). Τα δεδομένα αυτά παρέχονται απευθείας από το υποκείμενο των δεδομένων, εν προκειμένω δηλαδή από το χρήστη ηλεκτρονικής τραπεζικής ή/ και από δημόσια προσβάσιμες πηγές, ή/ και από δημόσια προσβάσιμα κοινωνικά δίκτυα, όπως το facebook, το twitter.
- **Δεδομένα επικοινωνίας:** όπως η διεύθυνση κατοικίας, η ηλεκτρονική διεύθυνση, ο αριθμός σταθερού/κινητού τηλεφώνου. Τα δεδομένα αυτά επίσης συλλέγονται απευθείας από το υποκείμενο των δεδομένων, ή/ και από δημόσια προσβάσιμες πηγές, ή/ και από δημόσια προσβάσιμα κοινωνικά δίκτυα, όπως το facebook, το twitter. Επιπροσθέτως, είναι πιθανόν να επαληθεύονται και από συνεργαζόμενες με το πιστωτικό ίδρυμα εταιρείες ενημέρωσης οφειλετών (Ν.3758/2009), εταιρείες διαχείρισης απαιτήσεων (Ν. 4354/2015), ή εντολοδόχους δικηγόρους, δικηγορικές εταιρείες ή δικαστικούς επιμελητές.
- **Δημογραφικά δεδομένα:** όπως το φύλο, η εθνικότητα, η οικογενειακή κατάσταση. Τα στοιχεία αυτά ομοίως συλλέγονται απευθείας από το υποκείμενο των δεδομένων, ή/ και από δημόσια προσβάσιμες πηγές, ή/ και από δημόσια προσβάσιμα κοινωνικά δίκτυα, όπως το facebook, το twitter.
- **Δεδομένα οικονομικής και περιουσιακής κατάστασης**: όπως το επάγγελμα, οι αποδοχές, τα εξαρτώμενα μέλη, οι φορολογικές δηλώσεις (τα έντυπα Ε1 και Ε9), τα εκκαθαριστικά σημειώματα, οι βεβαιώσεις ασφαλιστικής ή/και φορολογικής ενημερότητας. Τα εν λόγω δεδομένα συλλέγονται είτε απευθείας από το υποκείμενο των δεδομένων είτε από δημόσια προσβάσιμες πηγές, όπως υποθηκοφυλακεία, κτηματολογικά γραφεία κλπ.
- **Δεδομένα αθέτησης οικονομικών υποχρεώσεων:** όπως ακάλυπτες επιταγές, καταγγελίες συμβάσεων δανείων και πιστώσεων, διαταγές πληρωμής, κατασχέσεις και επιταγές προς πληρωμή, αιτήσεις και υπαγωγές σε εξυγίανση ή πτώχευση. Τα εν λόγω δεδομένα συλλέγονται από το πιστωτικό ίδρυμα στο πλαίσιο της συναλλακτικής τους σχέσης από αρχεία

δεδομένων και κυρίως από την εταιρεία με την επωνυμία «ΤΡΑΠΕΖΙΚΑ ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΟΦΟΡΙΩΝ ΑΕ» και διακριτικό τίτλο «ΤΕΙΡΕΣΙΑΣ Α.Ε.» ή οποιαδήποτε άλλη εταιρεία, η οποία επεξεργάζεται δεδομένα οικονομικής συμπεριφοράς στην Ελλάδα ή άλλο κράτος μέλος της Ευρωπαϊκής Ένωσης ή από άλλες πηγές όπως Δικαστήρια.

- **Δεδομένα σχετικά με την πιστοληπτική ικανότητα των υποκειμένων:** τα στοιχεία αυτά αφορούν οφειλές σε πιστωτικά ή και χρηματοδοτικά ιδρύματα. Τα εν λόγω δεδομένα επίσης συλλέγονται από το πιστωτικό ίδρυμα στο πλαίσιο της συναλλακτικής τους σχέσης με τους πελάτες είτε από άλλα πιστωτικά ιδρύματα, όταν αυτό είναι επιτρεπτό είτε από αρχεία δεδομένων οικονομικής συμπεριφοράς και κυρίως από την «ΤΕΙΡΕΣΙΑΣ Α.Ε.» ή οποιαδήποτε άλλη εταιρεία η οποία επεξεργάζεται δεδομένα οικονομικής συμπεριφοράς στην Ελλάδα ή άλλο κράτος μέλος της Ευρωπαϊκής Ένωσης.
- **Δεδομένα σχετικά με τη συναλλακτική συμπεριφορά του πελάτη:** τα δεδομένα αυτά απορρέουν και συλλέγονται είτε κατά την εκτέλεση της σύμβασης/συμβάσεων με το πιστωτικό ίδρυμα όπως από τη χρήση των προϊόντων και υπηρεσιών του πιστωτικού ιδρύματος (πιστωτικές ή χρεωστικές κάρτες). Επιπροσθέτως, τα δεδομένα αυτά μπορεί να συλλέγονται και από δημόσια προσβάσιμα κοινωνικά δίκτυα.
- **Δεδομένα πιστωτικής βαθμολόγησης (credit scoring- credit profiling):** τα δεδομένα αυτά είτε παράγονται από το πιστωτικό ίδρυμα, είτε συλλέγονται από την «ΤΕΙΡΕΣΙΑΣ Α.Ε.» ή οποιαδήποτε άλλη εταιρεία η οποία επεξεργάζεται δεδομένα οικονομικής συμπεριφοράς στην Ελλάδα ή άλλο κράτος μέλος της Ευρωπαϊκής Ένωσης και έχουν στόχο τη βαθμολόγηση της πιστοληπτικής ικανότητας ενός ιδιώτη ή μιας επιχείρησης, η οποία γίνεται σύμφωνα με στατιστική ανάλυση της προγενέστερης συναλλακτικής συμπεριφοράς τους και αξιοποιείται από την κάθε τράπεζα βάσει του δικού της συστήματος εγκρίσεων χορηγήσεων.
- **Δεδομένα ηλεκτρονικής ταυτοποίησης του πελάτη και σύνδεσης στις υπηρεσίες και εφαρμογές ηλεκτρονικής τραπεζικής:** όπως δεδομένα για τη διενέργεια συναλλαγών, όπως η φύση/ το είδος της συναλλαγής, ο χρόνος και ο

τόπος συναλλαγής, διευθύνσεις διαδικτυακού πρωτοκόλλου (IP Address) ή άλλα online αναγνωστικά στοιχεία ταυτότητας, δεδομένα θέσης. Τα δεδομένα αυτά συλλέγονται απευθείας από τον πελάτη από συσκευές ή εφαρμογές που χρησιμοποιεί, κατόπιν **σχετικής ενημέρωσης και παροχής σχετικής συγκατάθεσης,** με εξαίρεση την περίπτωση όπου η συλλογή είναι απαραίτητη τη λειτουργία του συστήματος του πιστωτικού ιδρύματος, όπως τα βασικά cookies.

- **Δεδομένα επικοινωνίας του πελάτη με το πιστωτικό ίδρυμα:** όπως δια ζώσης ή τηλεφωνικές ή ηλεκτρονικές συνομιλίες, συμπεριλαμβανομένων ενδεικτικά υποβαλλόμενων παραπόνων και αιτημάτων, που καταγράφονται κατόπιν προηγούμενης ενημέρωσης σύμφωνα με το κατά περίπτωση θεσμικό πλαίσιο.

- **Δεδομένα σχετικά με τη διενέργεια πράξεων πληρωμών και παροχής υπηρεσιών πληρωμών:** ενδεικτικά μπορεί να αφορούν σε δεδομένα για την εκτέλεση των εντολών μεταφοράς χρημάτων από / σε λογαριασμό, δεδομένα τραπεζικών εμβασμάτων, περιπτώσεις πάγιας εντολής. Σε αυτή την περίπτωση είναι πιθανό να περιλαμβάνονται και δεδομένα τρίτων προσώπων που συνδέονται με την εκάστοτε διενέργεια συναλλαγής είτε ως πληρωτές είτε ως δικαιούχοι. Τα δεδομένα αυτά συλλέγονται είτε από τον πελάτη είτε από τον πάροχο υπηρεσιών πληρωμών που έχει επιλέξει.

- **Δεδομένα που χρησιμοποιούνται για την αξιολόγηση κινδύνου νομιμοποίησης εσόδων από παράνομες δραστηριότητες, ή/και χρηματοδότησης της τρομοκρατίας:** Τα δεδομένα αυτά συλλέγονται είτε απευθείας από το υποκείμενο μέσω των τραπεζικών συναλλαγών που πραγματοποιεί είτε από την «ΤΕΙΡΕΣΙΑΣ Α.Ε.» είτε από αστυνομικές αρχές και αρμόδιους φορείς του εξωτερικού που είναι επιφορτισμένοι με την πρόληψη και καταστολή των εν λόγω εγκλημάτων.

- **Δεδομένα αναφορικά με τις γνώσεις και την εμπειρία του πελάτη στον τομέα των επενδύσεων ή στον τομέα των ασφαλίσεων, τη χρηματοοικονομική κατάσταση, περιλαμβανομένης της ανοχής στον κίνδυνο και τους επενδυτικούς στόχους:** Τα δεδομένα αυτά συλλέγονται

απευθείας από το υποκείμενο και είναι σημαντικά ως προς την κατηγοριοποίηση του πελάτη σε ιδιώτη ή σε επαγγελματία και αντίστοιχα ως προς την ευθύνη της τράπεζας από την παροχή επενδυτικών υπηρεσιών, σύμφωνα με τα προβλεπόμενα στο Ν.3606/2007.

- **Δεδομένα εικόνας από συστήματα βιντεοσκόπησης σε κατάστημα του πιστωτικού ιδρύματος:** Τα δεδομένα αυτά συλλέγονται από την καταγραφή μέσω συστήματος βιντεοσκόπησης στο χώρο του πιστωτικού ιδρύματος, στον οποίο θα πρέπει να υπάρχει η σχετική σήμανση.
- **Δεδομένα που αφορούν παιδιά:** Τα δεδομένα αυτά τηρούνται από την τράπεζα μόνον κατόπιν της παροχής συγκατάθεσης των γονέων ή των ασκούντων τη γονική μέριμνα και για σκοπούς εκπλήρωσης σχετικής συναλλακτικής σχέσης προς όφελος των ανηλίκων.

3.2.2. Ειδικές κατηγορίες προσωπικών δεδομένων υποκειμένων - χρηστών ηλεκτρονικής τραπεζικής

Επιπροσθέτως, αναφορικά με τις **ειδικές κατηγορίες προσωπικών δεδομένων χρηστών ηλεκτρονικής τραπεζικής,** σύμφωνα με **το άρθ. 9 του ΓΚΠΔ**: «*Απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό*».

Παρατηρούμε ότι συγκριτικά με την προϊσχύουσα **Οδ. 1995/46/ΕΚ,** προστέθηκαν στην ειδική κατηγορία δεδομένων ως «ευαίσθητα δεδομένα», **τα γενετικά και τα βιομετρικά δεδομένα** με σκοπό την αδιαμφισβήτητη ταυτοποίηση του προσώπου και εντάχθηκαν επίσης στα ευαίσθητα και τα δεδομένα που αφορούν το γενετήσιο προσανατολισμό. Για τις πληροφορίες που αφορούν ποινικές διώξεις ή καταδίκες, οι οποίες περιλαμβάνονταν στον

προϊσχύοντα Ν. 2472/1997, υπάρχει ξεχωριστή ρύθμιση στο **άρθ. 10 του ΓΚΠΔ.**

Σύμφωνα με τον ορισμό του άρθ.4 περ.13 του ΓΚΠΔ «τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα **γενετικά χαρακτηριστικά** φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου», ιδίως από ανάλυση δεοξυριβονουκλεϊκού οξέος (DNA) ή ριβοζονουκλεϊκούοξέως (RNA) ή από άλλο στοιχείο που επιτρέπει την απόκτηση ισοδύναμων πληροφοριών.

Αναφορικά με τα **βιομετρικά δεδομένα**, κατά το άρθ.4 περ. 14 του ΓΚΠΔ, αφορούν «*δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα*». Έτσι, ενδεικτικά μπορούν να θεωρηθούν ως βιομετρικά δεδομένα τα εξής: η ίρις του ματιού, το δακτυλικό αποτύπωμα, η κατατομή του προσώπου, ο τρόπος βαδίσματος, ο τρόπος πληκτρολόγησης, το ηχόχρωμα της φωνής.

Αναφορικά με τα δεδομένα που αφορούν την **υγεία, κατά το άθρ.4περ. 15 του ΓΚΠΔ**, αυτά είναι «*δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του*»

Ως προς τα **δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα**, δεν συμπεριλαμβάνονται αυτά καθαυτά στον κατάλογο των ειδικών κατηγοριών δεδομένων, σε αντίθεση με την Εκσυγχρονισμένη Σύμβαση 108 του Συμβουλίου της Ευρώπης, η οποία συγκαταλέγει στον κατάλογο των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα **του άρθ. 6**, τα εν λόγω δεδομένα.

Ειδικότερα, στον τραπεζικό τομέα και κατά τη χρήση υπηρεσιών ηλεκτρονικής τραπεζικής, ως προς τις ειδικές κατηγορίες προσωπικών

δεδομένων, εφαρμογή βρίσκει το **άρθ.7.1 του Κώδικα Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα**. Πιο συγκεκριμένα, απαγορεύεται από τα πιστωτικά ιδρύματα η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα οι οποίες αναπτύχθηκαν ανωτέρω.

Εντούτοις, τα πιστωτικά ιδρύματα, σύμφωνα με το άρθ. 7.2 του Κώδικα Δεοντολογίας για την επεξεργασία των προσωπικών δεδομένων, ενδέχεται να προβούν σε επεξεργασία ειδικών κατηγοριών δεδομένων στις εξής περιπτώσεις:

- Κατόπιν της **ρητής συγκατάθεσης του υποκειμένου** για την επεξεργασία αυτού του είδους των δεδομένων στο πλαίσιο της συναλλακτικής σχέσης με το πιστωτικό ίδρυμα. Λόγου χάρη, υποψήφιος πελάτης τράπεζας που επιθυμεί να προχωρήσει σε άνοιγμα ηλεκτρονικού τραπεζικού λογαριασμού, ήτοι τραπεζικής σύμβασης εξ αποστάσεως, δύναται να συναινέσει στην επεξεργασία φωτογραφίας selfie, η οποία θα υποβληθεί σε ειδική τεχνική επεξεργασία και βιομετρική ανάλυση και θα εξεταστεί σε αντιπαραβολή με την αστυνομική του ταυτότητα προκειμένου να πραγματοποιηθεί η ηλεκτρονική του ταυτοποίηση. Επιπροσθέτως, το υποκείμενο δεδομένων μπορεί να παρέχει τη συγκατάθεσή του για επεξεργασία ευαίσθητων προσωπικών δεδομένων που το αφορούν, όταν υποβάλλει αίτημα προς την Τράπεζα για επίτευξη καλύτερων όρων ρύθμισης υφιστάμενης σύμβασης πίστωσης ή εξαίρεσης από περιορισμούς στην ανάληψη μετρητών ή για πραγματοποίηση συναλλαγών με ειδικούς όρους λόγω προβλημάτων υγείας όπως όρασης ακοής, κλπ, τα οποία επικαλείται και οικειοθελώς προσκομίζει τα απαιτούμενα ιατρικά έγγραφα στην Τράπεζα, δεδομένου ότι η επεξεργασία τους εν προκειμένω είναι απαραίτητη για τη διερεύνηση του σχετικού αιτήματος.
- Η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα, τα οποία **έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων,** παραδείγματος χάριν μέσω δημοσιοποίησης σε μέσα κοινωνικής δικτύωσης.
- Η επεξεργασία είναι αναγκαία για **τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων**.

- Η επεξεργασία είναι **αναγκαία για την εκτέλεση της σύμβασης ή το υποκείμενο των δεδομένων έχει άμεσα έννομο συμφέρον**, όπως για την επιλεξιμότητα σε συγκεκριμένη θέση εργασίας, λόγου χάρη σε θέση διαχείρισης χρημάτων.
- Η επεξεργασία είναι αναγκαία **για λόγους ουσιαστικού δημοσίου συμφέροντος,** όπως η διερεύνηση ποινικά διωκόμενης πράξης και για την για την πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και χρηματοδότησης της τρομοκρατίας.

3.2.3. Διαβίβαση προσωπικών δεδομένων υποκειμένων - χρηστών ηλεκτρονικής τραπεζικής σε τρίτες χώρες

Αναφορικά με τη διαβίβαση των προσωπικών δεδομένων των χρηστών ηλεκτρονικής τραπεζικής σε άλλες χώρες, οι τράπεζες θα πρέπει να συμμορφώνονται με τις επιταγές **του άρθ. 12 του Κώδικα Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα και του άρθρ. 44 επ. του ΓΚΠΔ** για διαβιβάσεις δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ή διεθνείς οργανισμούς. Συγκεκριμένα, διαβιβάσεις σε τρίτες εκτός Ε.Ο.Χ. μπορούν να πραγματοποιούνται βάσει απόφασης επάρκειας της Ευρωπαϊκής Επιτροπής (άρθ.45 του ΓΚΠΔ) ή ελλείψει απόφασης, εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία παρέχει τις κατάλληλες εγγυήσεις, συμπεριλαμβανομένων εκτελεστών δικαιωμάτων και ένδικων μέσων για το υποκείμενο των δεδομένων (άρθ.46 του ΓΚΠΔ). Σε περίπτωση που δεν συντρέχει κάποια από τις ανωτέρω προϋποθέσεις, μπορεί να γίνει διαβίβαση, ενδεικτικά: εάν το υποκείμενο συγκατατίθεται ρητά στη διαβίβαση των δεδομένων, ή εάν η διαβίβαση είναι απαραίτητη στο πλαίσιο εκτέλεσης σύμβασης με την τράπεζας, όπως για παράδειγμα για την εκτέλεση μιας εντολής αποστολής εμβάσματος, οπότε τα δεδομένα θα διαβιβασθούν υποχρεωτικά στους φορείς που παρεμβάλλονται, ή εάν η διαβίβαση είναι απαραίτητη για τη θεμελίωση ή άσκηση νομικών αξιώσεων ή ένα η διαβίβαση είναι απαραίτητη για λόγους δημοσίου συμφέροντος.

3.3. Επεξεργασία προσωπικών δεδομένων υποκειμένων - χρηστών ηλεκτρονικής τραπεζικής

Σύμφωνα με τον ορισμό του **άρθ. 4 παρ.2 του ΓΠΚΠΔ, ως επεξεργασία** νοείται: «*κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή*».

Πρόκειται για έναν τεχνολογικά ουδέτερο ορισμό και αρκετά ευρύ, καθώς η επεξεργασία προσωπικών δεδομένων αφορά σε κάθε πράξη που διενεργείται σε δεδομένα προσωπικού χαρακτήρα από τη συλλογή τους έως την καταστροφή τους και έτσι επεξεργασία μπορεί να συνιστούν κι άλλες ενέργειες, οι οποίες δεν καταγράφονται στον παραπάνω ορισμό. Η επεξεργασία καλύπτει την αυτοματοποιημένη όσο και μη αυτοματοποιημένη επεξεργασία και σύμφωνα με το Συμβούλιο της Ευρώπης, στην έννοια της επεξεργασίας περιλαμβάνεται και η χειροκίνητη επεξεργασία.

Παρότι τα χρηματοοικονομικά δεδομένα δε θεωρούνται ευαίσθητα δεδομένα βάσει της Εκσυγχρονισμένης Σύμβασης 108 ή του ΓΠΔ, για την επεξεργασία τους απαιτούνται ιδιαίτερες εγγυήσεις, ώστε να διασφαλίζεται η ακρίβεια και η ασφάλεια των δεδομένων.[49] Η επεξεργασία των προσωπικών δεδομένων των υποκειμένων – χρηστών ηλεκτρονικής τραπεζικής, θα πρέπει να διέπεται από συγκεκριμένες αρχές και να πληροί συγκεκριμένες προϋποθέσεις ώστε να είναι επιτρεπτή από το πιστωτικό ίδρυμα. Οι εν λόγω αρχές και βάσεις νομιμότητας της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα στα πλαίσια χρήσης ηλεκτρονικής τραπεζικής αναπτύσσεται κάτωθι.

---

[49] *Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ένωσης σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, Διαθέσιμο στο:* https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf *σελ.434,*

3.3.1 Γενικές αρχές που διέπουν την επεξεργασία των προσωπικών δεδομένων των υποκειμένων - χρηστών ηλεκτρονικής τραπεζικής

Κατά το **άρθ. 5 του ΓΚΠΔ,** η επεξεργασία των προσωπικών δεδομένων (απλών και ειδικών κατηγοριών) των χρηστών ηλεκτρονικής τραπεζικής θα πρέπει να διεξάγεται υπό το πρίσμα συγκεκριμένων αρχών, όπως αυτές καθορίζονται τόσο στο άρθ. 5 του ΓΚΠΔ όσο και στο άρθ. 3 του Κώδικα Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα. Οι αρχές αυτές, οι οποίες δεσμεύουν τα πιστωτικά ιδρύματα που λειτουργούν ως υπεύθυνοι επεξεργασίας των προσωπικών δεδομένων των χρηστών της ηλεκτρονικής τραπεζικής είναι οι εξής:

- **Αρχή νομιμότητας, αντικειμενικότητας και διαφάνειας**: Η εν λόγω αρχή καταγράφεται στο άρθ. 5 παρ.1. στοιχ. α΄ του ΓΚΠΔ, βάσει της οποίας τα προσωπικά δεδομένα των χρηστών θα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο, σε σχέση με το υποκείμενο των δεδομένων. Αντίστοιχα η εν λόγω αρχή κατοχυρώνεται και στα άρθ.8 παρ.2 και άρθ. 52 παρ.2 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Η θέσπιση της εν λόγω αρχής έχει ως σκοπό την προστασία του υποκειμένου σε περιπτώσεις όπου συχνά δεν λαμβάνει γνώση ότι τα προσωπικά του δεδομένα που τον αφορούν υπόκεινται σε επεξεργασία και ιδίως για τους σκοπούς για τους οποίους συλλέγονται και επεξεργάζονται όπως παραδείγματος χάρη στο πλαίσιο της συμπεριφορικής διαφήμισης. Τα πιστωτικά ιδρύματα, ως υπεύθυνοι επεξεργασίας θα πρέπει για αυτό το λόγο να λαμβάνουν τα κατάλληλα μέτρα ώστε να τηρούν τα υποκείμενα των δεδομένα ενήμερα. Όπως προκύπτει και από την αιτ. σκ. 39 του ΓΚΠΔ, η αρχή της διαφάνειας σημαίνει ότι η **ενημέρωση του υποκειμένου θα πρέπει να γίνεται με σαφή, συνοπτική και απλή διατύπωση**, ώστε οι ενδιαφερόμενοι να έχουν επίγνωση των κινδύνων, των κανόνων εγγυήσεων και του τρόπου που μπορούν να ασκούν τα δικαιώματα τους αναφορικά την επεξεργασία των δεδομένων τους. Η υποχρέωση αυτή απορρέει από την τραπεζική πληροφόρηση ή άλλως

υποχρέωση ενημέρωσης η οποία θα πρέπει να εκπληρώνεται από τον προμηθευτή, πριν την κατάρτιση της αρχικής σύμβασης η οποία θα μπορούσε να χαρακτηριστεί ως σύμβαση πλαίσιο, όπως η δυνατότητα χρήσης e–banking και αφορά πληροφορίες ως προς την ταυτότητα, τη δραστηριότητα του προμηθευτή και την ίδια τη χρηματοοικονομική υπηρεσία.

- **Αρχή του σαφούς και περιορισμού σκοπού**: Σύμφωνα με το άρθ. 5 παρ.1 στοιχ. β' του ΓΚΠΔ και το άρθ.8του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, τα δεδομένα του ενδιαφερόμενου υποκειμένου πρέπει να συλλέγονται για σκοπούς καθορισμένους, ρητούς, σαφείς και νόμιμους και μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς αυτούς τους σκοπούς. Περαιτέρω επεξεργασία δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς μόνο όταν λαμβάνει χώρα για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, όπως ρυθμίζεται στο άρθ. 89 παρ. 1 του ΓΚΠΔ. Συνιστά κεντρικό πυλώνα της ρύθμισης της επεξεργασίας των δεδομένων ότι **η νομιμότητα της επεξεργασίας είναι συνάρτηση του σκοπού της επεξεργασίας**. Κάθε νέος σκοπός επεξεργασίας που δεν είναι συμβατός με τον προηγούμενο, θα πρέπει να ερείδεται σε δική του νομική βάση. Ως προς τους προκαθορισμένους, ρητούς και νόμιμους σκοπούς ώστε να είναι επιτρεπτή η επεξεργασία των δεδομένων από τα πιστωτικά ιδρύματα γίνεται ειδική αναφορά στο κεφάλαιο που ακολουθεί τούτου.

- **Αρχή ελαχιστοποίησης των δεδομένων/αρχή αναλογικότητας:** Σύμφωνα με το άρθ. 5 παρ.1 στοιχ. γ' του ΓΚΠΔ, τα δεδομένα που θα υποβληθούν σε επεξεργασία θα πρέπει να είναι **κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία**. Η συγκεκριμένη αρχή αποτελεί έκφανση της αρχής της αναλογικότητας, όπως αυτή κατοχυρώνεται στο άρθ. 25 παρ.1 του Συντάγματος. Σύμφωνα μάλιστα με τον Οργανισμό Θεμελιωδών Δικαιωμάτων της ΕΕ, ως αναλογικότητα θεωρείται ότι τα πλεονεκτήματα από τον περιορισμό ενός δικαιώματος θα πρέπει να υπερτερούν σε σχέση με τα μειονεκτήματα που

αυτός συνεπάγεται αναφορικά με την άσκηση των διακυβευόμενων θεμελιωδών δικαιωμάτων.[50]

- **Αρχή της ακρίβειας των δεδομένων / επικαιροποίηση:** Βάσει του άρθ. παρ.1 στοιχ. δ' του ΓΚΠΔ αλλά και του άρθ. 9 του Κώδικα Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα, τα δεδομένα πρέπει να είναι **ακριβή** και να κοινοποιούνται σε αποδέκτες που έχουν αυτό το δικαίωμα. Εφόσον απαιτείται τα δεδομένα θα πρέπει να επικαιροποιούνται, ενώ παράλληλα το πιστωτικό ίδρυμα ως υπεύθυνος επεξεργασίας θα πρέπει να λαμβάνει τα κατάλληλα μέτρα για την άμεση διόρθωση ή διαγραφή των δεδομένων που είναι ανακριβή σε σχέση με τους επιδιωκόμενους σκοπούς επεξεργασίας. Η υποχρέωση ελέγχου ακρίβειας των προσωπικών δεδομένων θεωρείται απαραίτητο στοιχείο της ποιότητας ώστε να αποτραπεί τυχόν βλάβη στα έννομα συμφέροντα των συναλλασσόμενων με το πιστωτικό ίδρυμα πελατών αναφορικά με την πιστοληπτική του ικανότητα τους. Χαρακτηριστικό είναι το παράδειγμα όπου ένα πρόσωπο επιθυμεί να συνάψει σύμβαση δανείου με πιστωτικό ίδρυμα, όταν σε περίπτωση που μια βάση δεδομένων της Τράπεζας παρέχει ανακριβή ή παρωχημένα στοιχεία για τον ενδιαφερόμενο, αυτό μπορεί να λειτουργήσει εις βάρος του[51].

- **Αρχή του καθορισμού του χρονικού διαστήματος επεξεργασίας /περιορισμός της περιόδου αποθήκευσης:** Κατά το άρθ. 5 παρ.1 στοιχ. ε' του ΓΚΠΔ, σε συνδυασμό με το άρθ. 5 παρ. 4 στοιχ. ε' της Εκσυγχρονισμένης Σύμβασης 108 και το άρθ. 10του Κώδικα Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα, προβλέπεται ότι τα προσωπικά δεδομένα θα πρέπει τηρούνται από τον υπεύθυνο επεξεργασίας σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων **μόνο για το χρονικό διάστημα που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας**. Σύμφωνα μάλιστα με την αιτ. σκ. 39 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας θα πρέπει να ορίζει προθεσμίες για τη διαγραφή τους ή για την περιοδική επανεξέτασή τους.

---

[50] Βλ.Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ένωσης, ό.π., σελ.55

[51]Βλ.Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ένωσης, ό.π., σελ.166

Εξαίρεση από την εν λόγω αρχή μπορεί να υπάρξει στην περίπτωση της αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, καθώς μπορεί να επιτραπεί η διατήρηση των δεδομένων για μεγαλύτερο χρονικό διάστημα, μόνο εάν τα εν λόγω δεδομένα χρησιμοποιηθούν για αυτούς τους σκοπούς. Επιπροσθέτως, στο άρθ. 11 της Εκσυγχρονισμένης Σύμβασης 108, προβλέπονται επίσης εξαιρέσεις, εάν προκύπτει υποχρέωση εκ του νόμου για την άσκηση, θεμελίωση και υπεράσπιση αξιώσεων που είναι αναγκαίες και ανάλογες προς την επιδίωξη περιορισμού αριθμού θεμιτών σκοπών, όπως μεταξύ άλλων η προστασία της εθνικής ασφάλειας, η διερεύνηση και δίωξη ποινικών αδικημάτων, η εκτέλεση ποινικών κυρώσεων, η προστασία του υποκειμένου των δεδομένων και η προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών άλλων προσώπων. Ειδικότερα, στον τραπεζικό τομέα, τα προσωπικά δεδομένα τηρούνται για όσο χρονικό διάστημα είναι απαραίτητο για την εκπλήρωση σκοπού που εξυπηρετεί την επεξεργασία τους, διαφορετικά για τον ελάχιστο χρόνο που απαιτεί η εκάστοτε ισχύουσα νομοθεσία για τη λειτουργία των πιστωτικών ιδρυμάτων και **σε κάθε περίπτωση όχι για μεγαλύτερο διάστημα των είκοσι ετών** από τη λήξη σύμβασης ή της συναλλαγής, σύμφωνα με τα προβλεπόμενα στο άρθ. 249 του ΑΚ περί γενικής παραγραφής αξιώσεων. Σε περίπτωση που υφίσταται σε εξέλιξη δικαστική υπόθεση που αφορά άμεσα ή έμμεσα το υποκείμενο δεδομένων, ο χρόνος αυτός παρατείνεται μέχρι την έκδοση αμετάκλητης δικαστικής απόφασης. Όταν παρέλθει το χρονικό διάστημα τήρησης, η Τράπεζα θα πρέπει να μεριμνήσει για την καταστροφή των αρχείων που εμπεριέχουν τα σχετικά δεδομένα.

- **Αρχή της ενδεδειγμένης ασφάλειας (ακεραιότητας και της εμπιστευτικότητας)**: Σύμφωνα με το άρθ. 5 παρ.1 στοιχ. στ' του ΓΚΠΔ και σε συνδυασμό με την αιτ. σκ. 39 του ΓΚΠΔ και το άρθ. 7 της Εκσυγχρονισμένης Σύμβασης 108, τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία από τον υπεύθυνο επεξεργασίας κατά τέτοιο τρόπο ώστε να εγγυάται την ενδεδειγμένη ασφάλεια. Η αρχή της ασφάλειας δεσμεύει εν προκειμένω τα πιστωτικά ιδρύματα να λαμβάνουν **τα κατάλληλα τεχνικά και οργανωτικά μέτρα κατά**

την επεξεργασία δεδομένων προσωπικού χαρακτήρα για προστασία κατά τυχαίας, μη εξουσιοδοτημένης ή παράνομης πρόσβασης, χρήσης, τροποποίησης, κοινολόγησης, απώλειας, καταστροφής ή φθοράς. Αναφορικά με τα τεχνικά και οργανωτικά μέτρα, σύμφωνα με το άρθ. 32 του ΓΠΔ, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία, θα πρέπει να λαμβάνουν υπόψη «*τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων*» *όταν εφαρμόζουν τέτοια μέτρα.* Τα κατάλληλα τεχνικά και οργανωτικά μέτρα ανάλογα με τις ειδικές συνθήκες μπορούν να περιλαμβάνουν την **ψευδωνυμοποίηση**, ήτοι τη διαδικασία ώστε τα δεδομένα να μην μπορούν να αποδοθούν πλέον σε συγκεκριμένο υποκείμενο, την **κρυπτογράφηση** και/ή τη διασφάλιση του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση, τη δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο, την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των μέτρων. Ειδικά για τα πιστωτικά ιδρύματα, σημαντική για την εγγύηση της ενδεδειγμένης ασφάλειας των δεδομένων των χρηστών τους είναι η τήρηση εγκεκριμένου κώδικα δεοντολογίας, κατά τις προβλέψεις του άρθ. 40 του ΓΚΠΔ ή εγκεκριμένου μηχανισμού πιστοποίησης, κατά το άρθ. 42 του ΓΚΠΔ, η οποία συμβάλλει στην απόδειξη της απαίτησης συμμόρφωσης τους.

- **Αρχή της λογοδοσίας του υπεύθυνου επεξεργασίας:** Προβλέπεται στο άρθ. 5 παρ.2 του ΓΚΠΔ και στο άρθ. 10 παρ.1 της Εκσυγχρονισμένης Σύμβασης 108και αποτελεί μια νέα ρύθμιση σε σχέση με τις ρυθμίσεις της Οδηγίας 95/46/ΕΚ, βάσει της οποίας ο υπεύθυνος επεξεργασίας και εν προκειμένω τα πιστωτικά ιδρύματα, φέρει την ευθύνη και πρέπει να επιδεικνύει και να αποδεικνύει να αποδείξει τη συμμόρφωσή του με τον ΓΚΠΔ τόσο στο ευρύ κοινό όσο και ενώπιον των εποπτικών αρχών και των δικαστηρίων. Πέραν του υπευθύνου επεξεργασίας, θα πρέπει και ο εκτελών την επεξεργασία να

συμμορφώνεται με υποχρεώσεις που αφορούν τη λογοδοσία, όπως η τήρηση αρχείου πράξεων επεξεργασίας και διορισμός του υπευθύνου προστασίας δεδομένων[52].

3.3.2. Νομιμότητα επεξεργασίας προσωπικών δεδομένων των υποκειμένων - χρηστών ηλεκτρονικής τραπεζικής

Προκειμένου να θεωρείται **σύννομη** η επεξεργασία των προσωπικών δεδομένων των χρηστών της ηλεκτρονικής τραπεζικής από το πιστωτικό ίδρυμα, θα πρέπει πέραν της τηρήσεως των βασικών αρχών επεξεργασίας που αναπτύχθηκαν ανωτέρω, να συντρέχει τουλάχιστον μία από **τις βάσεις νομιμότητας επεξεργασίας,** οι οποίες προβλέπονται στο άρθ. 6 του ΓΚΠ**,** ήτοι:

- **Έχει παρασχεθεί η συγκατάθεση του υποκειμένου των δεδομένων-χρήστη ηλεκτρονικής τραπεζικής:** Έτσι, σύμφωνα με το άρθ.6 παρ. 1.στοιχ. *α':* «*Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον το υποκείμενο των δεδομένων* έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς».

Ως προς την **έννοια της συγκατάθεσης**, γίνεται αναφορά στον ορισμό του άρθ. 4 περ. 11 του ΓΚΠΔ, στην αιτ. σκ. 32 του ΓΚΠΔ, στο άρθ. 5 παρ. 2 της Εκσυγχρονισμένης Σύμβασης 108 καθώς και ειδικότερα στο άρθ. 5 του Κώδικα Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα. Σύμφωνα με τα οριζόμενα στην προαναφερόμενη νομοθεσία συγκατάθεση συνιστά «***κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, εν πλήρειεπιγνώσει και αδιαμφισβήτητη, 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***».

Κατά την Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης, δεν επιτρέπεται να ασκείται άμεση ή έμμεση ή αδικαιολόγητη επιρροή ή πίεση,

---

[52] *Βλ.Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ένωσης, ό.π., σελ.177*

οικονομικού ή άλλου χαρακτήρα στο υποκείμενο των δεδομένων και κάθε στοιχείο «ανάρμοστης πίεσης ή επιρροής» θεωρείται πως δεν επιτρέπει στο υποκείμενο να ασκήσει ελεύθερα τη βούλησή του. Περαιτέρω, οι προϋποθέσεις για τη συγκατάθεση, καταγράφονται στο **άρθ.7 του ΓΚΠΔ,** βάσει του οποίου, ο υπεύθυνος επεξεργασίας φέρει το βάρος της απόδειξης σχετικά με τη λήψη συγκατάθεσης, η οποία θα πρέπει να είναι ειδική, να ανακαλείται ελεύθερα και πρέπει να λαμβάνεται υπόψη εάν σε μια σύμβαση για παροχή υπηρεσίας τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων, που δεν είναι απαραίτητη για την εκτέλεση της εν λόγω σύμβασης

Ειδικότερα, κατά την επεξεργασία των προσωπικών δεδομένων του χρήστη ηλεκτρονικής τραπεζικής από το πιστωτικό ίδρυμα, προκειμένου η επεξεργασία των δεδομένων του να θεωρείται σύννομη, θα πρέπει η συγκατάθεση ή η άρνηση αυτής να **παρέχεται ελεύθερα**, **με προσιτό τρόπο**, **με θετική ενέργεια** και όχι δια παραλείψεως, **να είναι ειδική** και να παρέχεται μετά από ειδική και κατανοητή ενημέρωση από το πιστωτικό ίδρυμα. Όταν μάλιστα η επεξεργασία των δεδομένων έχει πολλαπλούς και διαφορετικούς σκοπούς, θα πρέπει να παρέχεται ξεχωριστή ενημέρωση από τον υπεύθυνο επεξεργασίας και αντίστοιχη συγκατάθεση για τον εκάστοτε σκοπό, όπου αυτή απαιτείται προς διασφάλιση του ελέγχου και της διαφάνειας. Η συγκατάθεση μπορεί να δοθεί με πρόσφορο τρόπο κατά τις περιστάσεις, όπως με έγγραφο, με μαγνητοφωνημένη τηλεφωνική επικοινωνία ή με ηλεκτρονικό ή άλλο μέσο που καθιστά εφικτή την ταυτοποίηση του υποκειμένου και την απόδειξη της εκδήλωσης βούλησής του.

- **Η επεξεργασία είναι σύννομη όταν είναι απαραίτητη στο πλαίσιο εκτέλεσης της σύμβασης ή πριν από τη σύναψη της σύμβασης με την Τράπεζα:** Σύμφωνα με το **άρθ.6 παρ. 1.**στοιχ. β' «η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης». Ειδικότερα, στον τομέα της ηλεκτρονικής τραπεζικής, η τράπεζα μπορεί να προβεί σε επεξεργασία προσωπικών δεδομένων των πελατών της είτε κατά την έναρξη της

συναλλακτικής τους σχέσης είτε μεταγενέστερα για σκοπούς που προβλέπονται και στο άρθρ. 4 του Κώδικα Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα**.** Πιο συγκεκριμένα, στο πλαίσιο εκτέλεσης της σύμβασης ή πριν από τη σύναψη της , η επεξεργασία των δεδομένων μπορεί να εξυπηρετεί σκοπούς όπως: για την ταυτοποίηση και για την επαλήθευση των στοιχείων των πελατών, για την επικοινωνία με τους πελάτες είτε σε προσυμβατικό στάδιο, είτε κατά τη διάρκεια της σύμβασης για ζητήματα που αφορούν τη συναλλακτική τους σχέση, για την αξιολόγηση αιτημάτων, την κατάρτιση της σύμβασης και την ομαλή εκτέλεσή της και εν γένει τη διασφάλιση των υποχρεώσεων της τράπεζας, την εξυπηρέτηση, διεκπεραίωση των συναλλαγών και την εν γένει παροχή προϊόντος ή και υπηρεσίας της Τράπεζας, για την εξυπηρέτηση, υποστήριξη, εκτέλεση και παρακολούθηση των συναλλαγών μέσω ηλεκτρονικής τραπεζικής (e-banking), για την αξιολόγηση της δυνατότητας διάθεσης προϊόντος ή υπηρεσίας καθώς και για την αξιολόγηση καταλληλότητας κατά την παροχή επενδυτικών ή παρεπόμενων υπηρεσιών.

- **Η επεξεργασία είναι σύννομη όταν είναι απαραίτητη για τη συμμόρφωση της Τράπεζας με τις έννομες υποχρεώσεις της:** Σύμφωνα με το **άρθ.6 παρ. 1.**στοιχ. β' *«η επεξεργασία είναι σύννομη όταν είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας».*

Έτσι, το τραπεζικό ίδρυμα μπορεί να συλλέγει και να επεξεργάζεται σύννομα δεδομένα των χρηστών στο πλαίσιο συμμόρφωσης με τις υποχρεώσεις που θεσπίζονται με το εκάστοτε νομοθετικό πλαίσιο, όπως ενδεικτικά: για την πρόληψη και καταστολή νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας, η οποία απορρέει από το Ν.4557/2018 καθώς και την αποτροπή της απάτης κατά της Τράπεζας ή/και των πελατών της, όπως και κάθε άλλης παράνομης πράξης, για την εκτίμηση της πιστοληπτικής ικανότητας του πελάτη, για την αξιολόγηση της γνώσης και εμπειρίας του πελάτη στον επενδυτικό τομέα και κάθε άλλης αξιολόγησης ή κατηγοριοποίησης του πελάτη σύμφωνα με την Οδ.2014/65/ΕΕ(MIFID II), για την καταγραφή και αρχειοθέτηση εντολών των πελατών, συμπεριλαμβανομένης της ηχογράφησης εντολών που δίνονται τηλεφωνικώς, για την καταγραφή και

τήρηση αρχείου τηλεφωνικών επικοινωνιών στο πλαίσιο ενημέρωσης των οφειλετών για ληξιπρόθεσμες οφειλές, σύμφωνα με το Ν. 3758/2009.

- **Η επεξεργασία είναι σύννομη όταν είναι απαραίτητη για τους σκοπούς των εννόμων συμφερόντων που επιδιώκει η Τράπεζα**: Σύμφωνα με το άρθ.6 παρ. 1.στοιχ. στ' *«η επεξεργασία είναι σύννομη όταν* η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί».

Εν προκειμένω, η επεξεργασία δεδομένων προσωπικού χαρακτήρα του χρήστη ηλεκτρονικής τραπεζικής από το πιστωτικό ίδρυμα είναι σύννομη όταν εξυπηρετεί σκοπούς προς διαφύλαξη των έννομων συμφερόντων της, οι οποίοι μπορεί να είναι ενδεικτικά: για την ασφάλεια των πληροφοριακών συστημάτων της Τράπεζας, των εγκαταστάσεων και περιουσιακών στοιχείων της συμπεριλαμβανομένου του συστήματος βιντεοεπιτήρησης, για την πρόληψη και τον εντοπισμό εγκληματικών ενεργειών, για την έρευνα ικανοποίησης των πελατών με σκοπό την ανάπτυξη ή και βελτίωση των προϊόντων και υπηρεσιών της Τράπεζας, για την πρόληψη και διαχείριση κινδύνων, για την πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας στο πλαίσιο ταυτοποίησης του χρήστη κατά τη διαδικασίας ανοίγματος τραπεζικού λογαριασμού εξ αποστάσεως μέσω e-banking, για τη μεταβίβαση, εκχώρηση απαιτήσεων από χορηγήσεις ή/και τιτλοποίηση οιουδήποτε ή του συνόλου των βαρών, απαιτήσεων, εγγυήσεων, προνομίων, τίτλων στο πλαίσιο οιασδήποτε συμφωνίας του πελάτη με την Τράπεζα, σε οποιονδήποτε τρίτο καθώς και για την άσκηση αξιώσεων και υπεράσπισης εννόμων συμφερόντων ενώπιων των Δικαστηρίων ή άλλων φορέων εξωδικαστικής επίλυσης διαφορών.

3.3.3. Τραπεζικό απόρρητο

Τα χρηματοπιστωτικά ιδρύματα, στο πλαίσιο της συνεργασίας με τους πελάτες τους όπως αναπτύχθηκε και παραπάνω συλλέγουν και επεξεργάζονται πληθώρα προσωπικών δεδομένων τους. Η υποχρέωση των πιστωτικών ιδρυμάτων **να μην αποκαλύπτουν τις οικονομικές, ή/ και προσωπικές πληροφορίες που περιέρχονται σε αυτά από την επαφή με τους συναλλασσόμενους πελάτες τους σε τρίτους**[53], συνιστά το **γενικό τραπεζικό απόρρητο,** το οποίο ισοδυναμεί ουσιαστικά με την **υποχρέωση της επαγγελματικής εχεμύθειας**. Στο γενικό τραπεζικό απόρρητο εντάσσονται γενικές πληροφορίες των πελατών. Η υποχρέωση αυτή ερείδεται στη σχέση πίστης και εχεμύθειας ανάμεσα στο πιστωτικό ίδρυμα και στον πελάτη, σύμφωνα με τα άρθ. 197, 198, 200, 281,288 του ΑΚ, δεδομένου ότι ο πελάτης ευλόγως προσδοκά ότι δεν θα κοινολογηθούν οι οικονομικές πληροφορίες τους στο πλαίσιο της διαφύλαξης του ιδιωτικού απορρήτου, το οποίο αποτελεί έκφανση του δικαιώματος της προσωπικότητας τους, βάσει της διάταξης του άρθ. 5 παρ.1 του Συντάγματος. Το δικαίωμα αυτό βρίσκει εφαρμογή πέραν των φυσικών προσώπων και στα νομικά πρόσωπα, τα οποία ενδιαφέρονται για τη διατήρηση της καλής τους φήμης και της πίστεως, στοιχεία που επίσης προστατεύονται από το τραπεζικό απόρρητο[54]. Επιπροσθέτως, η εν λόγω νομική υποχρέωση των Τραπεζών, απορρέει από τις νομοθετικές διατάξεις που αφορούν το επαγγελματικό και υπηρεσιακό απόρρητο, όπως οι διατάξεις των αρ. 252 του ΠΚ, αρ. 371 του ΠΚ και κατά το οποίο, τα πιστωτικά ιδρύματα, βαρύνονται με την τήρηση της επαγγελματικής εχεμύθειας σε προσυμβατικό, συμβατικό και μετασυμβατικό στάδιο. Πέραν του γενικού τραπεζικού απορρήτου, υφίσταται και τ**ο ειδικό τραπεζικό απόρρητο, αναφορικά με τις τραπεζικές καταθέσεις, όπως κατοχυρώνεται με το ν.δ. 1059/1971.**

Σε περιπτώσεις ηλεκτρονικής τραπεζικής απάτης, όπως αναπτύχθηκε

---

[53] *Ρόκας Ν./Γκόρτσος Χ./Μικρουλέα Α./Λιβαδά Χ., (2016), Στοιχεία Τραπεζικού Δικαίου, Αθήνα, Νομική Βιβλιοθήκη, σελ.475*

[54] *Καζαντζίδης, Π., (2022), Νομικά ζητήματα προστασίας προσωπικών δεδομένων στον τραπεζικό τομέα και υπολογιστική νέφους, Θεσσαλονίκη, σελ.138*

ανωτέρω, συχνά το θύμα αιτείται να πληροφορηθεί από τη συνεργαζόμενη τράπεζα, τα στοιχεία του δικαιούχου του τραπεζικού λογαριασμού, στον οποίο έγιναν οι αυθαίρετες μεταφορές χρημάτων. Έτσι συχνά παρατηρείται το τραπεζικό απόρρητο να έρχεται σε σύγκρουση με την αξίωση τρίτων για πληροφόρηση. Η λύση θα πρέπει να δίνεται ύστερα από στάθμιση των συγκρουόμενων συμφερόντων σε κάθε περίπτωση. Πάντως, η βασική αρχή είναι ότι το τραπεζικό ίδρυμα δεν είναι υποχρεωμένο να δώσει τις αιτούμενες πληροφορίες και αποφασίζει κατά την κρίση του[55], ενώ κατά κανόνα το τραπεζικό απόρρητο υποχωρεί έναντι εποπτικών, διωκτικών και φορολογικών αρχών.

3.4. Δικαιώματα υποκειμένων – χρηστών ηλεκτρονικής τραπεζικής

Σύμφωνα με έρευνα της Deloitte[56] μετά την εφαρμογή του ΓΚΠΔ, τα υποκείμενα δεδομένα ήταν πιο ενημερωμένα σε ποσοστό που ανήλθε μάλιστα το 80 % σχετικά με τα δικαιώματα που μπορούσαν να ασκήσουν σύμφωνα με τον ΓΚΠΔ σε σχέση με τους προηγούμενους ευρωπαϊκούς κανόνες και διεθνείς κανόνες που υφίσταντο έως το 1995. Ο χρήστης των υπηρεσιών ηλεκτρονικής τραπεζικής μπορεί να ασκήσει τα δικαιώματα του υποκειμένου των δεδομένων, όπως αυτά προβλέπονται στο Κεφάλαιο ΙΙΙ του ΓΚΠΔ αλλά και στο Κεφάλαιο Γ' του Κώδικα Δεοντολογίας για την Επεξεργασία των Προσωπικών Δεδομένων στο Τραπεζικό Σύστημα, όπως έχει δημοσιευτεί από την Ελληνική Ένωση Τραπεζών.

Πρώτα από όλα, το άρθ. 12 του ΓΚΠΔ όπως και το άρθ. 18 του Κώδικα Δεοντολογίας για την Επεξεργασία των Προσωπικών Δεδομένων στο Τραπεζικό Σύστημα, έχει το χαρακτήρα γενικής ρήτρας για την άσκηση των δικαιωμάτων του υποκειμένου, καθώς προβλέπεται η υποχρέωση του υπεύθυνου επεξεργασίας να λαμβάνει τα κατάλληλα μέτρα για να ικανοποιεί τα δικαιώματα του υποκειμένου όπως αυτά απαριθμούνται στα άρθ. 13 έως 22 του

[55] Ρόκας Ν./Γκόρτσος Χ./Μικρουλέα Α./Λιβαδά Χ., ό.π., σελ. 480
[56] *Deloitte, ό.π.*

ΓΚΠΔ καθώς και να ανακοινώνει σε αυτό ενδεχόμενη παραβίαση των προσωπικών του δεδομένων, βάσει του άρθ. 34 του ΓΚΠΔ.[57] Πιο συγκεκριμένα, ο πελάτης μιας τράπεζας ως χρήστης υπηρεσιών ηλεκτρονικής τραπεζικής – υποκείμενο δεδομένων, έχει τα ακόλουθα δικαιώματα:

- **Δικαίωμα διαφανούς ενημέρωσης**, σύμφωνα με τις προβλέψεις του άρθ. 13 και 14 του ΓΚΠΔ, του άρθ. 17 του Κώδικα Δεοντολογίας για την Επεξεργασία των Προσωπικών Δεδομένων στο Τραπεζικό Σύστημα καθώς και του άρθ. 8 της Εκσυγχρονισμένης Σύμβασης 108 και συγκεκριμένα: Ο χρήστης των υπηρεσιών ηλεκτρονικής τραπεζικής, έχει το δικαίωμα να ενημερωθεί από το πιστωτικό ίδρυμα για το ποιος επεξεργάζεται τα προσωπικά του δεδομένα (ταυτότητα και στοιχεία επικοινωνίας), τις κατηγορίες των προσωπικών δεδομένων που τηρεί και επεξεργάζεται, την προέλευσή τους, τους σκοπούς επεξεργασίας, τη νόμιμη βάση για την επεξεργασία, τις κατηγορίες των αποδεκτών των δεδομένων προσωπικού χαρακτήρα ένα υπάρχουν καθώς και το χρονικό διάστημα που η Τράπεζα διατηρεί τα δεδομένα. Η Τράπεζα οφείλει να παρέχει σαφείς σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή - με σαφή και απλή διατύπωση και δωρεάν, εκτός αν τα αιτήματα κριθούν υπερβολικά, ιδίως λόγω του επαναλαμβανόμενου χαρακτήρα τους. Ακόμη, σύμφωνα με την **Απόφαση 52/2022** της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα[58], οι πληροφορίες που δίνονται στο υποκείμενο των δεδομένων θα πρέπει να είναι συγκεκριμένες και οριστικές, ενώ η χρήση εκφράσεων όπως «ενδέχεται», «ορισμένος», «συχνά» και «πιθανός» θα πρέπει επίσης να αποφεύγεται. Όταν οι υπεύθυνοι επεξεργασίας δεδομένων επιλέγουν να χρησιμοποιούν αόριστη διατύπωση, θα πρέπει να είναι σε θέση, σύμφωνα με την αρχή της λογοδοσίας, να αποδεικνύουν τον λόγο για τον οποίο η χρήση τέτοιας διατύπωσης δεν ήταν δυνατό να αποφευχθεί και γιατί δεν υπονομεύει τη νομιμότητα της επεξεργασίας» και σε κάθε άλλη περίπτωση ο υπεύθυνος

[57] *Ιγγλεζάκης, ό.π., σελ. 344*

[58] *Απόφαση* ***52/2022*** *της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Επιβολή προστίμου στην AlphaBankγια παράνομη και αδιαφανή επεξεργασία δεδομένων, Διαθέσιμο στο :* *https://www.dpa.gr/sites/default/files/2022-11/52_2022%20anonym.pdf*

επεξεργασίας φέρει το βάρος απόδειξης επί της νομιμότητας της μη ικανοποίησης του δικαιώματος της ενημέρωσης.

- **Δικαίωμα πρόσβασης,** σύμφωνα με τις προβλέψεις του άρθ. 15 του ΓΚΠΔ, του άρθ. 17 του Κώδικα Δεοντολογίας για την Επεξεργασία των Προσωπικών Δεδομένων στο Τραπεζικό Σύστημα καθώς και του άρθ. 8 παρ. 2, εδ. β' του ΧΘΔΕΕ: Ο χρήστης των υπηρεσιών ηλεκτρονικής τραπεζικής, έχει το δικαίωμα να λάβει από την Τράπεζα επιβεβαίωση για το κατά πόσο τα προσωπικά του δεδομένα υφίστανται επεξεργασία και να έχει, να έχει πρόσβαση στα δεδομένα του και στους σκοπούς επεξεργασίας, τις κατηγορίες δεδομένων, τους αποδέκτες,(παρελθόντες, παρόντες και μελλοντικούς), το χρονικό διάστημα αποθήκευσης, στα δικαιώματα του υποκειμένου, στη προέλευση προσωπικών δεδομένων, στην ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, στις εγγυήσεις του άρθρου 46 σχετικά με τις διαβιβάσεις σε τρίτη χώρα ή διεθνή οργανισμό. Σύμφωνα μάλιστα με την παρ.3 του άρθ. 15 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να παρέχει αντίγραφο των προσωπικών δεδομένων που υπόκεινται σε επεξεργασία.

Η άσκηση του δικαιώματος πρόσβασης του υποκειμένου των δεδομένων αποκτά ιδιαίτερη σημασία στις περιπτώσεις τραπεζικής απάτης όπου παραβιάστηκαν τα τραπεζικά δεδομένα του χρήστη υπηρεσιών ηλεκτρονικής τραπεζικής και εν συνέχεια ο πελάτης επικοινωνεί με το αρμόδιο τμήμα της τράπεζας. Όταν στρέφεται νομικά κατά της τράπεζας για να διεκδικήσει την επιστροφή των χρημάτων του, συχνά αιτείται την πρόσβαση και αντίγραφο των εν λόγω ηχογραφημένων τηλεφωνικών συνομιλιών προς επίρρωση των ισχυρισμών του. Το θύμα όμως ορισμένες φορές έρχεται αντιμέτωπο με την άρνηση χορήγησης των τηλεφωνικών συνομιλιών ή την ελλιπή χορήγηση των επίμαχων συνομιλιών που θα αποδείκνυαν εάν η τράπεζα προχώρησε άμεσα σε ενέργειες για τη διαφύλαξη των έννομων συμφερόντων του πελάτη της. Εντούτοις, δέον όπως αναφερθεί η απόφαση **ΜΠρΧίου 245/2022,** σύμφωνα με την οποία κρίθηκε ότι: «ο ενάγων, ως υποκείμενο των δεδομένων, έχει, σύμφωνα με τη διάταξη του άρθρου 15 παρ. 3 του ΓΚΠΔ, δικαίωμα πρόσβασης στις καταγεγραμμένες συνομιλίες με τους υπαλλήλους της τράπεζας και δη της

χορήγησης (έναντι της καταβολής εύλογου τέλους για διοικητικά έξοδα) αντιγράφου των δεδομένων του προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Η **εναγομένη, ως υπεύθυνος επεξεργασίας, κατά τα προαναφερθέντα δεν ικανοποίησε το σχετικώς υποβληθέν δικαίωμα πρόσβασης του πρώτου ενάγοντος ως όφειλε παραβιάζοντας τη διάταξη του άρθρου 15 του ΓΚΠΔ, με συνέπεια να υποστεί εκείνος ζημία και δη ηθική βλάβη από την εν λόγω παραβίασε και να γεννάται υπέρ του τελευταίου αξίωση αποζημίωσης κατά το άρθρου 82 παρ. 1 του ΓΚΠΔ.** Ενόψει των ανωτέρω, το παρόν Δικαστήριο καταλήγει στο συμπέρασμα ότι ο πρώτος ενάγων υπέστη ηθική βλάβη (μη υλική ζημία κατά το άρθρο 82 παρ. 1 του ΓΚΠΔ) από την προαναφερόμενη συμπεριφορά της εναγομένης για την οποία δικαιούται χρηματικής ικανοποίησης.

- **Δικαίωμα διόρθωσης,** σύμφωνα με τις προβλέψεις του άρθ. 16 του ΓΚΠΔ, του άρθ. 20 του Κώδικα Δεοντολογίας για την Επεξεργασία των Προσωπικών Δεδομένων στο Τραπεζικό Σύστημα καθώς του άρθ. 8 της Εκσυγχρονισμένης Σύμβασης 108: Το υποκείμενο των δεδομένων μπορεί να αιτηθεί από το τραπεζικό ίδρυμα τη **διόρθωση** ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν καθώς και τη **συμπλήρωση** των ελλιπών δεδομένων προσωπικού χαρακτήρα. Τα ανακριβή δεδομένα θα πρέπει να διορθώνονται χωρίς αδικαιολόγητη ή υπερβολική καθυστέρηση, ενώ ο υπεύθυνος επεξεργασίας δεν στερείται του δικαιώματος να ζητήσει απόδειξη της επικαλούμενης ανακρίβειας ή έλλειψης με την προσκόμιση σχετικών εγγράφων από τον πελάτη. Αναφορικά μάλιστα με το εν λόγω δικαίωμα, η Αρχή Προστασίας Δεδομένων, αφού εξέτασε το ζήτημα της ακρίβειας και διαδικασίας διόρθωσης δεδομένων, κατόπιν της Απόφασης 57/2018[59] επέβαλε πρόστιμο 10.000,00 Ευρώ κατά της τράπεζας Alpha Bank σχετικά με τηλεφωνικές οχλήσεις για ληξιπρόθεσμες οφειλές που αφορούσαν σε όχληση λάθος πρόσωπο.

[59] *Απόφαση* ***57/2018*** *της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Πρόστιμο σε τράπεζα για μη εκπλήρωσή της να τηρεί και να επεξεργάζεται ακριβή στοιχεία για τους οφειλέτες της, Διαθέσιμο στο:* https://www.dpa.gr/sites/default/files/2019-10/57_2018anonym.pdf

- **Δικαίωμα διαγραφής (δικαίωμα στη λήθη),** σύμφωνα με το άρθ. 17 του ΓΚΠΔ, το άρθ. 21 του Κώδικα Δεοντολογίας για την Επεξεργασία των Προσωπικών Δεδομένων στο Τραπεζικό Σύστημα και το άρθ. 9 παρ. 1, στοιχ. ε' της Εκσυγχρονισμένης Σύμβασης 108: Ο χρήστης υπηρεσιών ηλεκτρονικής τραπεζικής, έχει το δικαίωμα να ζητήσει από την Τράπεζα τη διαγραφή των προσωπικών δεδομένων του από το αρχείο που τηρεί η Τράπεζα, υπό ορισμένες προϋποθέσεις: όπως όταν τα δεδομένα δεν είναι πλέον απαραίτητα, το υποκείμενο έχει ανακαλέσει τη συγκατάθεσή του επί της οποίας βασίζεται η συγκατάθεσηή τα δεδομένα του έχουν υποβληθεί σε παράνομη επεξεργασία. Στο **άρθ. 34 του Ν.4624/2019**, προβλέπονται εξαιρέσεις από το δικαίωμα: α) εάν η διαγραφή σε περίπτωση μη αυτοματοποιημένης επεξεργασίας λόγω της ιδιαίτερης φύσης της αποθήκευσης δεν είναι δυνατή ή είναι δυνατή μόνο με δυσανάλογα μεγάλη προσπάθεια και το συμφέρον του υποκειμένου των δεδομένων για τη διαγραφή δεν θεωρείται σημαντικό, β) στο βαθμό που ο υπεύθυνος επεξεργασίας έχει λόγους να πιστεύει ότι η διαγραφή θα ήταν επιζήμια για τα έννομα συμφέροντα του υποκειμένου των δεδομένων προσωπικού χαρακτήρα και γ) εάν η διαγραφή θα ερχόταν σε σύγκρουση με τις νόμιμες ή συμβατικές περιόδους διατήρησης.
- **Δικαίωμα περιορισμού της επεξεργασίας**, σύμφωνα με το άρθ. 18 του ΓΚΠΔ, το άρθ. 22 του Κώδικα Δεοντολογίας για την Επεξεργασία των Προσωπικών Δεδομένων στο Τραπεζικό Σύστημα: Ο χρήστης υπηρεσιών ηλεκτρονικής τραπεζικής, έχει το δικαίωμα να ζητήσει από την Τράπεζα τον περιορισμό της επεξεργασίας των προσωπικών του δεδομένων, όταν η ακρίβεια των δεδομένων αμφισβητείται, όταν η επεξεργασία είναι παράνομη και το υποκείμενο των δικαιωμάτων αντιτάσσεται στη διαγραφή, όταν τα δεδομένα πρέπει να διατηρηθούν για την άσκηση ή θεμελίωση νομικών αξιώσεων, ή όταν εκκρεμεί απόφαση κατά πόσο οι νόμιμοι λόγοι της Τράπεζας υπερισχύουν έναντι των λόγων του υποκειμένου.
- **Δικαίωμα στη φορητότητα των δεδομένων** σύμφωνα με το άρθ. 20 του ΓΚΠΔ και το άρθ. 24 του Κώδικα Δεοντολογίας για την Επεξεργασία των Προσωπικών Δεδομένων στο Τραπεζικό Σύστημα: Το υποκείμενο των δεδομένων

μπορεί να ζητήσει να λάβει από την Τράπεζα τα προσωπικά του δεδομένα, τα οποία έχει παράσχει σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο καθώς και να ζητήσει από την Τράπεζα να διαβιβάσει δεδομένα που το αφορούν σε άλλον υπεύθυνο επεξεργασίας, χωρίς αντίρρηση από το πιστωτικό ίδρυμα, στις περιπτώσεις που η επεξεργασία βασίζεται στη συγκατάθεση του υποκειμένου ή αφορά στην εκτέλεση της σύμβασης. Στον τραπεζικό τομέα τέτοια περίπτωση φορητότητας είναι αυτή που αφορά στη μεταβίβαση σύμβασης δανείου ή πίστωσης σε άλλο πιστωτικό ίδρυμα ή στην μεταφορά καταθετικού λογαριασμού σε άλλο πιστωτικό ίδρυμα. Σύμφωνα με τις κατευθυντήριες γραμμές της Ομάδας Εργασίας του άρθρου 29[60], το εν λόγω δικαίωμα «αυξάνει τις δυνατότητες επιλογής των χρηστών, τον βαθμό ελέγχου των χρηστών και τη δύναμη των χρηστών», με στόχο να παρέχεται στα υποκείμενα των δεδομένων η δυνατότητα ελέγχου επί των προσωπικών δεδομένων τους.

- **Δικαίωμα εναντίωσης,** σύμφωνα με το άρθ.21 του ΓΚΠΔ και το άρθ. 25 του Κώδικα Δεοντολογίας για την Επεξεργασία των Προσωπικών Δεδομένων στο Τραπεζικό Σύστημα: Το υποκείμενο των δεδομένων έχει το δικαίωμα να εναντιωθεί στην επεξεργασία των προσωπικών του δεδομένων από την Τράπεζα που το αφορούν. Η Τράπεζα θα πρέπει σε αυτή την περίπτωση να σταματήσει να υποβάλλει σε επεξεργασία τα δεδομένα του χρήστη, εκτός εάν καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία, οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου. Θα πρέπει δηλαδή να γίνεται μια στάθμιση συμφερόντων με το βάρος της απόδειξης να το φέρει ο υπεύθυνος της επεξεργασίας. Περαιτέρω, τόσο στο άρθ. 21 παρ. 2 του ΓΚΠΔ και το άρθ. 25 παρ. 2του Κώδικα Δεοντολογίας για την Επεξεργασία των Προσωπικών Δεδομένων στο Τραπεζικό Σύστημα**,** προβλέπεται το ειδικότερο δικαίωμα εναντίωσης στη χρήση δεδομένων προσωπικού χαρακτήρα για σκοπούς απευθείας εμπορικής προώθησης.

---

[60] *Ομάδα εργασίας του άρθρου 29 (2016), Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων, WP 242, 13 Δεκεμβρίου 2016, αναθεωρήθηκαν στις 5 Απριλίου 2017, Διαθέσιμο στο:* https://www.dpa.gr/sites/default/files/2020-05/wp242rev01_el.pdf

- **Δικαίωμα στην αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανόμενης της κατάρτισης προφίλ** (δικαίωμα στην ανθρώπινη παρέμβαση), σύμφωνα με το άρθ. 22 του ΓΚΠΔ, το άρθ. 26 του Κώδικα Δεοντολογίας για την Επεξεργασία των Προσωπικών Δεδομένων στο Τραπεζικό Σύστημα**:**Το υποκείμενο των δεδομένων μπορεί να ζητήσει από την Τράπεζα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, **συμπεριλαμβανομένης της κατάρτισης προφίλ**, η οποία παράγει **έννομα αποτελέσματα που το αφορούν ή το επηρεάζει** σημαντικά με παρόμοιο τρόπο. Κατ' εξαίρεση, είναι επιτρεπτή η λήψη απόφασης που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, όταν: α) είναι αναγκαία για τη σύναψη ή εκτέλεση της σύμβασης μεταξύ πελάτη και τράπεζας όπως στην περίπτωση κατάρτισης πιστοληπτικού προφίλ (credit scoring) αιτούντος για δάνειο ή πίστωσης του δανειολήπτη, β) υπάρχει ρητή πρόβλεψη στο νόμο όπως για την παρακολούθηση και την πρόληψη της απάτης και της φοροδιαφυγής σύμφωνα με το κανονιστικό πλαίσιο της Ένωσης ή των αρχών εποπτείας και προκειμένου να διασφαλιστεί η ασφάλεια και αξιοπιστία των υπηρεσιών που παρέχει το πιστωτικό ίδρυμα ως υπεύθυνος επεξεργασίας και γ) όταν το υποκείμενο των δεδομένων παρέσχε τη ρητή προς τούτου συγκατάθεσή του.

3.5. Προστασία δεδομένων από τον σχεδιασμό και εξ ορισμού στον τομέα της ηλεκτρονικής τραπεζικής

Τα συστήματα ηλεκτρονικών πληρωμών θα πρέπει να διαθέτουν ενσωματωμένη προστασία δεδομένων, δηλαδή τη λεγόμενη προστασία της ιδιωτικής ζωής ή των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού[61] σύμφωνα με τις προβλέψεις του άρθ. 25 του ΓΚΠΔ. Με γνώμονα ότι κατά τη χρήση υπηρεσιών ηλεκτρονικής τραπεζικής, πιθανόν να ανακύπτουν ζητήματα προστασίας των τραπεζικών δεδομένων των χρηστών, πρέπει να

[61] *Βλ. Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ένωσης, ό.π., σελ.434*

χρησιμοποιούνται οι κατάλληλοι μηχανισμοί επαλήθευσης της ταυτότητας του χρήστη της ηλεκτρονικής τραπεζικής και επιβεβαίωσης πριν τη διενέργεια μιας συναλλαγής.

Έτσι, **η προστασία των δεδομένων ήδη από το σχεδιασμό (privacy by design**), κατά την παρ.1 του άρθ.25 του ΓΚΠΔ, επιβάλλει στον υπεύθυνο προστασίας των δεδομένων, εν προκειμένω το τραπεζικό ίδρυμα να εφαρμόζει τα κατάλληλα **τεχνικά** και **οργανωτικά μέτρα,** σχεδιασμένα για την εφαρμογή των αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων και η ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία όπως η διαφάνεια. Η αρχή διατυπώνεται πριν την εφαρμογή του ΓΚΠΔ, ήδη στη ρύθμιση του Ν. 2774/1999 για την προστασία προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα, με έμφαση για την ελαχιστοποίηση των προς επεξεργασία δεδομένων, ενώ αντίστοιχη ρύθμιση περιλαμβάνει και ο Ν. 3979/2011 για την ηλεκτρονική διακυβέρνηση.

Η **προστασία δεδομένων εξ ορισμού**, κατά την παρ. 2 του άρθ. 25 του ΓΚΠΔ, σημαίνει ότι ο υπεύθυνος προστασίας δεδομένων, δηλαδή η Τράπεζα θα πρέπει να διασφαλίζει ότι υπόκεινται σε επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό επεξεργασίας. Αυτή η υποχρέωση αφορά το εύρος των δεδομένων, το βαθμό της επεξεργασίας, την περίοδο της αποθήκευσης και την προσβασιμότητα.

3.6. Εκτίμηση αντικτύπου (DPIA) στην περίπτωση των τραπεζών

Οι πράξεις επεξεργασίας ενέχουν ορισμένους εγγενείς κινδύνους για τα δικαιώματα των υποκειμένων, σε περίπτωση που χαθούν, κοινοποιηθούν σε μη εξουσιοδοτημένα πρόσωπα ή υποβληθούν σε παράνομη επεξεργασία. Πράξεις επεξεργασίας μεγάλης κλίμακας, εγκυμονούν μεγαλύτερους κινδύνους για τα υποκείμενα των δεδομένων. Έτσι, βάσει του άρθ. 35 του ΓΚΠΔ, του άρθ. 13 του Κώδικα του Κώδικα Δεοντολογίας για την Επεξεργασία των Προσωπικών Δεδομένων στο Τραπεζικό Σύστημα και του άρθ. 10 παρ. 2 της Εκσυγχρονισμένης Σύμβασης 108, προβλέπεται ότι όταν ένα είδος επεξεργασίας που τελείται κυρίως με τεχνολογικά μέσα και συνεκτιμώντας τη φύση, το πεδίο

εφαρμογής, το πλαίσιο και τους σκοπούς επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Με αυτό τον τρόπο παρέχεται η δυνατότητα στους οργανισμούς να μετριάζουν τους κινδύνους αρνητικού αντικτύπου στα φυσικά πρόσωπα. Η DPIA απαιτείται ιδίως στην περίπτωση:

- συστηματικής κι εκτενούς αξιολόγησης προσώπων σχετικά με φυσικά πρόσωπα η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία περιλαμβανομένης της κατάρτισης προφίλ
- μεγάλης κλίμακας επεξεργασίας ειδικών κατηγοριών δεδομένων κατά το άρθ. 9 του ΓΚΠΔ, παρ.1 ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθ. 10 του ΓΚΠΔ
- συστηματικής παρακολούθησης δημόσια προσβάσιμων χώρων

Οι εποπτικές αρχές, εν προκειμένω η ΑΠΔΠΧ θα πρέπει να καταρτίζει και να δημοσιοποιεί σχετικούς καταλόγους επεξεργασιών. **Η DPIA είναι υποχρεωτική για τα τραπεζικά ιδρύματα στο πλαίσιο της γενικότερης υποχρέωσης τους για την ενδεδειγμένη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων**. Επιπροσθέτως, αποτελεί σημαντικό εργαλείο στα πλαίσια της αρχής λογοδοσίας και θα πρέπει να περιέχει τουλάχιστον, κατά το άρθ. 35 παρ. 7 του ΓΚΠΔ:

- συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας
- εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας
- εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες
- προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας

3.7. Παραβίαση ασφαλείας προσωπικών δεδομένων υποκειμένων – χρηστών ηλεκτρονικής τραπεζικής και προβλεπόμενες κυρώσεις

Τον Σεπτέμβριο του 2022, η τράπεζα και εταιρεία χρηματοοικονομικής τεχνολογίας «REVOLUT» ανακοίνωσε ότι δέχτηκε κυβερνοεπίθεση από hackers, οι οποίοι κατάφεραν να αποκτήσουν πρόσβαση σε προσωπικά δεδομένα των πελατών της και συγκεκριμένα σε δεδομένα πληρωμής με κάρτες, ονόματα πελατών και στοιχεία επικοινωνίας, όπως ταχυδρομικές και ηλεκτρονικές διευθύνσεις. Ο εκπρόσωπος μάλιστα της εν λόγω εταιρίας αποκάλυψε ότι «ένα μη εξουσιοδοτημένο τρίτο μέρος απέκτησε πρόσβαση στα στοιχεία ενός ποσοστού της τάξης του 0,16 % των πελατών για ένα σύντομο χρονικό διάστημα». Εντούτοις, η εν λόγω παραβίαση είχε ως αποτέλεσμα να αφαιρεθούν παράνομα σχεδόν 20 εκατομμύρια δολάρια ΗΠΑ από τους λογαριασμούς των πελατών[62].

Ως ελέχθη, η τράπεζα επεξεργάζεται τεράστιο όγκο δεδομένων των πελατών της. Ζητήματα εγείρονται σε περιπτώσεις που υφίστανται κενά ασφαλείας στο σύστημα των τραπεζών με αποτέλεσμα να παραβιάζονται τα προσωπικά δεδομένα του χρήστη της ηλεκτρονικής τραπεζικής.

Πρώτα απ' όλα, σύμφωνα με τον ορισμό που δίνεται στο άρθ. 4, στοιχ. 12 ως **παραβίαση ασφαλείας δεδομένων** νοείται η «*παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία». Πιο συγκεκριμένα:*

- **Καταστροφή** δεδομένων προσωπικού χαρακτήρα συντρέχει είτε ότι τα δεδομένα παύουν να υπάρχουν εντελώς είτε συνεχίζουν να υπάρχουν αλλά σε μορφή την οποία δεν μπορεί να τα χρησιμοποιήσει ο υπεύθυνος επεξεργασίας[63].

---

[62] *Jackson,A. (2023) «Revolut hacked as cyber criminals steal US $ 2O m, Cybermagazine, Διαθέσιμοστο: https://cybermagazine.com/cyber-security/revolut-hacked-as-cyber-criminals-steal-us-20m*

[63] *Κανέλλος Λ.,(2020) «THEGDPRHANDBOOK – Για DPOs, Επιχειρήσεις & Οργανισμούς, Αθήνα, Νομική Βιβλιοθήκη, σελ. 48 επ.*

- **Φθορά** δεδομένων προσωπικού χαρακτήρα συμβαίνει όταν τα δεδομένα έχουν μεταβληθεί, έχουν αλλοιωθεί ή δεν είναι πλήρη.
- **Απώλεια** δεδομένων προσωπικού χαρακτήρα υφίσταται σε περίπτωση που τα δεδομένα εξακολουθούν να υπάρχουν κάπου, αλλά ο υπεύθυνος επεξεργασία έχει χάσει πλέον τον έλεγχο τους ή την πρόσβαση σε αυτά, είτε δεν τα έχει πλέον στην κατοχή του.
- **Μη εξουσιοδοτημένη ή παράνομη επεξεργασία** συμβαίνει όταν αποκαλύπτονται τα προσωπικά δεδομένα σε μη εξουσιοδοτημένους παραλήπτες ή υφίσταται οποιαδήποτε άλλη μορφή επεξεργασίας που είναι αντίθετη με τα προβλεπόμενα στον ΓΚΠΔ.

Θα πρέπει να διευκρινιστεί ότι ενώ μια παραβίαση αποτελεί περιστατικό ασφαλείας, ο ΓΚΠΔ βρίσκει εφαρμογή μόνο όταν υπάρχει παραβίαση προσωπικών δεδομένων και συνεπώς ενώ **όλες οι παραβιάσεις προσωπικών δεδομένων είναι περιστατικά ασφαλείας δεν είναι όλα τα περιστατικά ασφαλείας και παραβιάσεις προσωπικών δεδομένων**[64]. Περαιτέρω, οι παραβιάσεις μπορούν να ομαδοποιηθούν σε τρεις κατηγορίες βάσεις των τριών αρχών ασφάλειας των πληροφοριών σε:

- **Παραβίαση εμπιστευτικότητας**: συντρέχει όταν τα προσωπικά δεδομένα αποκαλύφθηκαν σε μη εξουσιοδοτημένα άτομα.
- **Παραβίαση διαθεσιμότητας:** συντρέχει σε περίπτωση απώλειας πρόσβασης ή καταστροφής των δεδομένων.
- **Παραβίαση ακεραιότητας:** συντρέχει όταν υφίσταται αλλοίωση των προσωπικών δεδομένων και δεν είναι ακριβή, ακέραια και γνήσια.

Με γνώμονα ότι μια παραβίαση προσωπικών δεδομένων μπορεί να ενέχει σημαντικές αρνητικές επιπτώσεις για τα υποκείμενα των δεδομένων και εν προκειμένω για τους χρήστες της ηλεκτρονικής τραπεζικής, όπως η απώλεια του ελέγχου του ηλεκτρονικού λογαριασμού (e- banking) και των τραπεζικών δεδομένων τους, την οικονομική απώλεια, τη βλάβη της φήμης και αξιοπιστίας όταν πρόκειται ιδίως για επαγγελματία πελάτη τράπεζας, ο ΓΚΠΔ θέτει

[64] *Κυπραίος, Ι. (2018) «Οι επιπτώσεις του Γενικού Κανονισμού Προστασίας Δεδομένων στον Τραπεζικό Τομέα: Μελέτη Περίπτωσης, Σάμος, σελ. 20 επ.*

συγκεκριμένες υποχρεώσεις γνωστοποίησης της παραβίασης των προσωπικών δεδομένων του χρήστη.

Βάσει του άρθ. 33 του ΓΚΠΔ, επιβάλλεται στον υπεύθυνο επεξεργασίας η υποχρέωση χειρισμού περιστατικού παραβίασης προσωπικών στο πλαίσιο των υποχρεώσεων του για την ασφάλεια της επεξεργασίας[65]. Ο υπεύθυνος επεξεργασίας οφείλει να γνωστοποιήσει στην Αρχή το περιστατικό, εάν **ενδέχεται να προκληθεί κίνδυνος στα δικαιώματα και τις ελευθερίες των προσώπων τα οποία αφορά.** Αν το περιστατικό δεν ενδέχεται να προκαλέσει τέτοιο κίνδυνο, μπορεί να μην απαιτείται γνωστοποίηση στην αρχή, εντούτοις ο υπεύθυνος επεξεργασίας θα πρέπει να το καταγράψει στο εσωτερικό αρχείο που τηρεί η τράπεζα.

Η γνωστοποίηση θα πρέπει να γίνει **αμελλητί,** εντός **72 ωρών** από τη στιγμή που αποκτά γνώση η Τράπεζα και να παρέχονται στην Αρχή συγκεκριμένες πληροφορίες, όπως η φύση της παραβίασης, οι κατηγορίες και κατά προσέγγιση ο αριθμός των θιγομένων, οι κατηγορίες και κατά προσέγγιση ο αριθμός των αρχείων, τα στοιχεία επικοινωνίας, οι ενδεχόμενες επιπτώσεις, τα ληφθέντα και προτεινόμενα μέτρα για την αντιμετώπιση των επιπτώσεων. Σε περίπτωση που αυτές οι πληροφορίες δεν είναι διαθέσιμες κατά την υποβολή της γνωστοποίησης, θα πρέπει σύμφωνα με τις οδηγίες της Αρχής Προστασίας Δεδομένων να υποβληθεί μια αρχική γνωστοποίηση και εν συνεχεία να ακολουθήσει σταδιακά χωρίς αδικαιολόγητη καθυστέρηση συμπληρωματική.

Όταν η παραβίαση προσωπικών δεδομένων, ενδέχεται να θέσει σε **υψηλό κίνδυνο** τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που σχετίζονται με το περιστατικό, τότε υφίσταται η υποχρέωση της τράπεζας **να ανακοινώνει αμελλητί την παραβίαση και στα θιγόμενα αυτά πρόσωπα**, ανεξάρτητα από την προαναφερθείσα γνωστοποίηση στην Αρχή. Η ανακοίνωση αυτή θα πρέπει να γίνεται στο πλαίσιο της αρχής της αναλογικότητας με πρόσφορο και αποτελεσματικό τρόπο, με μορφή προσωποποιημένης πληροφόρησης και όχι μέσω κάποιας γενικής ανακοίνωσης. Στο πλέγμα

---

[65] *Αρχή Προστασίας Δεδομένων, Γνωστοποίηση περιστατικών παραβίασης δεδομένων άρθρα 33-34 ΓΚΠΔ, Διαθέσιμο στο:* https://www.dpa.gr/index.php/el/foreis/asfaleia_dedomenwn/gnwstopoiisi_paraviasis

εξουσιών της Αρχής, κατά το άρθ. 58 παρ. 2 , στοιχ. ε΄ του ΓΚΠΔ, η Αρχή έχει την εξουσία να δώσει εντολή στον υπεύθυνο επεξεργασίας να ενημερώσει το υποκείμενο δεδομένων για την παραβίαση των προσωπικών δεδομένων του.

Επιπροσθέτως, σύμφωνα με την Ομάδα Εργασίας του άρθρου 29 για την προστασία των δεδομένων, η παράβαση του κανονισμού θα πρέπει να οδηγεί στην επιβολή ισοδύναμων κυρώσεων και όλα τα διοικητικά μέτρα θα πρέπει να είναι αποτελεσματικά, αναλογικά και ανατρεπτικά, ενώ η αρμόδια εποπτική αρχή θα πρέπει να προβεί σε **αξιολόγηση σε κάθε μεμονωμένη περίπτωση**.[66] Στο **άρθ. 83 παρ.2 του ΓΚΠΔ**, παρατίθεται ο κατάλογος με τα **κριτήρια** που μπορούν να χρησιμοποιηθούν από τις εποπτικές αρχές, κατά **πόσο είναι αναγκαίο** να επιβληθεί πρόστιμο και το ποσό του προστίμου. Ειδικότερα, ως προς τα κριτήρια που λαμβάνονται υπόψη αυτά ενδεικτικά μπορούν να είναι: η φύση, η βαρύτητα, η διάρκεια της παράβασης, ο αριθμός των οικείων υποκειμένων, ο σκοπός της επεξεργασίας, ο βαθμός της ζημίας, ο δόλος ή η αμέλεια που προκάλεσε την παράβαση, οι ενέργειες στις οποίες προέβη ο υπεύθυνος ή εκτελών την επεξεργασία για να μετριάσει τη ζημία που υπέστη το υποκείμενο, ο βαθμός ευθύνης του υπεύθυνου ή του εκτελούντος την επεξεργασία με γνώμονα τα τεχνικά και οργανωτικά μέτρα των άρθρων 25 και 32 του ΓΚΠΔ, τυχόν προηγούμενες παραβάσεις, ο βαθμός συνεργασίας με την αρχή για την επανόρθωση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεων, οι κατηγορίες δεδομένων που πλήττονται από την παράβαση, εάν και κατά πόσο ο υπεύθυνος ή εκτελών την επεξεργασία γνωστοποίησε την παράβαση στην εποπτική αρχή, κατά πόσο είχε διαταχθεί προηγουμένως η λήψη μέτρων που απαριθμούνται στο άρθ. 58 παρ. 2 του ΓΚΠΔ, η τήρηση ή μη κωδίκων δεοντολογίας βάσει του άρθ. 40 του ΓΚΠΔ ή εγκεκριμένων μηχανισμών πιστοποίησης βάσει του άρθ. 42 του ΓΚΠΔ και κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο που προκύπτει από τις περιστάσεις της εκάστοτε περίστασης όπως τα οικονομικά οφέλη που αποκομίστηκαν ή ζημιών που αποφεύχθηκαν άμεσα ή έμμεσα από την παράβαση.

---

[66] *Ομάδα Εργασίας του άρθρου 29 (2017), Κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του Κανονισμού 2016/679, WP 253, 3 Οκτωβρίου 2017, Διαθέσιμο στο :* https://www.dpa.gr/sites/default/files/2019-12/wp253_el.pdf

Στην Ελλάδα, η Αρχή Προστασίας με την Απόφαση 6/2022 [67]και βάσει της εξουσίας της που απορρέει από το **άρθ. 58 παρ. 2, περ. θ' του ΓΚΠΔ** σε συνδυασμό με το **άρθ. 83 του ΓΚΠ,** επέβαλε πρόστιμο ύψους 10.000,00 Ευρώ κατά της Τράπεζας Πειραιώς **για περιστατικό παραβίασης προσωπικών δεδομένων** και συγκεκριμένα παραβίαση της αρχή της εμπιστευτικότητας, καθώς αποστέλλονταν ειδοποιήσεις winbankalerts σε τρίτο μη εξουσιοδοτημένο πρόσωπο συνονόματο και συνεπώνυμο με την καταγγέλλουσα και όχι στη διεύθυνση της καταγγέλλουσας, το οποίο εξακολουθούσε να λαμβάνει χώρα παρά τη σχετική ενημέρωση της τράπεζας. Παράλληλα, διαπιστώθηκε παράβαση της τράπεζας αναφορικά με την υποχρέωσή της να γνωστοποιήσει το εν λόγω περιστατικό παραβίασης τόσο στην Αρχή όσο και στο υποκείμενο δεδομένων σύμφωνα με το άρθ. 33 και 34 του ΓΚΠΔ. Επιπροσθέτως, η Αρχή απηύθυνε προειδοποίηση προς την Τράπεζα Πειραιώς Α.Ε. να θέσει σε εφαρμογή τεχνικά και οργανωτικά μέτρα, κατά τις επιταγές των 24 και 32 του ΓΚΠΔ εξαιτίας της έλλειψης μέτρων επιβεβαίωσης των ηλεκτρονικών διευθύνσεων που δηλώνονται στην τράπεζα για τη λήψη ειδοποιήσεων winbankalerts.

[67] *Απόφαση* **6/2022** *της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Επιβολή προστίμου για συνεχιζόμενο περιστατικό παραβίασης προσωπικών δεδομένων από Τράπεζα, Διαθέσιμο στο:* https://www.dpa.gr/sites/default/files/2022-04/6_2022anonym.pdf

4. Επίλογος

Εκ των όσων αναπτύχθηκαν ανωτέρω, τίθεται το δίλημμα κατά πόσο η αξιοποίηση των ψηφιακών τεχνολογιών στον τραπεζικό τομέα «λύνει ή δένει τα χέρια» του χρήστη της ηλεκτρονικής τραπεζικής. Από τη μία η δυνατότητα διενέργειας συναλλαγών εξ αποστάσεως μέσω ηλεκτρονικής τραπεζικής, καταργεί χωρικούς και χρονικούς περιορισμούς, παρέχει άνεση και οργάνωση για τον χρήστη και αυξάνει την ανταγωνιστικότητα στον τραπεζικό χώρο. Από την άλλη, δημιουργείται ένα πρόσθετο πεδίο δράσης για τους κυβερνοεγκληματίες, οι οποίοι αφαιρώντας αυθαίρετα χρηματικά ποσά από τους λογαριασμούς των χρηστών ηλεκτρονικής τραπεζικής, θέτουν σε κίνδυνο τη φήμη και αξιοπιστία της τράπεζας με την προσβολή του εννόμου αγαθού της περιουσίας των πελατών της και ορισμένες φορές και της παραβίασης της ασφάλειας των τραπεζικών δεδομένων τους. Η ανίχνευση και πρόληψη των κινδύνων που ελλοχεύουν από τη χρήση από τους πελάτες και από την παροχή υπηρεσιών ηλεκτρονικής τραπεζικής από τις τράπεζες μπορεί να αποτελέσει σημαντικό εργαλείο στον περιορισμό του φαινομένου των επιθέσεων phishing και συνεπώς προτείνονται τα ακόλουθα:

Σε ατομικό επίπεδο, είναι σημαντική η ευαισθητοποίησή και η επίδειξη δέουσας επιμέλειας από τον εκάστοτε χρήστη υπηρεσιών ηλεκτρονικής τραπεζικής. Όπως επισημαίνεται άλλωστε και στην αιτ .σκ. 8 του Κανονισμού 2019/881, η κυβερνοασφάλεια δεν είναι μόνο ζήτημα που αφορά την τεχνολογία αλλά σημαντικός είναι **ο ρόλος του ανθρώπινου παράγοντα**. Με σκοπό την προστασία από το ανθρώπινο λάθος, σημαντική είναι η «κυβερνουγιεινή» και ο «κυβερνοπρογραμματισμός», δηλαδή απλά μέτρα ρουτίνας ευαισθητοποίησης και εκπαίδευσης των πολιτών ως προς την κυνεροασφάλεια. Ιδιαίτερη προσοχή απαιτείται ως προς τους κωδικούς πρόσβασης, οι οποίοι θα πρέπει να είναι κατά το δυνατόν ισχυροί, ήτοι να περιέχουν συνδυασμό γραμμάτων πεζών και κεφαλαίων, αριθμών, συμβόλων και να μην παραπέμπουν σε μια εύκολα ανιχνεύσιμη πληροφορία όπως για παράδειγμα το όνομά τους ή η ημερομηνία γέννησής τους. Οι χρήστες θα πρέπει επίσης να προβαίνουν σε αλλαγή του

κωδικού ανά τακτά χρονικά διαστήματα, από τρεις έως έξι μήνες και να μην κοινολογούν τους μυστικούς κωδικούς πρόσβασής τους σε τρίτα πρόσωπα Σημαντικό επίσης να μην επιλέγουν την αποθήκευση των κωδικών πρόσβασης στο πρόγραμμα περιήγησης από όπου συνδέονται στις υπηρεσίες ηλεκτρονικής τραπεζικής και να αποφεύγουν να συνδέονται από δημόσια δίκτυα. Επιπλέον, οφείλουν να μεριμνούν για την ασφάλεια των προσωπικών τους συσκευών μέσω της εγκατάστασης και της ενημέρωσης των στοιχείων ασφαλείας τους χρησιμοποιώντας λογισμικά προστασίας από ιούς, τείχη προστασίας, ενημερώσεις ασφαλείας. Συνίσταται επίσης να πληκτρολογούν τη διεύθυνση της τράπεζας για σύνδεση στην ηλεκτρονική τραπεζική και να μην ανακατευθύνονται μέσω μηχανής αναζήτησης ώστε να αποφύγουν τον κίνδυνο να συνδεθούν σε ιστότοπο κλώνο που μιμείται τη γνήσια ιστοσελίδα της τράπεζας που συνεργάζονται. Σε κάθε περίπτωση, καλό είναι οι χρήστες ηλεκτρονικές τραπεζικής να ενημερώνονται από καμπάνιες όπως αυτή της Ελληνική Ένωση Τραπεζών με τίτλο «Κάποιες ειδοποιήσεις είναι καλύτερο να τις αγνοείς»[68] αλλά και το «Μια παύση αρκεί για να αποφύγουμε την ηλεκτρονική απάτη»[69]. Τέλος, πρέπει είναι να μεριμνούν για την ενεργοποίηση των σχετικών ρυθμίσεων του συστήματος ηλεκτρονικής τραπεζικής αναφορικά με την αποστολή ειδοποίησης μέσω push notification ώστε να λαμβάνουν γνώση άμεσα για τις κινήσεις που πραγματοποιούνται από τον τραπεζικό τους λογαριασμό και να ειδοποιούν άμεσα και χωρίς καθυστέρηση την τράπεζα για ύποπτη συναλλαγή, η οποία έλαβε χώρα χωρίς τη γνώση και συγκατάθεσή τους.

Σε επίπεδο τραπεζών, λαμβάνοντας υπόψη ότι οι επιθέσεις με μορφή phishing, μπορεί να συνιστούν και παραβίαση δεδομένων προσωπικού χαρακτήρα των υποκειμένων – χρηστών ηλεκτρονικής τραπεζικής αναγκαία είναι η υιοθέτηση πολιτικών αναφορικά με τη διαχείριση κινδύνων, η ικανότητα πρόληψης εντοπισμού και αντιμετώπισης των κυβερνοαπειλών και τήρησης των μέτρων κυβερνοασφαλείας σύμφωνα με τις επιταγές των Οδ. PSD 2, NIS 2 και

[68] *Ελληνική Ένωση Τραπεζών, 2023, Κάποιες ειδοποιήσεις είναι καλύτερο να τις αγνοείς, Διαθέσιμο στο: https://www.hba.gr/info/PhishingCamp2023*

[69] *Ελληνική Ένωση Τραπεζών, 2022, Μια παύση αρκεί για να αποφύγουμε την ηλεκτρονική απάτη, Διαθέσιμο στο: https://www.hba.gr/info/PhishingCamp*

των κανονισμών DORA και GDPR. Οι τράπεζες, οι οποίες ανήκουν στους τομείς υψηλής κρισιμότητας αναφορικά με την ασφάλεια δικτύου και πληροφοριών, θα πρέπει να διασφαλίζουν **ένα σύγχρονο και ασφαλές περιβάλλον πληροφοριακών και δικτυακών υποδομών, που θα στοχεύει στην οικονομική και κοινωνική ευημερία υπό την ασπίδα προστασίας θεμελιωδών δικαιωμάτων των πολιτών, την ασφαλή χρήση ψηφιακών υπηρεσιών και εφαρμογών και την επαυξημένη εμπιστοσύνη των πολιτών και επιχειρήσεων στις ψηφιακές τεχνολογίες**[70]. Η επιτυχής συμμόρφωση του τραπεζικού τομέα με τις ανωτέρω απαιτήσεις ασφαλείας και προστασίας των προσωπικών δεδομένων μπορεί να μετατραπεί σε όφελος καθώς η φήμη μιας τράπεζας για την παροχή εχέγγυων ασφάλειας των συστημάτων της και διασφάλισης της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, αποτελεί σημαντικό πλεονέκτημα έναντι των ανταγωνιστών της fintech βιομηχανίας[71] και να αποτρέψει τις τεράστιες οικονομικές και κοινωνικές δυσμενείς συνέπειες της ηλεκτρονικής τραπεζικής απάτης.

[70] *Βλ., Ελληνική Δημοκρατία, Υπουργείο Ψηφιακής Διακυβέρνησης, Εθνική Αρχή Κυβερνοασφάλειας, 2020, Εθνική Στρατηγική Κυβερνοασφάλειας* 2020-2025, *ό.π., σελ. 18*

[71] *PWC, (2017) The EU General Data Protection Regulation (GDPR) in the banking industry, An impact analysis on banks and wealth managers with the focus on Switzerland*

Ελληνική βιβλιογραφία

Γέρμανος Γ., Γεωργίου Ν., (2021) «Κυβερνοέγκλημα, Πρόληψη-Διερεύνηση-Αντιμετώπιση», Αθήνα, ISBN 978-618-00-2651-1, σελ.115 επ.

Κανέλλος Λ., (2020) «THE GDPR HANDBOOK – Για DPOs, Επιχειρήσεις & Οργανισμούς, Αθήνα, Νομική Βιβλιοθήκη, σελ. 48 επ.

Ιγγλεζάκης, Ι., (2021) Δίκαιο Πληροφορικής, Δ' Έκδοση, Αθήνα – Θεσσαλονίκη, Εκδόσεις Σάκκουλα

Μυλωνόπουλος, Χ., (1991), Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο. Συμβολή στην ερμηνεία των άρθρων 13γ, 370 Β, 370 Γ και 386 Α Π.Κ. (άρθρ. 2-5 ν. 1805/88)

Παπαδαμάκης, Α., (2020) Τα περιουσιακά εγκλήματα, Αθήνα – Θεσσαλονίκη, Εκδόσεις Σάκκουλα, σελ. 153 επ.

Ρόκας, Ν./Γκόρτσος , Χ./Μικρουλέα, Α./Λιβαδά, Χ., (2016) Στοιχεία Τραπεζικού Δικαίου, Αθήνα, Νομική Βιβλιοθήκη, σελ.475

Jougleux, P., (2016) «Ευρωπαϊκό δίκαιο του διαδικτύου, Νομικές πτυχές του διαδικτύου στην Ευρώπη», Αθήνα – Θεσσαλονίκη, σελ. 133 επ

Διπλωματικές εργασίες

Βαϊτσούδης , Ι., (2020) Απάτη μέσω υπολογιστή και απάτη με υπολογιστή (Άρθρα 386, 386 Α ΠΚ), Θεσσαλονίκη, σελ. 70 επ.

Καζαντζίδης, Π., (2022), Νομικά ζητήματα προστασίας προσωπικών δεδομένων στον τραπεζικό τομέα και υπολογιστική νέφους, Θεσσαλονίκη

Κυπραίος, Ι., (2018)«Οι επιπτώσεις του Γενικού Κανονισμού Προστασίας Δεδομένων στον Τραπεζικό Τομέα: Μελέτη Περίπτωσης, Σάμος

Λυμπεροπούλου, Β. (2019), Ο Κανονισμός Προστασίας Προσωπικών Δεδομένων, επεξεργασία των προσωπικών δεδομένων στον τραπεζικό χώρο και η άρση του τραπεζικού απορρήτου, Θεσσαλονίκη

Μήτια, (Α), 2021, Εκτέλεση τραπεζικών εργασιών και προσωπικά δεδομένα στον ελληνικό τραπεζικό τομέα, Θεσσαλονίκη

Ξυγκάκη, Α. (2020), Η προσαρμογή των τραπεζών στο νέο κανονισμό για την προστασία των προσωπικών δεδομένων, Πειραιάς

Ροϊδου, Α. (2021), Η προστασία των προσωπικών δεδομένων στον τραπεζικό χώρο και η χρήση νέων τεχνολογιών, Θεσσαλονίκη

Ελληνική αρθογραφία

Βασιλάκη Ε., Τα φαινόμενα «Phishing», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ ΝΖ/2007, σελ. 860-863

Γιαννόπουλος Γ., Internet Banking: Νομικά ζητήματα από τη διεξαγωγή τραπεζικών συναλλαγών στο διαδίκτυο, Ελληνική Ένωση Τραπεζών, Διαθέσιμο στο: https://www.hba.gr/5Ekdosis/UplPDFs/deltia/3_2003/97-108.pdf

Μήτσου, Α.-Ο.,2021, Η προστασία του πληρωτή από την απατηλή χρήση των μέσων πληρωμής στθς συναλλαγές του ηλεκτρονικού εμπορίου, ΤΝΠ Qualex, ΔΕΕ, σελ. 606-619

Παπαδόπουλος Μ, 2005, Phishing: Η νέα μέθοδος εξαπάτησης στο Διαδίκτυο, 3ο Πανελλήνιο Συνέδριο Ηλεκτρονικό Έγκλημα 2005, Δικτυοπειρατεία &

Τηλεπικοινωνιακή απάτη, Πρόληψη – Αντιμετώπιση – Λύσεις - Εφαρμογές

Τζίβα, Ε., 2021, Εφαρμογές της ψηφιακής τεχνολογίας στις τραπεζικές συναλλαγές, ΤΝΠ Qualex, ΔΕΕ, σελ. 316-325

Ξενόγλωσση αρθογραφία

Cambridge University Press, (2021), Know your customer: Balancing innovation and regulation for financial inclusion

Douglas W. Arner, Ross P. Buckley and Dirk A.Zetzsche, (2021), Open Banking, Open Data and Open Finance: Lessons from the European Union, University of New South Wales Law Research Series

Saloni, M., Swapnesh T., Dilbag S., (2019), Detection of pharming Attack on Websites using SVM Classifier, International Journal of Scientific & Technology Research,Volume 1, Issue

Ελληνικές Μελέτες - εγχειρίδια

Ελληνική Δημοκρατία, Υπουργείο Ψηφιακής Διακυβέρνησης, Εθνική Αρχή Κυβερνοασφάλειας, 2020, Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025, Διαθέσιμο στο:
https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7%CC%81-%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7%CC%81-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf

Ελληνική Δημοκρατία, Υπουργείο Ψηφιακής Διακυβέρνησης, (2021), Εγχειρίδιο Κυβερνοασφάλειας, Διαθέσιμο στο :
https://mindigital.gr/wp-

content/uploads/2021/06/%CE%95%CE%B3%CF%87%CE%B5%CE%B9%CF%81%CE%AF%CE%B4%CE%B9%CE%BF-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf

Ελληνική Συνομοσπονδία Εμπορίας & Επιχειρηματικότητας, (2021), Η Λευκή Βίβλος του Λιανικού Εμπορίου 2040, Προβληματισμοί και εκτιμήσεις για τον μετασχηματισμό του λιανικού εμπορίου

Ξενόγλωσσες μελέτες

Deloitte, (2019), After the dust settles, How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on

PWC, (2017), The EU General Data Protection Regulation (GDPR) in the banking industry, An impact analysis on banks and wealth managers with the focus on Switzerland

Κατευθυντήριες γραμμές

Ευρωπαϊκή Αρχή Τραπεζών, 2014, Τελικές κατευθυντήριες γραμμές σχετικά με την ασφάλεια πληρωμών μέσω διαδικτύου, Διαθέσιμο στο: https://www.eba.europa.eu/sites/default/files/documents/10180/1004450/b636aaaa-fdf9-47ef-a100-e03a75448bb0/EBA-GL-2014-12_EL_rev1%20GL%20on%20Internet%20Payments.pdf

Ομάδα εργασίας του άρθρου 29 (2016), Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων, WP 242, 13 Δεκεμβρίου 2016, αναθεωρήθηκαν στις 5 Απριλίου 2017, σελ.5., Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2020-05/wp242rev01_el.pdf

Ομάδα Εργασίας του άρθρου 29 (2017), Κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του

Κανονισμού 2016/679, WP 253, 3 Οκτωβρίου 2017, Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2019-12/wp253_el.pdf

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, (2020), Κατευθυντήριες γραμμές 06/2020 σχετικά με την αλληλεπίδραση μεταξύ της δεύτερης οδηγίας για τις υπηρεσίες πληρωμών και του ΓΚΠΔ, Διαθέσιμο στο: https://edpb.europa.eu/ourwork-tools/our-documents/guidelines/guidelines-062020-interplay-second-paymentservices_el

Κείμενα οργάνων της ΕΕ

Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ένωσης σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.166, Διαθέσιμο στο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

Ανακοίνωση της Ευρωπαϊκής Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή οικονομική και κοινωνική Επιτροπή και την Επιτροπή Περιφερειών σχετικά με μια στρατηγική ψηφιακών χρηματοοικονομικών υπηρεσιών για την ΕΕ της 24ης Σεπτεμβρίου 2020, COM (2020) 591, Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:52020DC0591

Ευρωπαϊκό Κοινοβούλιο, (2021) Γιατί η κυβερνοασφάλεια είναι τόσο σημαντική για την ΕΕ; Διαθέσιμο στο: https://www.europarl.europa.eu/news/el/headlines/society/20211008STO14521/giati-i-kuvernoasfaleia-einai-toso-simantiki-gia-tin-ee

Νομολογία

Ελληνική νομολογία

Απόφαση ΣυμβΠλημΘεσ 828/2022 (Ποιν. Δικαιοσύνη, σελ. 1228)

Απόφαση ΜΠρΧίου 245/2022 (Πηγή Τετράβιβλος)

Απόφαση ΕιρΜυτ24/2023**,** *Sakkoulas-online, Διαθέσιμο στο:* ***https://www.sakkoulas-online.gr/reader/d27b6c02fa3398d81c33/?utm_source=%CE%95%CE%BA%CE%B4%CF%8C%CF%83%CE%B5%CE%B9%CF%82+%CE%A3%CE%AC%CE%BA%CE%BA%CE%BF%CF%85%CE%BB%CE%B1+%CE%91%CE%95&utm_campaign=a19b562d52-e-info-18.7.2023&utm_medium=email&utm_term=0_7bee924d9b-a19b562d52-146922345&ct=t(e-info-18.7.2023)&mc_cid=a19b562d52&mc_eid=5bd0876ef5***

Αποφάσεις της Τράπεζας της Ελλάδος

ΠΕΕ, Αριθμ. απόφ. 190/2/16.06.2021, «Υιοθέτηση των κατευθυντήριων γραμμών της Ευρωπαϊκής Αρχής Τραπεζών (EBA/GL/2019/04) σχετικά με τη διαχείριση κινδύνων Τεχνολογίας Πληροφορικής και & Επικοινωνιών (ΤΠΕ) και Ασφαλείας»

Αποφάσεις της Ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Απόφαση 57/2018 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Πρόστιμο σε τράπεζα για μη εκπλήρωσή της να τηρεί και να επεξεργάζεται ακριβή στοιχεία για τους οφειλέτες της, Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2019-10/57_2018anonym.pdf

Απόφαση 6/2022 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Επιβολή προστίμου για συνεχιζόμενο περιστατικό παραβίασης προσωπικών δεδομένων από Τράπεζα, Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2022-04/6_2022anonym.pdf

Απόφαση 52/2022 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Επιβολή προστίμου στην Alpha Bank για παράνομη και αδιαφανή επεξεργασία δεδομένων, Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2022-

11/52_2022%20anonym.pdf

Νομολογία ΔΕΕ

ΔΕΕ C-70/10 Scarlet v. Extended SA Societe belge des auteurs, compositeurs et Editeurs SCRL (SABAM),απόφαση της 24ης Νοεμβρίου 2011, Διαθέσιμο στο: https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&lgrec=en&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-70%252F10&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=el&avg=&cid=3771539

Διαδικτυακοί τόποι

Ελληνικοί διαδικτυακοί τόποι

Αρχή Προστασίας Δεδομένων, Ασφάλεια προσωπικών δεδομένων, Διαθέσιμο στο: https://dpa.gr/el/enimerwtiko/thematikes_enotites/asfaleia

Αρχή Προστασίας Δεδομένων, Γνωστοποίηση περιστατικών παραβίασης δεδομένων άρθρα 33-34 ΓΚΠΔ, Διαθέσιμο στο: https://www.dpa.gr/index.php/el/foreis/asfaleia_dedomenwn/gnwstopoiisi_paraviasis

ΔΙΑΣ-Διατραπεζικά συστήματα Α.Ε.,(2022), Στατιστικά στοιχεία 2022, Διαθέσιμο στο: https://www.dias.com.gr/el/statistika2022/

Ελληνική Δημοκρατία, Υπουργείο Ψηφιακής Διακυβέρνησης, Ανακοίνωσης της 15ης Ιουλίου 2023 της Εθνικής Αρχής Κυβερνοασφάλειας, Διαθέσιμο στο: https://mindigital.gr/archives/5310

Ελληνική Ένωση Τραπεζών, 2022, Μια παύση αρκεί για να αποφύγουμε την ηλεκτρονική απάτη, Διαθέσιμο στο: https://www.hba.gr/info/PhishingCamp

Ελληνική Ένωση Τραπεζών, 2023, Κάποιες ειδοποιήσεις είναι καλύτερο να τις αγνοείς, Διαθέσιμο στο: https://www.hba.gr/info/PhishingCamp2023

Ε.Κ.ΠΟΙ.ΖΩ,2023, Αναποτελεσματική η προστασία καταναλωτών από τις ηλεκτρονικές απάτες στο νομοσχέδιο προς συζήτηση στη Βουλή, Διαθέσιμο στο: https://www.ekpizo.gr/%CE%BF%CE%B9-%CE%B4%CF%81%CE%AC%CF%83%CE%B5%CE%B9%CF%82-%CE%BC%CE%B1%CF%82/%CF%87%CF%81%CE%B7%CE%BC%CE%B1%CF%84%CE%BF%CE%BF%CE%B9%CE%BA%CE%BF%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CE%AC/%CE%B1%CE%BD%CE%B1%CF%80%CE%BF%CF%84%CE%B5%CE%BB%CE%B5%CF%83%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE-%CE%B7-%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1-%CF%84%CF%89%CE%BD-%CE%BA%CE%B1%CF%84%CE%B1%CE%BD%CE%B1%CE%BB%CF%89%CF%84%CF%8E%CE%BD-%CE%B1%CF%80%CF%8C-%CF%84%CE%B9%CF%82-%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CE%AD%CF%82

ΤΕΙΡΕΣΙΑΣ Α.Ε., Ποια δεδομένα τηρούνται, Διαθέσιμο στο: https://www.tiresias.gr/el/idiotes/poia-dedomena-tirountai/

Τράπεζα της Ελλάδος, Κόμβος Καινοτομίας FinTech, Διαθέσιμο στο: https://www.bankofgreece.gr/kiries-leitourgies/epopteia/komvos-kainotomias-fintech

Τράπεζα της Ελλάδος, (2023), Έκθεση Χρηματοπιστωτικής Σταθερότητας, Διαθέσιμο στο: https://www.bankofgreece.gr/Publications/FINANCIAL_STABILITY_REVIEW_MAY_2023_EL.pdf

Lawspot.gr, 2023, Δημοσιεύτηκε ο Νόμος για τις αντιπροσωπευτικές αγωγές και την προστασία των καταναλωτών (Ν. 5019/2023), Διαθέσιμο στο: https://www.lawspot.gr/nomika-nea/dimosieythike-o-nomos-gia-tis-antiprosopeytikes-agoges-kai-tin-prostasia-ton-katanaloton

Lawspot.gr, (2023), Διαδικτυακές απάτες, τήρηση μέτρων ασφαλείας και ευθύνη τράπεζας (ΕιρΘεσ 232/2023), Διαθέσιμο στο: https://www.lawspot.gr/nomika-nea/diadiktyakes-apates-tirisi-metron-asfaleias-kai-eythyni-trapezas-eirthes-232-2023

Newsroom, Emea Business Voice, Ξεπερνούν τα 22 εκατ. ευρώ οι ηλεκτρονικές απάτες στην Ελλάδα, Διαθέσιμο στο: https://emea.gr/kyrio-thema/653181/xepernoun-ta-22-ekat-evro-oi-ilektronikes-apates-stin-ellada/

Ξενόγλωσσοι διαδικτυακοί τόποι

Jackson ,A. (2023) «Revolut hacked as cyber criminals steal US $ 2O m, Cybermagazine, Διαθέσιμο στο: https://cybermagazine.com/cyber-security/revolut-hacked-as-cyber-criminals-steal-us-20m

Νομοθεσία

Ελληνική νομοθεσία

Ν.1805/1955: Εκσυγχρονισμός τον θεσμού τον ποινικού μητρώου, τροποποίηση ποινικών διατάξεων και ρύθμιση άλλων σχετικών θεμάτων

Ν. 2251/1994 : Προστασία των καταναλωτών

Ν.2472/1997: Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Ν.2774/1994: Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα

Ν.3474/2006: Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997

Ν.3606/2007:Αγορές χρηματοπιστωτικών μέσων και άλλες διατάξεις

Ν.3758/2009: Εταιρείες ενημέρωσης οφειλετών για ληξιπρόθεσμες απαιτήσεις και άλλες διατάξεις

Ν. 3979/2011: Για την ηλεκτρονική διακυβέρνηση και λοιπές διατάξεις

Ν.4354/2015: Διαχείριση των μη εξυπηρετούμενων δανείων, μισθολογικές ρυθμίσεις και άλλες επείγουσες διατάξεις εφαρμογής της συμφωνίας δημοσιονομικών στόχων και διαρθρωτικών μεταρρυθμίσεων

Ν.4411/2016: Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών

Ν. 4537/2018: Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2015/2366/ΕΕ για τις υπηρεσίες πληρωμών και άλλες διατάξεις

Ν.4557/2018: Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας (ενσωμάτωση της Οδηγίας 2015/849/ΕΕ) και άλλες διατάξεις

Ν.4577/2018: Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ευρώπη και άλλες διατάξεις

Ν.5019/2023: Ενσωμάτωση της Οδηγίας (ΕΕ) 2020/1828 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2020 «σχετικά με τις

αντιπροσωπευτικές αγωγές για την προστασία των συλλογικών συμφερόντων των καταναλωτών και για την κατάργηση της Οδηγίας 2009/22/ΕΚ», ενίσχυση της προστασίας των καταναλωτών, ρυθμιστικό πλαίσιο για την παλαίωση οίνων και άλλες επείγουσες διατάξεις

Κώδικες

Κώδικας Τραπεζικής Δεοντολογίας, Ένωση ελληνικών Τραπεζών, Μάρτιος 1997

Κώδικας Δεοντολογίας για την Επεξεργασία των Προσωπικών Δεδομένων στο Τραπεζικό Σύστημα, Ελληνική Ένωση Τραπεζών, Σχέδιο 16.1.2019

Διεθνείς Συμβάσεις

Σύμβαση για το έγκλημα στον κυβερνοχώρο (Βουδαπέστη, 23 Νοεμβρίου 2001)

Νομοθεσία της ΕΕ

Κανονισμοί

Κανονισμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (Γενικός Κανονισμός για την Προστασία των Δεδομένων), για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ

Κανονισμός 2018/389 για τη συμπλήρωση της οδηγίας (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά ρυθμιστικά τεχνικά πρότυπα για την αυστηρή εξακρίβωση ταυτότητας του πελάτη και τα κοινά και ασφαλή ανοικτά πρότυπα επικοινωνίας

Κανονισμός 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της

κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια)

Κανονισμός 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011

Οδηγίες

Οδηγία 1995/46 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

Οδηγία 2013/40 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου

Οδηγία 2014/65 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014 , για τις αγορές χρηματοπιστωτικών μέσων

Οδηγία 2015/849 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2015, σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας

Οδηγία 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2015 σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά

Οδηγία 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση

Οδηγία 2019/713 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών και την αντικατάσταση της απόφασης-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου

Οδηγία 2020/1828 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2020 «σχετικά με τις αντιπροσωπευτικές αγωγές για την προστασία των συλλογικών συμφερόντων των καταναλωτών και για την κατάργηση της Οδηγίας 2009/22/ΕΚ ρυθμιστικό πλαίσιο για την παλαίωση των οίνων και άλλες επείγουσες διατάξεις

Οδηγία 2022/2555 (NIS2) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148

Χάρτες

Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

Συμβάσεις

Σύμβαση 108 του Συμβουλίου της Ευρώπης, για την προστασία των φυσικών προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, (Επικαιροποίηση της Σύμβασης, Έλσινορ,18-05-2018)