

Ελληνικό Ανοικτό Πανεπιστήμιο

Πανεπιστήμιο Λευκωσίας

Διπλωματική Εργασία



Θ Ε Μ Α :

Η μέθοδος του "phishing" στις ηλεκτρονικές πληρωμές και η προστασία του καταναλωτή.

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: Βακράκος Νικόλαος του Θωμά

1^η Επιβλέπουσα : κα Καλλιόπη Μήτκα

2^{ος} Επιβλέπων :κος Κωνσταντίνος Βουλγαράκης

Ακαδημαϊκό Έτος : 2025-2026

Ευχαριστίες

*Στη σύζυγό μου Ζαχαρούλα...
για την αμέριστη συμπαράστασή της...*

Πίνακας περιεχομένων

Περίληψη.....	5
Εισαγωγή.....	6
Κεφάλαιο 1: Επιθέσεις phishing και κυβερνοασφάλεια στον τομέα της ηλεκτρονικής τραπεζικής.....	8
1.1. Ορισμός του phishing στον Τραπεζικό τομέα.....	8
1.2. Συνηθέστερες μορφές επιθέσεων phishing κατά τη χρήση υπηρεσιών ηλεκτρονικής τραπεζικής.....	10
1.2.1. Μαζική επίθεση.....	12
1.2.2. Στοχευμένη επίθεση (spear phishing).....	12
1.2.3. Man-in-the-middle attack.....	13
1.2.4. Search Engine Phishing.....	14
1.2.5. Επιθέσεις συσκότισης URL και HTML.....	14
1.2.6. Επίθεση μέσω κοινωνικής δικτύωσης (Soshing, Social Media Phishing).....	15
1.2.7. Phone phishing (Vishing and Smishing).....	15
1.2.8. SIM Swapping.....	16
1.3. Το phishing ως απειλή για την ασφάλεια των τραπεζικών συναλλαγών.....	17
Κεφάλαιο 2: Νομική προστασία του καταναλωτή στις ηλεκτρονικές πληρωμές και στις απάτες phishing.....	19
2.1. Η προστασία του καταναλωτή στο πλαίσιο των ηλεκτρονικών πληρωμών-Βασικό νομοθετικό πλαίσιο-ΓΣΟ.....	19
2.2. Νομικό πλαίσιο θεμελίωσης ευθύνης της Τράπεζας από απάτες phishing.....	22
2.2.1. Ενδοσυμβατική ευθύνη.....	22
2.2.2. Αδικοπρακτική ευθύνη.....	24
2.3. Νομικό πλαίσιο ευθύνης πληρωτή από μη εγκεκριμένες πράξεις πληρωμής.....	26
2.4. Η έννοια της ισχυρής ταυτοποίησης πελάτη (SCA) και τα όριά της.....	28
2.5. Ευθύνη παρόχων στο ηλεκτρονικό εμπόριο μετά τον Κανονισμό ΕΕ 2022/2065.....	31
2.6. Μηχανισμοί αποκατάστασης και ένδικης προστασίας καταναλωτή.....	46
Κεφάλαιο 3: Ανάλυση πραγματικών περιστατικών phishing.....	48
Κεφάλαιο 4: Μεθοδολογία και εμπειρική προσέγγιση της έρευνας.....	61

<i>4.1. Βασικά στοιχεία της έρευνας</i>	<i>61</i>
<i>4.2. Σκοπός της έρευνας</i>	<i>62</i>
<i>4.3. Μεθοδολογία της έρευνας</i>	<i>63</i>
<i>4.4. Περιγραφή του δείγματος</i>	<i>64</i>
<i>4.5. Εμπειρία των καταναλωτών με περιστατικά phishing</i>	<i>65</i>
<i>4.6. Επίπεδο ενημέρωσης και αίσθημα ασφάλειας των καταναλωτών/εμπιστοσύνης προς τις τράπεζες</i>	<i>66</i>
<i>4.7. Παρατηρήσεις από την εμπειρική έρευνα.....</i>	<i>66</i>
<i>Κεφάλαιο 5: Συμπεράσματα-προτάσεις</i>	<i>67</i>
<i>Ξενόγλωσση Βιβλιογραφία και Αρθρογραφία.....</i>	<i>69</i>
<i>Ελληνόγλωσση Βιβλιογραφία και Αρθρογραφία</i>	<i>72</i>
<i>ΠΑΡΑΡΤΗΜΑ.....</i>	<i>75</i>
<i>ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΕΡΕΥΝΑΣ</i>	<i>75</i>

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία εξετάζει το φαινόμενο της ηλεκτρονικής απάτης τύπου «phishing» (ηλεκτρονικό ψάρεμα) στο πλαίσιο των ψηφιακών συναλλαγών, αναλύοντας τις τεχνικές μορφές του, το υφιστάμενο νομικό πλαίσιο προστασίας του καταναλωτή και την κατανομή της ευθύνης μεταξύ των χρηστών και των πιστωτικών ιδρυμάτων.

Στο θεωρητικό μέρος, παρουσιάζεται ο ψηφιακός μετασχηματισμός του τραπεζικού τομέα και αναλύονται οι συνηθέστερες μεθοδολογίες επίθεσης, όπως το email phishing, το spear phishing, οι επιθέσεις man-in-the-middle, το phone phishing (vishing/smishing) και το SIM swapping. Οι τεχνικές αυτές, βασιζόμενες κυρίως στην κοινωνική μηχανική και στον ψυχολογικό χειρισμό, στοχεύουν στην απόσπαση ευαίσθητων διαπιστευτηρίων ασφαλείας από ανυποψίαστους καταναλωτές.

Στο νομικό μέρος, εξετάζεται η συμβατική φύση της τραπεζικής κατάθεσης ως ανώμαλης παρακαταθήκης και αναλύεται η θεμελίωση της ενδοσυμβατικής και αδικοπρακτικής ευθύνης των τραπεζών βάσει των άρθρων του Αστικού Κώδικα και του ν. 2251/1994. Κεντρικό σημείο αποτελεί ο επαναπροσδιορισμός της ευθύνης του πληρωτή για μη εγκεκριμένες πράξεις πληρωμής μετά τις πρόσφατες τροποποιήσεις των ν. 4537/2018 και ν. 5019/2023. Παράλληλα, θίγονται τα όρια της ισχυρής ταυτοποίησης πελάτη (SCA) σε συνδυασμό με τον ΓΚΠΔ, καθώς και η ευθύνη των παρόχων στο ηλεκτρονικό εμπόριο βάσει της Πράξης για τις Ψηφιακές Υπηρεσίες (DSA).

Μέσα από την κριτική επισκόπηση πρόσφατων δικαστικών αποφάσεων (όπως των ΕφεΔωδ 23/2025, ΕιρΒολ 36/2023 και ΠρΑθ 71756/2025), αναδεικνύεται η νομολογιακή τάση να αντιμετωπίζεται το phishing ως συστημικός κίνδυνος που βαρύνει πρωτίστως τον επαγγελματία πάροχο, καθιστώντας σαφές ότι η τυπική χρήση κωδικών OTP δεν ισοδυναμεί αυτόματα με πραγματική συναίνεση του χρήστη, εκτός αν αποδεικνύεται βαριά αμέλεια (όπως στην ΕφΘρακ 145/2025).

Το ερευνητικό μέρος πλαισιώνεται από ποσοτική εμπειρική έρευνα σε δείγμα 30 χρηστών. Τα ευρήματα καταγράφουν ευρεία ενσωμάτωση των ηλεκτρονικών πληρωμών στην καθημερινότητα, η οποία όμως συνοδεύεται από συγκρατημένη εμπιστοσύνη προς τις τράπεζες και αίσθημα ανασφάλειας. Η εργασία καταλήγει σε προτάσεις για τη λήψη πολυεπίπεδων μέτρων, εστιάζοντας στην ανάγκη εξειδίκευσης των κριτηρίων της βαριάς αμέλειας, στην εντατικοποίηση των τραπεζικών προγραμμάτων ενημέρωσης και στην καλλιέργεια μιας ευρύτερης κουλτούρας ψηφιακής παιδείας και κυβερνοασφάλειας.

Εισαγωγή

Ο ρυθμός ανάπτυξης του Διαδικτύου από την αρχή του νέου αιώνα και η αύξηση των υπολογιστών έχουν επιφέρει άνευ προηγουμένου μετασχηματισμό στην οργάνωση της οικονομικής δραστηριότητας, με μετατοπίσεις από το παραδοσιακό λιανικό εμπόριο με φυσική παρουσία, όπου τόσο ο πωλητής όσο και ο καταναλωτής βρίσκονταν στον ίδιο χώρο, προς το ηλεκτρονικό εμπόριο και τις απομακρυσμένες συναλλαγές (ΕΣΕΕ, 2021). Σε αυτή τη νέα εποχή, βρίσκουμε μια νέα εποχή ψηφιακού μετασχηματισμού στην οικονομία που επιταχύνεται ολοένα και περισσότερο από τη γέννηση και την ευρεία χρήση της "έξυπνης" τεχνολογίας στα τέλη της δεκαετίας του 2000, έως την ενίσχυση των κοινωνικών μέσων ως νέα μέσα επικοινωνίας και συναλλαγής με τους τελικούς χρήστες. Η ταχεία ανάπτυξη των έξυπνων συσκευών και των τεχνολογιών ψηφιακών πλατφορμών στην εποχή 2010-2020 οδήγησε στην ανάπτυξη ενός "ψηφιακού οικοσυστήματος" στο οποίο η τεχνολογία αλληλεπιδρά συνεχώς με τις καταναλωτικές συνήθειες (συμπεριφορά στην αγορά και επίσης τις απαιτήσεις του χρήστη) που επιδιώκει να προβλέψει ή ακόμα και να δημιουργήσει τις ανάγκες των χρηστών (ΕΣΕΕ, 2021).

Στην εποχή της Τέταρτης Βιομηχανικής Επανάστασης, η ψηφιοποίηση των εταιρειών και των χρηματοπιστωτικών ιδρυμάτων γίνεται ουσιαστικό στοιχείο τόσο για τη βιωσιμότητα όσο και για την ανταγωνιστικότητα, καθώς οι εταιρείες που διαθέτουν ψηφιακό αποτύπωμα θεωρούνται ότι αποκτούν το συγκριτικό πλεονέκτημα έναντι εκείνων που δεν προσαρμόζονται γρήγορα στις νέες τεχνολογικές συνθήκες. Αυτές οι αλλαγές δεν θα μπορούσαν να μείνουν ανεπηρέαστες από τον τραπεζικό τομέα. Στη στρατηγική της Ευρώπης για τις ψηφιακές χρηματοοικονομικές υπηρεσίες, η Ευρωπαϊκή Επιτροπή υπογραμμίζει ότι το μέλλον των χρηματοοικονομικών υπηρεσιών θα είναι ψηφιακό, επικεντρωμένο στην καινοτομία, την ασφάλεια και την προστασία των χρηστών (Ευρωπαϊκή Επιτροπή, 2020). Η εξάπλωση της ψηφιακής οικονομίας τα τελευταία χρόνια, σε συνδυασμό με τα εξαιρετικά περιβάλλοντα που δημιούργησε η πανδημία Covid-19 και άλλες διαταραχές, οδήγησε τόσο τις ιδιωτικές τράπεζες όσο και τους καταναλωτές να κάνουν μεγαλύτερη χρήση των ηλεκτρονικών τραπεζικών υπηρεσιών (e-banking), κάτι που είχε βαθιές επιπτώσεις στα επιχειρηματικά μοντέλα και την παροχή υπηρεσιών. Η ηλεκτρονική τραπεζική είναι ένας όρος που αναφέρεται σε οποιαδήποτε εμπορική συναλλαγή που πραγματοποιείται μεταξύ μιας τράπεζας και ενός πελάτη σε ένα ηλεκτρονικό δίκτυο, όπου μια τράπεζα ή ένας διαμεσολαβητής υπηρεσιών ή εταιρεία προσπαθεί να παρέχει ή να προσφέρει ένα τραπεζικό προϊόν ή υπηρεσία (Γιαννόπουλος, 2003).

Αυτές οι συναλλαγές μπορεί να είναι με τη μορφή μεμονωμένων πελατών (λιανική τραπεζική - B2C) και επιχειρηματικών συναλλαγών (B2B), που περιλαμβάνουν μια ποικιλία δραστηριοτήτων που περιλαμβάνουν συναλλαγές μέσω διαδικτύου (διαδικτυακή τραπεζική), κινητού τηλεφώνου (κινητή τραπεζική), σταθερού τηλεφώνου (τραπεζική μέσω τηλεφώνου) ή συναλλαγές μέσω ATM. Οι υπηρεσίες ηλεκτρονικής τραπεζικής περιλαμβάνουν τόσο λειτουργίες πληροφόρησης (παρακολούθηση λογαριασμών ή συναλλαγών) όσο και χρηματοοικονομικές συναλλαγές (όπως αποστολή χρημάτων, πληρωμή λογαριασμών και εξόφληση χρεών). Η εφαρμογή των ηλεκτρονικών τραπεζικών υπηρεσιών στην Ελλάδα έχει αυξηθεί τα τελευταία χρόνια. Σύμφωνα με την DIAS A.E., σημειώθηκε διψήφια αύξηση των συναλλαγών μέσω διατραπεζικών συστημάτων για δεύτερη συνεχόμενη χρονιά το 2022, λόγω των πολλών πλεονεκτημάτων που προσφέρει η ηλεκτρονική τραπεζική τόσο στους καταναλωτές όσο και στα πιστωτικά ιδρύματα. Οι χρήστες κερδίζουν ευκολία, ταχύτητα και συνεχή πρόσβαση στις τραπεζικές τους υπηρεσίες, καθώς και την αυξημένη πελατειακή βάση και τις εξοικονομήσεις κόστους που απολαμβάνουν οι τράπεζες. Αλλά υπάρχουν νέοι και ενισχυμένοι κίνδυνοι που συνοδεύουν τον ψηφιακό μετασχηματισμό του τραπεζικού τομέα, όπως κάθε τεχνολογία. Η εκτεταμένη χρήση ηλεκτρονικών συναλλαγών έχει οδηγήσει στην εμφάνιση διαφόρων τύπων κυβερνοεγκλημάτων, όπου το phishing είναι η κύρια μεθοδολογία. Από απατηλά μηνύματα, ψεύτικες ιστοσελίδες ή τηλεφωνικές κλήσεις, οι επιτιθέμενοι προσπαθούν να αποκτήσουν ευαίσθητα προσωπικά και τραπεζικά δεδομένα, κυρίως επιδιώκοντας οικονομική αποζημίωση μέσω απατών (ΟΟΣΑ, 2023). Η αυξημένη χρήση κινητού τηλεφώνου ή ηλεκτρονικών τραπεζικών καναλιών (ιδιαίτερα μετά την πανδημία) μπορεί να αυξήσει τις πιθανότητες έκθεσης σε τέτοιες απάτες. Η διαθεσιμότητα στατιστικών δεδομένων κάνει το φαινόμενο να φαίνεται πραγματικό. Οι οικονομικές απώλειες από απάτες ηλεκτρονικών συναλλαγών συνεχίζουν να είναι ιδιαίτερα υψηλές, σύμφωνα με δεδομένα από την Τράπεζα της Ελλάδος και την Ευρωπαϊκή Αρχή Τραπεζών, με την Ελλάδα να αναφέρει ποσοστά πάνω από τον μέσο όρο της ΕΕ (Τράπεζα της Ελλάδος, 2023; EAT, 2022). Η Εθνική Αρχή Κυβερνοασφάλειας έχει επίσης αναφέρει σχετικά με αυξανόμενο αριθμό αδικημάτων phishing μέσω email, μηνυμάτων κειμένου και κοινωνικών μέσων, υπογραμμίζοντας την επιτακτική ανάγκη να προωθηθεί καλύτερη ευαισθητοποίηση των πολιτών και η προστασία των πολιτών από επιθέσεις phishing (Υπουργείο Ψηφιακής Διακυβέρνησης, 2023). Βάσει αυτού, είναι σημαντικό να εισαχθεί μηχανισμός προστασίας των καταναλωτών για το ηλεκτρονικό σύστημα πληρωμών που αποκτά μεγάλη σημασία τόσο σε εθνικό, ευρωπαϊκό όσο και διεθνές επίπεδο.

Αυτή η μελέτη στοχεύει να διερευνήσει το εύρος του phishing ως τύπο ηλεκτρονικής απάτης που στοχεύει άμεσα στις ηλεκτρονικές πληρωμές, τον μηχανισμό εξαπάτησης των χρηστών, τα υπάρχοντα νομικά και τεχνολογικά πλαίσια προστασίας των καταναλωτών και την επάρκειά τους για την προστασία των καταναλωτών ώστε να διατηρήσουν τις συναλλαγές τους ασφαλείς και να διατηρήσουν την εμπιστοσύνη στο ηλεκτρονικό χρηματοοικονομικό σύστημα των επιχειρήσεων.

Κεφάλαιο 1: Επιθέσεις phishing και κυβερνοασφάλεια στον τομέα της ηλεκτρονικής τραπεζικής

1.1. Ορισμός του phishing στον Τραπεζικό τομέα

Το ηλεκτρονικό ψάρεμα, γνωστό ως phishing, περιλαμβάνει την απόκτηση προσωπικών και οικονομικών πληροφοριών (όπως ονόματα χρήστη, κωδικούς πρόσβασης κ.λπ.) μέσω απατηλών μεθόδων, όπως παραπλανητικά τηλεμηνύματα ή αντίγραφα αυθεντικών ιστοσελίδων. Μία από τις διαθέσιμες ορισμούς βρίσκεται στην αιτιολογική σκέψη 13 της Οδηγίας 2019/73, η οποία εισήχθη για την καταπολέμηση της απάτης και της παραχάραξης μη μετρητών μεθόδων πληρωμής, και ορίζει το phishing ως "την αντιγραφή δεδομένων καρτών ή την κατεύθυνση ή ανακατεύθυνση χρηστών υπηρεσιών πληρωμών σε ψεύτικες ιστοσελίδες και τη διανομή τους." Επιπλέον, σύμφωνα με την επεξηγηματική έκθεση για το Άρθρο 20 του σχεδίου Νόμου για την Ενσωμάτωση της Οδηγίας 2020/1828: "Το phishing ορίζεται ως 'μία πρακτική εξαπάτησης (με ψεύτικες ιστοσελίδες, ηλεκτρονικά μηνύματα ή ειδοποιήσεις), στην οποία οι δράστες αποκτούν ή κλέβουν τους μυστικούς κωδικούς ('PIN,' 'TAN') των καταναλωτών για να πραγματοποιήσουν διαδικτυακές συναλλαγές και μεταφορές χρημάτων.'" Το phishing είναι ένας τύπος επίθεσης κοινωνικής μηχανικής που αναφέρεται με παρόμοιο τρόπο με τη λέξη αλιεία, συμπεριλαμβανομένης της αλιείας με δόλωμα, που αναφέρεται στις τεχνικές που χρησιμοποιούν οι απατεώνες για να εκμεταλλευτούν ανυποψίαστους χρήστες, ψαρεύοντας ευαίσθητες προσωπικές και οικονομικές λεπτομέρειες από "δόλωμα," καταναλωτές ψηφιακών τραπεζικών υπηρεσιών. Συγκεκριμένα, χρησιμοποιώντας τη μεταμφίεση ενός αξιόπιστου φορέα όπως μια τράπεζα, ο δράστης προσπαθεί να εξαπατήσει ανυποψίαστα θύματα ώστε να αποκαλύψουν προσωπικές τραπεζικές πληροφορίες όπως όνομα

χρήστη και κωδικό πρόσβασης για να συνδεθούν σε ηλεκτρονικές τραπεζικές υπηρεσίες και/ή λεπτομέρειες πιστωτικών/χρεωστικών καρτών μέσω μιας απατηλής φόρμας που είναι πανομοιότυπη με την αρχική. Αυτή η τεχνική βασίζεται στον ψυχολογικό/συναισθηματικό χειρισμό του θύματος καθώς και στην έλλειψη γνώσης και προσοχής, με αποτέλεσμα το θύμα να αποκαλύπτει εμπιστευτικές πληροφορίες στον δράστη ή να ενεργεί ενάντια στη συνειδητή του θέληση και συνεπώς να χάνει τα χρήματά του. (OECD, 2023).

Το phishing έχει σοβαρές επιπτώσεις στον τραπεζικό τομέα, που αφορούν ιδιαίτερα την παροχή διαδικτυακής τραπεζικής, καθώς και την ασφάλεια των ηλεκτρονικών πληρωμών. Οι κυβερνοεγκληματίες συνήθως εμφανίζονται ως εκπρόσωποι τραπεζών ή άλλων αξιόπιστων οντοτήτων και ζητούν από τους χρήστες να λάβουν άμεση δράση, όπως να "επιβεβαιώσουν" τα στοιχεία του λογαριασμού τους ή να "ασφαλίσουν" συναλλαγές, κατευθύνοντάς τους σε ψεύτικες ιστοσελίδες ή εκθέτοντας ευαίσθητα δεδομένα. Οι επιτιθέμενοι που εκμεταλλεύονται αυτό το σύστημα αποκτούν πρόσβαση στους λογαριασμούς πληρωμών των χρηστών και πραγματοποιούν μεταφορές χρημάτων ή άλλες συναλλαγές χωρίς τη συγκατάθεση των πραγματικών πληρωτών.

Η ελληνική νομοθεσία σπάνια θέτει μια εννοιολογική ή θεωρητική ορισμό του phishing, επικεντρώνοντας μάλλον στη πρακτική του φύση, με όρους πραγματικών παραδειγμάτων. Ειδικότερα, σε περιπτώσεις απάτης διαδικτυακής τραπεζικής, τα δικαστήρια ορίζουν το phishing ως εμπλοκή σε εξαπάτηση του χρήστη με την προσδοκία να αποκαλύψει τα τραπεζικά του στοιχεία διαδικτυακά και να πραγματοποιηθεί πληρωτική ενέργεια μη εξουσιοδοτημένη από τρίτους. Στο πλαίσιο αυτό, μια σημαντική πτυχή είναι το γεγονός ότι οι συναλλαγές δεν είναι εξ ορισμού η θέληση του καταναλωτή και είναι αποτέλεσμα εξαπάτησης και κατάχρησης (με όρους πρόσβασης στα δεδομένα τους) (βλ. ενδεικτικά ΜΠρΑθ 71756/2025; ΕιρΒολ 36/2023). Αυτή η μέθοδος συνδέει άμεσα το phishing με το δίκαιο πληρωμών και συγκεκριμένα με την "μη εξουσιοδοτημένη πληρωτική ενέργεια" στα ευρωπαϊκά και εθνικά νομοθετικά πλαίσια. Με αυτή την απατηλή εξαγωγή των στοιχείων ασφαλείας του χρήστη, οι συναλλαγές εκτελούνται χωρίς τη συγκατάθεσή τους, οδηγώντας σε ζητήματα σχετικά με τη διανομή των ατομικών ευθυνών μεταξύ του καταναλωτή και του παρόχου υπηρεσιών πληρωμών. Από αυτή την άποψη, το phishing δεν είναι μόνο ένας τύπος γενικής ηλεκτρονικής απάτης αλλά και ένα εργαλείο που έχει άμεση επίδραση στην ασφάλεια των τραπεζικών συναλλαγών και στον δεσμό εμπιστοσύνης μεταξύ τραπεζών και πελατών τους (EBA, 2022).

Έτσι, στον τομέα της τραπεζικής, το phishing μπορεί να θεωρηθεί ως μια μορφή ηλεκτρονικής εξαπάτησης με την οποία μη εξουσιοδοτημένα τρίτα μέρη εκμεταλλεύονται την εμπιστοσύνη των χρηστών και τη φύση των ψηφιακών καναλιών συναλλαγών, αποκτώντας παράνομα πρόσβαση σε πληροφορίες σχετικά με τις διαδικτυακές τραπεζικές υπηρεσίες και πραγματοποιώντας μη εξουσιοδοτημένες πληρωτικές συναλλαγές. Η ακριβής κατανόηση του τι σημαίνει αυτός ο ορισμός είναι απαραίτητη για την ανάλυση της ευθύνης των τραπεζών και της προστασίας των καταναλωτών, η οποία θα εξεταστεί στα επόμενα κεφάλαια αυτού του έργου.

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

Οι μέθοδοι που χρησιμοποιούνται από τους δράστες επιθέσεων phishing στον τομέα της ηλεκτρονικής τραπεζικής εξελίσσονται διαρκώς και προσαρμόζονται στις τεχνολογικές εξελίξεις και στις μεταβαλλόμενες συνήθειες των χρηστών. Η δυναμική αυτή καθιστά τις επιθέσεις phishing δύσκολα προβλέψιμες, καθώς οι επιτιθέμενοι αξιοποιούν τόσο τεχνικά μέσα όσο και ψυχολογικές τεχνικές παραπλάνησης, με σκοπό την απόσπαση ευαίσθητων τραπεζικών δεδομένων και την πραγματοποίηση μη εξουσιοδοτημένων συναλλαγών (Germannos and Georgiou, 2022, ENISA, 2023).

Η πλέον διαδεδομένη μορφή phishing παραμένει η απάτη μέσω ηλεκτρονικού ταχυδρομείου (email phishing). Στην περίπτωση αυτή, οι δράστες αποστέλλουν μαζικά παραπλανητικά μηνύματα, συχνά μέσω αυτοματοποιημένων συστημάτων (spam bots), τα οποία εμφανίζονται ως δήθεν εξατομικευμένες επικοινωνίες από το τραπεζικό ίδρυμα με το οποίο συναλλάσσεται το θύμα. Τα μηνύματα αυτά είναι σχεδιασμένα έτσι ώστε να μιμούνται το ύφος, τη γλώσσα και τα λογότυπα της τράπεζας, ενισχύοντας την αξιοπιστία τους και αυξάνοντας την πιθανότητα ανταπόκρισης του χρήστη (Παπαδόπουλος, 2005; Germannos and Georgiou, 2021).

Συνήθως, τα παραπλανητικά emails περιέχουν υπερσυνδέσμους που οδηγούν σε ψευδείς ιστοσελίδες ή συνημμένα αρχεία που περιλαμβάνουν κακόβουλο λογισμικό. Οι τεχνικές που χρησιμοποιούνται περιλαμβάνουν, μεταξύ άλλων, την παραποίηση της ένδειξης του αποστολέα (email spoofing), την αλλοίωση των URLs και των hyperlinks, καθώς και την αποστολή συνημμένων αρχείων που περιέχουν ιούς ή σκουλήκια (viruses και worms). Τα

λεγόμενα spoofed μηνύματα ηλεκτρονικού ταχυδρομείου καλούν τον παραλήπτη να προβεί άμεσα σε συγκεκριμένες ενέργειες, όπως η επιβεβαίωση στοιχείων κάρτας ή η «ασφάλιση» του λογαριασμού του, οδηγώντας στην αποκάλυψη κρίσιμων τραπεζικών δεδομένων (Παπαδόπουλος, 2005; Europol, 2022).

Παρά τη βελτίωση των μηχανισμών φιλτραρίσματος ανεπιθύμητης αλληλογραφίας και τη χρήση εργαλείων τεχνητής νοημοσύνης για τον εντοπισμό ύποπτων μηνυμάτων, το email phishing εξακολουθεί να αποτελεί αποτελεσματική μέθοδο εξαπάτησης. Αυτό οφείλεται, αφενός, στο χαμηλό κόστος αποστολής μαζικών μηνυμάτων και, αφετέρου, στο γεγονός ότι ακόμη και ένα εξαιρετικά μικρό ποσοστό επιτυχίας μπορεί να αποφέρει σημαντικά οικονομικά οφέλη στους δράστες. Ενδεικτικά, έχει υποστηριχθεί ότι ποσοστό επιτυχίας της τάξης του 0,1% καθιστά την αποστολή χιλιάδων μηνυμάτων ιδιαίτερα αποδοτική για τους επιτιθέμενους (Jougleux, 2016). Σε ορισμένες περιπτώσεις, οι δράστες εισάγουν σκόπιμα ορθογραφικά ή συντακτικά λάθη στα μηνύματά τους, με στόχο να απευθυνθούν σε πιο ευάλωτες ομάδες χρηστών, οι οποίες είναι πιθανότερο να παρασυρθούν από το περιεχόμενο του μηνύματος (ENISA, 2023).

Πέραν του ηλεκτρονικού ταχυδρομείου, ιδιαίτερη διάδοση έχουν παρουσιάσει οι επιθέσεις phishing μέσω ψευδών ή παραποιημένων διαδικτυακών τόπων. Οι επιτιθέμενοι δημιουργούν ιστοσελίδες που προσομοιάζουν τον επίσημο ιστότοπο μιας τράπεζας ή άλλου παρόχου υπηρεσιών πληρωμών, χρησιμοποιώντας παρόμοια ονόματα χώρου (domain names), διευθύνσεις URL και γραφιστικό σχεδιασμό. Η πρόσβαση στις ιστοσελίδες αυτές επιτυγχάνεται συνήθως μέσω παραπλανητικών υπερσυνδέσμων που αποστέλλονται στον χρήστη μέσω email ή γραπτών μηνυμάτων, ή μέσω ανακατεύθυνσης από άλλες ιστοσελίδες (Παπαδόπουλος, 2005 and Europol, 2022).

Ιδιαίτερη μορφή της πρακτικής αυτής αποτελεί το λεγόμενο brand phishing, κατά το οποίο οι δράστες εκμεταλλεύονται τη φήμη και την αναγνωρισιμότητα συγκεκριμένων τραπεζικών επωνυμιών. Ο ψευδής ιστότοπος εμφανίζεται σχεδόν πανομοιότυπος με τον αυθεντικό, ενώ συχνά περιλαμβάνει φόρμες εισαγωγής στοιχείων που αποσκοπούν στην κλοπή διαπιστευτηρίων ηλεκτρονικής τραπεζικής, στοιχείων πληρωμής και κωδικών πρόσβασης. Με την υποβολή των στοιχείων αυτών από το θύμα, οι δράστες αποκτούν πλήρη πρόσβαση στους λογαριασμούς πληρωμών και μπορούν να προχωρήσουν σε μη εγκεκριμένες συναλλαγές (EBA, 2022; ENISA, 2023).

Οι ανωτέρω μέθοδοι καταδεικνύουν ότι το phishing στον τραπεζικό τομέα δεν αποτελεί στατικό φαινόμενο, αλλά εξελίσσεται συνεχώς, συνδυάζοντας τεχνικές παραπλάνησης με εκμετάλλευση της ανθρώπινης συμπεριφοράς. Η κατανόηση των συνηθέστερων μορφών επιθέσεων phishing αποτελεί κρίσιμο βήμα για την αξιολόγηση της επάρκειας των μέτρων κυβερνοασφάλειας και για τη διαμόρφωση αποτελεσματικών μηχανισμών προστασίας των χρηστών ηλεκτρονικής τραπεζικής.

Στο πλαίσιο αυτό, πρόκειται να εξεταστούν στη συνέχεια οι βασικότερες μορφές επιθέσεων phishing που εμφανίζονται συχνότερα κατά τη χρήση υπηρεσιών ηλεκτρονικής συναλλαγής.

1.2.1. Μαζική επίθεση

Στις μαζικές επιθέσεις phishing τα μηνύματα αποστέλλονται σε πολύ μεγάλο αριθμό χρηστών και συνήθως χωρίς καμία ιδιαίτερη στόχευση. Πρόκειται για e-mails ή SMS που μοιάζουν με ειδοποιήσεις από Τράπεζες ή άλλους αξιόπιστους φορείς και περιέχουν γενικά μηνύματα όπως ότι υπάρχει πρόβλημα με τον λογαριασμό ή ότι η χρεωστική κάρτα έχει προσωρινά μπλοκαριστεί. Το περιεχόμενο έχει δημιουργηθεί με σκοπιμότητα απλό και άμεσο ώστε να προκαλέσει ανησυχία και να τραβήξει την προσοχή του καταναλωτή. Ο δράστης στέλνει το ίδιο μήνυμα μαζικά γνωρίζοντας ότι θα το αγνοήσουν οι περισσότεροι από τους παραλήπτες. Δε χρειάζεται όμως να ανταποκριθούν όλοι. Αρκεί κάποιοι από τους χρήστες να πανικοβληθούν και να ακολουθήσουν τις οδηγίες του μηνύματος, ώστε να θεωρηθεί επιτυχημένη η επίθεση. Με αυτόν τον τρόπο οι μαζικές επιθέσεις phishing βασίζονται λιγότερο στην ποιότητα της εξαπάτησης και περισσότερο στην ανθρώπινη αντίδραση απέναντι σε ξαφνικές και φαινομενικά επείγουσες ειδοποιήσεις (Ιγγλεζάκης, 2024).

1.2.2. Στοχευμένη επίθεση (spear phishing)

Σε αυτόν τον τύπο επίθεσης το μήνυμα δεν είναι τυχαίο ούτε απρόσωπο. Είναι πιο προσεγμένο και απευθύνεται σε συγκεκριμένο άτομο ή σε μια μικρή ομάδα χρηστών. Συνήθως είναι γραμμένο στον ενικό και δίνει την εντύπωση ότι ο αποστολέας γνωρίζει προσωπικά τον παραλήπτη, γεγονός που το κάνει να μοιάζει πιο αληθινό και αξιόπιστο. Για να πετύχει τον

σκοπό του ο αποστολέας χρησιμοποιεί πληροφορίες που μπορεί εύκολα να αλιεύσει από το διαδίκτυο. Στοιχεία από κοινωνικά δίκτυα, δημόσιες αναρτήσεις, ή άλλες διαδικτυακές πηγές αρκούν για να χτιστεί ένα μήνυμα που φαίνεται προσωπικό. Ακόμη και κάτι τόσο απλό και προσωπικό όπως η χρήση του ονοματεπωνύμου του παραλήπτη μπορεί να δημιουργήσει την εντύπωση ότι πρόκειται για πραγματική και στοχευμένη επικοινωνία.

Σε πιο προχωρημένες περιπτώσεις αυτού του είδους οι επιθέσεις στρέφονται σε πρόσωπα με αυξημένη αρμοδιότητα μέσα σε έναν οργανισμό. Η πρακτική αυτή είναι γνωστή ως whaling phishing και αφορά κυρίως υψηλόβαθμα στελέχη όπως τον διευθύνοντα σύμβουλο ή τον οικονομικό διευθυντή μιας εταιρείας. Οι επιτιθέμενοι εκμεταλλεύονται τη θέση και την ευθύνη των προσώπων αυτών γνωρίζοντας ότι μια λανθασμένη ενέργεια ενδέχεται να οδηγήσει σε ιδιαίτερα σοβαρές οικονομικές συνέπειες (Alkhalil, 2021).

1.2.3. Man-in-the-middle attack

Σε αυτή τη μορφή επίθεσης phishing, ο επιτιθέμενος δεν έρχεται σε άμεση επαφή με το θύμα από την αρχή. Παρεμβάλλεται σιωπηρά στην επικοινωνία μεταξύ δύο μερών, για παράδειγμα μεταξύ ενός χρήστη και μιας νόμιμης ιστοσελίδας, και παρακολουθεί ή επηρεάζει τη ροή των μηνυμάτων χωρίς αυτό να γίνεται άμεσα αντιληπτό. Με τον τρόπο αυτό, αποκτά πρόσβαση σε πληροφορίες και από τις δύο πλευρές, είτε απλώς «ακούγοντας» την επικοινωνία, είτε τροποποιώντας το περιεχόμενό της ή εισάγοντας κακόβουλο κώδικα. Στην πράξη, τα μηνύματα δεν καταλήγουν στον πραγματικό αποδέκτη, αλλά περνούν πρώτα από τον επιτιθέμενο, ο οποίος τα ελέγχει και τα αξιοποιεί. Ένα συνηθισμένο παράδειγμα είναι η υποκλοπή επικοινωνίας μεταξύ του θύματος και ενός αξιόπιστου οργανισμού, όπως ενός τραπεζικού ιδρύματος ή ενός προμηθευτή. Ο δράστης, έχοντας πλέον εικόνα της συναλλαγής, μπορεί να παρουσιαστεί ως η νόμιμη εταιρία και να καθοδηγήσει το θύμα σε μια πληρωμή, συνήθως μέσω τραπεζικής μεταφοράς, για την υποτιθέμενη αγορά προϊόντων ή υπηρεσιών που στην πραγματικότητα δεν πρόκειται ποτέ να παραδοθούν. Συχνά, για να ενισχύσει την αξιοπιστία της απάτης, ο επιτιθέμενος χρησιμοποιεί διευθύνσεις ηλεκτρονικού ταχυδρομείου που μοιάζουν σχεδόν ταυτόσημες με τις πραγματικές, με μικρές και δύσκολα αντιληπτές παραλλαγές. Με αυτόν τον τρόπο παραπλανά το θύμα και το οδηγεί είτε σε πληρωμή προς έναν ψεύτικο λογαριασμό είτε σε ανακατεύθυνση σε δόλιο ιστότοπο, όπου αποσπώνται περαιτέρω στοιχεία (Ιγγλεζάκης, 2024).

1.2.4. Search Engine Phishing

Σε αυτή τη μορφή phishing, ο επιτιθέμενος δημιουργεί ψεύτικους ιστότοπους που παρουσιάζονται ως ιδιαίτερα ελκυστικές προσφορές ή ευκαιρίες. Στη συνέχεια, αξιοποιεί τεχνικές βελτιστοποίησης για μηχανές αναζήτησης, ώστε οι σελίδες αυτές να εμφανίζονται ψηλά στα αποτελέσματα αναζήτησης και να φαίνονται απολύτως νόμιμες. Έτσι, όταν ο χρήστης αναζητά ένα προϊόν ή μια υπηρεσία, μπορεί εύκολα να οδηγηθεί σε έναν κακόβουλο ιστότοπο χωρίς να το αντιληφθεί. Η επιτυχία της μεθόδου αυτής βασίζεται στο γεγονός ότι οι περισσότεροι χρήστες εμπιστεύονται τα πρώτα αποτελέσματα μιας αναζήτησης, θεωρώντας τα ασφαλή. Με τον τρόπο αυτό, ο επιτιθέμενος εκμεταλλεύεται την καθημερινή συμπεριφορά των χρηστών και τη φαινομενική αξιοπιστία των μηχανών αναζήτησης για να αποσπάσει προσωπικά ή οικονομικά στοιχεία (Alkhalil, 2021).

1.2.5. Επιθέσεις συσκότισης URL και HTML

Στις περισσότερες επιθέσεις phishing, ο βασικός στόχος του δράστη είναι να πείσει τον χρήστη να πατήσει έναν σύνδεσμο. Έναν σύνδεσμο που μοιάζει ακίνδυνος, αλλά στην πραγματικότητα δεν οδηγεί εκεί που φαίνεται. Αντί να κατευθυνθεί στον κανονικό διακομιστή ή στην επίσημη ιστοσελίδα που περιμένει, ο χρήστης καταλήγει σε έναν κακόβουλο ιστότοπο, χωρίς να το αντιληφθεί άμεσα. Πρόκειται για μία από τις πιο συνηθισμένες και αποτελεσματικές τεχνικές phishing σήμερα. Για να το πετύχουν αυτό, οι επιτιθέμενοι «καμουφλάρουν» τη διεύθυνση του συνδέσμου. Η πραγματική URL αλλοιώνεται με τέτοιον τρόπο ώστε να μοιάζει σχεδόν ίδια με τη νόμιμη, εκμεταλλευόμενη μικρές διαφορές που δύσκολα προσέχει ο χρήστης με μια πρώτη ματιά. Συχνά χρησιμοποιούνται παραπλανητικά ονόματα χώρου ή τροποποιήσεις στο όνομα του κεντρικού υπολογιστή, ώστε ο σύνδεσμος να φαίνεται αξιόπιστος, ενώ στην πραγματικότητα οδηγεί αλλού. Με αυτόν τον τρόπο, ο χρήστης πιστεύει ότι επισκέπτεται μια αυθεντική ιστοσελίδα, ενώ στην πράξη παραδίδει τα στοιχεία του σε έναν ψεύτικο ιστότοπο που έχει σχεδιαστεί αποκλειστικά για να τα αποσπάσει (Alkhalil, 2021).

1.2.6. Επίθεση μέσω κοινωνικής δικτύωσης (Soshing, Social Media Phishing)

Τα μέσα κοινωνικής δικτύωσης έχουν εξελιχθεί σε ένα από τα πιο “βολικά” κανάλια για τους εγκληματίες του κυβερνοχώρου όταν θέλουν να στήσουν επιθέσεις phishing. Δεν είναι μόνο ότι εκεί βρίσκονται καθημερινά εκατομμύρια χρήστες. Είναι και το ότι η επικοινωνία στα social είναι πιο άμεση και πιο «ανεπίσημη», άρα συχνά ο χρήστης δεν κρατάει την ίδια άμυνα που θα κρατούσε σε ένα τραπεζικό περιβάλλον ή σε ένα κλασικό εταιρικό email. Στο πλαίσιο αυτό, οι απειλές που συνδέονται με τα μέσα κοινωνικής δικτύωσης περιλαμβάνουν παραβιάσεις λογαριασμών χρηστών, επιθέσεις πλαστοπροσωπίας, απάτες, αλλά και διανομή κακόβουλου λογισμικού. Αυτό που κάνει τις επιθέσεις μέσω social ακόμη πιο δύσκολες στην αντιμετώπιση είναι ότι ο εντοπισμός και ο περιορισμός τους, στην πράξη, απαιτεί συχνά περισσότερο χρόνο σε σύγκριση με τις πιο “παραδοσιακές” μεθόδους phishing. Ένας λόγος είναι ότι τα μέσα κοινωνικής δικτύωσης λειτουργούν εκτός της κλασικής περιμέτρου των δικτύων, οπότε οι μηχανισμοί ελέγχου και οι διαδικασίες απόκρισης δεν είναι πάντα τόσο άμεσες ή τόσο αποτελεσματικές. Χαρακτηριστικό παράδειγμα είναι ότι το 2014 φορείς απειλών που συνδέθηκαν με έθνη-κράτη πραγματοποίησαν εκτεταμένη σειρά επιθέσεων μέσω μέσων κοινωνικής δικτύωσης κατά της Microsoft (Ramzan, 2010). Από τις επιθέσεις αυτές παραβιάστηκαν πολλοί λογαριασμοί στο Twitter και αποκαλύφθηκαν κωδικοί πρόσβασης και διευθύνσεις ηλεκτρονικού ταχυδρομείου για δεκάδες υπαλλήλους της Microsoft. Παράλληλα, σύμφωνα με στοιχεία της Kaspersky Lab, μόνο το πρώτο τρίμηνο του 2018 καταγράφηκαν περισσότερες από 3,7 εκατομμύρια προσπάθειες phishing που οδηγούσαν σε δόλιες σελίδες κοινωνικών δικτύων, ενώ το 60% αυτών αφορούσε ψεύτικες σελίδες στο Facebook (Raggo, 2016).

Όλα αυτά δείχνουν ότι το phishing στα social δεν είναι απλώς μια «παραλλαγή» των γνωστών τεχνικών. Είναι ένα πεδίο όπου η εξαπάτηση γίνεται συχνά πιο εύκολη, ακριβώς επειδή πατάει πάνω στη συνήθεια του χρήστη να εμπιστεύεται το περιβάλλον στο οποίο κινείται καθημερινά.

1.2.7. Phone phishing (Vishing and Smishing)

Τα μέσα κοινωνικής δικτύωσης αποτελούν πλέον ένα ιδιαίτερα πρόσφορο περιβάλλον για τη διεξαγωγή επιθέσεων phishing. Οι εγκληματίες του κυβερνοχώρου τα προτιμούν όχι μόνο λόγω της ευρείας χρήσης τους, αλλά και επειδή η επικοινωνία σε αυτά είναι άμεση και λιγότερο τυπική, γεγονός που μειώνει την επιφυλακτικότητα των χρηστών. Στο πλαίσιο αυτό,

οι απειλές που συνδέονται με τα μέσα κοινωνικής δικτύωσης περιλαμβάνουν την παραβίαση λογαριασμών χρηστών, επιθέσεις πλαστοπροσωπίας, διάφορες μορφές απάτης, καθώς και τη διανομή κακόβουλου λογισμικού. Ένα ζήτημα που καθιστά τις επιθέσεις αυτές πιο δύσκολες στη διαχείρισή τους είναι ότι ο εντοπισμός και ο περιορισμός τους απαιτούν συχνά περισσότερο χρόνο σε σύγκριση με τις παραδοσιακές μεθόδους phishing. Αυτό οφείλεται στο γεγονός ότι τα μέσα κοινωνικής δικτύωσης λειτουργούν εκτός της κλασικής περιμέτρου των δικτύων, με αποτέλεσμα οι μηχανισμοί ελέγχου και απόκρισης να μην ενεργοποιούνται άμεσα. Στην πράξη, η καθυστέρηση αυτή μπορεί να αποβεί καθοριστική). Χαρακτηριστικό παράδειγμα αποτελεί η σειρά επιθέσεων που πραγματοποιήθηκαν το 2014 κατά της Microsoft, από φορείς απειλών που συνδέθηκαν με έθνη-κράτη. Στο πλαίσιο των επιθέσεων αυτών παραβιάστηκαν πολλοί λογαριασμοί στο Twitter και αποκαλύφθηκαν κωδικοί πρόσβασης και διευθύνσεις ηλεκτρονικού ταχυδρομείου δεκάδων υπαλλήλων της εταιρίας.

Τα δεδομένα αυτά δείχνουν ότι το phishing μέσω κοινωνικών δικτύων δεν αποτελεί περιθωριακό φαινόμενο. Αντίθετα, συνδέεται άμεσα με τον τρόπο που οι χρήστες αντιλαμβάνονται το ίδιο το περιβάλλον των social media και με την τάση να εμπιστεύονται επικοινωνίες που εντάσσονται στην καθημερινή τους ψηφιακή δραστηριότητα.

1.2.8. SIM Swapping

Η αντικατάσταση κάρτας SIM αποτελεί μια ειδική μορφή επίθεσης phishing, με βασικό στόχο τον έλεγχο του τηλεφωνικού αριθμού του θύματος από τον δράστη. Στην πράξη ο επιτιθέμενος επικοινωνεί με τον πάροχο τηλεπικοινωνιών και χρησιμοποιώντας πλαστά έγγραφα και ψευδή στοιχεία προσποιείται ότι ενεργεί κατόπιν εξουσιοδότησης του νόμιμου κατόχου του αριθμού. Συνήθως επικαλείται απώλεια, κλοπή ή καταστροφή της αρχικής κάρτας SIM προκειμένου να αιτηθεί την έκδοση νέας. Αφού παραλάβει τη νέα κάρτα SIM, ο δράστης την ενεργοποιεί στη δική του συσκευή. Με την ενεργοποίηση αυτή, η προηγούμενη κάρτα απενεργοποιείται αυτομάτως και όλες οι επικοινωνίες που συνδέονται με τον συγκεκριμένο αριθμό, γραπτά μηνύματα και πρόσβαση στο διαδίκτυο, δρομολογούνται πλέον μέσω της συσκευής του δράστη. Με τον τρόπο αυτό, αποκτά τη δυνατότητα να λαμβάνει κωδικούς μιας χρήσης (OTP) ή μηνύματα ισχυρής ταυτοποίησης (2FA), τα οποία χρησιμοποιούνται για τη σύνδεση σε τραπεζικούς λογαριασμούς, ηλεκτρονικά πορτοφόλια ή άλλες υπηρεσίες πληρωμών (Ιγγλεζάκης, 2024).

Ως αποτέλεσμα, ο δράστης μπορεί να αποκτήσει πλήρη πρόσβαση στον λογαριασμό ηλεκτρονικής τραπεζικής του θύματος και να προχωρήσει σε μη εξουσιοδοτημένες μεταφορές χρημάτων, είτε προς τον προσωπικό του λογαριασμό είτε προς τρίτους.

Ολοκληρώνοντας την ανάλυση των συνηθέστερων μορφών επιθέσεων phishing στον χώρο της ηλεκτρονικής τραπεζικής, γίνεται σαφές ότι δεν πρόκειται απλώς για τεχνικά τεχνάσματα ή μεμονωμένα περιστατικά ψηφιακής απάτης. Αντίθετα, το phishing εξελίσσεται σε ένα σύνθετο φαινόμενο, το οποίο αξιοποιεί συστηματικά την ανθρώπινη συμπεριφορά, την εμπιστοσύνη και την καθημερινή συνήθεια των χρηστών να αλληλεπιδρούν με ψηφιακά μέσα χωρίς διαρκή επιφυλακή. Είτε πρόκειται για ένα απλό μαζικό μήνυμα, είτε για μια ιδιαίτερα στοχευμένη επίθεση, είτε για πιο σύνθετες πρακτικές όπως το man-in-the-middle ή το SIM swapping, ο κοινός παρονομαστής παραμένει ο ίδιος: η προσπάθεια του δράστη να εκμεταλλευτεί τη στιγμή αδυναμίας, άγχους ή βιασύνης του χρήστη. Το γεγονός ότι οι επιθέσεις αυτές προσαρμόζονται συνεχώς στις τεχνολογικές εξελίξεις και στις συνήθειες των χρηστών καθιστά σαφές ότι η αντιμετώπισή τους δεν μπορεί να στηριχθεί αποκλειστικά σε τεχνικά μέτρα ασφαλείας. Όσο προηγμένα και αν είναι τα συστήματα προστασίας, παραμένουν ευάλωτα όταν ο ίδιος ο χρήστης παραπλανείται. Συνεπώς, η ουσιαστική άμυνα απέναντι στο phishing προϋποθέτει συνδυασμό τεχνολογικών μηχανισμών, θεσμικών ρυθμίσεων και, κυρίως, ενίσχυση της ψηφιακής εγγραμματοσύνης και της κριτικής ικανότητας των χρηστών. Μόνο μέσα από τη συνειδητοποίηση του τρόπου με τον οποίο λειτουργούν αυτές οι επιθέσεις μπορεί να περιοριστεί αποτελεσματικά ο κίνδυνος και να ενισχυθεί η ασφάλεια των ηλεκτρονικών τραπεζικών συναλλαγών.

1.3. Το phishing ως απειλή για την ασφάλεια των τραπεζικών συναλλαγών

Η ηλεκτρονική τραπεζική έχει αλλάξει δραματικά τον τρόπο που διαχειριζόμαστε τα χρήματά μας. Σήμερα, μπορούμε να κάνουμε σχεδόν τα πάντα από απόσταση, γρήγορα και χωρίς να χρειάζεται να πάμε στην τράπεζα. Αυτή η ευκολία, όμως, δεν είναι μόνο θετική. Δημιουργεί ένα περιβάλλον όπου είμαστε πιο εκτεθειμένοι σε κινδύνους που δεν είναι πάντα εμφανείς. Ένας από τους πιο σοβαρούς κινδύνους για την ασφάλεια των τραπεζικών μας συναλλαγών είναι το phishing. Δεν πρόκειται για επίθεση που στοχεύει σε περίπλοκα συστήματα ασφαλείας. Αντίθετα, βασίζεται σε κάτι πολύ πιο απλό, αλλά και πιο ευάλωτο: τον ίδιο τον

άνθρωπο που χρησιμοποιεί την ηλεκτρονική τραπεζική (Mell, Kent and Nusbaum, 2005). Οι επιθέσεις phishing χρησιμοποιούν κυρίως τεχνικές «κοινωνικής μηχανικής». Ο απατεώνας δεν προσπαθεί να «χακάρει» την τράπεζα, αλλά να μας πείσει ότι επικοινωνούμε με κάποιον αξιόπιστο. Έτσι, καταλήγουμε να δίνουμε μόνοι μας ευαίσθητα στοιχεία, όπως κωδικούς ή στοιχεία καρτών, χωρίς να καταλάβουμε αμέσως ότι μας εξαπατούν (Furnell, 2006). Δεν είναι τυχαίο που οι πελάτες είναι ο βασικός στόχος αυτών των επιθέσεων. Οι τράπεζες επενδύουν συνεχώς σε κρυπτογράφηση και συστήματα ασφαλείας, κάνοντας την τεχνική παραβίασή τους πολύ δύσκολη. Αντίθετα, εμείς, οι χρήστες, συχνά δεν είμαστε τόσο εξοικειωμένοι με τους κινδύνους του διαδικτύου και είναι πιο εύκολο να παρασυρθούμε από ένα πειστικό μήνυμα ή μια φαινομενικά επίσημη ειδοποίηση (Utakrit, 2012).

Η πιο συνηθισμένη μορφή phishing είναι τα παραπλανητικά email. Αυτά τα μηνύματα μοιάζουν με ειδοποιήσεις από τράπεζες και μας δημιουργούν ένα αίσθημα επείγοντος. Μας ζητούν να δράσουμε άμεσα, συνήθως πατώντας σε έναν σύνδεσμο που οδηγεί σε μια ψεύτικη ιστοσελίδα, σχεδόν ίδια με την πραγματική (Papadopoulos, 2005). Σε πολλές περιπτώσεις, η απάτη δεν σταματά εκεί. Μέσω συνημμένων αρχείων ή κακόβουλου κώδικα, ο δράστης μπορεί να εγκαταστήσει λογισμικό που κλέβει τα δεδομένα μας χωρίς εμείς να καταλάβουμε τίποτα περίεργο. Έτσι, η παραβίαση μπορεί να συνεχίζεται για καιρό χωρίς εμφανή σημάδια (Cole, 2012). Τα τελευταία χρόνια, το phishing έχει προσαρμοστεί στις νέες συνήθειές μας. Επιθέσεις μέσω μηνυμάτων στα κινητά, των κοινωνικών δικτύων και των εφαρμογών είναι πλέον εξίσου συχνές. Οι απατεώνες μας ακολουθούν παντού, αυξάνοντας τα σημεία όπου μπορούμε να εκτεθούμε σε κίνδυνο (Gupta et al., 2018).

Οι συνέπειες τέτοιων επιθέσεων δεν είναι μόνο η άμεση απώλεια χρημάτων. Εκτός από τα χρήματα που μπορεί να χάσουμε από τον λογαριασμό μας, υπάρχει και ένα σημαντικό έμμεσο κόστος. Οι τράπεζες επιβαρύνονται με έρευνες, αποκαταστάσεις και υποστήριξη πελατών, ενώ εμείς οι ίδιοι χάνουμε χρόνο και νιώθουμε ανασφαλείς στις συναλλαγές μας (Jakobsson and Myers, 2007). Ακόμη πιο σημαντικό είναι το πλήγμα στην εμπιστοσύνη. Όταν νιώθουμε ότι κινδυνεύουμε, αποφεύγουμε τα ψηφιακά κανάλια και επιστρέφουμε σε πιο παραδοσιακές συναλλαγές. Αυτό δεν επηρεάζει μόνο την καθημερινότητά μας, αλλά και τη συνολική λειτουργία του τραπεζικού συστήματος (Utakrit, 2012). Αν και το phishing δεν είναι καινούργια απειλή, παραμένει πολύ αποτελεσματικό. Οι σύγχρονες επιθέσεις είναι πλέον τόσο καλοσχεδιασμένες, που ακόμη και έμπειροι χρήστες δυσκολεύονται να ξεχωρίσουν το αληθινό από το ψεύτικο. Έρευνες δείχνουν ότι η οπτική και λειτουργική ομοιότητα των ψεύτικων

ιστοσελίδων με τις αυθεντικές παίζει καθοριστικό ρόλο στην επιτυχία της απάτης (Dhamija et al., 2006). Η διεθνής βιβλιογραφία δείχνει ότι το να πέσουμε θύμα δεν σημαίνει απαραίτητα άγνοια. Συχνά προκύπτει από μια στιγμή απροσεξίας ή από νέες μεθόδους απάτης που δεν έχουν γίνει ακόμη ευρέως γνωστές. Έτσι, οποιοσδήποτε από εμάς μπορεί να βρεθεί εκτεθειμένος (Alsharnouby, Alaca and Chiasson, 2015, Jansen and Leukfeldt, 2016).

Το phishing, λοιπόν, παραμένει μια ζωντανή και εξελισσόμενη απειλή για την ασφάλεια των τραπεζικών συναλλαγών μας. Η αντιμετώπισή του δεν μπορεί να βασιστεί μόνο στην τεχνολογία. Χρειάζεται συνεχή ενημέρωση, εκπαίδευση και ενίσχυση της κριτικής μας ικανότητας, καθώς η ασφάλεια της ηλεκτρονικής τραπεζικής εξαρτάται σε μεγάλο βαθμό από τον ανθρώπινο παράγοντα (Rashid, 2012).

Κεφάλαιο 2: Νομική προστασία του καταναλωτή στις ηλεκτρονικές πληρωμές και στις απάτες phishing

2.1. Η προστασία του καταναλωτή στο πλαίσιο των ηλεκτρονικών πληρωμών-Βασικό νομοθετικό πλαίσιο-ΓΣΟ

Οι ηλεκτρονικές συναλλαγές, και ιδίως οι πληρωμές που πραγματοποιούνται μέσω διαδικτύου, εντάσσονται στο ευρύτερο πλαίσιο των συμβάσεων από απόσταση, καθώς τα συμβαλλόμενα μέρη δεν βρίσκονται ποτέ σε φυσική επαφή. Ο καταναλωτής καλείται να συνάψει σύμβαση και να προβεί σε πληρωμή χωρίς να έχει άμεση εικόνα του αγαθού ή της υπηρεσίας, ούτε τη δυνατότητα προσωπικής επικοινωνίας με τον αντισυμβαλλόμενο του. Το στοιχείο αυτό θεωρείται κρίσιμο από τον νομοθέτη, καθώς κατά τη στιγμή της δήλωσης βούλησης ο καταναλωτής συχνά δεν διαθέτει επαρκή γνώση ούτε για το αντικείμενο της σύμβασης ούτε για το πραγματικό περιεχόμενο των όρων που τη διέπουν, γεγονός που τον καθιστά ευάλωτο σε καταχρηστικές πρακτικές (Δούβλης και Μπώλος, 2008).

Για τον λόγο αυτό, τόσο ο εθνικός όσο και ο ενωσιακός νομοθέτης έχουν θεσπίσει ένα πλέγμα προστατευτικών διατάξεων, οι οποίες λειτουργούν ως δικλείδες ασφαλείας υπέρ του καταναλωτή. Οι διατάξεις αυτές αφορούν αφενός το προσυμβατικό στάδιο, όπου ο αντισυμβαλλόμενος του καταναλωτή υπέχει αυξημένες υποχρεώσεις ενημέρωσης και

διαφάνειας, και αφετέρου το μεταγενέστερο στάδιο της σύμβασης, κατά το οποίο ο καταναλωτής απολαμβάνει ειδικά δικαιώματα λόγω της φύσης της συναλλαγής ως σύμβασης από απόσταση. Οι ρυθμίσεις αυτές αποκτούν ιδιαίτερη σημασία στις ηλεκτρονικές πληρωμές, όπου η ταχύτητα και η αυτοματοποίηση της διαδικασίας συχνά δεν αφήνουν περιθώριο ουσιαστικής στάθμισης των κινδύνων από την πλευρά του καταναλωτή. Στον πυρήνα της ελληνικής νομοθεσίας για την προστασία του καταναλωτή βρίσκεται ο ν. 2251/1994, ο οποίος έχει υποστεί αλλεπάλληλες τροποποιήσεις προκειμένου να ευθυγραμμιστεί με το ενωσιακό δίκαιο. Σημαντική επιρροή στη διαμόρφωσή του άσκησαν, μεταξύ άλλων, η Οδηγία 93/13/ΕΟΚ για τις καταχρηστικές ρήτρες, η Οδηγία 97/7/ΕΚ για τις εξ αποστάσεως συμβάσεις, η Οδηγία 2005/29/ΕΚ για τις αθέμιτες εμπορικές πρακτικές, η Οδηγία 2011/83/ΕΕ για τα δικαιώματα των καταναλωτών, καθώς και οι νεότερες Οδηγίες (ΕΕ) 2019/2161, 2019/770 και 2019/771, οι οποίες ενσωματώθηκαν στην ελληνική έννομη τάξη με τους ν. 4933/2022 και 4967/2022 αντίστοιχα. Ως εκ τούτου, οι συμβάσεις που συνάπτονται μέσω διαδικτύου και συνοδεύονται από ηλεκτρονικές πληρωμές υπάγονται πλήρως στο προστατευτικό αυτό πλαίσιο (Οδηγία (ΕΕ) 2019/770).

Ιδιαίτερη σημασία στο πλαίσιο των ηλεκτρονικών πληρωμών έχουν οι γενικοί όροι συναλλαγών, οι οποίοι στις περισσότερες περιπτώσεις είναι προδιατυπωμένοι και εφαρμόζονται σε μεγάλο αριθμό συμβάσεων. Οι όροι αυτοί ρυθμίζουν κρίσιμα ζητήματα της συναλλαγής, όπως τις διαδικασίες πληρωμής, τις ευθύνες των μερών, τις επιστροφές χρημάτων και τις εγγυήσεις (Ιγγλεζάκης, 2008). Ωστόσο, το γεγονός ότι δεν αποτελούν αντικείμενο ατομικής διαπραγμάτευσης δημιουργεί σοβαρό κίνδυνο για τον καταναλωτή, ιδίως όταν οι όροι είναι δυσνόητοι, εκτενείς ή διατυπωμένοι κατά τρόπο που αποθαρρύνει την ανάγνωσή τους. Δεν είναι σπάνιο να περιλαμβάνουν ρήτρες που περιορίζουν υπέρμετρα την ευθύνη του προμηθευτή ή επιβαρύνουν δυσανάλογα τον καταναλωτή, γεγονός που αναδεικνύει την ανισορροπία ισχύος μεταξύ των συμβαλλομένων μερών (Καράκωστας, 2009).

Το άρθρο 2 του ν. 2251/1994 αφιερώνεται ειδικά στους γενικούς όρους συναλλαγών και θέτει τις βασικές αρχές που διέπουν τη χρήση τους. Προβλέπεται, καταρχάς, ότι οι προδιατυπωμένοι όροι δεν δεσμεύουν τον καταναλωτή όταν αυτός τους αγνοούσε ανυπαίτιως κατά τη σύναψη της σύμβασης, ιδίως όταν δεν του επισημάνθηκε η ύπαρξή τους ή δεν είχε πραγματική δυνατότητα να λάβει γνώση του περιεχομένου τους. Παράλληλα, οι όροι αυτοί πρέπει να διατυπώνονται γραπτώς, στην ελληνική γλώσσα, με σαφή και εύληπτο τρόπο, ώστε ο καταναλωτής να μπορεί να κατανοήσει το νόημά τους, ενώ οι ειδικοί όροι που συμφωνούνται

κατόπιν ατομικής διαπραγμάτευσης υπερισχύουν των γενικών. Σε περίπτωση αμφιβολίας ως προς την ερμηνεία τους, οι όροι που διατυπώθηκαν μονομερώς ερμηνεύονται υπέρ του καταναλωτή, σύμφωνα με την ανάγκη ενίσχυσης της προστασίας του. Ως βασικά χαρακτηριστικά των γενικών όρων συναλλαγών αναγνωρίζονται η εκ των προτέρων διατύπωσή τους και η προορισμένη για πολλαπλή χρήση εφαρμογή τους (Μεντής, 2020). Η μεταβολή της διατύπωσης του νόμου, από την αναφορά σε «απροσδιόριστο αριθμό μελλοντικών συμβάσεων» σε απλή αναφορά σε «μελλοντικές συμβάσεις», καταδεικνύει ότι δεν απαιτείται η πραγματική πολλαπλή χρήση ενός όρου, αλλά αρκεί ο προορισμός του για ομοιόμορφη εφαρμογή. Η προσθήκη της απαίτησης της έγγραφης μορφής με τον ν. 3587/2007 δημιούργησε προβληματισμούς ως προς την υπαγωγή προφορικών όρων στον έλεγχο καταχρηστικότητας. Η απάντηση δόθηκε με την παρ. 9 του άρθρου 2, η οποία επιτρέπει τον έλεγχο κάθε όρου που δεν αποτέλεσε αντικείμενο ατομικής διαπραγμάτευσης, υπό συγκεκριμένες προϋποθέσεις, καθορίζοντας ταυτόχρονα τα βάρη απόδειξης για τα συμβαλλόμενα μέρη (Δέλλιος, 2013).

Η ανάγκη ύπαρξης ειδικού καταναλωτικού πλαισίου αναδεικνύεται και από την αιτιολογική έκθεση του ν. 4512/2018, όπου επισημαίνεται ότι, παρά την εφαρμογή των γενικών διατάξεων του Αστικού Κώδικα, και ιδίως των άρθρων 281 και 288, τα δικαστήρια δεν κατόρθωναν πάντοτε να εξασφαλίσουν επαρκή επίπεδα προστασίας για τον καταναλωτή. Η εξειδικευμένη ρύθμιση των γενικών όρων συναλλαγών κρίθηκε, συνεπώς, αναγκαία. Στις ηλεκτρονικές συναλλαγές, ο καταναλωτής πρέπει να έχει τη δυνατότητα να λάβει γνώση των γενικών όρων ήδη πριν από την ολοκλήρωση της πληρωμής. Η πρακτική αυτή ενισχύεται και από το ΠΔ 131/2003, το οποίο προβλέπει ότι οι όροι της σύμβασης πρέπει να παρέχονται κατά τρόπο που να επιτρέπει την αποθήκευση και την αναπαραγωγή τους. Η υποχρέωση αυτή αποκτά ιδιαίτερη σημασία στο ψηφιακό περιβάλλον, όπου η προσβασιμότητα των όρων αποτελεί προϋπόθεση για την ουσιαστική ενημέρωση του καταναλωτή (Αιτιολογική Έκθεση ν. 4512/2018).

Τέλος, ο έλεγχος καταχρηστικότητας των γενικών όρων συναλλαγών πραγματοποιείται τόσο μέσω μιας γενικής ρήτρας ακυρότητας όσο και μέσω ενός ενδεικτικού καταλόγου συγκεκριμένων κατηγοριών όρων που θεωρούνται καταχρηστικοί. Ο νομοθέτης επιλέγει να ακυρώνει τον καταχρηστικό όρο χωρίς να οδηγεί αυτομάτως σε ακυρότητα ολόκληρης της σύμβασης, καθώς ο προμηθευτής δεν μπορεί να επικαλεστεί την ακυρότητα προς ίδιον όφελος. Από τον συνδυασμό των σχετικών διατάξεων προκύπτει ότι η ακυρότητα λειτουργεί υπέρ του

καταναλωτή, διασφαλίζοντας ότι η σύμβαση διατηρείται στο μέτρο που δεν προσβάλλει την προστασία που του παρέχει ο νόμος (Τσιαφούτης, 2021).

2.2. Νομικό πλαίσιο θεμελίωσης ευθύνης της Τράπεζας από απάτες phishing

2.2.1. Ενδοσυμβατική ευθύνη

Όταν ολοκληρωθεί μια απάτη phishing, το θύμα συνήθως αντιλαμβάνεται τι έχει συμβεί τη στιγμή που συνδέεται στον ηλεκτρονικό τραπεζικό του λογαριασμό και διαπιστώνει ότι τα χρήματά του έχουν εξαφανιστεί. Η πρώτη αντίδραση είναι σχεδόν πάντα η ίδια. Επικοινωνεί με την τράπεζα, αναζητώντας εξηγήσεις και αποκατάσταση της ζημίας. Στην πράξη, όμως, η απάντηση που λαμβάνει συχνά δεν είναι αυτή που θα ανέμενε. Η τράπεζα αποποιείται την ευθύνη της, αποδίδοντας την απώλεια σε αμέλεια του ίδιου του πελάτη, ιδίως όταν έχει προηγηθεί αποκάλυψη στοιχείων όπως το username και το password. Έτσι τίθεται ένα κρίσιμο ερώτημα. Αν η αποκάλυψη αυτών των στοιχείων αρκεί πράγματι για να απαλλάξει την τράπεζα από κάθε ευθύνη ή αν, παρά τη συμπεριφορά του πελάτη, εξακολουθεί να υφίσταται νομική υποχρέωση αποζημίωσης. Η απάντηση στο ερώτημα αυτό δεν μπορεί να δοθεί χωρίς να εξεταστεί πρώτα η ίδια η φύση της τραπεζικής κατάθεσης. Η κατάθεση χρημάτων σε τράπεζα δεν αποτελεί απλώς μια τεχνική πράξη φύλαξης, αλλά φέρει τον χαρακτήρα της ανώμαλης παρακαταθήκης. Σύμφωνα με το άρθρο 830 παρ. 1 ΑΚ, εφαρμόζονται αφενός οι διατάξεις περί δανείου του άρθρου 806 ΑΚ, βάσει των οποίων η τράπεζα αποκτά την κυριότητα των κατατεθειμένων χρημάτων, και αφετέρου το άρθρο 827 ΑΚ, που επιβάλλει την υποχρέωση απόδοσης των χρημάτων στον καταθέτη όταν εκείνος τα ζητήσει. Στην πράξη, αυτό σημαίνει ότι, αν τρίτο πρόσωπο μέσω αξιόποινης πράξης καταφέρει να αποσπάσει τα χρήματα, η περιουσιακή ζημία πλήττει πρωτίστως την τράπεζα, ως κυρία των χρημάτων. Η αξίωση του καταθέτη από τη σύμβαση της ανώμαλης παρακαταθήκης παραμένει ακέραιη, εκτός αν συντρέχει λόγος απαλλαγής της τράπεζας κατά το άρθρο 3 του Ν.Δ. 17.7/13.8.1923, όπως έχει γίνει δεκτό και από τη νομολογία (ΑΠ 830/2003 Δ 45.176, ΑΠ 1083/1991).

Το πλαίσιο αυτό συμπληρώνεται από τις ειδικές υποχρεώσεις που φέρει η τράπεζα ως θεματοφύλακας. Το άρθρο 824 ΑΚ δεν της επιτρέπει να μεταχειρίζεται τα κατατεθειμένα χρήματα χωρίς την άδεια του παρακαταθέτη, ούτε να τα καταθέτει σε τρίτο, εκτός αν αυτό

επιβάλλεται από τις περιστάσεις ή αποτελεί συνήθη πρακτική. Όταν η τράπεζα παραβιάζει αυτούς τους κανόνες, το άρθρο 825 ΑΚ προβλέπει ευθύνη της για κάθε πταίσμα έναντι του πελάτη, ενώ η συμπεριφορά της κρίνεται και υπό το πρίσμα των διατάξεων περί εντολής των άρθρων 713 επ. ΑΚ. Η νομική αυτή βάση δείχνει ότι η ευθύνη της τράπεζας δεν περιορίζεται απλώς στη μηχανική εκτέλεση συναλλαγών.

Η σύμβαση παροχής υπηρεσιών ηλεκτρονικής τραπεζικής εντάσσεται σε αυτό το πλαίσιο και παρουσιάζει χαρακτήρα μικτής σύμβασης. Από τη μία πλευρά, περιλαμβάνει στοιχεία εντολής, καθώς η τράπεζα εκτελεί μεταφορές χρημάτων κατ' εντολή του πελάτη. Από την άλλη, ενσωματώνει στοιχεία σύμβασης έργου, δεδομένου ότι η τράπεζα αναλαμβάνει να οργανώσει και να λειτουργήσει ένα ασφαλές σύστημα ηλεκτρονικών συναλλαγών, έναντι αμοιβής είτε με τη μορφή συνδρομής είτε μέσω προμηθειών. Κατά την εκτέλεση της σύμβασης αυτής, η τράπεζα οφείλει να ενεργεί σύμφωνα με την καλή πίστη και τα συναλλακτικά ήθη, όπως επιβάλλουν τα άρθρα 200 και 288 ΑΚ. Στις περιπτώσεις απάτης phishing, το ζήτημα μετατοπίζεται από την απλή ύπαρξη απώλειας χρημάτων στην αιτία της απώλειας. Ιδιαίτερη σημασία αποκτά το αν η μεταφορά πραγματοποιήθηκε χωρίς τη βούληση και τη συναίνεση του πελάτη, ως αποτέλεσμα πλημμελούς εκτέλεσης των υπηρεσιών ηλεκτρονικής τραπεζικής. Στην πράξη, εξετάζεται αν η τράπεζα έλαβε τα κατάλληλα μέτρα ασφαλείας ή αν η απώλεια οφείλεται σε βαριά αμέλεια ως προς την προστασία των συναλλαγών.

Κεντρικό ρόλο στο σημείο αυτό διαδραματίζει η ταυτοποίηση του χρήστη και ιδίως η ισχυρή ταυτοποίηση πελάτη. Σύμφωνα με το άρθρο 4 περ. 29 του Ν. 4537/2018, ταυτοποίηση είναι η διαδικασία μέσω της οποίας ο πάροχος υπηρεσιών πληρωμών επαληθεύει την ταυτότητα του χρήστη ή την εγκυρότητα χρήσης συγκεκριμένου μέσου πληρωμής, με τη χρήση εξατομικευμένων διαπιστευτηρίων ασφάλειας. Αντίστοιχα, η Οδηγία (ΕΕ) 2015/2366 ορίζει την ισχυρή ταυτοποίηση ως διαδικασία που βασίζεται στη χρήση δύο ή περισσότερων στοιχείων που αφορούν γνώση, κατοχή και εγγενές χαρακτηριστικό του χρήστη, τα οποία είναι ανεξάρτητα μεταξύ τους και σχεδιασμένα ώστε να προστατεύεται η εμπιστευτικότητα των δεδομένων.

Στην πράξη, η ισχυρή ταυτοποίηση προϋποθέτει συνδυασμό στοιχείων, όπως κωδικό ή PIN, στοιχείο κατοχής, για παράδειγμα μια κάρτα ή κινητή συσκευή, και κάποιο μοναδικό βιομετρικό χαρακτηριστικό, όπως το δακτυλικό αποτύπωμα ή η αναγνώριση φωνής. Το κανονιστικό πλαίσιο, ωστόσο, προβλέπει και εξαιρέσεις από την υποχρέωση εφαρμογής της,

ιδίως για συναλλαγές που κρίνονται χαμηλού κινδύνου, σύμφωνα με το άρθρο 18 του Κανονισμού (ΕΕ) 389/2018 (Μήτσου, 2021).

Καθοριστικό στοιχείο για την κατανομή της ευθύνης αποτελεί, τελικά, το αν μια πράξη πληρωμής μπορεί να θεωρηθεί εγκεκριμένη. Το άρθρο 64 του Ν. 4537/2018 ορίζει ότι πράξη πληρωμής είναι εγκεκριμένη μόνο όταν ο πληρωτής έχει δώσει τη συγκατάθεσή του για την εκτέλεσή της. Αν η συγκατάθεση αυτή απουσιάζει, η πράξη θεωρείται μη εγκεκριμένη. Η γνησιότητα της πράξης πληρωμής, όπως εξειδικεύεται στο άρθρο 72 του ίδιου νόμου, προϋποθέτει την πραγματική συναίνεση του χρήστη και δεν υφίσταται όταν η συναλλαγή πραγματοποιείται από τρίτο χωρίς δικαίωμα, ακόμη και αν τυπικά φαίνεται ότι ακολουθήθηκαν οι συμφωνημένες διαδικασίες.

Σε αυτές τις περιπτώσεις, και εφόσον ο χρήστης ενημερώσει την τράπεζα χωρίς υπαίτια καθυστέρηση, το άρθρο 71 του Ν. 4537/2018 του αναγνωρίζει δικαίωμα αποζημίωσης από τον πάροχο υπηρεσιών πληρωμών. Χαρακτηριστική εφαρμογή των ανωτέρω αποτελεί η απόφαση ΕιρΜυτ 24/2023, με την οποία κρίθηκε ότι δεν αποδείχθηκε η γνησιότητα της επίδικης συναλλαγής, καθώς κανένας από τους δικαιούχους του λογαριασμού δεν είχε παράσχει συγκατάθεση. Ιδιαίτερη βαρύτητα αποδόθηκε στο γεγονός ότι δεν είχε αποσταλεί κωδικός μιας χρήσης (OTP) για την έγκριση της συναλλαγής, γεγονός που οδήγησε το δικαστήριο να απορρίψει τους ισχυρισμούς της τράπεζας περί απαλλαγής της ευθύνης της και να την υποχρεώσει σε αποζημίωση του θύματος.

2.2.2. Αδικοπρακτική ευθύνη

Όσον αφορά τη θεμελίωση ευθύνης της τράπεζας από αδικοπραξία, αφετηρία αποτελεί η γενική διάταξη του άρθρου 914 ΑΚ, σύμφωνα με την οποία όποιος προκαλεί ζημία σε άλλον με παράνομη και υπαίτια συμπεριφορά υποχρεούται σε αποζημίωση. Για να γεννηθεί αδικοπρακτική ευθύνη απαιτείται, αφενός, η ύπαρξη ζημίας που να οφείλεται σε παράνομη και υπαίτια πράξη ή παράλειψη, δηλαδή σε δόλο ή αμέλεια κατά την έννοια του άρθρου 330 ΑΚ, και αφετέρου να υφίσταται αιτιώδης σύνδεσμος μεταξύ της συμπεριφοράς αυτής και της ζημίας που επήλθε. Η νομολογία έχει επανειλημμένως επισημάνει ότι χωρίς την ύπαρξη πρόσφορης αιτιώδους συνάφειας δεν μπορεί να θεμελιωθεί αξίωση αποζημίωσης (ΑΠ 263/1996 ΕλλΔνη 37.1453, ΑΠ 574/1994 ΕλλΔνη 36.828). Η έννοια της παρανομίας δεν

περιορίζεται μόνο στην παραβίαση συγκεκριμένης απαγορευτικής διάταξης. Παρανομία συνιστά και η παράβαση της γενικής υποχρέωσης πρόνοιας και ασφάλειας που επιβάλλεται στο πλαίσιο της συναλλακτικής και κοινωνικής δραστηριότητας. Η υποχρέωση αυτή απορρέει από τις διατάξεις των άρθρων 281 και 288 ΑΚ και από τη θεμελιώδη αρχή της συνεπούς συμπεριφοράς, σύμφωνα με την οποία κάθε πρόσωπο οφείλει να λαμβάνει τα αναγκαία μέτρα επιμέλειας ώστε να μην προκαλεί ζημία σε έννομα αγαθά τρίτων.

Στην περίπτωση των τραπεζικών ιδρυμάτων, η υποχρέωση αυτή αποκτά ιδιαίτερη βαρύτητα λόγω της σχέσης εμπιστοσύνης που τα συνδέει με τους πελάτες τους. Οι τράπεζες οφείλουν να διαθέτουν επαρκή εσωτερική οργάνωση και να μεριμνούν ενεργά για την προστασία των συμφερόντων των πελατών τους. Στο πλαίσιο αυτό, ειδικότερες εκφάνσεις της υποχρέωσης πρόνοιας και ασφάλειας αποτελούν η υποχρέωση ενημέρωσης και διαφώτισης των πελατών, καθώς και η τήρηση αυξημένων κανόνων ασφάλειας για τη θωράκιση τόσο της περιουσίας όσο και των προσωπικών δεδομένων των χρηστών υπηρεσιών ηλεκτρονικής τραπεζικής. Η λήψη τεχνικών μέτρων από τους παρόχους εξ αποστάσεως τραπεζικών υπηρεσιών, με σκοπό την αποτροπή ή έστω τον περιορισμό φαινομένων παράνομης απόσπασης προσωπικών στοιχείων και κωδικών, μπορεί να περιλαμβάνει, μεταξύ άλλων, τη διπλή ταυτοποίηση και την αποστολή κωδικού μιας χρήσης μέσω κινητού τηλεφώνου για την ολοκλήρωση συναλλαγών. Όταν τα μέτρα αυτά δεν εφαρμόζονται ή αποδεικνύονται ανεπαρκή, η παράλειψη αυτή δύναται να θεμελιώσει αδικοπρακτική ευθύνη της τράπεζας (Τζίβα, 2021).

Κομβικό ρόλο στη θωράκιση των συμφερόντων των πελατών διαδραματίζει η υποχρέωση πληροφόρησης, η οποία διατρέχει όλα τα στάδια της συναλλακτικής σχέσης με την τράπεζα. Ιδίως στις περιπτώσεις αυθαίρετων ή ύποπτων συναλλαγών, αποκτά σημασία το αν η τράπεζα προέβη σε έλεγχο συναλλαγών που αποκλίνουν από το συνήθες συναλλακτικό προφίλ του πελάτη και αν υπήρξε έγκαιρη ενημέρωση ή τηλεφωνική επιβεβαίωση. Οι υποχρεώσεις αυτές απορρέουν τόσο από τον Κώδικα Τραπεζικής Δεοντολογίας, στο πλαίσιο της διαφάνειας των συναλλαγών, όσο και από τις προβλέψεις του Ν. 4457/2018. Παράλληλα, το πιστωτικό ίδρυμα οφείλει να συλλέγει και να αξιολογεί πληροφορίες σχετικά με τον σκοπό και το αντικείμενο της συναλλακτικής σχέσης που συνδέεται με μια ύποπτη συναλλαγή.

Η Τράπεζα της Ελλάδος, με την ΠΕΕ 190/2/16.06.2021, έχει εξειδικεύσει τις απαιτήσεις και τις υποχρεώσεις των πιστωτικών ιδρυμάτων ως προς τη διαχείριση κινδύνων ΤΠΕ και την ασφάλεια των συστημάτων τους. Ιδιαίτερη μνεία γίνεται στο κεφάλαιο VIII της πράξης αυτής,

όπου τονίζεται η ανάγκη ύπαρξης διαδικασιών πρόληψης, εντοπισμού και αποκατάστασης ευπαθειών στα συστήματα ασφαλείας. Στην πράξη, αυτό σημαίνει ότι όταν εμφανίζονται ιστοσελίδες που μιμούνται την επίσημη ιστοσελίδα μιας τράπεζας, το πιστωτικό ίδρυμα οφείλει να ενημερώνει εγκαίρως τους πελάτες του και να λαμβάνει αυξημένα μέτρα προστασίας προκειμένου να τους προφυλάξει από κακόβουλες ενέργειες. Πρόσθετο επίπεδο υποχρεώσεων απορρέει από το άρθρο 13 του Ν. 4557/2018, το οποίο επιβάλλει στα πιστωτικά ιδρύματα την εφαρμογή μέτρων συνήθους δέουσας επιμέλειας προς τον σκοπό της πρόληψης της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας. Στα μέτρα αυτά περιλαμβάνεται η επαλήθευση της ταυτότητας του πελάτη και του πραγματικού δικαιούχου πριν από τη σύναψη επιχειρηματικής σχέσης ή την πραγματοποίηση συναλλαγής. Η μη εφαρμογή των προβλεπόμενων διαδικασιών συνιστά παράνομη συμπεριφορά που αντίκειται τόσο στην Οδηγία 849/2015 όσο και στον Ν. 4557/2018 και στον Κώδικα Τραπεζικής Δεοντολογίας.

Ιδιαίτερο ενδιαφέρον παρουσιάζει η απόφαση ΕιρΘεσ 232/2023, με την οποία κρίθηκε ότι η εναγόμενη τράπεζα έφερε ευθύνη για πλημμελή θωράκιση των συστημάτων ασφαλείας της έναντι των εξελισσόμενων μεθόδων ηλεκτρονικής απάτης, γεγονός που οδήγησε σε περιουσιακή ζημία του πελάτη. Το δικαστήριο υποχρέωσε την τράπεζα στην καταβολή αποζημίωσης ύψους 2.500 ευρώ, αναγνωρίζοντας ωστόσο και συντρέχουσα ευθύνη του ενάγοντος, ο οποίος δεν διαφύλαξε επαρκώς τα προσωπικά τραπεζικά του στοιχεία και τα γνωστοποίησε στον δράστη (Lawspot.gr, 2023).

Υπό το πρίσμα των ανωτέρω, καθίσταται αναγκαία η περαιτέρω εξέταση της προστασίας του χρήστη ηλεκτρονικής τραπεζικής από πρακτικές phishing, η οποία αναλύεται στη συνέχεια.

2.3. Νομικό πλαίσιο ευθύνης πληρωτή από μη εγκεκριμένες πράξεις πληρωμής

Σύμφωνα με το προγενέστερο νομοθετικό καθεστώς του άρθρου 74 του Ν. 4537/2018, ο πληρωτής έφερε ευθύνη για τις ζημίες που προέκυπταν από πρακτικές εξαπάτησης τύπου phishing, εφόσον αυτές οφείλονταν σε δόλο ή βαριά αμέλειά του. Η προσέγγιση αυτή στηριζόταν στην αντίληψη ότι ο χρήστης των μέσων πληρωμής φέρει αυξημένη ευθύνη για τη διαχείριση και την προστασία των προσωπικών του στοιχείων, ακόμη και σε ένα περιβάλλον

αυξημένων ψηφιακών κινδύνων. Ωστόσο, η συνεχής εξέλιξη των μεθόδων ηλεκτρονικής απάτης ανέδειξε την ανάγκη αναθεώρησης του πλαισίου αυτού. Στο πλαίσιο αυτό, με τον Ν. 5019/2023 εισήχθησαν νέοι κανόνες, οι οποίοι τέθηκαν σε ισχύ από την 1η Σεπτεμβρίου 2023, σε εναρμόνιση με την Οδηγία 2020/1828. Οι ρυθμίσεις αυτές στοχεύουν στην ενίσχυση της προστασίας του καταναλωτή από πρακτικές phishing, οι οποίες εκδηλώνονται μέσω πλαστών ιστοσελίδων, παραπλανητικών ηλεκτρονικών μηνυμάτων ή ειδοποιήσεων και αποσκοπούν στην απόσπαση ευαίσθητων προσωπικών κωδικών, όπως PIN και TAN, με σκοπό τη διενέργεια μη εξουσιοδοτημένων μεταφορών χρημάτων (Lawspot.gr, 2023).

Ιδιαίτερη σημασία παρουσιάζει το άρθρο 22 του Ν. 5019/2023, με το οποίο τροποποιήθηκε η παράγραφος 1 του άρθρου 74 του Ν. 4537/2018 και επαναπροσδιορίστηκε το καθεστώς ευθύνης του πληρωτή για μη εγκεκριμένες πράξεις πληρωμής. Σύμφωνα με τη νέα ρύθμιση, και κατά παρέκκλιση από το άρθρο 73 που θεμελιώνει την ευθύνη του παρόχου υπηρεσιών πληρωμών, ο πληρωτής ευθύνεται έως του ανώτατου ποσού των πενήντα ευρώ για ζημίες που προκύπτουν από τη χρήση απολεσθέντος ή κλαπέντος μέσου πληρωμών ή από υπεξαίρεσή του.

Παράλληλα, προβλέπεται ότι ο πληρωτής δεν ευθύνεται για ζημίες που προκλήθηκαν από phishing, όταν η απώλεια, κλοπή ή υπεξαίρεση του μέσου πληρωμών δεν μπορούσε να εντοπιστεί από τον ίδιο πριν από τη διενέργεια της πράξης πληρωμής ή όταν η ζημία οφείλεται σε πράξεις ή παραλείψεις, ιδίως υπαλλήλων ή υποκαταστημάτων παρόχου υπηρεσιών πληρωμών, όπως είναι τα πιστωτικά ιδρύματα. Στην περίπτωση, όμως, που ο πληρωτής έχει την ιδιότητα του καταναλωτή, ο νόμος προβλέπει ότι ευθύνεται μέχρι του ποσού των 1.000,00 ευρώ, εφόσον οι ζημίες οφείλονται σε βαριά αμέλεια. Όταν ο αντισυμβαλλόμενος του τραπεζικού ιδρύματος είναι καταναλωτής, εφαρμογή βρίσκουν επιπλέον και οι διατάξεις του άρθρου 8 του Ν. 2251/1994 περί προστασίας του καταναλωτή. Σύμφωνα με τις διατάξεις αυτές, ο πάροχος υπηρεσιών ευθύνεται για κάθε περιουσιακή ζημία ή ηθική βλάβη που προκαλείται παράνομα και υπαίτια, με πράξη ή παράλειψή του, κατά την παροχή των υπηρεσιών στον καταναλωτή. Υπό το πρίσμα αυτό, η τράπεζα, ως προμηθευτής, υπέχει ευθύνη για ζημίες που προκαλεί στον καταναλωτή κατά την παροχή των τραπεζικών της υπηρεσιών.

Ο νόμος προβλέπει, ωστόσο, και περιπτώσεις πλήρους ευθύνης του πληρωτή. Ειδικότερα, ο πληρωτής ευθύνεται για το σύνολο της ζημίας όταν ο πάροχος υπηρεσιών πληρωμών εφαρμόζει μέτρα ασφάλειας ανώτερα από εκείνα που απαιτούνται για την ισχυρή ταυτοποίηση

των συναλλαγών, όπως προηγμένους μηχανισμούς που αξιοποιούν τεχνολογίες τεχνητής νοημοσύνης, πρόσθετους κωδικούς, βιομετρική ταυτοποίηση ή τηλεφωνική επιβεβαίωση για συναλλαγές που ενδέχεται να προκαλέσουν ζημία άνω των 1.000 ευρώ. Περαιτέρω, πλήρης ευθύνη του πληρωτή προβλέπεται όταν η ζημία προκλήθηκε από δόλο του ίδιου ή όταν αυτός αθέτησε εκ δόλου βασικές υποχρεώσεις του, όπως η άμεση ενημέρωση του πιστωτικού ιδρύματος. Αξίζει να σημειωθεί ότι η πρόβλεψη περί πλήρους ευθύνης του πληρωτή, σε περίπτωση που το τραπεζικό ίδρυμα αποδείξει ότι διαθέτει και εφαρμόζει πρόσθετους και πιο εξελιγμένους μηχανισμούς ελέγχου συναλλαγών για ποσά άνω των 1.000 ευρώ, ενσωματώθηκε στο άρθρο 22 του Ν. 5019/2023 κατόπιν αντιδράσεων των τραπεζών (Ν. 5019/2023, άρθρο 22). Η συγκεκριμένη ρύθμιση προκάλεσε έντονη κριτική από ενώσεις καταναλωτών, οι οποίες υποστήριζαν ότι δεν συνάδει με το πνεύμα αναθεώρησης του Ν. 4537/2018 και της Οδηγίας 2015/2366, που επιδίωκαν μια πιο συντονισμένη και ισορροπημένη κατανομή ευθύνης και ζημιών στις μη εγκεκριμένες πράξεις πληρωμής (ΕΚΠΟΙΖΩ, 2023).

Η κριτική αυτή εστιάζει στο γεγονός ότι η ρύθμιση ενδέχεται να λειτουργήσει εις βάρος των εννόμων συμφερόντων των καταναλωτών, οι οποίοι θεωρούνται το ασθενέστερο μέρος στη συναλλακτική σχέση με την τράπεζα και ενδέχεται να επωμιστούν ζημίες που υπερβαίνουν το ποσό των 1.000 ευρώ. Παρά τις επιφυλάξεις αυτές, αξιολογείται θετικά το γεγονός ότι το βάρος απόδειξης σχετικά με την ύπαρξη και την αποτελεσματική εφαρμογή των εξελιγμένων μηχανισμών ασφαλείας φέρουν τα τραπεζικά ιδρύματα, ενώ καθίσταται ιδιαίτερα σημαντικός και ο ενεργός εποπτικός ρόλος της Τράπεζας της Ελλάδος (Βαϊτσούδης, 2020).

2.4. Η έννοια της ισχυρής ταυτοποίησης πελάτη (SCA) και τα όριά της

Η ταυτοποίηση στο περιβάλλον των ηλεκτρονικών πληρωμών δεν λειτουργεί όπως οι παραδοσιακοί έλεγχοι ταυτότητας σε φυσική παρουσία. Εδώ, ο έλεγχος γίνεται απομακρυσμένα και διαδικτυακά, άρα η ασφάλεια της διαδικασίας εξαρτάται σε μεγάλο βαθμό από τα τεχνικά μέτρα που εφαρμόζουν οι πάροχοι υπηρεσιών πληρωμών, αλλά και από το πόσο ανθεκτικό είναι το συνολικό «οικοσύστημα» μιας συναλλαγής απέναντι σε απάτη, υποκλοπή ή παραπλάνηση (Fabcic, 2021).

Στο ενωσιακό δίκαιο, ο βασικός κορμός για την ισχυρή ταυτοποίηση πελάτη (Strong Customer Authentication - SCA) προκύπτει από την PSD2. Η PSD2 ορίζει την «ταυτοποίηση» ως διαδικασία που επιτρέπει στον πάροχο να επαληθεύει την ταυτότητα του χρήστη ή/και την εγκυρότητα χρήσης συγκεκριμένου μέσου πληρωμών, μέσω εξατομικευμένων διαπιστευτηρίων ασφαλείας (European Union, 2015). Η «ισχυρή ταυτοποίηση πελάτη» εξειδικεύεται ως ταυτοποίηση που στηρίζεται στη χρήση δύο ή περισσότερων στοιχείων, τα οποία ανήκουν σε διαφορετικές κατηγορίες: γνώση (κάτι που μόνο ο χρήστης γνωρίζει), κατοχή (κάτι που μόνο ο χρήστης κατέχει) και εγγενές χαρακτηριστικό (κάτι που ο χρήστης είναι). Το κρίσιμο σημείο είναι ότι τα στοιχεία αυτά πρέπει να είναι ανεξάρτητα μεταξύ τους, έτσι ώστε η παραβίαση του ενός να μην «παρασύρει» την αξιοπιστία των υπολοίπων, και συνολικά να προστατεύεται η εμπιστευτικότητα των δεδομένων ταυτοποίησης (European Union, 2015).

Η κανονιστική εικόνα συμπληρώνεται από τον Κατ' Εξουσιοδότηση Κανονισμό (RTS) 2018/389, ο οποίος, παρότι συχνά αποκαλείται «πρότυπο», είναι δεσμευτικός και εξειδικεύει τις τεχνικές και οργανωτικές απαιτήσεις για την SCA, καθώς και για την ασφαλή επικοινωνία στο πλαίσιο των υπηρεσιών πληρωμών (European Commission, 2018). Εκεί αποτυπώνεται και η λογική ότι η SCA ενεργοποιείται, ιδίως, όταν ο πληρωτής έχει πρόσβαση online σε λογαριασμό, όταν εκκινεί ηλεκτρονική πράξη πληρωμής ή όταν διενεργεί ενέργεια από απόσταση που ενέχει κίνδυνο απάτης (European Union, 2015· European Commission, 2018). Παρά τη σαφή κατεύθυνση, η SCA δεν είναι «μαγική λύση» και τα όριά της φαίνονται κυρίως σε δύο επίπεδα. Πρώτον, η SCA αποτελεί μεν ισχυρό αντίβαρο απέναντι στην μη εξουσιοδοτημένη πρόσβαση, όμως δεν αρκεί από μόνη της. Η αποτελεσματικότητα της ασφάλειας στις πληρωμές εξαρτάται από την ευρύτερη διαχείριση επιχειρησιακών και τεχνολογικών κινδύνων, από μηχανισμούς ανίχνευσης περιστατικών και από συνολικές πολιτικές ασφαλείας που καλύπτουν όλη την αλυσίδα πληρωμής (European Union, 2015; Fabrice, 2021). Με άλλα λόγια, η SCA λειτουργεί ως βασικό «φίλτρο», αλλά δεν υποκαθιστά τους ελέγχους κινδύνου, τις διαδικασίες παρακολούθησης, ούτε τις υποχρεώσεις πρόληψης περιστατικών.

Έπειτα, η ίδια η ρύθμιση προβλέπει εξαιρέσεις από την εφαρμογή SCA, κυρίως για χαμηλής αξίας ή χαμηλού κινδύνου συναλλαγές. Αυτές οι εξαιρέσεις, αν και εξυπηρετούν την ευχρηστία και τη ροή του ηλεκτρονικού εμπορίου, δημιουργούν πρόσθετες παραμέτρους κυβερνοασφάλειας: όσο πιο σύνθετο γίνεται ένα σύστημα ασφαλείας, τόσο αυξάνονται

δυννητικά τα σημεία αστοχίας ή οι ευπάθειες που μπορεί να αξιοποιηθούν (Fabrice, 2021). Η Fabrice επισημαίνει εύστοχα ότι οι εξαιρέσεις εισάγουν δικές τους απαιτήσεις ασφαλείας, ακριβώς επειδή η «πολυπλοκότητα» δεν είναι ουδέτερη έννοια στην ασφάλεια.

Ένα ιδιαίτερα σημαντικό κομμάτι της συζήτησης αφορά τη σχέση PSD2-GDPR, επειδή οι διαδικασίες ταυτοποίησης συχνά προϋποθέτουν επεξεργασία προσωπικών δεδομένων. Η SCA μπορεί να «αγγίξει» δεδομένα που συνδέονται άμεσα με ταυτοποιήσιμο πρόσωπο (διαπιστευτήρια, συσκευές, μοτίβα χρήσης), ενώ στην περίπτωση βιομετρικών παραγόντων (π.χ. δακτυλικό αποτύπωμα) η επεξεργασία μπορεί να εισέλθει και στο πεδίο των ειδικών κατηγοριών δεδομένων (European Union, 2016; Fabrice, 2021). Γι' αυτό, στην πράξη, η συμμόρφωση δεν κρίνεται μόνο από το αν τηρήθηκαν οι απαιτήσεις της PSD2/RTS, αλλά και από το αν το σχήμα ταυτοποίησης είναι συμβατό με τις αρχές του GDPR (Fabrice, 2021).

Στο ζήτημα αυτό, η Fabrice υποστηρίζει ότι η σχέση PSD2 και GDPR προσεγγίζεται ορθότερα ως σωρευτική εφαρμογή και όχι ως μια απλή σχέση «ειδικού–γενικού νόμου». Δηλαδή, όταν υπάρχει επικάλυψη, οι κανόνες πρέπει να διαβάζονται μαζί, και η συμμόρφωση μπορεί να σημαίνει ότι ο πάροχος οφείλει να πιάνει το υψηλότερο επίπεδο απαιτήσεων όπου αυτό προκύπτει (Fabrice, 2021). Η προσέγγιση αυτή συνδέεται και με την επεξεργασία/ερμηνεία από ευρωπαϊκά όργανα σε επίπεδο κατευθυντήριων γραμμών, όπου το πλαίσιο PSD2 και οι απαιτήσεις του GDPR εξετάζονται παράλληλα ως προς ρόλους και νόμιμες βάσεις (EDPB, 2020).

Πρακτικά, αυτό οδηγεί σε τρία κρίσιμα ερωτήματα για την SCA. Πρώτον, ποιος θεωρείται υπεύθυνος επεξεργασίας (controller) κατά GDPR όταν εφαρμόζονται διαδικασίες ταυτοποίησης. Η Fabrice, αξιοποιώντας το τεστ «means reasonably likely» από τη νομολογία Breyer, θεωρεί ότι οι πάροχοι μπορούν να αντιμετωπιστούν ως υπεύθυνοι επεξεργασίας ακόμη και όταν επεξεργάζονται ψευδωνυμοποιημένα διαπιστευτήρια, εφόσον υφίστανται εύλογα μέσα που καθιστούν πιθανή την ταυτοποίηση (CJEU, 2016; Fabrice, 2021). Δεύτερον, ποια είναι η νόμιμη βάση για την επεξεργασία δεδομένων στο πλαίσιο της ταυτοποίησης: ως περισσότερο ρεαλιστικές βάσεις προβάλλονται η εκτέλεση σύμβασης ή το έννομο συμφέρον, υπό την προϋπόθεση ότι τηρείται το κριτήριο της αναγκαιότητας, ενώ η επίκληση «νομικής υποχρέωσης» εμφανίζεται πιο αμφίβολη ως θεμέλιο (European Union, 2016; Fabrice, 2021). Τρίτον, ποιο είναι το απαιτούμενο επίπεδο ασφάλειας: ο GDPR (άρθρο 32) προϋποθέτει κατάλληλα τεχνικά και οργανωτικά μέτρα με βάση τον κίνδυνο, και όταν συντρέχει σωρευτική

εφαρμογή, μπορεί να σημαίνει ότι ο πάροχος οφείλει να κινηθεί προς το αυστηρότερο standard, ακόμη και όταν το RTS αφήνει περιθώρια επιλογής ως προς ορισμένες εξαιρέσεις (European Union, 2016· European Commission, 2018; Fabcic, 2021).

Συνολικά, η SCA είναι αναμφίβολα βασικός πυλώνας της ασφάλειας στις πληρωμές, αλλά τα όριά της φαίνονται καθαρά όταν αντιμετωπίζεται ως «αυτόνομο» μέτρο. Στην πράξη, λειτουργεί σωστά μόνο όταν εντάσσεται σε ένα ευρύτερο πλαίσιο διαχείρισης κινδύνων, παρακολούθησης και συμμόρφωσης, στο οποίο PSD2/RTS και GDPR δεν ανταγωνίζονται, αλλά συνυπάρχουν σωρευτικά, δημιουργώντας ένα πιο απαιτητικό και τελικά πιο προστατευτικό πλέγμα υποχρεώσεων (Fabcic, 2021; EDPB, 2020).

2.5. Ευθύνη παρόχων στο ηλεκτρονικό εμπόριο μετά τον Κανονισμό ΕΕ 2022/2065

Οι αγορές μέσω επιγραμμικών πλατφορμών αποτελούν σήμερα μέρος της καθημερινότητας των πολιτών της ΕΕ. Όμιλοι εταιριών που κυριαρχούν διεθνώς στην αγορά των ψηφιακών πλατφορμών, όπως Google, Amazon, Facebook, Apple και Microsoft (GAFAM), στηρίζονται κυρίως σε εφαρμογές μεγαδεδομένων, νέων αλγορίθμων και νεφο-υπολογιστικής. Τα επιχειρηματικά αυτά μοντέλα δραστηριοποιούνται σε τομείς όπως οι λιανικές πωλήσεις (Amazon, e-bay), τα καταλύματα (Airbnb), οι μεταφορές κ.ά., και τίθεται το ερώτημα ποιες είναι οι επιπτώσεις του διαρκώς εξελισσόμενου ψηφιακού μετασχηματισμού για τους καταναλωτές και για την κοινωνία γενικότερα. Τα δεδομένα (data) έχουν καταστεί κινητήρια δύναμη της οικονομίας. Το ψηφιακό περιβάλλον χαρακτηρίζεται από τη συγκέντρωση και επεξεργασία τεράστιου αριθμού προσωπικών δεδομένων των καταναλωτών, τα οποία μπορούν να συνδυάζονται με αλγορίθμους και Τεχνητή Νοημοσύνη (TN), ώστε να μετατρέπονται σε χρήσιμες πληροφορίες για εμπορικούς σκοπούς. Οι επιχειρήσεις αξιοποιούν ολοένα περισσότερο την TN στην ψηφιακή αγορά, για να κατανοήσουν και να επηρεάσουν τις συνήθειες, ενδεχομένως και να ελέγξουν τη συναλλακτική συμπεριφορά των καταναλωτών, μέσω των δεδομένων που συλλέγουν σχετικά με δραστηριότητες, προσωπικές επαφές, online συμπεριφορά, αγορές, τραπεζικές συναλλαγές κ.ά..

Οι υπηρεσίες που παρέχονται από ψηφιακές πλατφόρμες, όπως π.χ. της Google, οι οποίες αποτελούν βασικές διαδικτυακές πηγές πληροφόρησης για τον καταναλωτή κατά τη λήψη αποφάσεων, δημιουργούν ανησυχίες για πιθανή χειραγώγηση των καταναλωτών ως προς την

παροχή των πληροφοριών(Μικρουλέα, 2023). Ανησυχητική είναι και η διαπίστωση ότι η εκτεταμένη χρήση ΤΝ στις σχέσεις επιχειρήσεων προς καταναλωτές (b2c), με αποτελέσματα όπως προβλέψεις, περιεχόμενο, συστάσεις ή αποφάσεις, μπορεί να περιορίζει τη δυνατότητα των καταναλωτών να λαμβάνουν αυτόνομα αποφάσεις όταν πραγματοποιούν αγορές μέσω ψηφιακών πλατφορμών (Koolen, 2023).

1. Άμεση ζημίωση των συμφερόντων των καταναλωτών μπορεί να προκύπτει όταν οι επιχειρήσεις, μέσω επιγραμμικών πλατφορμών, εφαρμόζουν παραπλανητικές, επιθετικές ή γενικά αθέμιτες εμπορικές πρακτικές που οδηγούν σε χειραγώγηση και εκμετάλλευση. Ειδικότερα:

α. Υπάρχουν περιπτώσεις όπου σύστημα ΤΝ μπορεί να συμβάλει σε εξαπάτηση, όταν χρησιμοποιούνται τεχνικές χειραγώγησης που απευθύνονται στο υποσυνείδητο (subliminal manipulation techniques).

β. Παραπλανητικές πρακτικές αποτελούν και μορφές συγκαλυμμένης διαφήμισης μέσω πλατφορμών, όταν η διαφήμιση δεν αναγνωρίζεται ευδιάκριτα από τον καταναλωτή. Το ίδιο ισχύει όταν δημιουργείται εντύπωση ή προβάλλεται ψευδής ισχυρισμός ότι ο διαδικτυακός έμπορος δεν θα χρησιμοποιήσει τα δεδομένα του καταναλωτή για εμπορικούς σκοπούς (Δελούκα-Ιγγλέση, 2023).

γ. Υπό προϋποθέσεις μπορεί να θεωρηθεί αθέμιτη εμπορική πρακτική και η χρήση καταχρηστικών γενικών όρων συναλλαγών μέσω ψηφιακής πλατφόρμας, ιδίως όταν λόγω αδιαφάνειας προκαλούν παραπλάνηση και ενδέχεται να οδηγήσουν τον καταναλωτή σε απόφαση συναλλαγής που αλλιώς δεν θα λάμβανε (Μεντή, 2018).

δ. Παραπλανητική πρακτική μπορεί επίσης να είναι η υψηλότερη κατάταξη (ranking) προϊόντων μετά από ερώτημα σε μηχανή αναζήτησης, όταν δεν παρέχονται πληροφορίες για τα βασικά κριτήρια που καθορίζουν την κατάταξη και τη βαρύτητά τους. Οι πληροφορίες αυτές είναι κρίσιμες, γιατί η υψηλότερη θέση μπορεί να οφείλεται απλώς σε καταβολή τιμήματος από την επιχείρηση. Αντίστοιχα, πρόβλημα δημιουργείται και όταν δεν παρέχεται πληροφόρηση για το κατά πόσον ο προμηθευτής διασφαλίζει ότι οι αξιολογήσεις προέρχονται από καταναλωτές που έχουν πράγματι χρησιμοποιήσει το προϊόν.

ε. Η χρήση ΤΝ μπορεί ακόμη να οδηγεί σε «μη επιτρεπόμενη επιρροή», δηλαδή άσκηση πίεσης που περιορίζει ουσιαστικά την ελευθερία επιλογής του μέσου καταναλωτή και επηρεάζει την ικανότητά του για τεκμηριωμένη απόφαση. Σε τέτοια περίπτωση πρόκειται για επιθετική εμπορική πρακτική, αθέμιτη κατά το αρθρ. 9ζ Ν. 2251/94.

Όταν εμφανίζονται πρακτικές σαν τις παραπάνω, εφαρμόζεται η οδηγία 2005/29/ΕΚ για τις αθέμιτες εμπορικές πρακτικές (και αντίστοιχα τα αρθρ. 9γ έως 9η του Ν. 2251/94), που

καλύπτουν και πρακτικές διαδικτυακών ενδιάμεσων, όπως μέσα κοινωνικής δικτύωσης, επιγραμμικές πλατφόρμες και μηχανές αναζήτησης.

2. Πολλές ζημιογόνες συνέπειες συνδέονται με την εξατομίκευση. Η δυνατότητα συλλογής ολοένα μεγαλύτερου όγκου προσωπικών δεδομένων, σε συνδυασμό με αλγοριθμικά συστήματα, επιτρέπει στις επιχειρήσεις να εξατομικεύουν τη συμπεριφορά κάθε καταναλωτή, να τον κατηγοριοποιούν (π.χ. νέος/παλιός πελάτης) και να ακολουθούν άνιση μεταχείριση ανά κατηγορία, με κίνδυνο επιζήμιας ή απαράδεκτης διακριτικής μεταχείρισης, ιδίως όταν το κοινό είναι παιδιά. Επιπλέον, οι εξατομικευμένες διαφημίσεις που περιορίζουν τις διαθέσιμες επιλογές της αγοράς μπορεί να περιορίζουν τον ανταγωνισμό, καθώς ο καταναλωτής οδηγείται σε επιλογές μόνο από ένα μέρος των προϊόντων.

3. Με αλγοριθμικές αναλύσεις μπορεί να εκτιμάται και η τιμή που θα ήταν διατεθειμένος να πληρώσει κάθε πελάτης για ένα προϊόν. Όταν οι καταναλωτές στρέφονται στην ψηφιακή αγορά, το προφίλ τους μπορεί να αξιοποιείται άμεσα από μηχανισμό διαμόρφωσης τιμών, με αποτέλεσμα σε ορισμένες κατηγορίες καταναλωτών να εμφανίζονται υψηλότερες τιμές για τα ίδια προϊόντα ή υπηρεσίες (Durovic and Lech, 2021). Όταν μάλιστα αποστέλλονται στοχευμένες διαφημίσεις με διαφορετικές τιμές ή εφαρμόζονται πρακτικές με αντίστοιχο αποτέλεσμα (π.χ. εκπτώσεις μόνο σε επιλεγμένους πελάτες), η εξατομικευμένη τιμολόγηση μπορεί να έχει αρνητικές συνέπειες. Η ασυμμετρία πληροφόρησης ως προς τις τιμές μειώνει τη δυνατότητα σύγκρισης, επηρεάζει τον αποτελεσματικό ανταγωνισμό, περιορίζει τη διαφάνεια και κλονίζει την εμπιστοσύνη των καταναλωτών στις online αγορές (Durovic and Lech, 2021).

4. Σημαντικός είναι και ο κίνδυνος έμμεσης αλγοριθμικής διακριτικής μεταχείρισης, που μπορεί να δημιουργήσει σοβαρά προβλήματα σε άτομα όταν επιδιώκουν υπηρεσίες ζωτικής σημασίας (π.χ. πίστωση), με πιθανή αύξηση ανισοτήτων και κοινωνική διαστρωμάτωση (Durovic and Lech, 2021).

5. Ζήτημα δημιουργεί και η αξιοποίηση μεγαδεδομένων (Big Data): παρά τη χρησιμότητά τους, η εμπορευματοποίησή τους μπορεί να απειλεί τους καταναλωτές, καθώς τροφοδοτούν ισχυρούς αλγορίθμους που οδηγούν σε αυτοματοποιημένη λήψη αποφάσεων. Τα αποτελέσματα μιας αναζήτησης μπορεί να υπηρετούν όχι τις ανάγκες του καταναλωτή αλλά το συμφέρον της μηχανής αναζήτησης, όπως ενδέχεται να συμβαίνει π.χ. σε αναζήτηση μέσω “Google shopping” (Μικρουλέα, 2023).

6. Οικονομική ζημία μπορεί να προκύπτει και όταν οι καταναλωτές βρίσκονται σε εικονικούς κόσμους, είτε μέσω διαδικτύου (π.χ. βιντεοπαιχνίδια) είτε σε άλλα περιβάλλοντα (Hyde-Cartwright, 2023). Τέτοια περιβάλλοντα εμβύθισης στην εικονική πραγματικότητα μπορεί να

δημιουργούν εικονικές κοινότητες (virtual communities) και την αίσθηση φυσικής παρουσίας, ενώ ο χρήστης βρίσκεται σε μη φυσικό χώρο, καθιστώντας τον καταναλωτή πιο επιρρεπή σε ζημία. Για την αντιμετώπιση αυτού του κινδύνου, ρόλο μπορούν να παίξουν οι ρυθμίσεις της οδηγίας για τις αθέμιτες εμπορικές πρακτικές, ιδίως αυτές για ευάλωτες ομάδες. Η Επιτροπή της ΕΕ έχει δώσει ευρεία ερμηνεία στην έννοια του «μέσου ευάλωτου καταναλωτή» και έχει δεχθεί ότι «οι πολυδιάστατες μορφές ευάλωτου χαρακτήρα είναι ιδιαίτερα έντονες στο ψηφιακό περιβάλλον» (Hyde-Cartwright, 2023).

Όταν μέσω των ψηφιακών πλατφορμών οι επιχειρήσεις εφαρμόζουν αθέμιτες εμπορικές πρακτικές κατά παράβαση των αρθρ. 9γ έως 9η Ν. 2251/94, κάθε καταναλωτής, αλλά και οι ενώσεις καταναλωτών (εφόσον έχουν την ιδιότητα του νομιμοποιούμενου φορέα), μπορούν με την άσκηση αντιπροσωπευτικής αγωγής να ζητήσουν την παύση της αθέμιτης πρακτικής και την παράλειψή της στο μέλλον. Ο καταναλωτής που υπέστη ζημία από την αθέμιτη πρακτική μπορεί επίσης να αξιώσει αποζημίωση και επιπλέον να ζητήσει μείωση της τιμής ή να καταγγείλει τη συναφθείσα σύμβαση (βλ. αρθρ. 9θ παρ. 2 Ν. 2251/94), (Αλεξανδρίδου και Απαλαγάκη, 2023).

Όταν συντρέχουν λόγοι δημοσίου συμφέροντος, ο Υπουργός Ανάπτυξης δύναται με απόφασή του να διατάξει άμεση παύση της αθέμιτης εμπορικής πρακτικής. Σε περίπτωση μη συμμόρφωσης προς την απόφαση, επιβάλλονται οι διοικητικές κυρώσεις του αρθρ. 13α Ν. 2251/94(βλ. αρθρ. 9θ παρ. 6 Ν. 2251/94), (Καραγκουνίδη και Λιναρίτη, 2023).

Πρέπει ακόμη να ληφθούν υπόψη ειδικότερες ρυθμίσεις που θεσπίστηκαν για την προστασία του καταναλωτή στην ψηφιακή αγορά και επέφεραν τροποποιήσεις στην οδηγία 2005/29/EK για τις αθέμιτες εμπορικές πρακτικές.

Στο πλαίσιο της πρωτοβουλίας «Νέα Συμφωνία για τους καταναλωτές» (New Deal for Consumers) ψηφίστηκε η οδηγία 2019/2161/ΕΕ, σχετικά με την καλύτερη επιβολή και τον εκσυγχρονισμό της προστασίας των καταναλωτών στην ΕΕ (γνωστή ως “Omnibus” ή “Modernization Directive”). Η οδηγία ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 4933/22, τροποποιώντας τον Ν. 2251/94. Ως προς τις αλλαγές που επέφερε η Omnibus ειδικά στην οδηγία 2005/29/EK, συνοπτικά ενίσχυσε τη διαφάνεια και επέβαλε πρόσθετες υποχρεώσεις ενημέρωσης των καταναλωτών κατά τις επιγραμμικές αγορές.

α. Ειδικότερα, στον κατάλογο των περιπτώσεων όπου προσδιορίζεται ποιες παραλείψεις πληροφοριών θεωρούνται ουσιώδεις ώστε μια πρακτική να εκληφθεί ως παραπλανητική, όταν πρόκειται για πρόσκληση προς αγορά (αρθρ. 9ε Ν. 2251/94), προστέθηκαν νέες περιπτώσεις σχετικές με τις αγορές μέσω ψηφιακών πλατφορμών. Όταν παρέχεται στον καταναλωτή δυνατότητα αναζήτησης προϊόντων από διαφορετικούς εμπόρους με βάση λέξη-κλειδί, θεωρείται ουσιώδης η παροχή γενικών πληροφοριών (σε ειδικό, άμεσα και εύκολα προσβάσιμο τμήμα της επιγραμμικής διεπαφής) σχετικά με τις βασικές παραμέτρους που καθορίζουν την κατάταξη (ranking) των προϊόντων και τη σημασία τους (προσθήκη παρ. 4α στο αρθρ. 7 οδηγίας 2005/29/EK και αντίστοιχα παρ. 4α στο αρθρ. 9ε Ν. 2251/94). Η παράλειψη των πληροφοριών αυτών συνιστά παραπλανητική εμπορική πρακτική.

Επίσης, όταν ο έμπορος παρέχει πρόσβαση σε αξιολογήσεις προϊόντων από καταναλωτές, θεωρείται ουσιώδης η πληροφόρηση για το αν και με ποιον τρόπο διασφαλίζει ότι οι δημοσιευμένες αξιολογήσεις προέρχονται από καταναλωτές που πράγματι χρησιμοποίησαν ή αγόρασαν το προϊόν (προσθήκη παρ. 6 στο αρθρ. 7 οδηγίας 2005/29/EK και αντίστοιχα παρ. 6 στο αρθρ. 9ε Ν. 2251/94). Η παράλειψη αυτών των πληροφοριών αποτελεί επίσης παραπλανητική πρακτική. Πριν αποφασίσουν, οι καταναλωτές πρέπει να γνωρίζουν αν το αποτέλεσμα της αξιολόγησης είναι αμερόληπτο ή αν πρόκειται για χορηγούμενο αποτέλεσμα, δηλαδή διαφήμιση.

β. Στο Παράρτημα Ι της οδηγίας 2005/29/EK προστέθηκαν τρεις νέες περιπτώσεις *per se* παραπλανητικών πρακτικών, που αφορούν παραλείψεις ενημέρωσης σχετικά με την κατάταξη και την αξιολόγηση προϊόντων. Ως νέα *per se* παραπλανητική πρακτική θεωρείται η παροχή αποτελεσμάτων μετά από επιγραμμική αναζήτηση καταναλωτή, όταν δεν αναφέρεται σαφώς αν πρόκειται για διαφήμιση επί πληρωμή ή αν έχει καταβληθεί τίμημα για την επίτευξη υψηλότερης κατάταξης στα αποτελέσματα (βλ. αρθρ. 9στ στοιχ. κ1 Ν. 2251/94), (Δελούκα-Ιγγλέση, 2023).

Ως *per se* παραπλανητική πρακτική προστέθηκε και η δήλωση του προμηθευτή ότι οι αξιολογήσεις προέρχονται από καταναλωτές που έχουν χρησιμοποιήσει ή αγοράσει το προϊόν, όταν δεν έχουν ληφθεί εύλογα και αναλογικά μέτρα ελέγχου ως προς αυτό (βλ. αρθρ. 9στ περιπτ. λγ' Ν. 2251/94). Επίσης, *per se* παραπλανητική πρακτική αποτελεί η υποβολή ψευδών αξιολογήσεων ή ψευδών θετικών κριτικών, καθώς και η διαστρέβλωση

αξιολογήσεων/κριτικών με σκοπό την προώθηση προϊόντων (αρθρ. 9στ περιπτ. λδ' Ν. 2251/94), (Δελούκα-Ιγγλέση, 2023).

Για τη διασφάλιση της ευημερίας των καταναλωτών (consumer welfare), ως απώτερου πολιτικού στόχου της ΕΕ, οι ειδικές ρυθμίσεις που θεσπίστηκαν για την ψηφιακή αγορά (οι δύο ψηφιακές οδηγίες και οι δύο ψηφιακοί κανονισμοί) δεν φαίνεται να επαρκούν. Αντίστοιχα, ούτε το παράλληλα ισχύον εθνικό πλαίσιο, δηλαδή οι διατάξεις του Ν. 2251/94 (και μετά τις σχετικές τροποποιήσεις), μπορεί να καλύψει πλήρως τα κενά που ανακύπτουν. Η μαζική, αυτοματοποιημένη λήψη αλγοριθμικών αποφάσεων και οι προκλήσεις της «επανάστασης» των μεγαδεδομένων συγκρούονται με θεμελιώδεις βάσεις του ενωσιακού δικαίου του καταναλωτή, ιδίως με τη διατήρηση της αυτονομίας του καταναλωτή. Παράλληλα, δημιουργούνται κίνδυνοι διακριτικής μεταχείρισης και υπονόμησης της ιδιωτικής σφαίρας, ενώ η αυτονομία στη λήψη αποφάσεων αποτελεί βασική αρχή του ενωσιακού κεκτημένου προστασίας των καταναλωτών (Durovic and Lech, 2021).

Καθίσταται έτσι σαφές ότι οι αρνητικές συνέπειες για την ευημερία των καταναλωτών δεν μπορούν να αντιμετωπιστούν μόνο μέσω του δικαίου προστασίας του καταναλωτή. Λόγω του δυναμικού ψηφιακού μετασχηματισμού απαιτείται συνδυαστική/συμπληρωματική εφαρμογή και των ρυθμίσεων του δικαίου του ανταγωνισμού, καθώς και του δικαίου προστασίας προσωπικών δεδομένων. Οι τρεις αυτοί κλάδοι δικαίου, που υπηρετούν την ολοκλήρωση της εσωτερικής αγοράς, έχουν ως άμεσο ή έμμεσο σκοπό την ευημερία των καταναλωτών και των υποκειμένων δεδομένων, με κοινή βάση την αρχή του θεμιτού. Στο δίκαιο προστασίας του καταναλωτή, υπό την αρχή του θεμιτού, γίνεται δεκτό ότι στις συμβάσεις b2c δεν επιτρέπεται σημαντική διατάραξη της ισορροπίας δικαιωμάτων και υποχρεώσεων σε βάρος του καταναλωτή (Volmar and Helmdach, 2018).

Στο δίκαιο του ανταγωνισμού, η αρχή του θεμιτού επιδρά διασφαλίζοντας την οικονομική ελευθερία των συμμετεχόντων στην αγορά. Η απαγόρευση καταχρηστικής εκμετάλλευσης δεσπόζουσας θέσης αποβλέπει στη διατήρηση ανταγωνιστικών δομών και στην προστασία του ανταγωνισμού υπέρ των γενικών συμφερόντων των καταναλωτών, όχι μόνο ως προς χαμηλές τιμές/ποιότητα/καινοτομία, αλλά και ως προς τη δυνατότητα επιλογής (consumer choice). Ειδικότερα, το αρθρ. 102 ΣΛΕΕ ερμηνεύεται από το ΔικΕΕ ως διάταξη που δεν καταλαμβάνει μόνο συμπεριφορές με άμεση ζημία στους καταναλωτές, αλλά και πρακτικές που τους ζημιώνουν έμμεσα, μέσω πλήγματος στη λειτουργία του ανταγωνισμού. Στο δίκαιο

προστασίας προσωπικών δεδομένων, η αρχή του θεμιτού περιλαμβάνεται στο άρθρ. 5(1) ΓΚΠΔ, σύμφωνα με το οποίο τα προσωπικά δεδομένα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο, επιδιώκοντας ισορροπία στις ασύμμετρες σχέσεις μεταξύ υποκειμένων και εκείνων που ελέγχουν τα δεδομένα, ώστε να εξασφαλίζεται στα υποκείμενα έλεγχος επί των δεδομένων τους (Μαργαρίτη, 2020).

Καθώς οι ρυθμίσεις των τριών κλάδων μπορούν να αλληλοεπιδρούν, η συμπληρωματική εφαρμογή τους μπορεί να συνθέσει συνεκτικό πλαίσιο προστασίας στο ψηφιακό περιβάλλον. Σημειώνεται ότι το ΔικΕΕ, με απόφαση 28/4/22 στην υπόθ. Meta Platforms Ireland Limited, αναφέρει ρητά (σκ. 23, με αναφορά στην αιτιολ. σκ. 15 του προοιμίου της οδηγίας 2020/1828 περί αντιπροσωπευτικής αγωγής) ότι οι μηχανισμοί επιβολής που προβλέπονται ή βασίζονται στον ΓΚΠΔ μπορούν, κατά περίπτωση, να εξακολουθούν να χρησιμοποιούνται για την προστασία συλλογικών συμφερόντων των καταναλωτών. Έτσι γίνεται σαφής αναφορά στη σχέση των δύο κλάδων και στη δυνατότητα οι μηχανισμοί επιβολής του δικαίου δεδομένων να συμπληρώνουν κενά της προστασίας καταναλωτή και μετά την εναρμόνιση με την οδηγία 2020/1828. Παρότι υπάρχουν διαφορές μεταξύ δικαίου καταναλωτή και δικαίου προσωπικών δεδομένων (ως προς παράδοση, έννοιες και στόχους), δεν συνιστούν ανυπέρβλητα εμπόδια. Το ότι συνδέονται από όμοιες αρχές μπορεί να δικαιολογήσει την αλληλοσυμπλήρωση στην εφαρμογή τους, ώστε να επιτυγχάνεται αποτελεσματικότερη προστασία έναντι της μαζικής εμπορευματοποίησης προσωπικών δεδομένων (Durovic and Lech, 2021).

Ο ενωσιακός νομοθέτης διατηρεί ως παράλληλη προτεραιότητα στην ψηφιοποιημένη ενιαία αγορά και την προστασία των καταναλωτών. Αυτό προκύπτει από το ότι στο αρθρ. 2 αριθ. 9 του Κανονισμού (ΕΕ) 2024/1684 αναφέρεται ότι η εφαρμογή του δεν θίγει το ενωσιακό δίκαιο προστασίας του καταναλωτή και τις ρυθμίσεις περί ευθύνης παραγωγού (χωρίς επιφύλαξη, σε αντίθεση με άλλες διατυπώσεις σε παλαιότερα κείμενα). Επιπλέον, με το αρθρ. 110 ο Κανονισμός τροποποιεί την οδηγία 2020/1828, προσθέτοντάς τον στο Παράρτημα Ι, ώστε παραβάσεις του να μπορούν να στηρίζουν αντιπροσωπευτικές αγωγές από νομιμοποιούμενους φορείς. Ο Κανονισμός ταξινομεί τα συστήματα ΤΝ ανάλογα με τον κίνδυνο (μη αποδεκτός, υψηλός, χαμηλός, και μοντέλα γενικού σκοπού) και προβλέπει υποχρεώσεις για παρόχους και χρήστες ανάλογα με το επίπεδο κινδύνου (risk based assessment). Η κατηγορία που ενδιαφέρει εδώ είναι τα συστήματα μη αποδεκτού κινδύνου του αρθρ. 5. Η παρ. 1 στοιχ. α) του αρθρ. 5 απαγορεύει πρακτικές που επηρεάζουν υποβολιμαία το υποσυνείδητο ή είναι σκόπιμα χειριστικές/παραπλανητικές, όταν έχουν σκοπό ή αποτέλεσμα ουσιώδη στρέβλωση της

συμπεριφοράς προσώπου ή ομάδας, υποβαθμίζοντας σημαντικά την ικανότητα για τεκμηριωμένη απόφαση, με αποτέλεσμα απόφαση που αλλιώς δεν θα λαμβανόταν, και όταν αυτό προκαλεί ή εύλογα ενδέχεται να προκαλέσει σημαντική βλάβη (σωματική, ψυχολογική ή στα οικονομικά συμφέροντα), (Graaf and Veldt, 2022).

Σημαντικό είναι ότι η συγκεκριμένη προστασία δεν περιορίζεται μόνο στους καταναλωτές με στενή έννοια (όπως στην οδηγία 2005/29/EK για τις αθέμιτες πρακτικές και στον Κανονισμό (ΕΕ) 2022/2065 για την Ενιαία Αγορά Ψηφιακών Υπηρεσιών), αλλά καταλαμβάνει γενικά κάθε πρόσωπο. Έτσι διευρύνεται το πεδίο προστασίας: καλύπτονται όλοι οι πολίτες της ΕΕ έναντι πρακτικών που απευθύνονται στο υποσυνείδητο ή λοιπών χειριστικών/παραπλανητικών πρακτικών μέσω συστημάτων ΤΝ. Η διεύρυνση αυτή συνδέεται με την αντίληψη ότι στο ψηφιοποιημένο περιβάλλον κάθε συναλλασσόμενος μπορεί να βρίσκεται σε ασθενέστερη θέση στις ψηφιακές συναλλαγές. Συνεπώς, υπό τις προϋποθέσεις του Κανονισμού, προστατεύονται όχι μόνο οι καταναλωτές με στενή έννοια, αλλά όλοι οι πολίτες της ΕΕ στις ψηφιακές συναλλαγές.

Κατά την παρ. 1 στοιχ. β) του αρθρ. 5 απαγορεύεται η εκμετάλλευση ευάλωτων προσώπων ή ομάδων μέσω συστημάτων ΤΝ, όταν οδηγεί σε ουσιώδη στρέβλωση της συμπεριφοράς τους και προκαλεί ή εύλογα ενδέχεται να προκαλέσει σημαντική βλάβη. Η ευαλωτότητα μπορεί να οφείλεται σε ηλικία, αναπηρία ή συγκεκριμένη κοινωνική/οικονομική κατάσταση, και η πρόβλεψη έχει ιδιαίτερη σημασία για την προστασία των παιδιών.

Τέλος, οι ρυθμίσεις του αρθρ. 5 παρ. 1 στοιχ. α) και β) μπορούν να λειτουργούν συμπληρωματικά προς τις διατάξεις της οδηγίας 2005/29/EK.

Η εξάρτηση των επιχειρήσεων από τα μεγαδεδομένα για ανταγωνιστικό πλεονέκτημα και βιωσιμότητα στο ψηφιακό περιβάλλον αυξάνεται διαρκώς. Η αυξανόμενη αξία των προσωπικών δεδομένων για τις επιχειρήσεις μέσω αλγοριθμικής ανάλυσης, καθώς και η πιθανότητα χρήσης τους και από τρίτους για διαφήμιση, εντείνουν την προοπτική επιτάχυνσης της εμπορευματοποίησης και τη συχνή στόχευση των «αλγοριθμικών» καταναλωτών, δημιουργώντας προκλήσεις που το δίκαιο οφείλει να αντιμετωπίσει (Durovic and Lech, 2021).

Εφόσον ο νομοθέτης δυσκολεύεται να συμβαδίζει με τους ρυθμούς τεχνολογικής εξέλιξης των μεγαδεδομένων ώστε να εξασφαλίζεται επαρκής προστασία θεμελιωδών δικαιωμάτων, το δίκαιο καταναλωτή χρειάζεται στήριξη από άλλους κλάδους του ενωσιακού δικαίου με ίδιο ή

συγγενή στόχο, όπως το δίκαιο ανταγωνισμού και το δίκαιο προστασίας προσωπικών δεδομένων. Το δίκαιο καταναλωτή ενισχύει τη δυνατότητα αυτόνομης απόφασης μέσω επαρκούς προσυμβατικής ενημέρωσης, το δίκαιο ανταγωνισμού υποστηρίζει τη δυνατότητα επιλογής, διασφαλίζοντας ανταγωνιστικές αγορές, ενώ το δίκαιο προσωπικών δεδομένων προστατεύει το βασικό δικαίωμα στην προστασία δεδομένων. Μέσω της συμπληρωματικής εφαρμογής των κλάδων αυτών προστατεύονται διαφορετικές πλευρές της «ψηφιακής» καθημερινότητας των καταναλωτών/πολιτών της ΕΕ. Παράλληλα, η προοπτική δημιουργίας Ευρωπαϊκού Χώρου Δεδομένων (European Data Space) και η εφαρμογή των Κανονισμών (ΕΕ) 2022/668 (Data Governance Act) και (ΕΕ) 2024/1689 (Artificial Intelligence Act), ως σημαντικών κειμένων για την ψηφιακή πολιτική, εκτιμάται ότι θα στηρίξουν ένα ανθρωποκεντρικό, ανθεκτικό και με μεγαλύτερη ευημερία ψηφιακό μέλλον.

Στις 12.1.2015 η Heather Oberdorf φόρεσε στον σκύλο της ένα κολάρο με αναδιπλούμενο λουρί, το οποίο είχε αγοράσει περίπου έναν μήνα νωρίτερα μέσω της πλατφόρμας της Amazon, και τον έβγαλε βόλτα. Κατά τη διάρκεια της βόλτας, όταν ο σκύλος όρμησε ξαφνικά, το λουρί αποσπάστηκε από το κολάρο και εκτινάχθηκε προς τα γυαλιά της Oberdorf, με αποτέλεσμα να χάσει οριστικά την όραση από το αριστερό της μάτι. Ούτε η ίδια ούτε η Amazon μπόρεσαν να εντοπίσουν τον πωλητή του κολάρου, ο οποίος είχε ήδη παύσει να διαθέτει ενεργό λογαριασμό στην Amazon από τον Μάιο του 2016. Η Oberdorf άσκησε αγωγή αποζημίωσης κατά της Amazon, υποστηρίζοντας ότι η Amazon υπέχει αντικειμενική ευθύνη ως «πωλήτρια» με βάση τους κανόνες του δικαίου της Pennsylvania περί αντικειμενικής ευθύνης πωλητή.

Κρίσιμο λοιπόν προαπαιτούμενο για την κατάφαση της αντικειμενικής ευθύνης ήταν το αν η Amazon μπορούσε να χαρακτηριστεί «πωλήτρια» στη συγκεκριμένη συναλλαγή. Το Πρωτοδικείο απέρριψε την αγωγή, αποδεχόμενο τους ισχυρισμούς της Amazon ότι δεν δρα ως πωλήτρια, αλλά απλώς διακινεί μέσω της πλατφόρμας προϊόντα που πωλούνται από τρίτους πωλητές.

Το Εφετείο (US Court of Appeals for the 3d Circuit), αντίθετα, έκρινε ότι η Amazon είναι πωλήτρια, διότι δεν περιορίζεται σε απλή διακίνηση: μέσω της πλατφόρμας της υλοποιεί η ίδια τις πωλήσεις προϊόντων που προσφέρονται από τρίτους. Ως αποτέλεσμα, εξαφάνισε την πρωτόδικη απόφαση, δίκασε εκ νέου και δέχθηκε την αγωγή. Προτού αναπτύξει την επιχειρηματολογία του, το Εφετείο περιέγραψε τον τρόπο λειτουργίας της πλατφόρμας,

δίνοντας έμφαση στη συμβατική οργάνωση της σχέσης Amazon–εμπόρου, η οποία στηρίζεται σε μονομερώς προδιατυπωμένους όρους της Amazon.

Κατά τους όρους αυτούς, η Amazon αναλαμβάνει να αναρτά τα προϊόντα προς πώληση στη διαδικτυακή πλατφόρμα, να συλλέγει τις παραγγελίες των καταναλωτών και να διαχειρίζεται τις πληρωμές, αποδίδοντας τα έσοδα στους πωλητές δύο φορές τον μήνα, αφού πρώτα παρακρατήσει την αμοιβή της, η οποία περιλαμβάνει ποσοστιαία προμήθεια επί της τιμής πώλησης και μία μηνιαία πρόσθετη χρέωση. Ο πωλητής, με ορισμένες εξαιρέσεις, επιλέγει τα προϊόντα που θα διαθέσει και το προσφερόμενο τίμημα, υποχρεούται όμως να παράσχει συγκεκριμένες πληροφορίες (περιγραφή, σήμα, διαθεσιμότητα, μεταφορά κ.λπ.). Η Amazon προβάλλει τις πληροφορίες μαζί με την ψηφιακή εικόνα του προϊόντος και, κατ' επιλογήν του εμπόρου, μπορεί να παρέχει και προαιρετικές υπηρεσίες, όπως διαφήμιση ή παράδοση στον καταναλωτή. Ιδίως τονίζεται ότι στη συναλλαγή αυτή η Amazon λειτουργεί ως ο μοναδικός δίαυλος επικοινωνίας με τον καταναλωτή και διατηρεί το δικαίωμα να καταγγείλει οποτεδήποτε τη σύμβαση παροχής υπηρεσιών με τον έμπορο και να αφαιρέσει τα προϊόντα του από την πλατφόρμα, όταν δεν ανταποκρίνεται σε απαιτήσεις έγκαιρης παράδοσης ή ποιότητας, οι οποίες αξιολογούνται και από τους ίδιους τους καταναλωτές μέσω της πλατφόρμας.

Το Εφετείο στήριξε την κρίση του ότι η Amazon συνιστά τον πωλητή στη συγκεκριμένη συναλλαγή (και άρα υπέχει αντικειμενική ευθύνη προς αποζημίωση της Oberdorf) αναδεικνύοντας τέσσερα ιδιόμορφα στοιχεία:

α) Η Amazon είναι το μόνο διαθέσιμο μέρος της εφοδιαστικής αλυσίδας προς τον καταναλωτή για άσκηση έννομου βοηθήματος: ακριβώς επειδή αποτελεί τον μοναδικό δίαυλο επικοινωνίας με τον αγοραστή-καταναλωτή, επιτρέπει στους τρίτους πωλητές να συγκαλύπτουν ταυτότητα και έδρα, αποφεύγοντας τελικά την ευθύνη.

β) Η επιβολή αντικειμενικής ευθύνης στην Amazon λειτουργεί ως κίνητρο για την ασφάλεια των προϊόντων: παρότι δεν έχει άμεση επιρροή στον σχεδιασμό/κατασκευή, ασκεί ουσιώδη έλεγχο στους πωλητές, διότι μέσω των ΓΟΣ έχει πλήρη διακριτική ευχέρεια να απομακρύνει μη ασφαλή προϊόντα από την πλατφόρμα.

γ) Η Amazon βρίσκεται σε καλύτερη θέση από τον καταναλωτή για να αποτρέψει την κυκλοφορία ελαττωματικών προϊόντων: η πλατφόρμα λειτουργεί ως «δημόσια αγορά» όπου διακινούνται όχι μόνο προϊόντα, αλλά και πληροφορίες/αξιολογήσεις των αγοραστών για

ποιότητα και τήρηση υποχρεώσεων, χωρίς οι πωλητές να διαθέτουν άλλο δίαυλο επικοινωνίας με τους καταναλωτές.

δ) Η Amazon μπορεί να μετακυλίσει το κόστος αποζημίωσης λόγω ελαττωματικού προϊόντος: πέρα από το αναγωγικό δικαίωμα κατά του εμπόρου (μέσω των ΓΟΣ), μπορεί να προσαρμόζει την προμήθειά της, ενσωματώνοντας και τον εκτιμώμενο κίνδυνο διακίνησης ελαττωματικών προϊόντων από συγκεκριμένο πωλητή.

Από τη συνοπτική επισκόπηση του τρόπου λειτουργίας της Amazon καθίσταται σαφές ότι δεν παραμένει σε έναν παθητικό ρόλο απλής μεσάζουσας μεταξύ εμπόρων και καταναλωτών, που διευκολύνει μόνο την κατάρτιση της σύμβασης πώλησης. Αντίθετα, διαδραματίζει ενεργό ρόλο σε όλα τα στάδια, από την κατάρτιση έως και την εκπλήρωση, καθώς αφενός ασκεί αποφασιστική επιρροή στην παρουσίαση και τη διακίνηση των προϊόντων, αφετέρου δε δύναται να καταγγείλει τη σύμβαση παροχής υπηρεσιών με τον έμπορο όταν αυτός δεν ανταποκρίνεται στις υποχρεώσεις του έναντι των καταναλωτών.

Επιπλέον, η πλατφόρμα λειτουργεί ως χώρος δημόσιας αγοράς που, μέσω των αξιολογήσεων των καταναλωτών ως προς την ποιότητα και την ασφάλεια, μπορεί να ενισχύει τις συναλλαγές και να αυξάνει τις τιμές ή ακόμη και να οδηγεί, σε ακραίες περιπτώσεις, σε «αφανισμό» του εμπόρου από την οικεία αγορά. Κάθε πλατφόρμα, ως πάροχος υπηρεσίας της Κοινωνίας της Πληροφορίας (ΚτΠ), δημιουργεί έτσι το απαιτούμενο υπόβαθρο εμπιστοσύνης μεταξύ αγνώστων ώστε να καταστεί δυνατή η κατάρτιση και ολοκλήρωση συναλλαγών στο ψηφιακό περιβάλλον, και δεν περιορίζεται εξ αρχής στον ρόλο ενός απλού μεσάζοντος (Husovec, 2024).

Η Πράξη για τις Ψηφιακές Υπηρεσίες (ΠΨΥ) αποτελεί τον πρώτο Κανονισμό που εκδόθηκε με σκοπό τη συνολική ρύθμιση των ψηφιακών υπηρεσιών. (Wilman, Kalèda and Loewenthal, 2024). Σύμφωνα με το άρθρο 1 παρ. 1 ΠΨΥ, σκοπός του Κανονισμού είναι να συμβάλει στην εύρυθμη λειτουργία της εσωτερικής αγοράς ενδιάμεσων υπηρεσιών, θεσπίζοντας εναρμονισμένους κανόνες για ένα ασφαλές, προβλέψιμο και αξιόπιστο επιγραμμικό περιβάλλον που διευκολύνει την καινοτομία και διασφαλίζει ουσιαστική προστασία θεμελιωδών δικαιωμάτων του Χάρτη, συμπεριλαμβανομένης της αρχής προστασίας των καταναλωτών. Ήδη από το πρώτο άρθρο διαφαίνεται η έμφαση στη δημιουργία ενός «ασφαλούς, προβλέψιμου και αξιόπιστου» επιγραμμικού περιβάλλοντος.

Σχεδόν δύο δεκαετίες μετά την οδηγία 2000/31/EK, και με την ανάδειξη οικονομικών κολοσσών που κυριαρχούν στην ψηφιακή αγορά, ο ενωσιακός νομοθέτης στοχεύει αφενός στην εισαγωγή ενιαίων κανόνων για την προώθηση της ελεύθερης κυκλοφορίας εμπορευμάτων και υπηρεσιών στην εσωτερική αγορά (άρθρο 26 ΣΛΕΕ) και αφετέρου στην ενίσχυση της προστασίας των καταναλωτών, η οποία έχει αναγνωριστεί ρητά ως θεμελιώδες δικαίωμα (άρθρο 38 ΧΘΔΕΕ). Η ρητή αναφορά στην αρχή προστασίας των καταναλωτών ήδη στο προοιμιακό άρθρο της ΠΨΥ αναδεικνύει τόσο τη θέση της στο ενωσιακό κεκτημένο όσο και την αντίληψη ότι ο σεβασμός του καταναλωτή στο επιγραμμικό περιβάλλον είναι προϋπόθεση για ασφάλεια, αξιοπιστία και διαφάνεια στις διαδικτυακές συναλλαγές (Wilman, Kalèda and Loewenthal, 2024).

Η ΠΨΥ ρυθμίζει τις ψηφιακές υπηρεσίες και, ακριβέστερα, τις «ενδιάμεσες υπηρεσίες». Για την κατανόηση του αντικειμενικού πεδίου εφαρμογής, καθοριστικοί είναι οι ορισμοί του άρθρου 3: οι «ενδιάμεσες υπηρεσίες» αποτελούν υποκατηγορία των «υπηρεσιών της κοινωνίας των πληροφοριών». Ο ορισμός της «υπηρεσίας της κοινωνίας των πληροφοριών» στο άρθρο 3 περ. α) ΠΨΥ παραπέμπει στο άρθρο 1 παρ. 1 στοιχ. β) της οδηγίας (ΕΕ) 2015/1535, όπου ως τέτοια νοείται κάθε υπηρεσία που συνήθως παρέχεται έναντι αμοιβής, με ηλεκτρονικά μέσα, εξ αποστάσεως και κατόπιν συγκεκριμένης παραγγελίας αποδέκτη υπηρεσιών. Κάθε υπηρεσία ΚτΠ συνιστά καταρχάς «υπηρεσία» κατά την έννοια του άρθρου 57 ΣΛΕΕ και προσφέρεται κατά κανόνα έναντι αμοιβής. Η έννοια της αμοιβής, όμως, έχει ερμηνευτεί ευρέως από το ΔΕΕ: δεν απαιτείται να καταβάλλεται από τον ίδιο τον αποδέκτη της υπηρεσίας, αλλά μπορεί να προέρχεται από διαφημιστικά έσοδα τρίτων προς τον πάροχο. Έτσι, ακόμη και «δωρεάν» παροχές υπηρεσιών ΚτΠ προς καταναλωτές, που χρηματοδοτούνται από διαφημιστικά έσοδα, εμπίπτουν στην έννοια της αμειβόμενης υπηρεσίας όταν τα έσοδα προέρχονται από συγκεκριμένο έμπορο/πάροχο περιεχομένου που πληρώνει για να διαφημιστούν προϊόντα ή υπηρεσίες του. Το ίδιο ισχύει και όταν ο πάροχος ενδιάμεσων υπηρεσιών παρέχει πρόσβαση σε αποδέκτες, προβάλλοντας διαφημίσεις τρίτων: το οικονομικό όφελος παραμένει έμμεσο και προερχόμενο από τους διαφημιζόμενους. Η έννοια της «ενδιάμεσης υπηρεσίας» είναι καθοριστική για τον προσδιορισμό του αντικειμενικού πεδίου εφαρμογής της ΠΨΥ. Παρότι στο άρθρο 3 υπάρχουν πολλοί ορισμοί, η ίδια η «ενδιάμεση υπηρεσία» δεν ορίζεται ρητά. Αντί αυτού, στο άρθρο 3 περ. ζ) γίνεται αναφορά σε τρεις χαρακτηριστικές υπηρεσίες ΚτΠ ως αποκλειστικές κατηγορίες ενδιάμεσων υπηρεσιών: απλή μετάδοση, προσωρινή αποθήκευση και φιλοξενία. (Köhler, 2024).

Κεντρική έννοια της ΠΨΥ είναι ο πάροχος ενδιάμεσων υπηρεσιών. Ως τέτοιος νοείται όποιος, κατά κανόνα έναντι αμοιβής, διαμεσολαβεί στη διακίνηση περιεχομένου τρίτων (η ΠΨΥ μιλά για «πληροφορίες») χωρίς να το ελέγχει. Το περιεχόμενο προέρχεται από τους αποδέκτες της υπηρεσίας, δηλαδή φυσικά ή νομικά πρόσωπα που χρησιμοποιούν την ενδιάμεση υπηρεσία είτε για να αναζητήσουν πληροφορίες είτε για να παρέχουν πρόσβαση σε αυτές (άρθρο 3 περ. β) ΠΨΥ), (Köhler, 2024).

Ενδεικτικά, το Spotify λειτουργεί ως πάροχος περιεχομένου, αφού αναρτά το ίδιο το περιεχόμενο και το ελέγχει. Αντίθετα, το YouTube αποτελεί πάροχο ενδιάμεσων υπηρεσιών: επιτρέπει σε τρίτους να αναρτούν περιεχόμενο και καταρχήν δεν ασκεί έλεγχο στο περιεχόμενο των τρίτων. Υποκατηγορία παρόχου ενδιάμεσων υπηρεσιών είναι ο πάροχος υπηρεσιών φιλοξενίας, ο οποίος αποθηκεύει πληροφορίες/περιεχόμενο που παρέχει αποδέκτης της υπηρεσίας κατόπιν αιτήματός του (άρθρο 3 περ. ζ υποπερ. iii ΠΨΥ). Παρότι ο ρόλος φιλοξενίας φαίνεται κατ' αρχήν στατικός, η ΠΨΥ αναγνωρίζει ότι επιγραμμικές πλατφόρμες μπορεί να έχουν ενεργητικό ρόλο, διότι όχι μόνο αποθηκεύουν, αλλά και διαδίδουν το περιεχόμενο στο κοινό (άρθρο 3 περ. θ) ΠΨΥ). Η «διάδοση στο κοινό» ορίζεται ως η διάθεση πληροφοριών, κατόπιν αιτήματος του αποδέκτη που τις παρείχε, σε δυνητικά απεριόριστο αριθμό τρίτων (άρθρο 3 περ. ια) ΠΨΥ). Η ουσιώδης διαφορά της επιγραμμικής πλατφόρμας από τον απλό πάροχο φιλοξενίας είναι ότι ο διαμεσολαβητικός της ρόλος συνίσταται στο να επιτρέπει πρόσβαση στο κοινό σε περιεχόμενο που παρέχουν τρίτοι αποδέκτες της υπηρεσίας, δηλαδή σε απεριόριστο και μεταβλητό αριθμό προσώπων (Hofmann, 2023).

Για να γίνει κατανοητός ο ρόλος των επιγραμμικών πλατφορμών ως παρόχων ενδιάμεσων υπηρεσιών, έχει σημασία η διάκριση των επιμέρους ενδιάμεσων λειτουργιών: μια πλατφόρμα μπορεί να έχει διαδραστική λειτουργία (διάδοση περιεχομένου τρίτων, π.χ. YouTube), πληροφοριακή λειτουργία (μηχανές αναζήτησης, π.χ. Google Search) ή συναλλακτική λειτουργία (διαμεσολάβηση σε συμβάσεις εμπόρων–καταναλωτών, π.χ. Temu). Δεν αποκλείεται, βεβαίως, μια πλατφόρμα όπως η Amazon να συνδυάζει και τις τρεις: διευκολύνει αναζήτηση μέσω ευρετηρίου (πληροφοριακή), επιτρέπει αξιολογήσεις προϊόντων (διαδραστική) και διευκολύνει τη σύναψη συμβάσεων (συναλλακτική) (Hofmann, 2023).

Βασικό γνώρισμα της επιγραμμικής πλατφόρμας είναι ότι διαμεσολαβεί στη διάδοση περιεχομένου τρίτων προς το κοινό κατόπιν αιτήματος των αποδεκτών της υπηρεσίας. Παραδείγματα είναι τα μέσα κοινωνικής δικτύωσης (Facebook, Instagram) και οι επιγραμμικές

αγορές, δηλαδή πλατφόρμες που επιτρέπουν τη σύναψη εξ αποστάσεως συμβάσεων μεταξύ εμπόρων και καταναλωτών (Amazon, Temu, Booking, AirBnB, καθώς και πλατφόρμες ηλεκτρονικών παιχνιδιών Steam, PS Store, Epic Store, Origin κ.ά.). Στο μέτρο που οι επιγραμμικές πλατφόρμες ενεργοποιούνται στην κατάρτιση και εκτέλεση συμβάσεων μεταξύ εμπόρων και καταναλωτών, ο ενωσιακός νομοθέτης της ΠΨΥ έκρινε ότι πρέπει αφενός να παρουσιάζουν με διαφάνεια τη νομική τους θέση ως διαμεσολαβητών κατά την κατάρτιση της σύμβασης και αφετέρου να υπέχουν συγκεκριμένες υποχρεώσεις δέουσας επιμέλειας. Το χωρικό πεδίο εφαρμογής της ΠΨΥ προσδιορίζεται, κατά το άρθρο 2 παρ. 1, με βάση τον τόπο εγκατάστασης ή την τοποθεσία των αποδεκτών των ενδιάμεσων υπηρεσιών, δηλαδή των φυσικών ή νομικών προσώπων στα οποία προσφέρονται οι ενδιάμεσες υπηρεσίες. Ο τόπος εγκατάστασης των παρόχων είναι καταρχήν αδιάφορος. Η διάταξη ερμηνεύεται συστηματικά μαζί με το άρθρο 3 περ. δ) και ε) ΠΨΥ, ώστε να θεμελιωθεί (ιδίως για παρόχους εκτός Ένωσης) κριτήριο ουσιώδους σύνδεσης με την Ένωση. Έτσι, πάροχοι θεωρείται ότι προσφέρουν υπηρεσίες στην Ένωση όταν: α) παρέχουν σε πρόσωπα σε ένα ή περισσότερα κράτη μέλη τη δυνατότητα χρήσης των υπηρεσιών τους και β) έχουν ουσιώδη σύνδεση με την Ένωση.

Ως προς την πρώτη προϋπόθεση, η προσφορά υπηρεσιών σε πρόσωπα που είναι εγκατεστημένα ή βρίσκονται στην Ένωση (άρθρο 2 παρ. 1 σε συνδ. με άρθρο 3 περ. δ) ΠΨΥ) έχει ιδιαίτερα συμπεριληπτικό χαρακτήρα. Αρκεί η δυνατότητα χρήσης χωρίς να απαιτείται πραγματική χρήση. Έτσι αρκεί η δυνατότητα αναζήτησης/ανάκτησης πληροφοριών από χρήστες ή η δυνατότητα προς εμπόρους να διαφημίσουν/προωθήσουν προϊόντα ακόμη κι αν δεν την αξιοποιήσουν. Αν προστεθεί ότι οι αποδέκτες αρκεί να βρίσκονται απλώς στην επικράτεια της Ένωσης, γίνεται αντιληπτό ότι το χωρικό πεδίο εφαρμογής διευρύνεται ώστε να καλύπτει κάθε υποκείμενο δικαίου που έστω και προσωρινά βρίσκεται στην Ένωση. Ως «ουσιώδης σύνδεση με την Ένωση» ορίζεται η σύνδεση που προκύπτει είτε από εγκατάσταση στην Ένωση είτε από πραγματικά κριτήρια, όπως: σημαντικός αριθμός αποδεκτών σε κράτος/κράτη μέλη σε σχέση με τον πληθυσμό τους ή στόχευση δραστηριοτήτων προς κράτος/κράτη μέλη. Ο νομοθέτης υιοθετεί συμπεριληπτικά κριτήρια σύνδεσης, ώστε—παρά τη διάκριση τριών ενδεικτικών υποκατηγοριών παρόχων να αποκλείονται ουσιαστικά μόνο όσοι περιορίζονται στην παροχή καθαρά τεχνικής πρόσβασης σε ιστοτόπους (Barudi, 2024).

Οι τρεις υποκατηγορίες παρόχων που καταλαμβάνονται από την ΠΨΥ είναι:

α) Πάροχοι εγκατεστημένοι στην Ένωση (άρθρο 3 περ. ε υποπερ. α ΠΨΥ): ο τόπος εγκατάστασης είναι αυτόνομη έννοια και προϋποθέτει πραγματική και σταθερή παρουσία

μέσω της οποίας ασκείται εμπορική δραστηριότητα (προσωπικό/υλικός εξοπλισμός), με διαρκή εξωστρεφή εκδήλωση ως προέκταση της επιχείρησης· δεν είναι κρίσιμο αν η εγκατάσταση έχει νομική προσωπικότητα. Παρόμοια αντίληψη υπάρχει και στο άρθρο 3 παρ. 1 ΓΚΠΔ, με την αιτ. σκ. 22 να τονίζει την ουσιαστική και πραγματική άσκηση δραστηριότητας μέσω σταθερών ρυθμίσεων (fixed establishments), χωρίς να είναι καθοριστικός ο νομικός τύπος (παράρτημα/θυγατρική). Συνεπώς, πάροχοι με θυγατρικές/υποθυγατρικές ή υποκαταστήματα στην Ένωση θεωρούνται εγκατεστημένοι, καθώς δημιουργούν εντύπωση μόνιμης παρουσίας (Hofmann, 2023).

β) Πάροχοι με σημαντικό αριθμό αποδεκτών σε κράτος/κράτη μέλη σε σχέση με τον πληθυσμό (άρθρο 3 περ. ε υποπερ. β ΠΨΥ): το κριτήριο αυτό, για να είναι μετρήσιμο, αναφέρεται εκ των πραγμάτων σε αποδέκτες που κάνουν πραγματική χρήση της υπηρεσίας (είτε παρέχοντας πληροφορίες προς φιλοξενία/διάδοση είτε εκτιθέμενοι σε πληροφορίες τρίτων). Κατά την ορθότερη άποψη, ο αριθμός είναι μετρήσιμος ανά είδος ενδιάμεσης υπηρεσίας που παρέχει ο ίδιος πάροχος, εφόσον παρέχει περισσότερες από μία. Αρκεί ακόμη κι ένα κράτος μέλος, αν ο αριθμός αποδεκτών είναι σημαντικός σε σχέση με τον συνολικό πληθυσμό (Barudi, 2024).

γ) Πάροχοι που στοχεύουν δραστηριότητες σε κράτος/κράτη μέλη (άρθρο 3 περ. ε υποπερ. γ ΠΨΥ): η «στόχευση» είναι αυτόνομη έννοια και, κατά την αιτ. σκ. 8 ΠΨΥ, προσομοιάζει με την «κατεύθυνση δραστηριοτήτων» του εμπόρου προς κράτος μέλος κατά το άρθρο 17 παρ. 1 (γ) του Κανονισμού (ΕΕ) 1215/2012. Κρίσιμη είναι η νομολογία του ΔΕΕ για το άρθρο 15 παρ. 1 (γ) του Κανονισμού (ΕΚ) 44/2001 (αντίστοιχο του άρθρου 17 παρ. 1 (γ) του Κανονισμού 1215/2012): για να κριθεί ότι ο έμπορος «κατευθύνει» δραστηριότητες προς κράτος μέλος κατοικίας του καταναλωτή, πρέπει να έχει εκδηλώσει βούληση σύναψης εμπορικών σχέσεων με καταναλωτές εκεί. Ενδείξεις τέτοιας βούλησης, που μπορούν να συνδυάζονται, είναι μεταξύ άλλων ο διεθνής χαρακτήρας δραστηριότητας, η περιγραφή δρομολογίων προς τον τόπο εγκατάστασης, η χρήση διαφορετικής γλώσσας/νομίσματος και δυνατότητα κράτησης σε αυτά, η αναγραφή τηλεφώνου με διεθνή κωδικό, η πληρωμή υπηρεσιών ευρετηρίασης για διευκόλυνση πρόσβασης από άλλα κράτη μέλη, η χρήση domain διαφορετικού ανώτατου επιπέδου και η μνεία διεθνούς πελατείας.

Η εν λόγω νομολογία για τα κριτήρια «κατεύθυνσης» δραστηριοτήτων είναι πλέον πάγια και επεκτείνεται και σε παρεμφερείς έννοιες άλλων Κανονισμών, όπως του Κανονισμού (ΕΕ) 2017/1001 για το σήμα της ΕΕ. Τα ίδια κριτήρια απαντώνται και στην αιτ. σκ. 8 ΠΨΥ ως

ενδείκτες στόχευσης δραστηριοτήτων παρόχων προς κράτη μέλη, με βάση συνολική θεώρηση περιστάσεων (γλώσσα/νόμισμα του κράτους μέλους, δυνατότητα παραγγελίας, domain name, διαθεσιμότητα σε εθνικό app store, τοπικές διαφημίσεις ή διαφημίσεις στη γλώσσα του κράτους, εξυπηρέτηση πελατών στη γλώσσα κ.λπ.). (Wilman, Kalèda and Loewenthal, 2024). Επιστρέφοντας στην υπόθεση Oberdorf v. Amazon, γίνεται αντιληπτό ότι ακόμη κι αν η Amazon ήταν εγκατεστημένη στις ΗΠΑ χωρίς θυγατρική ή υποκατάστημα σε κράτος μέλος, εφόσον στοχεύει τη δραστηριότητά της προς κράτος μέλος της Ένωσης, είτε απευθυνόμενη σε καταναλωτές που έστω και προσωρινά διαμένουν σε αυτό, είτε προσφέροντας δυνατότητα παροχής υπηρεσιών της (π.χ. για προώθηση προϊόντων) σε εμπόρους που βρίσκονται απλώς σε κράτος μέλος, η ΠΨΥ θα ήταν εφαρμοστέα στη συγκεκριμένη υπόθεση.

2.6. Μηχανισμοί αποκατάστασης και ένδικης προστασίας καταναλωτή

Η απάτη μέσω phishing δεν αποτελεί πλέον ένα μεμονωμένο περιστατικό που μπορεί εύκολα να αποδοθεί σε απροσεξία του χρήστη. Αντίθετα, εντάσσεται σε ένα ευρύτερο ψηφιακό περιβάλλον, στο οποίο οι καταναλωτές καλούνται καθημερινά να λαμβάνουν αποφάσεις μέσα σε συνθήκες πίεσης, ταχύτητας και πληροφοριακού κορεσμού. Το στοιχείο αυτό έχει ιδιαίτερη σημασία όταν εξετάζονται οι μηχανισμοί αποκατάστασης της ζημίας και η ένδικη προστασία που παρέχεται στα θύματα τέτοιων επιθέσεων (Koolen, 2023). Στην πράξη, ο καταναλωτής που πέφτει θύμα phishing έρχεται αντιμέτωπος με άμεση οικονομική απώλεια, συχνά χωρίς να έχει πλήρη εικόνα του τι ακριβώς συνέβη. Η πρώτη και πιο κρίσιμη αντίδραση είναι η επικοινωνία με τον πάροχο υπηρεσιών πληρωμών, συνήθως την τράπεζα, προκειμένου να μπλοκαριστούν περαιτέρω συναλλαγές και να διερευνηθεί η μη εγκεκριμένη πράξη πληρωμής. Το σημείο αυτό είναι καθοριστικό, καθώς από τη στάση του παρόχου εξαρτάται σε μεγάλο βαθμό αν και πώς θα αποκατασταθεί η ζημία (ΜΠρΑθ 71756/2025).

Το ισχύον νομικό πλαίσιο αντιμετωπίζει τις μη εγκεκριμένες πράξεις πληρωμής με μια βασική παραδοχή: ο καταναλωτής δεν φέρει κατ' αρχήν τον κίνδυνο για πράξεις που δεν ενέκρινε. Η επιστροφή του ποσού θεωρείται ο κανόνας και όχι η εξαίρεση, εκτός εάν αποδειχθεί δόλος ή βαριά αμέλεια του πληρωτή, στοιχείο που βαρύνει τον πάροχο υπηρεσιών πληρωμών (Ν. 4537/2018, Ν. 5019/2023).

Εδώ ακριβώς εντοπίζεται και το βασικό πεδίο σύγκρουσης. Στις περισσότερες περιπτώσεις phishing, ο καταναλωτής έχει μεν προβεί σε κάποια ενέργεια, όπως η εισαγωγή κωδικών ή η επιβεβαίωση συναλλαγής, όμως η ενέργεια αυτή τελεί υπό καθεστώδες παραπλάνησης. Οι πρακτικές αυτές βασίζονται σε τεχνικές κοινωνικής μηχανικής, εκμεταλλευόμενες τον φόβο, την αίσθηση του επείγοντος ή την εμπιστοσύνη προς φαινομενικά αξιόπιστους φορείς (Hyde-Cartwright, 2023).

Η πρόσφατη ελληνική νομολογία δείχνει ότι τα δικαστήρια δεν αρκούνται πλέον στη διαπίστωση ότι «ο χρήστης γνωστοποίησε τους κωδικούς του». Αντίθετα, εξετάζουν το σύνολο των περιστάσεων, όπως το είδος της απάτης, τη μεθοδολογία των δραστών, τη χρονική αλληλουχία των συναλλαγών και, κυρίως, το αν ο πάροχος είχε τη δυνατότητα να εντοπίσει ύποπτη δραστηριότητα βάσει του συναλλακτικού προφίλ του πελάτη (ΜΕΦΔωδ 23/2025, ΜΕΦΘρακ 145/2025). Ιδιαίτερη βαρύτητα αποδίδεται στο γεγονός ότι οι τράπεζες διαθέτουν εξελιγμένα συστήματα παρακολούθησης συναλλαγών και μηχανισμούς ελέγχου κινδύνου. Όταν παρατηρούνται ασυνήθιστα μοτίβα, όπως αιφνίδιες μεταφορές χρημάτων ή διαδοχικές πράξεις που αποκλίνουν από τη συνήθη συμπεριφορά του πελάτη, γεννάται εύλογη προσδοκία ότι ο πάροχος θα ενεργήσει προληπτικά, ακόμη και με προσωρινή αναστολή της συναλλαγής (Husovec, 2024).

Πέρα από την ατομική αξίωση επιστροφής χρημάτων, ο καταναλωτής διαθέτει και συλλογικούς μηχανισμούς προστασίας. Οι ενώσεις καταναλωτών μπορούν να ασκήσουν αντιπροσωπευτικές αγωγές, επιδιώκοντας όχι μόνο την αποζημίωση αλλά και την παύση πρακτικών που εκθέτουν τους χρήστες σε αυξημένο κίνδυνο εξαπάτησης (Αλεξανδρίδου και Απαλαγάκη, 2023).

Σημαντικό ρόλο διαδραματίζει και η διοικητική προστασία, καθώς οι αρμόδιες αρχές δύνανται να επιβάλουν κυρώσεις σε περιπτώσεις πλημμελούς συμμόρφωσης των παρόχων με τις υποχρεώσεις ασφάλειας και ενημέρωσης. Οι παρεμβάσεις αυτές λειτουργούν συμπληρωματικά προς την ένδικη προστασία και ενισχύουν την πρόληψη μελλοντικών περιστατικών phishing (Καραγκουνίδη και Λιναρίτη, 2023).

Τελικά, η αποκατάσταση της ζημίας σε περιπτώσεις phishing δεν αφορά μόνο την επίλυση μιας ατομικής διαφοράς. Συνδέεται άμεσα με τη διατήρηση της εμπιστοσύνης στις ψηφιακές συναλλαγές και με τη θεμελιώδη αρχή ότι ο καταναλωτής δεν μπορεί να επωμίζεται

δυσανάλογα τον κίνδυνο σε ένα περιβάλλον που ελέγχεται τεχνικά και οργανωτικά από ισχυρούς παρόχους (Volmar and Helmdach, 2018).

Κεφάλαιο 3: Ανάλυση πραγματικών περιστατικών phishing

Η θεωρητική προσέγγιση του φαινομένου του phishing συμπληρώνεται ουσιαστικά από την ανάλυση πραγματικών περιστατικών, τα οποία αναδεικνύουν τον τρόπο με τον οποίο οι επιθέσεις αυτές εκδηλώνονται στην πράξη και τις έννομες συνέπειες που προκαλούν στον τομέα των ηλεκτρονικών πληρωμών. Τα περιστατικά αυτά καταδεικνύουν ότι το phishing δεν αποτελεί αφηρημένη ή υποθετική απειλή, αλλά μία επαναλαμβανόμενη πρακτική εξαπάτησης, με άμεσες οικονομικές επιπτώσεις για τους χρήστες υπηρεσιών πληρωμών και σημαντικές προκλήσεις για το υφιστάμενο σύστημα προστασίας του καταναλωτή.

Σύμφωνα με την καταγεγραμμένη πρακτική, τα συνηθέστερα περιστατικά phishing αφορούν περιπτώσεις όπου ο χρήστης οδηγείται, μέσω παραπλανητικού μηνύματος ή συνδέσμου, σε ψευδή ιστοσελίδα που προσομοιάζει με εκείνη πιστωτικού ιδρύματος ή παρόχου υπηρεσιών πληρωμών. Εκεί καλείται να εισαγάγει διαπιστευτήρια πρόσβασης (username και password), καθώς και πρόσθετους κωδικούς ασφαλείας, όπως κωδικούς μιας χρήσης (OTP). Οι δράστες, αποκτώντας τα στοιχεία αυτά, προβαίνουν άμεσα σε μη εγκεκριμένες πράξεις πληρωμής, συνήθως μέσω μεταφορών χρηματικών ποσών σε λογαριασμούς τρίτων, συχνά εγκατεστημένους στο εξωτερικό. Η πρακτική αυτή αποτυπώνεται με σαφήνεια σε σειρά δικαστικών αποφάσεων, όπου οι ενάγοντες καταναλωτές ισχυρίστηκαν ότι εισήλθαν σε ιστοσελίδα με χαρακτηριστικά παρόμοια με εκείνα της τράπεζάς τους και, αφού καταχώρησαν τους κωδικούς τους, διαπίστωσαν τη διενέργεια διαδοχικών μεταφορών χρημάτων χωρίς τη συγκατάθεσή τους. Τα περιστατικά αυτά αναδεικνύουν τη λεπτή γραμμή μεταξύ της συμπεριφοράς του χρήστη και της ευθύνης του παρόχου υπηρεσιών πληρωμών, ιδίως όταν η απάτη βασίζεται στην εκμετάλλευση της εμπιστοσύνης του καταναλωτή στο ψηφιακό περιβάλλον.

Ειδικότερα στην υπ' αριθμ. 23/2025 απόφαση του Μονομελούς Εφετείου Δωδεκανήσου, το δικαστήριο εξετάζει ένα χαρακτηριστικό και ιδιαίτερα αποκαλυπτικό περιστατικό phishing σε περιβάλλον ηλεκτρονικής τραπεζικής, το οποίο αναδεικνύει με σαφήνεια τόσο τον τρόπο εκδήλωσης της απάτης όσο και τα όρια της ευθύνης του καταναλωτή και του παρόχου

υπηρεσιών πληρωμών. Η υπόθεση αφορά συνταξιούχο, ο οποίος διατηρούσε αποταμιευτικό λογαριασμό συνδεδεμένο με υπηρεσία e-banking και επιδίωξε απλώς να ενημερωθεί για το διαθέσιμο υπόλοιπό του. Για τον σκοπό αυτό πληκτρολόγησε τον διακριτικό τίτλο της τράπεζας σε μηχανή αναζήτησης και επέλεξε το πρώτο αποτέλεσμα, το οποίο αποδείχθηκε ότι ήταν απομιμητικός ιστότοπος, με χαρακτηριστικά σχεδόν ταυτόσημα με εκείνα της επίσημης ιστοσελίδας της τράπεζας. Στο παραπλανητικό αυτό περιβάλλον εισήγαγε τους προσωπικούς του κωδικούς πρόσβασης (username και password) και, στη συνέχεια, πληκτρολόγησε οκταψήφιο μοναδικό κωδικό μίας χρήσης (OTP), τον οποίο έλαβε στο κινητό του τηλέφωνο. Αμέσως μετά την καταχώριση του κωδικού, η ιστοσελίδα ακινητοποιήθηκε, γεγονός που προκάλεσε εύλογη ανησυχία στον χρήστη, ο οποίος επικοινωνήσε άμεσα με το τμήμα εξυπηρέτησης πελατών της τράπεζας.

Κατά την επικοινωνία αυτή πληροφορήθηκε ότι, μέσα σε ελάχιστα λεπτά, είχαν ήδη πραγματοποιηθεί τέσσερις διαδοχικές μεταφορές εμβασμάτων από τον λογαριασμό του, συνολικού ύψους 37.340 ευρώ, προς άγνωστους δικαιούχους σε αλλοδαπή, και συγκεκριμένα σε ιρλανδική τράπεζα. Το δικαστήριο δέχθηκε ως κρίσιμο πραγματικό στοιχείο ότι, με την καταχώριση του OTP στο απομιμητικό περιβάλλον, εγκρίθηκε νέα συσκευή πιστοποίησης, γεγονός που επέτρεψε στους άγνωστους δράστες να αποκτήσουν ουσιαστική πρόσβαση στο σύστημα ηλεκτρονικών συναλλαγών και να εκτελέσουν τις μεταφορές κεφαλαίων σε εξαιρετικά σύντομο χρονικό διάστημα. Ο ενάγων προέβη αμελλητί σε κάθε ενέργεια που μπορούσε, ενημερώνοντας την τράπεζα, αποστέλλοντας σχετικό ηλεκτρονικό μήνυμα και επιχειρώντας να κινηθεί και προς τις αρμόδιες αρχές, ενώ λίγες ημέρες αργότερα ενημερώθηκε ότι η τράπεζα είχε προβεί σε αίτημα ανάκλησης των επίμαχων συναλλαγών, χωρίς ωστόσο να επιτευχθεί η ανάκτηση των χρηματικών ποσών. Καθώς η τράπεζα αρνήθηκε να του αποδώσει το αφαιρεθέν ποσό, ο ενάγων άσκησε αγωγή, η οποία έγινε εν μέρει δεκτή σε πρώτο βαθμό και οδήγησε στην άσκηση έφεσης από την τράπεζα. Το Εφετείο, εξετάζοντας την υπόθεση, δεν περιορίστηκε σε μία τυπική αξιολόγηση της χρήσης των εξατομικευμένων διαπιστευτηρίων ασφαλείας, αλλά προχώρησε σε ουσιαστική ανάλυση της έννοιας της «έγκρισης» πράξης πληρωμής κατά τον ν. 4537/2018. Το δικαστήριο τόνισε ότι η απλή χρήση του μέσου πληρωμών και η καταχώριση κωδικών δεν αρκούν, αφ' εαυτών, για να θεμελιώσουν πραγματική και έγκυρη συναίνεση του πληρωτή. Αντιθέτως, απαιτείται η συναλλαγή να ανταποκρίνεται στην αληθινή βούληση του χρήστη και να υπάρχει σαφής γνώση του ποσού και του δικαιούχου της πληρωμής. Στην κρίνόμενη περίπτωση, ο ενάγων τελούσε υπό την πεποίθηση ότι βρισκόταν στο στάδιο απλής ταυτοποίησης προκειμένου να εισέλθει στο σύστημα και να ελέγξει το υπόλοιπό του, χωρίς να έχει καμία γνώση ή πρόθεση έγκρισης

μεταφοράς χρηματικών ποσών σε τρίτους. Υπό το πρίσμα αυτό, το δικαστήριο έκρινε ότι οι επίμαχες συναλλαγές δεν μπορούσαν να θεωρηθούν εγκεκριμένες, ακόμη και αν τυπικά χρησιμοποιήθηκαν οι προβλεπόμενοι μηχανισμοί ασφαλείας.

Ιδιαίτερη σημασία αποδίδεται, επίσης, στην αξιολόγηση της συμπεριφοράς του ενάγοντος. Το Εφετείο αναγνώρισε ότι η επιλογή εισόδου στην ιστοσελίδα μέσω μηχανής αναζήτησης και όχι μέσω άμεσης πληκτρολόγησης της επίσημης διεύθυνσης συνιστά πλημμελή συμπεριφορά, πλην όμως έκρινε ότι αυτή δεν υπερβαίνει τα όρια της ελαφράς αμέλειας. Το δικαστήριο έλαβε υπόψη ότι η απομιμητική ιστοσελίδα ήταν ιδιαίτερα επιτυχής ως προς την εμφάνιση και τη δομή της, ώστε να μην είναι εύκολα διακριτή από την αυθεντική από έναν μέσο χρήστη, καθώς και ότι ο ενάγων αντέδρασε άμεσα μόλις αντιλήφθηκε δυσλειτουργία, ειδοποιώντας χωρίς καθυστέρηση την τράπεζα. Με τον τρόπο αυτό, απορρίφθηκαν οι ισχυρισμοί περί βαριάς αμέλειας ή συντρέχοντος πταίσματος σε εξαιρετικά υψηλό ποσοστό, οι οποίοι θα οδηγούσαν σε μετακύλιση του συνόλου σχεδόν της ζημίας στον καταναλωτή.

Αντιθέτως, το δικαστήριο εστίασε την κρίση του στις υποχρεώσεις πρόνοιας και ασφάλειας που υπέχει η τράπεζα ως πάροχος υπηρεσιών πληρωμών. Έκρινε ότι η γενική επίκληση της ασφάλειας των συστημάτων της δεν αρκεί για την απαλλαγή από την ευθύνη, ιδίως όταν συντρέχουν αντικειμενικές ενδείξεις αυξημένου κινδύνου, όπως η εκτέλεση πολλαπλών συναλλαγών σε ελάχιστο χρόνο, η αποστολή χρημάτων σε αλλοδαπούς λογαριασμούς και η υπέρβαση ημερήσιων ορίων συναλλαγών. Το Εφετείο έκρινε ότι, υπό τις συνθήκες αυτές, η τράπεζα όφειλε να έχει ενεργοποιήσει αυξημένους μηχανισμούς ελέγχου και να εφαρμόσει ουσιαστική ισχυρή ταυτοποίηση που να συνδέει δυναμικά τη συναλλαγή με συγκεκριμένο ποσό και δικαιούχο, καθώς και να ενημερώσει άμεσα τον πελάτη για τις ύποπτες κινήσεις. Η κριτική βαρύτητα της απόφασης ενισχύεται περαιτέρω από το γεγονός ότι είχε προηγηθεί, λίγες ημέρες πριν το επίδικο περιστατικό, ενημέρωση της τράπεζας από άλλον πελάτη για την ύπαρξη απομιμητικής ιστοσελίδας που εμφανιζόταν σε μηχανή αναζήτησης. Το δικαστήριο θεώρησε ότι η γνώση αυτή δημιουργούσε αυξημένη υποχρέωση επαγρύπνησης και άμεσης αντίδρασης εκ μέρους της τράπεζας, η οποία δεν μπορούσε να εξαντληθεί σε γενικά ενημερωτικά μηνύματα προς τους πελάτες, ιδίως όταν τα περισσότερα από αυτά απεστάλησαν μετά την επέλευση της ζημίας. Η έλλειψη έγκαιρης και στοχευμένης προειδοποίησης, σε συνδυασμό με την αδυναμία αποτροπής ή έγκαιρου εντοπισμού των ύποπτων συναλλαγών, οδήγησε το δικαστήριο στο συμπέρασμα ότι η τράπεζα παρέβη τις συμβατικές και νόμιμες υποχρεώσεις της και ευθύνεται για την αποκατάσταση της ζημίας του ενάγοντος,

περιοριζόμενης μόνο κατά το ποσό που προβλέπεται από τον νόμο σε περίπτωση ελαφράς αμέλειας του χρήστη.

Συνολικά, η απόφαση 23/2025 του Μονομελούς Εφετείου Δωδεκανήσου συνιστά χαρακτηριστικό παράδειγμα νομολογιακής προσέγγισης που αντιμετωπίζει το phishing όχι ως ατομική αποτυχία προσοχής του χρήστη, αλλά ως δομικό κίνδυνο των ηλεκτρονικών πληρωμών, ο οποίος πρέπει να βαρύνει πρωτίστως τον επαγγελματία πάροχο που διαθέτει τα τεχνικά μέσα και την οργανωτική δυνατότητα πρόληψης και διαχείρισης του κινδύνου. Ταυτόχρονα, η απόφαση αναδεικνύει τη σημασία της ουσιαστικής συναίνεσης του πληρωτή και ενισχύει την προστασία του καταναλωτή στο ψηφιακό χρηματοπιστωτικό περιβάλλον, θέτοντας σαφή όρια στη μετακύλιση της ευθύνης μέσω γενικών όρων και τυπικών μηχανισμών ασφαλείας.

Ενδεικτική είναι επίσης η απόφαση του Ειρηνοδικείου Βόλου (ΕιρΒολ 36/2023), στην οποία κρίθηκε ότι η μεταφορά χρημάτων σε λογαριασμούς αγνώστων, κατόπιν επίθεσης ηλεκτρονικής απάτης τύπου phishing, συνιστά μη εγκεκριμένη πράξη πληρωμής, με άμεση συνέπεια την ενεργοποίηση του προστατευτικού μηχανισμού του ν. 4537/2018 και, ιδίως, την αντιστροφή του βάρους απόδειξης εις βάρος του παρόχου υπηρεσιών πληρωμών. Η υπόθεση αφορούσε πελάτη τραπεζικού ιδρύματος, ο οποίος, έχοντας αναρτήσει αγγελία πώλησης σε ηλεκτρονική πλατφόρμα, δέχθηκε τηλεφωνική επικοινωνία από άγνωστο πρόσωπο που προσποιήθηκε τον υποψήφιο αγοραστή και, με τεχνικές παραπλάνησης, απέσπασε στοιχεία της κάρτας του. Στη συνέχεια, ο ενάγων έλαβε κωδικό μίας χρήσης (OTP) μέσω εφαρμογής επικοινωνίας, πλην όμως η πρόσβαση στην εφαρμογή χάθηκε αιφνίδια, ενώ μέσα σε ελάχιστο χρονικό διάστημα εκτελέστηκαν διαδοχικές μεταφορές χρημάτων από τον λογαριασμό του προς λογαριασμούς τρίτων, αγνώστων σε αυτόν, σε άλλα πιστωτικά ιδρύματα, συνολικού ύψους 18.800 ευρώ. Καθοριστικό για την κρίση του δικαστηρίου υπήρξε ότι ο ενάγων αντέδρασε άμεσα, ειδοποιώντας τις αρχές και την τράπεζα μέσα σε λίγα λεπτά από τη διαπίστωση της απώλειας και υποβάλλοντας την προβλεπόμενη αμφισβήτηση συναλλαγών, στοιχείο που τον ενέταξε καθαρά στο πλαίσιο της «ειδοποίησης χωρίς υπαίτια καθυστέρηση» του άρθρου 71 ν. 4537/2018.

Στο νομικό σκέλος, το δικαστήριο έδωσε έμφαση στη θεμελιώδη προϋπόθεση του άρθρου 64 ν. 4537/2018, σύμφωνα με την οποία πράξη πληρωμής λογίζεται ως εγκεκριμένη μόνο εφόσον έχει παρασχεθεί συγκατάθεση του χρήστη, ενώ στην περίπτωση απουσίας συγκατάθεσης εφαρμόζεται το καθεστώς των μη εγκεκριμένων πράξεων πληρωμής, που οδηγεί σε υποχρέωση άμεσης αποκατάστασης του χρεωθέντος λογαριασμού. Περαιτέρω, το

Ειρηνοδικείο αντιμετώπισε ρητά την κλασική άμυνα του παρόχου ότι «οι συναλλαγές έγιναν με χρήση κωδικών/μέσων ασφαλείας», επισημαίνοντας ότι το κρίσιμο δεν είναι η τυπική χρήση διαπιστευτηρίων, αλλά η γνησιότητα της πράξης, δηλαδή αν αυτή τελέστηκε με πραγματική συναίνεση του χρήστη. Έτσι, ενεργοποιήθηκε πρακτικά η δικονομική συνέπεια που προκύπτει από τη δομή του νόμου: στην τράπεζα εναπόκειται να επικαλεστεί και να αποδείξει, με συγκεκριμένα περιστατικά, ότι εξακριβώθηκε η γνησιότητα της πράξης πληρωμής, ότι αυτή καταγράφηκε και καταχωρίστηκε ορθά και ότι δεν επηρεάστηκε από τεχνική βλάβη ή άλλη δυσλειτουργία, δηλαδή να σηκώσει το βάρος απόδειξης της «γνήσιας» συναλλαγής και της ασφαλούς λειτουργίας του συστήματος. Το δικαστήριο έκρινε ότι ο πάροχος δεν ανταποκρίθηκε στο βάρος αυτό, καθώς δεν παρέθεσε επαρκή πραγματικά δεδομένα που να αποδεικνύουν ότι οι επίδικες μεταφορές έγιναν με πραγματική βούληση του ενάγοντος ή ότι ελήφθησαν αποτελεσματικά μέτρα για να αποτραπεί ή να ανακοπεί η καταχρηστική πρόσβαση, ιδίως όταν οι μεταφορές πραγματοποιήθηκαν ταχύτατα και σε πολλαπλές δόσεις.

Ιδιαίτερα σημαντική είναι και η αξιολογική τοποθέτηση της απόφασης ως προς την υποχρέωση πρόνοιας και ασφάλειας του παρόχου. Το Ειρηνοδικείο προσέγγισε το ζήτημα όχι ως αμιγώς «λάθος του χρήστη», αλλά ως κίνδυνο ενταγμένο στη σφαίρα οργάνωσης και λειτουργίας του συστήματος πληρωμών, τον οποίο ο πάροχος οφείλει να διαχειρίζεται. Μάλιστα, σε συνάφεια με το καθεστώς προστασίας καταναλωτή, συνέδεσε τη ρύθμιση του ν. 4537/2018 με το άρθρο 8 του ν. 2251/1994, αναγνωρίζοντας ότι οι τράπεζες ως πάροχοι υπηρεσιών υπέχουν αυξημένες συναλλακτικές υποχρεώσεις ασφάλειας, ενώ το σχετικό πλαίσιο λειτουργεί ως αναγκαστικό δίκαιο υπέρ του χρήστη και δεν μπορεί να αποδυναμωθεί από γενικούς όρους συναλλαγών. Στο ίδιο πνεύμα, το δικαστήριο απέρριψε την προσπάθεια μετακύλισης της ευθύνης στον πελάτη με επίκληση ότι «έδωσε στοιχεία» ή ότι «δεν στράφηκε κατά των δραστών», κρίνοντας ότι η αξίωση του χρήστη έναντι του παρόχου ερείδεται στον ειδικό μηχανισμό αποκατάστασης μη εγκεκριμένων πράξεων και δεν εξαρτάται από το αν ο ζημιωθείς θα επιτύχει να εντοπίσει ή να διεκδικήσει ποσά από τον τελικό αποδέκτη.

Με τα δεδομένα αυτά, το Ειρηνοδικείο Βόλου κατέληξε ότι οι επίδικες μεταφορές αποτελούσαν μη εγκεκριμένες πράξεις πληρωμής και υποχρέωσε την εναγόμενη τράπεζα να καταβάλει στον ενάγοντα το ποσό των 18.800 ευρώ, με νόμιμο τόκο από συγκεκριμένο χρονικό σημείο που προσδιορίστηκε στη βάση της όχλησης/υπερημερίας, κηρύσσοντας μάλιστα την απόφαση προσωρινά εκτελεστή για μέρος του ποσού. Η νομολογιακή αξία της απόφασης έγκειται στο ότι καθιστά σαφές πως η ύπαρξη OTP ή η τεχνική εμφάνιση «έγκυρης» ταυτοποίησης δεν αρκεί από μόνη της για να θεμελιώσει έγκριση, όταν ο χρήστης δεν είχε

πραγματική γνώση και βούληση για τη συγκεκριμένη πληρωμή, ενώ ταυτόχρονα επιβεβαιώνει ότι, σε περιβάλλον phishing, ο πυρήνας της προστασίας μετατοπίζεται στην υποχρέωση του παρόχου να αποδείξει τη γνησιότητα της συναλλαγής και να ανταποκριθεί στην ευλόγως προσδοκώμενη ασφάλεια των συστημάτων πληρωμών.

Αντίστοιχα, στην υπ' αριθμ. 71756/2025 απόφαση του Μονομελούς Πρωτοδικείου Αθηνών, το δικαστήριο αντιμετώπισε με πληρότητα το ζήτημα της απάτης phishing και της μη εγκεκριμένης πράξης πληρωμής, αναγνωρίζοντας την ευθύνη της τράπεζας τόσο σε συμβατικό όσο και σε ειδικό κανονιστικό επίπεδο. Η υπόθεση αφορούσε πελάτη της εναγόμενης τράπεζας, ο οποίος διατηρούσε λογαριασμό ταμειευτηρίου με πρόσβαση σε υπηρεσίες ηλεκτρονικής τραπεζικής και έπεσε θύμα ηλεκτρονικής απάτης μέσω παραπλανητικού ηλεκτρονικού μηνύματος. Ειδικότερα, ο ενάγων έλαβε μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο φαινόταν να προέρχεται από την τράπεζα και περιείχε υπερσύνδεσμο με την ένδειξη «ενεργοποίηση τώρα». Ακολουθώντας τον σύνδεσμο, εισήλθε σε ιστοσελίδα που αποτελούσε κλώνο του επίσημου περιβάλλοντος web banking, όπου πληκτρολόγησε τα στοιχεία πρόσβασης (username και password), θεωρώντας ευλόγως ότι πρόκειται για επίσημη ιστοσελίδα της τράπεζας. Στη συνέχεια ζητήθηκε ταυτοποίηση του κινητού του τηλεφώνου, μετά την οποία ο ενάγων απώλεσε τον έλεγχο της συσκευής του, με αποτέλεσμα να πραγματοποιηθούν εν αγνοία του ενέργειες μέσω push notifications και μηνυμάτων SMS.

Μέσα σε ελάχιστο χρονικό διάστημα εκτελέστηκε μεταφορά χρηματικού ποσού ύψους 15.000 ευρώ από τον τραπεζικό του λογαριασμό προς λογαριασμό άλλης τράπεζας του εξωτερικού, χωρίς ο ενάγων να έχει δώσει συγκατάθεση, να πληκτρολογήσει κωδικό μίας χρήσης για τη συγκεκριμένη συναλλαγή ή να έχει πρόθεση μετακίνησης κεφαλαίων. Μόλις αντιλήφθηκε τη συναλλαγή, ο ενάγων επικοινωνήσε αμελλητί με το Τμήμα Εξυπηρέτησης Πελατών της τράπεζας, ζήτησε την ακύρωση της συναλλαγής και την απενεργοποίηση των κωδικών του, ενώ στη συνέχεια προέβη σε όλες τις προβλεπόμενες ενέργειες, συμπεριλαμβανομένης της υποβολής έγκλησης, της αμφισβήτησης της συναλλαγής και της προσφυγής στον Συνήγορο του Καταναλωτή. Παρά ταύτα, η τράπεζα αρνήθηκε να του αποδώσει το αφαιρεθέν ποσό, επικαλούμενη ότι η συναλλαγή πραγματοποιήθηκε με χρήση των προσωπικών του κωδικών.

Το Δικαστήριο, εξετάζοντας το ιστορικό και το αποδεικτικό υλικό, έκρινε ότι η επίδικη μεταφορά συνιστά μη εγκεκριμένη πράξη πληρωμής κατά την έννοια του ν. 4537/2018, επισημαίνοντας ότι η χρήση εξατομικευμένων διαπιστευτηρίων ασφαλείας δεν αρκεί από μόνη της για να αποδείξει πραγματική συναίνεση του πληρωτή. Αντιθέτως, κατά το άρθρο 64 του νόμου, κρίσιμο στοιχείο είναι η ύπαρξη γνήσιας βούλησης για την εκτέλεση της

συγκεκριμένης πράξης πληρωμής, η οποία στην προκειμένη περίπτωση απουσίαζε πλήρως, καθώς ο ενάγων αγνοούσε τη συναλλαγή και δεν είχε καμία πρόθεση μεταφοράς χρημάτων. Το δικαστήριο τόνισε ότι, σύμφωνα με το άρθρο 72 του ίδιου νόμου, το βάρος απόδειξης της γνησιότητας της πράξης και της απουσίας τεχνικής δυσλειτουργίας φέρει ο πάροχος υπηρεσιών πληρωμών, ενώ η τράπεζα οφείλει να αποδείξει απάτη ή βαριά αμέλεια του χρήστη, εφόσον επιδιώκει την απαλλαγή της από την ευθύνη.

Παράλληλα, το Δικαστήριο θεμελίωσε την ευθύνη της τράπεζας και στις διατάξεις του Αστικού Κώδικα περί ανώμαλης παρακαταθήκης, επισημαίνοντας ότι η κατάθεση χρημάτων σε τράπεζα γεννά συμβατική υποχρέωση απόδοσης ίσου ποσού, ανεξαρτήτως κλοπής, υπεξαίρεσης ή απάτης τρίτων, δεδομένου ότι το χρήμα αποτελεί αντικαταστατό πράγμα. Η άρνηση της τράπεζας να αποδώσει το ποσό της κατάθεσης συνιστά, κατά το δικαστήριο, αθέτηση της σύμβασης, ενώ δεν αίρεται από το γεγονός ότι η πληρωμή κατευθύνθηκε σε τρίτο πρόσωπο χωρίς δικαίωμα είσπραξης. Περαιτέρω, έγινε δεκτό ότι η τράπεζα υπέχει αυξημένες παρεπόμενες υποχρεώσεις πρόνοιας, ασφάλειας, ενημέρωσης και προειδοποίησης, οι οποίες απορρέουν από την αρχή της καλής πίστης, τη διαρκή σχέση εμπιστοσύνης με τον πελάτη και τη θεσμική της θέση ως επαγγελματία παρόχου χρηματοπιστωτικών υπηρεσιών.

Ιδιαίτερη έμφαση δόθηκε στο γεγονός ότι οι κίνδυνοι απάτης μέσω phishing δεν συνιστούν ασυνήθεις ή απρόβλεπτες περιστάσεις, αλλά λειτουργικούς και οργανωτικούς κινδύνους των συστημάτων πληρωμών, οι οποίοι βαρύνουν κατ' αρχήν τον πάροχο. Το Δικαστήριο απέρριψε τον ισχυρισμό περί βαριάς αμέλειας του ενάγοντος, κρίνοντας ότι αυτός δεν παραβίασε τις υποχρεώσεις του άρθρου 69 ν. 4537/2018 με τέτοιο βαθμό ώστε να δικαιολογείται μετακύλιση της ζημίας, ενώ τόνισε ότι ακόμη και σε περίπτωση ελαφράς αμέλειας, η ευθύνη του χρήστη περιορίζεται κατ' ανώτατο όριο στο ποσό των πενήντα ευρώ. Περαιτέρω, αναγνωρίστηκε η δυνατότητα σωρευτικής θεμελίωσης ευθύνης της τράπεζας τόσο από τη σύμβαση όσο και από αδικοπραξία, καθώς και η εφαρμογή του άρθρου 8 του ν. 2251/1994 περί ευθύνης του παρέχοντος υπηρεσίες, με βάση την ευλόγως προσδοκώμενη ασφάλεια που δικαιούται ο καταναλωτής.

Με βάση τα ανωτέρω, το Μονομελές Πρωτοδικείο Αθηνών υποχρέωσε την εναγόμενη τράπεζα να καταβάλει στον ενάγοντα το ποσό των 15.000 ευρώ ως αποκατάσταση της περιουσιακής ζημίας, καθώς και χρηματική ικανοποίηση για την ηθική βλάβη που υπέστη, κρίνοντας ότι η ζημία συνδέεται αιτιωδώς με την πλημμελή θωράκιση των ηλεκτρονικών συστημάτων της τράπεζας και τη μη τήρηση των αυξημένων υποχρεώσεων ασφάλειας. Η απόφαση αυτή ενισχύει περαιτέρω τη νομολογιακή τάση που αντιμετωπίζει το phishing ως συστημικό κίνδυνο των ηλεκτρονικών πληρωμών και όχι ως ατομική αποτυχία προσοχής του

χρήστη, μετατοπίζοντας το βάρος προστασίας στον επαγγελματία πάροχο υπηρεσιών πληρωμών και ενισχύοντας ουσιαστικά τη θέση του καταναλωτή στο ψηφιακό χρηματοπιστωτικό περιβάλλον.

Ιδιαίτερη σημασία παρουσιάζει, ωστόσο, η υπ' αριθμ. 145/2025 απόφαση του Μονομελούς Εφετείου Θράκης, η οποία, παρότι αφορά επίσης περιστατικό ηλεκτρονικής απάτης μέσω phishing, καταλήγει σε διαφορετικό αποτέλεσμα ως προς την κατανομή της ευθύνης, απορρίπτοντας την αγωγή του ζημιωθέντος χρήστη και αναγνωρίζοντας βαριά αμέλεια στο πρόσωπό του. Η απόφαση αυτή αναδεικνύει τα όρια της προστασίας που παρέχει το ειδικό καθεστώς των μη εγκεκριμένων πράξεων πληρωμής και φωτίζει τις περιπτώσεις στις οποίες η συμπεριφορά του χρήστη δύναται να διακόψει τον αιτιώδη σύνδεσμο μεταξύ της απάτης και της ευθύνης του παρόχου υπηρεσιών πληρωμών. Στην υπό κρίση υπόθεση, ο ενάγων έπese θύμα τηλεφωνικής απάτης, στο πλαίσιο της οποίας άγνωστος δράστης προσποιήθηκε τρίτο πρόσωπο και, με διαδοχικά στάδια παραπλάνησης, τον έπεισε να του γνωστοποιήσει όχι μόνο στοιχεία κάρτας, αλλά και σειρά εξατομικευμένων διαπιστευτηρίων ασφαλείας, συμπεριλαμβανομένων πολλαπλών κωδικών μίας χρήσης (OTP), του username και του password του e-banking. Το δικαστήριο έκρινε ότι η αποκάλυψη αυτή δεν ήταν αποσπασματική ή στιγμιαία, αλλά επαναλαμβανόμενη και συνειδητή, παρά τις ρητές προειδοποιήσεις που περιλαμβάνονταν στα μηνύματα της τράπεζας να μην κοινοποιούνται οι κωδικοί σε τρίτους. Επιπλέον, αποδείχθηκε ότι ο ενάγων δεν ειδοποίησε άμεσα την τράπεζα μόλις αντιλήφθηκε την απάτη, μολονότι είχε τη δυνατότητα τηλεφωνικής επικοινωνίας ήδη από το απόγευμα της ίδιας ημέρας, αλλά μετέβη στο υποκατάστημα την επόμενη ημέρα, όταν η συναλλαγή είχε ήδη οριστικά εκτελεστεί.

Υπό τα δεδομένα αυτά, το Εφετείο Θράκης, παρότι αναγνώρισε ότι η επίμαχη μεταφορά συνιστούσε κατ' αρχήν μη εγκεκριμένη πράξη πληρωμής κατά την έννοια των άρθρων 64 και 72 του ν. 4537/2018, έκρινε ότι συντρέχει περίπτωση βαριάς αμέλειας του χρήστη κατά το άρθρο 69 του ίδιου νόμου. Η βαριά αυτή αμέλεια θεμελιώθηκε αφενός στην εκούσια και επανειλημμένη κοινοποίηση όλων των κρίσιμων στοιχείων ταυτοποίησης σε άγνωστο τρίτο και αφετέρου στην υπαίτια καθυστέρηση ειδοποίησης της τράπεζας, η οποία στέρησε κάθε πρακτική δυνατότητα άμεσης αντίδρασης ή ανάκλησης της συναλλαγής. Κατά το σκεπτικό του δικαστηρίου, η συμπεριφορά αυτή υπερέβαινε τα όρια της απλής απροσεξίας και συνιστούσε σοβαρή παραβίαση των υποχρεώσεων επιμέλειας που επιβάλλει ο νόμος στον χρήστη μέσων πληρωμής. Η απόφαση παρουσιάζει ιδιαίτερο ενδιαφέρον και ως προς την

αντιμετώπιση των γενικών όρων συναλλαγών της τράπεζας. Το δικαστήριο δέχθηκε ότι ορισμένοι όροι που τείνουν σε γενικό αποκλεισμό της ευθύνης της τράπεζας αντίκεινται στο αναγκαστικό δίκαιο του ν. 4537/2018 και είναι άκυροι. Ωστόσο, έκρινε ότι στην προκειμένη περίπτωση η απόρριψη της αγωγής δεν στηρίζεται σε αυτούς τους όρους, αλλά στην αυτοτελή διαπίστωση βαριάς αμέλειας του ενάγοντος, η οποία, σύμφωνα με το ισχύον νομοθετικό πλαίσιο, απαλλάσσει τον πάροχο από την υποχρέωση αποκατάστασης της ζημίας.

Σε επίπεδο συνολικής αξιολόγησης, η απόφαση 145/2025 λειτουργεί ως αναγκαίο αντίβαρο στη νομολογιακή τάση που ενισχύει την προστασία του καταναλωτή σε περιπτώσεις phishing. Αναδεικνύει ότι η ευθύνη της τράπεζας δεν είναι αντικειμενική ούτε απόλυτη και ότι η προστασία του χρήστη προϋποθέτει ελάχιστο επίπεδο συνεργασίας και τήρησης βασικών κανόνων ασφάλειας. Παράλληλα, η απόφαση καθιστά σαφές ότι η διάκριση μεταξύ ελαφράς και βαριάς αμέλειας αποτελεί το κρίσιμο φίλτρο για την κατανομή του κινδύνου στις ηλεκτρονικές πληρωμές, προσδίδοντας πρακτικό περιεχόμενο στην αρχή της ισορροπίας μεταξύ καταναλωτικής προστασίας και ευθύνης του ίδιου του χρήστη στο ψηφιακό περιβάλλον.

Συνεχίζοντας, το Μονομελές Πρωτοδικείο Ροδόπης, με τη σχολιαζόμενη απόφασή του, επιλήφθηκε μιας εξόχως ενδιαφέρουσας υπόθεσης, αναγνωρίζοντας ενδοσυμβατική και αδικοπρακτική ευθύνη της Τράπεζας σε συνδυασμό με τη διάταξη του άρθρου 8 του ν. 2251/1994, επί περιστατικού κατά το οποίο ο πελάτης της έπεσε θύμα ηλεκτρονικής απάτης μέσω e-banking. Η απόφαση αυτή επιχειρεί να επιλύσει με άρτιο νομικά τρόπο το ζήτημα της ευθύνης των τραπεζών, ιδίως ενόψει της διαπίστωσης ότι τα περιστατικά ηλεκτρονικής απάτης μέσω e-banking τα τελευταία χρόνια αυξάνονται σταθερά. Η υπόθεση έχει, κατά τα κρίσιμα πραγματικά περιστατικά, ως εξής: Οι ενάγοντες διατηρούσαν τραπεζικό λογαριασμό απλού ταμιευτηρίου στην εναγόμενη τράπεζα, από την οποία αιτήθηκαν και έλαβαν κωδικούς για τραπεζικές υπηρεσίες μέσω διαδικτύου (web-banking). Κατά την υποβολή της σχετικής αίτησης, η μία εκ των εναγόντων αποδέχθηκε με την υπογραφή της τους όρους ενός προδιατυπωμένου και άνευ ατομικής διαπραγμάτευσης εντύπου με τίτλο «Όροι Ενιαίας Σύμβασης Κατάθεσης και Συναφών Συναλλακτικών Σχέσεων». Στο έντυπο αυτό περιλαμβάνονταν, μεταξύ άλλων, όροι που ρύθμιζαν τον τρόπο πρόσβασης και ταυτοποίησης του πελάτη στο web-banking, τον τρόπο διενέργειας ισχυρής ταυτοποίησης που θα απαιτείτο σε ορισμένες συναλλαγές, την υποχρέωση του πελάτη να τηρεί μέτρα ασφαλείας και να μην γνωστοποιεί σε τρίτα πρόσωπα τα στοιχεία πρόσβασής του, την υποχρέωση της τράπεζας να

διαφυλάσσει την ασφάλεια παροχής υπηρεσιών και να διασφαλίζει την πρόσβαση του πελάτη στο δίκτυο, καθώς και όρο περί πλήρους απαλλαγής της από τυχόν ευθύνη υπό την προϋπόθεση ότι θα τηρήσει τις υποχρεώσεις της. Στη συνέχεια, κατόπιν τηλεφωνικής επικοινωνίας με τρίτο πρόσωπο, συμφωνήθηκε ότι ο πρώτος ενάγων, υπό την ιδιότητα του ιατρού, θα λάμβανε διατραπεζικά την αμοιβή του για ιατρική επίσκεψη συγγενικού προσώπου του τρίτου. Ο τελευταίος μάλιστα ανέφερε ότι η εναγόμενη τράπεζα θα απέστελλε μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο θα καθοδηγούσε τον πρώτο ενάγοντα ως προς τον τρόπο είσπραξης της συμφωνηθείσας αμοιβής, μετά από σχετική εντολή που δήθεν θα είχε δοθεί από τον τρίτο. Το μήνυμα πράγματι ελήφθη, πλην όμως επρόκειτο για απάτη, γεγονός που δεν έγινε αντιληπτό από τον πρώτο ενάγοντα, λόγω ελαφράς αμέλειας, η οποία αποδόθηκε στην ελλιπή εξοικείωσή του με τους ηλεκτρονικούς υπολογιστές. Με την επιλογή του συνδέσμου και τη χρήση των στοιχείων web-banking, ο τρίτος έλαβε γνώση των διαπιστευτηρίων και στη συνέχεια προέβη σε αλλαγή των πιστοποιητικών εισόδου με άλλα, ίδιας του γνώσης, υποκλέπτοντας κάθε φορά τους κωδικούς OTP μέσω της εφαρμογής Viber, όπου αυτοί αποστέλλονταν. Κατόπιν, πραγματοποίησε τέσσερις διαδοχικές μεταφορές χρημάτων σε τραπεζικούς λογαριασμούς τρίτων δικαιούχων, συνολικού ύψους 10.120 ευρώ.

Τελικώς, ο πρώτος ενάγων, αντιλαμβανόμενος ότι πιθανώς έχει πέσει θύμα απάτης, αυθημερόν προσήλθε σε υποκατάστημα της εναγόμενης τράπεζας προκειμένου να ενημερώσει για το συμβάν, ενώ προηγουμένως είχε ήδη ενημερώσει και τα κεντρικά της τράπεζας τηλεφωνικά. Οι αρμόδιοι υπάλληλοι, διαπιστώνοντας τις μεταφορές χρημάτων, κατάφεραν να δεσμεύσουν το τελευταίο έμβασμα, ενώ για τα υπόλοιπα επιρρίφθηκε η ευθύνη στους ενάγοντες, με αποτέλεσμα να απολέσουν το χρηματικό ποσό των 8.890 ευρώ.

Στο πλαίσιο του ανωτέρω πραγματικού, η σχολιαζόμενη απόφαση ερευνήσε αν υφίσταται ενδοσυμβατική και αδικοπρακτική ευθύνη της τράπεζας, σε συνδυασμό με την ευθύνη του άρθρου 8 του ν. 2251/1994, και αν οι βάσεις αυτές συρρέουν μεταξύ τους, με την αιτίαση ότι η τράπεζα δεν προστάτευσε ως όφειλε τους πελάτες της, με αποτέλεσμα να απολέσουν σημαντικά χρηματικά ποσά έπειτα από υποκλοπή των πιστοποιητικών εισόδου τους στο e-banking. Πριν από την ανάλυση του ειδικού νομοθετικού καθεστώτος που ισχύει στη χώρα μας αναφορικά με την προστασία των ηλεκτρονικών πληρωμών, κρίθηκε σκόπιμη μια συνοπτική παρουσίαση της συμβατικής σχέσης που συνδέει την τράπεζα με τον πελάτη της, όταν ο τελευταίος καταθέτει χρήματα σε τραπεζικό λογαριασμό. Η κατάθεση χρημάτων φέρει τον χαρακτήρα ανώμαλης παρακαταθήκης, στο πλαίσιο της οποίας η θεματοφύλακας τράπεζα

αποκτά την κυριότητα των κατατεθειμένων χρημάτων, υποχρεούται όμως, σε περίπτωση αμφιβολίας, να τα αποδώσει, εφόσον το απαιτεί ο παρακαταθέτης, ακόμη και αν δεν έχει παρέλθει η προθεσμία που ορίστηκε για τη φύλαξή τους. Εκτός της κύριας αυτής υποχρέωσης, η τράπεζα βαρύνεται και με παρεπόμενες και πρόσθετες υποχρεώσεις, οι οποίες πηγάζουν από τη γενική ρήτρα του άρθρου 288 ΑΚ και δημιουργούνται αυτοδικαίως, εφόσον συντρέχουν οι περιστάσεις που κατά την καλή πίστη απαιτούνται για την παραγωγή τους. Ενόψει της σχέσης εμπιστοσύνης που υφίσταται μεταξύ τράπεζας και πελάτη, η τράπεζα οφείλει, στο πλαίσιο της ανάγκης προστασίας του ασθενέστερου μέρους, να παρέχει τις αναγκαίες πληροφορίες και να ενημερώνει προσηκόντως για εγγενείς κινδύνους κατά την εκπλήρωση της κύριας παροχής. Ειδικότερα, οφείλει αφενός να παρέχει πληροφορίες και διευκρινίσεις σχετικά με το περιεχόμενο της σύμβασης, ώστε να διαφυλάσσεται η συμβατική ελευθερία και να μην επηρεάζεται από άγνοια η βούληση του άλλου μέρους, κατά τη σύναψη και διαμόρφωση του περιεχομένου της σύμβασης, αφετέρου δε να λαμβάνει μέτρα προστατευτικά των απόλυτων έννομων αγαθών, αλλά και της περιουσίας του άλλου μέρους. Έτσι, την τράπεζα βαρύνει γενική υποχρέωση διαφύλαξης των συμφερόντων των πελατών της, που εξειδικεύεται ιδίως σε υποχρέωση διαφύλαξης του τραπεζικού απορρήτου, υποχρέωση επιμελούς ακρόασης και εκτίμησης των συμφερόντων του πελάτη, υποχρέωση διαφώτισης, συμβουλευτικής καθοδήγησης και προειδοποίησης ενόψει συγκεκριμένων κινδύνων, υποχρέωση παροχής πληροφοριών, καθώς και σε υποχρέωση διαφύλαξης της κατάθεσης από κακόβουλες ενέργειες τρίτων. Η παράβαση των υποχρεώσεων αυτών συνιστά πλημμελή εκπλήρωση της παροχής και γεννά υποχρέωση προς αποζημίωση.

Παράλληλα, η παραβίαση της γενικής υποχρέωσης πρόνοιας, ασφάλειας και προστασίας των άλλων και των αγαθών τους, στο πλαίσιο της συναλλακτικής και γενικότερα της κοινωνικής δραστηριότητας, δηλαδή η παράβαση της κοινωνικώς επιβεβλημένης υποχρέωσης λήψης μέτρων επιμέλειας για την αποφυγή πρόκλησης ζημίας σε έννομα αγαθά τρίτων προσώπων, στοιχειοθετεί παράνομη συμπεριφορά κατά το άρθρο 914 ΑΚ. Επομένως, είναι δυνατόν η παραβίαση από τραπεζικό ίδρυμα των γενικών υποχρεώσεών του, που στηρίζονται στη διαρκή εμπιστοσύνη μεταξύ αυτού και του πελάτη, πέραν της ενδοσυμβατικής ευθύνης, να γεννά και αδικοπρακτική ευθύνη, όταν η ενέργεια αυτή καθ' εαυτή και χωρίς την προϋπάρχουσα συμβατική σχέση θα ήταν παράνομη, ως αντίθετη στο γενικό καθήκον να μην προκαλεί κανείς υπαιτίως ζημία σε άλλον. Περαιτέρω, η τεχνολογική εξέλιξη των τελευταίων ετών και η ευρεία υιοθέτηση ηλεκτρονικών μέσων πληρωμών, όπως πληρωμές με κάρτα, ανέπαφες συναλλαγές και μεταφορές χρηματικών ποσών μέσω e-banking, οι οποίες ενισχύθηκαν ακόμη περισσότερο κατά την περίοδο της Covid-19, συνέβαλαν στη δυνατότητα τρίτων να υποκλέπτουν ευαίσθητα

δεδομένα και προσωπικά στοιχεία πελατών τραπεζικών ιδρυμάτων με μεθόδους όπως phishing και pharming. Για τον λόγο αυτό κρίθηκε αναγκαίο, τόσο σε ευρωπαϊκό όσο και σε εθνικό επίπεδο, να ληφθούν προληπτικά μέτρα για τον περιορισμό της διαδικτυακής απάτης που απορρέει από την υποκλοπή δεδομένων ηλεκτρονικής τραπεζικής και καρτών. Έτσι, το πλαίσιο των υπηρεσιών πληρωμών ρυθμίστηκε αρχικά με τον ν. 3862/2010 και, ακολούθως, με τον ν. 4537/2018, ο οποίος ενσωμάτωσε την Οδηγία (ΕΕ) 2015/2366 και κατήργησε τον προηγούμενο νόμο, εξειδικεύοντας περαιτέρω την υποχρέωση προστασίας του ασθενέστερου μέρους που απορρέει από τη γενική ρήτρα του άρθρου 288 ΑΚ και εναρμονίζοντας την με το σύγχρονο σύστημα ηλεκτρονικών συναλλαγών.

Ο ν. 4537/2018 εισάγει ενισχυμένα μέτρα ασφαλείας για τους παρόχους υπηρεσιών πληρωμών, αυξάνοντας την προστασία του καταναλωτή έναντι απάτης και παράνομων πράξεων. Μεταξύ άλλων, προβλέπεται η εφαρμογή της ισχυρής ταυτοποίησης πελάτη, ενώ ο πάροχος οφείλει να παρέχει μέσα επικοινωνίας για τη γνωστοποίηση απώλειας, κλοπής, υπεξαίρεσης ή μη εγκεκριμένης χρήσης του μέσου πληρωμών, τηρώντας σχετικό αρχείο για ορισμένο χρόνο. Ιδιαίτερη σημασία έχει ότι το άρθρο 103 του ν. 4537/2018 καθιερώνει αναγκαστικό δίκαιο υπέρ των χρηστών, απαγορεύοντας παρεκκλίσεις εις βάρος τους, εκτός αν αυτό προβλέπεται ρητά, και επιτρέποντας μόνο ευνοϊκότερους όρους για τον χρήστη.

Στο πλαίσιο αυτό, κρίσιμη είναι η έννοια της μη εγκεκριμένης πράξης πληρωμής, αφού εγκεκριμένη θεωρείται εκείνη για την οποία ο πληρωτής έχει δώσει συγκατάθεση. Ο νόμος εισάγει, επίσης, αντιστροφή του βάρους απόδειξης ως προς τη γνησιότητα και την έγκριση της συναλλαγής, υπό την έννοια ότι, όταν ο χρήστης αμφισβητεί πράξη πληρωμής, ο πάροχος υπηρεσιών πληρωμών καλείται να αποδείξει ότι αυτή εγκρίθηκε και εκτελέστηκε ορθά και ότι δεν επηρεάστηκε από τεχνική βλάβη ή άλλη δυσλειτουργία. Οι διατάξεις των άρθρων 69 έως 74 ρυθμίζουν τις υποχρεώσεις του χρήστη και τις συνέπειες από την παραβίασή τους, ανάλογα με τον βαθμό πταίσματός του. Ο χρήστης οφείλει να διαφυλάσσει τα εξατομικευμένα διαπιστευτήρια ασφαλείας και να ειδοποιεί αμελλητί τον πάροχο σε περίπτωση απώλειας ή μη εγκεκριμένης χρήσης. Η ευθύνη του χρήστη διαφοροποιείται αναλόγως της υπαιτιότητας, ενώ το σύστημα του ν. 4537/2018, σε συνδυασμό με το άρθρο 8 του ν. 2251/1994, προσεγγίζει την ευθύνη των τραπεζών ως παρόχων υπηρεσιών που φέρουν συναλλακτικές υποχρεώσεις πρόνοιας και ασφάλειας, με κριτήριο την ευλόγως προσδοκώμενη ασφάλεια της παρεχόμενης υπηρεσίας.

Με βάση τα ανωτέρω, η σχολιαζόμενη απόφαση κατέληξε ότι υφίσταται ενδοσυμβατική ευθύνη της εναγόμενης τράπεζας, καθότι δεν τήρησε τις υποχρεώσεις που την βαρύνουν τόσο από τη γενική ρήτρα του άρθρου 288 ΑΚ όσο και από τον ν. 4537/2018, στο πλαίσιο παροχής υπηρεσιών ηλεκτρονικών συναλλαγών, χωρίς να μπορέσει να ανταποκριθεί στο βάρος απόδειξης της γνησιότητας της συναλλαγής. Παράλληλα, κρίθηκε ότι υφίσταται και αδικοπρακτική ευθύνη της τράπεζας, καθώς επέδειξε βαριά αμέλεια ως προς την παρεχόμενη ασφάλεια των υπηρεσιών ηλεκτρονικών συναλλαγών, με αποτέλεσμα η συμπεριφορά της να είναι παράνομη και ανεξάρτητα από την προϋπάρχουσα συμβατική σχέση, ως αντίθετη στο γενικό καθήκον του άρθρου 914 ΑΚ, δηλαδή στο «του μη ζημιούν άλλον υπαιτίως». Ειδικότερα, αποδόθηκε στην τράπεζα ότι παρέλειψε να ελέγξει την αυθεντικότητα των λογαριασμών στους οποίους αποστέλλονταν τα χρήματα, να λάβει πλήρη και υψηλά μέτρα ασφαλείας κατά τα πρότυπα του ν. 4537/2018, καθώς και να μεριμνήσει για την ενημέρωση και διαφώτιση των πελατών της για κρούσματα υποκλοπής των πιστοποιητικών εισόδου από το e-banking, ενώ επισημάνθηκε και το ζήτημα αποστολής OTP μέσω εφαρμογής όπως το Viber, που, λόγω των δυνατοτήτων διασύνδεσης, μπορεί να δημιουργεί αυξημένες πιθανότητες υποκλοπής.

Από την εξέταση των πραγματικών περιστατικών καθίσταται σαφές ότι το phishing δεν αποτελεί μια θεωρητική απειλή ή ένα σπάνιο συμβάν, αλλά μια πρακτική που επαναλαμβάνεται με εντυπωσιακή ομοιομορφία στον χώρο των ηλεκτρονικών πληρωμών. Σε όλες σχεδόν τις περιπτώσεις, ο μηχανισμός είναι παρόμοιος: ο χρήστης πείθεται ότι βρίσκεται σε ασφαλές περιβάλλον, εισάγει τα στοιχεία του και, μέσα σε ελάχιστο χρόνο, διαπιστώνει ότι έχουν εκτελεστεί συναλλαγές τις οποίες ουδέποτε είχε σκοπό να πραγματοποιήσει. Το στοιχείο αυτό αναδεικνύει ότι ο κίνδυνος δεν προκύπτει από σύνθετες τεχνικές επιθέσεις, αλλά από την εκμετάλλευση της εμπιστοσύνης και της καθημερινής εξοικείωσης του χρήστη με τις ψηφιακές συναλλαγές. Η νομολογιακή αντιμετώπιση των περιστατικών αυτών δείχνει μια σαφή μετατόπιση του ενδιαφέροντος από την τυπική χρήση κωδικών προς την ουσιαστική βούληση του πληρωτή. Τα δικαστήρια τείνουν να δέχονται ότι η ύπαρξη OTP ή η τεχνικά «επιτυχής» ταυτοποίηση δεν συνεπάγονται αυτομάτως έγκριση της πράξης πληρωμής, όταν ο χρήστης αγνοεί το ποσό και τον δικαιούχο και δεν έχει πραγματική πρόθεση μεταφοράς χρημάτων. Με τον τρόπο αυτό, το κέντρο βάρους μεταφέρεται από τη μηχανική λειτουργία του συστήματος στην πραγματική συναλλακτική βούληση, όπως αυτή προστατεύεται από τον ν. 4537/2018. Παράλληλα, τα εξεταζόμενα περιστατικά δείχνουν ότι η προστασία του χρήστη δεν λειτουργεί άνευ ορίων. Η συμπεριφορά του ίδιου του θύματος αξιολογείται ουσιαστικά και όχι τυπικά.

Όταν ο χρήστης παραπλανηθεί με τρόπο που θα μπορούσε να παρασύρει έναν μέσο συναλλασσόμενο και αντιδρά άμεσα, ενημερώνοντας χωρίς καθυστέρηση την τράπεζα, η ευθύνη μετατοπίζεται κατά βάση στον πάροχο υπηρεσιών πληρωμών. Αντίθετα, σε περιπτώσεις όπου ο χρήστης αποκαλύπτει επανειλημμένα κρίσιμα διαπιστευτήρια ή καθυστερεί υπαίτια να ειδοποιήσει, τα δικαστήρια θέτουν σαφή όρια στην καταναλωτική προστασία, αναγνωρίζοντας βαριά αμέλεια. Από τη νομολογία που αναλύθηκε προκύπτει ότι το phishing αντιμετωπίζεται πλέον ως συστημικός κίνδυνος των ηλεκτρονικών πληρωμών και όχι ως μεμονωμένη αποτυχία προσοχής του χρήστη. Η τράπεζα, ως επαγγελματίας πάροχος, καλείται να φέρει το κύριο βάρος πρόληψης και διαχείρισης του κινδύνου, ιδίως όταν εμφανίζονται ενδείξεις ύποπτης συναλλακτικής συμπεριφοράς. Την ίδια στιγμή, διατηρείται η απαίτηση στοιχειώδους επιμέλειας από τον χρήστη, ώστε να επιτυγχάνεται μια λειτουργική ισορροπία μεταξύ αποτελεσματικής προστασίας και προσωπικής ευθύνης στο σύγχρονο ψηφιακό περιβάλλον.

Κεφάλαιο 4: Μεθοδολογία και εμπειρική προσέγγιση της έρευνας

4.1. Βασικά στοιχεία της έρευνας

Η έρευνα πραγματοποιήθηκε στο πλαίσιο της παρούσας μεταπτυχιακής εργασίας και εστιάζει στο φαινόμενο του phishing, όπως αυτό εμφανίζεται στις ηλεκτρονικές πληρωμές και επηρεάζει την καθημερινή συναλλακτική πρακτική των καταναλωτών. Η προσέγγιση που επιλέχθηκε δεν περιορίζεται μόνο στη θεωρητική ανάλυση του νομικού πλαισίου, αλλά επιχειρεί να συνδυάσει τη θεωρία με εμπειρικά δεδομένα, ώστε να αποτυπωθεί και η πραγματική εικόνα που βιώνουν οι χρήστες των ψηφιακών συναλλαγών, επιλέχθηκε δηλαδή η λεγόμενη μικτή προσέγγιση. Για τον λόγο αυτό, εκτός από τη βιβλιογραφική και νομοθετική ανασκόπηση, αξιοποιήθηκε ποσοτική έρευνα μέσω ερωτηματολογίου. Στόχος του ερωτηματολογίου ήταν να καταγραφούν οι γνώσεις, οι αντιλήψεις και οι συνήθειες των καταναλωτών σε σχέση με την ηλεκτρονική τραπεζική, καθώς και ο βαθμός εξοικείωσής τους με τους κινδύνους απάτης και ειδικότερα με τις πρακτικές phishing.

Η συλλογή των δεδομένων πραγματοποιήθηκε κατά το χρονικό διάστημα από 29 Νοεμβρίου έως και 29 Δεκεμβρίου. Στην έρευνα συμμετείχαν συνολικά τριάντα άτομα, ενήλικους χρήστες ηλεκτρονικών μέσων πληρωμής και ηλεκτρονικής τραπεζικής. Το δείγμα περιλάμβανε άνδρες και γυναίκες διαφορετικών ηλικιών και μορφωτικών επιπέδων, με σκοπό να αποτυπωθούν όσο το δυνατόν περισσότερες διαφορετικές εμπειρίες και στάσεις απέναντι στις ψηφιακές συναλλαγές. Η επιλογή του δείγματος έγινε με βάση την ευκολία πρόσβασης στους συμμετέχοντες, γεγονός που συνδέεται με τους πρακτικούς περιορισμούς της έρευνας. Παρότι ο αριθμός των συμμετεχόντων είναι περιορισμένος και δεν επιτρέπει γενικεύσεις στο σύνολο του πληθυσμού, τα δεδομένα που προέκυψαν κρίνονται χρήσιμα, καθώς αναδεικνύουν βασικές τάσεις και προβληματισμούς γύρω από την ασφάλεια των ηλεκτρονικών πληρωμών και την αντίληψη των καταναλωτών για το phishing. Το ερωτηματολόγιο εμπεριείχε κυρίως ερωτήσεις κλειστού τύπου και ερωτήσεις κλίμακας, οι οποίες αφορούσαν τη συχνότητα χρήσης ηλεκτρονικών πληρωμών, το επίπεδο ενημέρωσης των συμμετεχόντων για θέματα ψηφιακής ασφάλειας, καθώς και τυχόν προσωπική εμπειρία ή επαφή με περιστατικά απάτης. Παράλληλα, διερευνήθηκε ο βαθμός εμπιστοσύνης που δείχνουν οι καταναλωτές προς τις τράπεζες και τους παρόχους υπηρεσιών πληρωμών, αλλά και το κατά πόσο αισθάνονται ότι προστατεύονται επαρκώς σε περίπτωση μη εγκεκριμένων συναλλαγών.

Τα αποτελέσματα της ποσοτικής έρευνας εξετάζονται σε συνδυασμό με την ανάλυση του ισχύοντος νομικού και θεσμικού πλαισίου, καθώς και με πραγματικά περιστατικά phishing που έχουν απασχολήσει τη νομολογία. Με τον τρόπο αυτό επιδιώκεται μια πιο ολοκληρωμένη προσέγγιση του ζητήματος, η οποία δεν περιορίζεται μόνο στη θεωρία, αλλά λαμβάνει υπόψη και την εμπειρία του ίδιου του καταναλωτή στο σύγχρονο ψηφιακό περιβάλλον.

4.2. Σκοπός της έρευνας

Η παρούσα έρευνα δεν επιδιώκει να εξετάσει ένα ακόμα εργαλείο ηλεκτρονικής απάτης, αλλά να προσεγγίσει το phishing μέσα από την προσωπική εμπειρία και στάση του καταναλωτή που χρησιμοποιεί καθημερινά ηλεκτρονικές πληρωμές. Στην πράξη οι επιθέσεις αυτές δεν εμφανίζονται ως απομονωμένα χαρακτηριστικά, αλλά εντάσσονται σε ένα περιβάλλον ψηφιακών συναλλαγών που χαρακτηρίζεται από ταχύτητα, αυτοματισμό και αυξημένη εξάρτηση από τεχνολογικά συστήματα. Βασικός σκοπός της παρούσας λοιπόν, είναι να διερευνηθεί το επίπεδο ενημέρωσης και ευαισθητοποίησης των καταναλωτών απέναντι στις

πρακτικές phishing, καθώς και ο τρόπος που αντιλαμβάνονται τους κινδύνους με τους οποίους επαπειλείται η συναλλακτική τους προστασία. Ιδιαίτερη έμφαση δίνεται στο κατά πόσο οι χρήστες αναγνωρίζουν τις συνήθεις τεχνικές εξαπάτησης και αν θεωρούν ότι διαθέτουν επαρκή γνώση και εργαλεία για την προστασία τους.

Την ίδια στιγμή η έρευνα στοχεύει να αποτυπώσει τον βαθμό εμπιστοσύνης των καταναλωτών προς τις τράπεζες και τους παρόχους υπηρεσιών πληρωμών, ιδίως σε περιπτώσεις μη εγκεκριμένων συναλλαγών. Εξετάζεται κατά πόσο οι καταναλωτές αισθάνονται πως το ισχύον θεσμικό και τεχνολογικό πλαίσιο τους εξασφαλίζει επαρκή και ουσιαστική προστασία ή εάν αντίθετα, θεωρούν ότι επωμίζονται δυσανάλογο μέρος του κινδύνου σε περίπτωση απάτης. Επιπρόσθετα, μέσω της εξέτασης των απαντήσεων του ερωτηματολογίου, η μελέτη σκοπεύει να ανακαλύψει πιθανές ελλείψεις στην πληροφόρηση των χρηστών, όπως επίσης και επαναλαμβανόμενες ενέργειες που δύνανται να μεγιστοποιούν την έκθεση σε επιθέσεις ηλεκτρονικού ψαρέματος. Αυτά τα διαπιστωθέντα λειτουργούν συμπληρωματικά προς τη νομική εξέταση και τη νομολογία που διερευνάται στα προηγούμενα κεφάλαια, συνεισφέροντας στη συνολική εκτίμηση της αποδοτικότητας των τρεχουσών μεθόδων προφύλαξης.

Τελική επιδίωξη της μελέτης είναι να φανερωθεί εάν η ασπίδα του καταναλωτή στις ηλεκτρονικές πληρωμές περιορίζεται σε ένα τυπικό νομικό όριο ή αν, στην πραγματικότητα, ανταποκρίνεται στις υπαρκτές συνθήκες και στους κινδύνους που αντιμετωπίζουν οι χρήστες στο σημερινό ψηφιακό πεδίο. Κατ' αυτόν τον τρόπο, η μελέτη επιθυμεί να λειτουργήσει ως θεμέλιο για σκέψη και πιθανές υποδείξεις ενδυνάμωσης τόσο της πληροφόρησης των καταναλωτών όσο και των συστημάτων αποτροπής και επανόρθωσης απωλειών από πρακτικές ηλεκτρονικού ψαρέματος.

4.3. Μεθοδολογία της έρευνας

Η παρούσα μελέτη προσεγγίζει το φαινόμενο του phishing μέσα από μια κυρίως βιβλιογραφική και νομική οπτική, με στόχο να αναδείξει τα κρίσιμα σημεία προστασίας του χρήστη στις σύγχρονες ψηφιακές συναλλαγές πληρωμής. Η επιλογή της συγκεκριμένης μεθοδολογίας συνδέεται άμεσα με τον χαρακτήρα της έρευνας, η οποία δεν επιδιώκει τεχνική ή αριθμητική αποτύπωση του φαινομένου, αλλά εστιάζει στην κατανόησή του ως κοινωνικού

και νομικού προβλήματος στο πλαίσιο της ψηφιακής οικονομίας. Για τον σκοπό αυτό πραγματοποιήθηκε συστηματική μελέτη της σχετικής βιβλιογραφίας και του ισχύοντος νομοθετικού πλαισίου, τόσο σε επίπεδο Ευρωπαϊκής Ένωσης όσο και σε εθνικό επίπεδο, με έμφαση στις ρυθμίσεις που αφορούν τις ηλεκτρονικές πληρωμές, την προστασία των καταναλωτών και την αντιμετώπιση των ψηφιακών απατών. Παράλληλα, εξετάστηκαν πραγματικά περιστατικά phishing που έχουν απασχολήσει τη δικαστηριακή πρακτική, προκειμένου να αποτυπωθεί ο τρόπος με τον οποίο το φαινόμενο εκδηλώνεται στην πράξη και να αναδειχθούν ζητήματα όπως η κατανομή της ευθύνης μεταξύ καταναλωτή και παρόχου υπηρεσιών πληρωμών, αλλά και τα όρια της έννοιας της αμέλειας του χρήστη σε συνθήκες παραπλάνησης.

Η έρευνα συμπληρώνεται από περιορισμένη ποσοτική προσέγγιση μέσω ερωτηματολογίου, η οποία έχει επικουρικό και όχι αυτοτελή χαρακτήρα. Το ερωτηματολόγιο χρησιμοποιείται ως μέσο καταγραφής βασικών εμπειριών και αντιλήψεων των χρηστών σχετικά με τις ηλεκτρονικές πληρωμές και την έκθεσή τους σε απόπειρες phishing, χωρίς αξιώσεις στατιστικής γενίκευσης ή σύνθετης ανάλυσης δεδομένων. Μέσα από απλές ερωτήσεις διερευνάται ο βαθμός εξοικείωσης των καταναλωτών με το φαινόμενο, η αίσθηση ασφάλειας κατά τις συναλλαγές τους και το επίπεδο εμπιστοσύνης προς τους παρόχους. Η επεξεργασία των απαντήσεων γίνεται σε περιγραφικό επίπεδο και λειτουργεί υποστηρικτικά προς τη βιβλιογραφική και νομική ανάλυση, γεφυρώνοντας τη θεωρητική προσέγγιση με την καθημερινή εμπειρία των χρηστών. Με τον τρόπο αυτό, η μεθοδολογία της εργασίας διατηρεί τον βιβλιογραφικό της προσανατολισμό και εστιάζει στην ουσιαστική κατανόηση του phishing ως φαινομένου που επηρεάζει άμεσα την εμπιστοσύνη και την ασφάλεια στις ψηφιακές συναλλαγές.

4.4. Περιγραφή του δείγματος

Το ερωτηματολόγιο συμπληρώθηκε από τριάντα άτομα που χρησιμοποιούν ηλεκτρονικές πληρωμές και ηλεκτρονική τραπεζική στην καθημερινότητά τους. Πρόκειται για άνδρες και γυναίκες διαφορετικών ηλικιών και μορφωτικών επιπέδων, οι οποίοι, ανεξάρτητα από τον βαθμό εξοικείωσης, έχουν εντάξει τις ψηφιακές συναλλαγές στη ζωή τους. Το δείγμα δεν επιλέχθηκε με κριτήρια αντιπροσωπευτικότητας, αλλά με βάση την πρακτική δυνατότητα πρόσβασης στους συμμετέχοντες. Για τον λόγο αυτό, τα αποτελέσματα δεν αποσκοπούν σε

γενικεύσεις, αλλά λειτουργούν περισσότερο ως αποτύπωση εμπειριών και στάσεων ανθρώπων που έρχονται καθημερινά σε επαφή με ηλεκτρονικά μέσα πληρωμής.

Από τις απαντήσεις προκύπτει ότι οι ηλεκτρονικές πληρωμές χρησιμοποιούνται σε μεγάλο βαθμό και θεωρούνται πλέον κάτι αυτονόητο. Οι περισσότεροι συμμετέχοντες ανέφεραν ότι τις επιλέγουν για λόγους ευκολίας και ταχύτητας, χωρίς να σκέφτονται ιδιαίτερα τη διαδικασία. Παράλληλα, όμως, γίνεται αισθητό ότι αυτή η συχνή χρήση δεν συνοδεύεται πάντα από αίσθημα πλήρους ασφάλειας. Αν και οι ψηφιακές συναλλαγές έχουν ενσωματωθεί στην καθημερινότητα, αρκετοί χρήστες δείχνουν να διατηρούν επιφυλάξεις ως προς τους κινδύνους που μπορεί να προκύψουν, ιδιαίτερα σε ό,τι αφορά την πιθανότητα απάτης και την ικανότητά τους να την αναγνωρίσουν εγκαίρως.

4.5. Εμπειρία των καταναλωτών με περιστατικά phishing

Οι απαντήσεις των συμμετεχόντων δείχνουν ότι το phishing δεν αποτελεί ένα εντελώς άγνωστο ή θεωρητικό φαινόμενο. Οι περισσότεροι ανέφεραν ότι έχουν έρθει, με τον έναν ή τον άλλον τρόπο, σε επαφή με απόπειρες ηλεκτρονικής απάτης, ακόμη κι αν δεν υπήρξαν οι ίδιοι θύματα. Μηνύματα ηλεκτρονικού ταχυδρομείου, ειδοποιήσεις στο κινητό ή επικοινωνίες που εμφανίζονταν να προέρχονται από τράπεζες ή γνωστές εταιρείες αναφέρθηκαν ως συχνές εμπειρίες. Σε αρκετές περιπτώσεις, οι συμμετέχοντες δήλωσαν ότι αντιλήφθηκαν την απάτη εγκαίρως και δεν προχώρησαν σε κάποια ενέργεια, γεγονός που δείχνει μια βασική, έστω και εμπειρική, εξοικείωση με το φαινόμενο.

Παράλληλα, καταγράφεται και μια αίσθηση αβεβαιότητας. Ορισμένοι συμμετέχοντες ανέφεραν ότι, αν και υποψιάστηκαν πως επρόκειτο για απάτη, δεν ήταν απόλυτα βέβαιοι τη στιγμή που έλαβαν το μήνυμα. Η αμφιβολία αυτή συνδέεται κυρίως με το γεγονός ότι οι επικοινωνίες εμφανίζονταν ιδιαίτερα πειστικές και προσαρμοσμένες στην καθημερινή τραπεζική πρακτική. Το στοιχείο αυτό αναδεικνύει ότι το phishing δεν βασίζεται μόνο σε τεχνικά τεχνάσματα, αλλά κυρίως στη δημιουργία σύγχυσης και πίεσης στον χρήστη, ο οποίος καλείται να αντιδράσει γρήγορα μέσα σε ένα ήδη φορτωμένο ψηφιακό περιβάλλον.

4.6. Επίπεδο ενημέρωσης και αίσθημα ασφάλειας των καταναλωτών/εμπιστοσύνης προς τις τράπεζες

Οι απαντήσεις των συμμετεχόντων δείχνουν ότι η εμπιστοσύνη προς τις τράπεζες σε περιπτώσεις απάτης δεν είναι ούτε δεδομένη ούτε απόλυτη. Οι περισσότεροι δηλώνουν ότι, σε ένα πρώτο επίπεδο, θεωρούν πως οι τράπεζες διαθέτουν τα μέσα και την τεχνογνωσία για να διαχειριστούν περιστατικά phishing και να προστατεύσουν τους πελάτες τους. Η αντίληψη αυτή φαίνεται να στηρίζεται κυρίως στην εικόνα των τραπεζών ως οργανωμένων και τεχνολογικά προηγμένων φορέων, οι οποίοι ελέγχουν τη ροή των συναλλαγών και διαθέτουν μηχανισμούς ασφαλείας. Παρ' όλα αυτά, η εμπιστοσύνη αυτή συνοδεύεται συχνά από επιφυλάξεις, ιδίως ως προς το αν η ευθύνη αποκαθίσταται πράγματι στην πράξη ή αν τελικά μετακυλιέται, έστω έμμεσα, στον ίδιο τον καταναλωτή. Ιδιαίτερο ενδιαφέρον παρουσιάζει το γεγονός ότι αρκετοί συμμετέχοντες εκφράζουν αβεβαιότητα για το τι θα συνέβαινε σε περίπτωση που έπεφταν θύματα phishing. Παρότι γνωρίζουν ότι υφίσταται νομικό πλαίσιο προστασίας, δεν είναι πάντοτε σαφές αν πιστεύουν ότι αυτό λειτουργεί αποτελεσματικά ή αν απαιτείται προσωπική επιμονή και διεκδίκηση για την αποκατάσταση της ζημίας. Η αίσθηση αυτή δημιουργεί ένα υπόβαθρο ανασφάλειας, στο οποίο ο καταναλωτής, ενώ χρησιμοποιεί καθημερινά τις ψηφιακές υπηρεσίες, δεν είναι βέβαιος ότι θα τύχει ουσιαστικής στήριξης αν κάτι πάει στραβά.

Τέλος, η εικόνα που προκύπτει είναι αυτή μιας «συγκρατημένης εμπιστοσύνης». Οι χρήστες δεν απορρίπτουν τον ρόλο των τραπεζών ως φορέων προστασίας, ωστόσο δεν αισθάνονται πλήρως θωρακισμένοι. Η στάση αυτή αναδεικνύει ότι η ασφάλεια στις ηλεκτρονικές πληρωμές δεν αφορά μόνο την ύπαρξη τεχνικών ή νομικών μηχανισμών, αλλά και το κατά πόσο αυτοί γίνονται αντιληπτοί ως προσβάσιμοι, δίκαιοι και αποτελεσματικοί από τον ίδιο τον καταναλωτή.

4.7. Παρατηρήσεις από την εμπειρική έρευνα

Από τη συνολική εικόνα που προκύπτει από το ερωτηματολόγιο, γίνεται φανερό ότι οι ηλεκτρονικές πληρωμές αποτελούν πλέον κομμάτι της καθημερινότητας των καταναλωτών, χωρίς όμως αυτό να σημαίνει ότι συνοδεύονται από αίσθημα απόλυτης ασφάλειας. Οι

περισσότεροι συμμετέχοντες χρησιμοποιούν συστηματικά ψηφιακές τραπεζικές υπηρεσίες και κινούνται με σχετική άνεση στο ηλεκτρονικό περιβάλλον, ωστόσο η γνώση τους γύρω από το phishing και τις πρακτικές του παραμένει συχνά αποσπασματική. Το φαινόμενο αναγνωρίζεται ως υπαρκτός κίνδυνος, αλλά σε αρκετές περιπτώσεις αντιμετωπίζεται περισσότερο ως κάτι θεωρητικό ή μακρινό, παρά ως απειλή που μπορεί να αφορά άμεσα τον ίδιο τον χρήστη. Ταυτόχρονα, αναδεικνύεται μια εμφανής απόσταση ανάμεσα στη νομική προστασία που προβλέπεται τυπικά και στην αίσθηση προστασίας που βιώνουν οι καταναλωτές στην πράξη. Παρότι γνωρίζουν ότι υπάρχουν κανόνες που ρυθμίζουν τις μη εγκεκριμένες συναλλαγές και ότι οι τράπεζες φέρουν συγκεκριμένες υποχρεώσεις, πολλοί δεν αισθάνονται βέβαιοι ότι σε περίπτωση απάτης η αποκατάσταση της ζημίας θα είναι άμεση ή αυτονόητη. Η αβεβαιότητα αυτή φαίνεται να συνδέεται με τη δυσκολία κατανόησης των διαδικασιών, αλλά και με τον φόβο ότι η ευθύνη μπορεί τελικά να μετακυλιστεί στον ίδιο τον χρήστη. Με αυτή την έννοια, τα ευρήματα της έρευνας έρχονται να επιβεβαιώσουν ότι το phishing δεν αποτελεί μόνο νομικό ή τεχνικό πρόβλημα, αλλά ζήτημα εμπιστοσύνης και αίσθησης ασφάλειας μέσα στο σύγχρονο ψηφιακό περιβάλλον.

Κεφάλαιο 5: Συμπεράσματα-προτάσεις

Η εργασία αυτή ανέδειξε ότι το phishing δεν είναι απλώς ένα τεχνικό ζήτημα, αλλά μια σύνθετη και διαρκώς μεταβαλλόμενη απειλή για την ασφάλεια των ηλεκτρονικών πληρωμών, με σοβαρό αντίκτυπο τόσο για τους ίδιους τους καταναλωτές όσο και για τη σταθερότητα του τραπεζικού συστήματος συνολικά. Μέσα από την ανάλυση φάνηκε καθαρά ότι, παρά τα μεγάλα βήματα στην τεχνολογία και τη θωράκιση των συστημάτων, οι επιθέσεις αυτές παραμένουν αποτελεσματικές κυρίως επειδή στοχεύουν στον ίδιο τον άνθρωπο και όχι αποκλειστικά σε τεχνικά κενά ασφαλείας. Έχει ιδιαίτερη σημασία το πώς η τρέχουσα νομοθεσία όπως εκφράζεται μέσα από την Οδηγία PSD2 και την ενσωμάτωσή της στα καθ' ημάς, προσπαθεί να βρει μια χρυσή τομή ανάμεσα στην προστασία του χρήστη και την εύρυθμη λειτουργία των τραπεζών. Ωστόσο, η μελέτη της θεωρίας και της νομολογίας δείχνει ότι η εφαρμογή αυτών των κανόνων στην πράξη συχνά στερείται ομοιομορφίας, ειδικά όταν πρόκειται να ερμηνευτούν έννοιες όπως η «βαριά αμέλεια» του χρήστη ή το τι συνιστά τελικά μια «μη εγκεκριμένη πράξη πληρωμής». Ένα από τα βασικά συμπεράσματα της εργασίας είναι ότι η χρήση μηχανισμών ισχυρής ταυτοποίησης δεν αποτελεί από μόνη της «συγχωροχάρτι» για τις τράπεζες ώστε να απαλλαγούν από την ευθύνη αποζημίωσης, αν δεν αποδεικνύεται ότι

ο καταναλωτής έδρασε με πραγματική και συνειδητή βούληση. Παράλληλα, έγινε φανερό ότι η έλλειψη σωστής ενημέρωσης και εκπαίδευσης των χρηστών αφήνει περιθώρια για τέτοιους είδους απάτες, κλονίζοντας τελικά την εμπιστοσύνη στις ψηφιακές συναλλαγές. Συμπερασματικά, το phishing δεν είναι ένα απομονωμένο πρόβλημα· είναι ένα πολυπαραγοντικό φαινόμενο όπου συμπλέκονται το δίκαιο, η τεχνολογία και η ανθρώπινη συμπεριφορά.

Η αντιμετώπιση των κινδύνων που συνδέονται με τις ηλεκτρονικές πληρωμές και ιδίως με τις επιθέσεις phishing απαιτεί μια πολυεπίπεδη προσέγγιση, η οποία να συνδυάζει τεχνικά, θεσμικά και εκπαιδευτικά μέτρα. Η διεθνής εμπειρία καταδεικνύει ότι η ενίσχυση της κυβερνοασφάλειας δεν μπορεί να βασίζεται αποκλειστικά στην τεχνολογική θωράκιση των συστημάτων, αλλά προϋποθέτει την ενεργό συμμετοχή και επαρκή εκπαίδευση των ίδιων των χρηστών. Σε πρακτικό επίπεδο, κρίνεται αναγκαία η συστηματικότερη επένδυση των παρόχων υπηρεσιών πληρωμών σε προγράμματα ενημέρωσης των καταναλωτών, τα οποία να υπερβαίνουν τη γενική και συχνά δυσνόητη πληροφόρηση μέσω τυποποιημένων όρων χρήσης. Η παροχή στοχευμένων ειδοποιήσεων για νέες μορφές απάτης, η χρήση απλών και κατανοητών παραδειγμάτων, καθώς και η προσομοίωση πραγματικών σεναρίων εξαπάτησης μπορούν να συμβάλουν ουσιαστικά στην πρόληψη. Ιδιαίτερη σημασία έχει η προσαρμογή της ενημέρωσης στο επίπεδο ψηφιακής επάρκειας των χρηστών, ώστε να αποφεύγεται η μετακύλιση δυσανάλογων ευθυνών σε πρόσωπα που δεν διαθέτουν εξειδικευμένες τεχνικές γνώσεις. Παράλληλα, σε θεσμικό επίπεδο, προβάλλει ως αναγκαία η περαιτέρω εξειδίκευση των κριτηρίων βάσει των οποίων θεμελιώνεται η έννοια της βαριάς αμέλειας του χρήστη. Η έλλειψη σαφών και αντικειμενικών ορίων δημιουργεί ανασφάλεια δικαίου και οδηγεί συχνά σε αντιφατικές ερμηνείες, ιδίως σε περιπτώσεις phishing όπου η εξαπάτηση στηρίζεται σε τεχνικές κοινωνικής μηχανικής. Μια πιο σαφής κανονιστική ή νομολογιακή προσέγγιση θα μπορούσε να ενισχύσει την προστασία των καταναλωτών, χωρίς να αποδυναμώνει την ανάγκη υπεύθυνης συμπεριφοράς εκ μέρους τους.

Τέλος, ιδιαίτερη βαρύτητα θα πρέπει να δοθεί στη μακροπρόθεσμη ψηφιακή εκπαίδευση, ήδη από το σχολικό περιβάλλον. Η καλλιέργεια βασικών δεξιοτήτων κυβερνοασφάλειας και κριτικής αξιολόγησης ψηφιακών πληροφοριών συμβάλλει στη διαμόρφωση μιας κουλτούρας πρόληψης και εγρήγορσης. Η συνδυαστική εφαρμογή εκπαίδευσης, θεσμικής σαφήνειας και τεχνικών μέτρων μπορεί να αποτελέσει τη βάση για ένα πιο αποτελεσματικό και δίκαιο πλαίσιο προστασίας των χρηστών στο διαρκώς εξελισσόμενο ψηφιακό περιβάλλον.

Ξενόγλωσση Βιβλιογραφία και Αρθρογραφία

Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I. (2021) ‘Phishing attacks: A recent comprehensive study and a new anatomy’, *Frontiers in Computer Science*, 3, 563060.

Alsharnouby, M., Alaca, F. and Chiasson, S. (2015) ‘Why phishing still works: User strategies for combating phishing attacks’, *International Journal of Human-Computer Studies*, 82, pp. 69-82.

Barudi (2024) σε Müller-Terpitz/Köhler (επιμ.) *Digital Services Act, Gesetz über digitale Dienste*, υπό το άρθρο 3, αρ. 36, 38.

CJEU (2016) *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, Judgment of 19 October 2016.

Cole, E. (2012) *Advanced Persistent Threat*. Amsterdam: Elsevier.

De Graaf, K. de and Veldt, D. van der (2022) ‘The AI Act and Its Impact on Product Safety, Contracts and Liability’, *European Review of Private Law (EurRPrL)*, σσ. 803–808.

Dhamija, R., Tygar, J.D. and Hearst, M. (2006) ‘Why phishing works’, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 581–590.

Dixon, M. (2013) ‘Phishing and fraud in financial services’, *Journal of Financial Crime*, 20(4), pp. 415–428.

Durovic, M. and Lech, F. (2021) ‘A Consumer Law Perspective on the Commercialization of Data’, *European Review of Private Law (EurRevPrL)*, σσ. 701 επ.

EAT (2022) *Fraud reporting under PSD2*. Paris: Ευρωπαϊκή Αρχή Τραπεζών (European Banking Authority).

EBA (2022) *Fraud statistics on payment services*. Paris: European Banking Authority.

EDPB (2020) *Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR*. European Data Protection Board.

ENISA (2023) *Phishing: Threat Landscape*. Heraklion: European Union Agency for Cybersecurity.

European Banking Authority - EBA (2022) *Fraud reporting under PSD2*. Paris: EBA.

European Commission (2020) *A digital finance strategy for the EU*. COM(2020) 591 final.

European Union (2015) *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2)*. Official Journal of the European Union, L 337.

European Union (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR)*. Official Journal of the European Union, L 119.

European Commission (2018) *Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication*. Official Journal of the European Union, L 69.

Europol (2022) *Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: Europol.

Fabrizio, D. (2021) ‘Strong Customer Authentication in Online Payments under GDPR and PSD2: A Case of Cumulative Application’, in Friedewald, M. et al. (eds.) *Privacy and Identity 2020*. IFIP Advances in Information and Communication Technology, 619, pp. 1–18. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-030-72465-8_5

Furnell, S. (2006) *Cybercrime: Vandalizing the Information Society*. Harlow: Addison-Wesley.

Germannos, G. and Georgiou, N. (2021) *Κυβερνοέγκλημα: Πρόληψη-Διερεύνηση-Αντιμετώπιση*. Αθήνα.

Gupta, B.B. et al. (2018) ‘Smishing attacks: Detection and prevention’, *Journal of Information Security and Applications*, 42, pp. 1–12.

Hofmann, F. and Raue, B. (eds.) (2023) *Digital Services Act: Gesetz über digitale Dienste*. Baden-Baden: Nomos.

Husovec, M. (2024) *Principles of the Digital Services Act*. Oxford: Oxford University Press.

Hyde-Cartwright, R. (2023) ‘Exploring Consumer Detriment in Immersive Gaming Technologies’, *Journal of Consumer Policy*, 46, pp. 335–356

Jakobsson, M. and Myers, S. (2007) *Phishing and Countermeasures*. Hoboken: Wiley.

Jansen, J. and Leukfeldt, R. (2016) ‘Phishing and malware attacks on online banking customers’, *Crime Science*, 5(1).

Jougleux, P. (2016) *Cybercrime and financial fraud*. Paris.

Kitten, T. (2012) *Why phishing still works*. Information Security Media Group.

Koolen, C. (2023) ‘Consumer Protection in the Age of Artificial Intelligence: Breaking Down the Silo Mentality Between Consumer, Competition and Data’, *European Review of Private Law*, (2–3), pp. 427–468.

Köhler, C. (2024) σε Müller-Terpitz, R. και Köhler, C. (επιμ.) *Digital Services Act: Gesetz über digitale Dienste*. Baden-Baden: Nomos.

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> (Ημερομηνία πρόσβασης: 10 Δεκεμβρίου 2025).

Mell, P., Kent, K. and Nusbaum, J. (2005) *Guide to Malware Incident Prevention and Handling*. Gaithersburg: NIST.

OECD (2023) *Supporting informed and safe use of digital payments through digital financial literacy*. Paris: OECD Publishing.

Papadopoulos, M. (2005) *Phishing: Η νέα μέθοδος εξαπάτησης στο Διαδίκτυο*. Πρακτικά 3ου Πανελληνίου Συνεδρίου Ηλεκτρονικού Εγκλήματος.

Rashid, A. (2012) ‘Human factors in phishing attacks’, *IEEE Security and Privacy*.

Utakrit, N. (2012) *User awareness of phishing threats in online banking*. PhD Thesis. Curtin University.

Volmar, C. and Helmdach, A. (2018) ‘Protecting consumers and their data through competition law? Rethinking abuse of dominance in light of the Federal Cartel Office’s Facebook investigation’, *European Competition Journal*, 14(2–3), pp. 195–215.

Wilman, F., Kalèda, S. and Loewenthal, P. (eds.) (2024) *The EU Digital Services Act: A Commentary*. Oxford: Oxford University Press.

Yeboah-Boateng, E.O. and Amanor, P.M. (2014) ‘Phishing, SMiShing and Vishing: An assessment of threats against mobile devices’, *Journal of Emerging Trends in Computing and Information Sciences*, 5(4), pp. 297–307. Available at: <http://www.cisjournal.org>

Ελληνόγλωσση Βιβλιογραφία και Αρθρογραφία

Αλεξανδρίδου, Ελ. και Απαλαγάκη, Χ. (2023) σε Αλεξανδρίδου, Ελ. (επιμ.) *Το νέο δίκαιο προστασίας του Καταναλωτή*, 4η έκδ., άρθρα 10α επ., σσ. 819 επ. και 833 επ.

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

Βλαχόπουλος, Π. (2007) *Ηλεκτρονική απάτη και τραπεζικές συναλλαγές*. Διπλωματική εργασία.

Γιαννόπουλος, Γ. (2003) *Internet Banking: Νομικά ζητήματα από τη διεξαγωγή τραπεζικών συναλλαγών στο διαδίκτυο*. Αθήνα: Ελληνική Ένωση Τραπεζών.

Δέλλιος, Γ. (2013) *Γενικοί Όροι Συναλλαγών*. 2η έκδ. Αθήνα: Εκδόσεις Σάκκουλα.

Δελούκα-Ιγγλέση, Κ. (2023) σε Αλεξανδρίδου, Ελ. (επιμ.) *Το Νέο Δίκαιο της προστασίας του καταναλωτή*. Ν.Β., αρ. 9, 9α–9θ Ν 2251/1994.

Δούβλης, Β. και Μώλος, Α. (2008) *Δίκαιο προστασίας καταναλωτών*, τόμ. 1. Αθήνα: Εκδόσεις Σάκκουλα.

ΕΚΠΟΙΖΩ (2023) *Αναποτελεσματική η προστασία καταναλωτών από τις ηλεκτρονικές απάτες στο νομοσχέδιο προς συζήτηση στη Βουλή*. Διαθέσιμο στο: <https://www.ekpizo.gr/oi-δράσεις-μας/χρηματοοικονομικά/αναποτελεσματική-η-προστασία-των-καταναλωτών-από-τις-ηλεκτρονικές> (Ημερομηνία πρόσβασης 15 Δεκεμβρίου 2025).

Ελληνική Συνομοσπονδία Εμπορίου και Επιχειρηματικότητας (ΕΣΕΕ) (2021) *Η Λευκή Βίβλος του Λιανικού Εμπορίου 2040*. Αθήνα.

Ιγγλεζάκης, Ι. (2008) *Δίκαιο της πληροφορικής*. 2η έκδ. Αθήνα: Εκδόσεις Σάκκουλα.

Ιγγλεζάκης, Ι. (2024) *Δίκαιο Πληροφορικής*. 5η έκδ. Αθήνα: Εκδόσεις Σάκκουλα.

Καραγκουνίδη, Α. και Λιναρίτη, Ι. (2023) σε Αλεξανδρίδου, Ελ. (επιμ.) *Το νέο δίκαιο προστασίας του καταναλωτή*, 4η έκδ. Αθήνα: Νομική Βιβλιοθήκη (άρθρο 13α)

Καράκωστας, Ι. (2009) *Δίκαιο και Internet: Νομικά ζητήματα του Διαδικτύου*. Αθήνα: Εκδόσεις Π.Ν. Σάκκουλας.

Μαργαρίτη, Ε. (2020) *Προσωπικά Δεδομένα και Προστασία Καταναλωτή*. Αθήνα: Νομική Βιβλιοθήκη.

Μεντής, Γ. (2020) *Γενικοί Όροι Συναλλαγών σε Καταναλωτικές και Εμπορικές Συμβάσεις*. Αθήνα: Εκδόσεις Π.Ν. Σάκκουλας.

Μήτσου, Α.-Ο. (2021) *Η προστασία του πληρωτή από την απατηλή χρήση των μέσων πληρωμής στις συναλλαγές του ηλεκτρονικού εμπορίου*, Δίκαιο Επιχειρήσεων και Εταιριών (ΔΕΕ), σελ. 606–619, διαθέσιμο στο ΤΝΠ Qualex.

Μικρουλέα (2023) *Ανταγωνισμός και ρύθμιση στην ψηφιακή οικονομία*. Αθήνα: Νομική Βιβλιοθήκη.

Τζίβα, Ε. (2021) *Εφαρμογές της ψηφιακής τεχνολογίας στις τραπεζικές συναλλαγές*, Δίκαιο Επιχειρήσεων και Εταιριών (ΔΕΕ), σελ. 316–325, διαθέσιμο στο ΤΝΠ Qualex.

Τράπεζα της Ελλάδος (2023) *Έκθεση Χρηματοπιστωτικής Σταθερότητας*. Αθήνα.

Τσιαφούτης, Β. (2021) σε Βενιέρης, Ι. και Βερβεσός, Ν. (επιμ.), *Δίκαιο Εμπορικών Συμβάσεων*. Αθήνα: Νομική Βιβλιοθήκη.

Υπουργείο Ψηφιακής Διακυβέρνησης (2023) *Ανακοίνωση Εθνικής Αρχής Κυβερνοασφάλειας για επιθέσεις phishing*.

ΠΑΡΑΡΤΗΜΑ

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΕΡΕΥΝΑΣ

1. Φύλο:
 - ☐ Άνδρας
 - ☐ Γυναίκα
 - ☐ Άλλο / Δεν επιθυμώ να απαντήσω
2. Ηλικιακή ομάδα:
 - ☐ 18–29
 - ☐ 30–39
 - ☐ 40–49
 - ☐ 50–59
 - ☐ 60+
3. Ανώτατο επίπεδο εκπαίδευσης:
 - ☐ Δευτεροβάθμια εκπαίδευση
 - ☐ Ανώτερη / Τεχνική εκπαίδευση
 - ☐ Ανώτατη εκπαίδευση (ΑΕΙ/ΤΕΙ)
 - ☐ Μεταπτυχιακές σπουδές
 - ☐ Διδακτορικό
4. Χρησιμοποιείτε ηλεκτρονικές πληρωμές (e-banking, κάρτες, mobile banking);
 - ☐ Ναι
 - ☐ Όχι
5. Πόσο συχνά χρησιμοποιείτε ηλεκτρονικές πληρωμές;
 - ☐ Καθημερινά
 - ☐ Πολλές φορές την εβδομάδα

- ☐ Περιστασιακά
 - ☐ Σπάνια
6. Ποιοι είναι οι βασικοί λόγοι χρήσης ηλεκτρονικών πληρωμών; (μπορείτε να επιλέξετε περισσότερα από ένα)
- ☐ Ευκολία
 - ☐ Ταχύτητα
 - ☐ Αποφυγή φυσικής παρουσίας
 - ☐ Συνήθεια
 - ☐ Άλλο:
7. Έχετε ακούσει τον όρο «phishing»;
- ☐ Ναι
 - ☐ Όχι
8. Πώς θα αξιολογούσατε το επίπεδο ενημέρωσής σας σχετικά με το phishing;
- ☐ Καθόλου
 - ☐ Λίγο
 - ☐ Μέτριο
 - ☐ Αρκετό
 - ☐ Πολύ καλό
9. Από ποιες πηγές έχετε ενημερωθεί για το phishing;
- ☐ Τράπεζες
 - ☐ Διαδίκτυο / ΜΜΕ
 - ☐ Κοινωνικά δίκτυα
 - ☐ Φίλους / γνωστούς
 - ☐ Δεν έχω ενημερωθεί
10. Έχετε λάβει ποτέ ύποπτο μήνυμα ή ειδοποίηση που να εμφανίζεται ως μήνυμα τράπεζας ή γνωστής εταιρείας;
- ☐ Ναι
 - ☐ Όχι

11. Αν ναι, πώς αντιδράσατε;
- ☐ Αγνόησα το μήνυμα
 - ☐ Υποψιάστηκα απάτη αλλά δεν ήμουν σίγουρος/η
 - ☐ Πάτησα τον σύνδεσμο
 - ☐ Εισήγαγα στοιχεία
 - ☐ Άλλο:
12. Έχετε πέσει ποτέ θύμα phishing;
- ☐ Ναι
 - ☐ Όχι
 - ☐ Δεν είμαι σίγουρος/η
13. Αν ναι, ενημερώσατε άμεσα την τράπεζα;
- ☐ Ναι
 - ☐ Όχι
 - ☐ Δεν εφαρμόζεται
14. Πόσο ασφαλής αισθάνεστε όταν πραγματοποιείτε ηλεκτρονικές πληρωμές;
- ☐ Καθόλου ασφαλής
 - ☐ Λίγο ασφαλής
 - ☐ Ούτε ασφαλής ούτε ανασφαλής
 - ☐ Αρκετά ασφαλής
 - ☐ Πολύ ασφαλής
15. Πιστεύετε ότι οι τράπεζες διαθέτουν επαρκή μέσα για την προστασία σας από περιστατικά phishing;
- ☐ Ναι
 - ☐ Όχι
 - ☐ Δεν γνωρίζω
16. Σε περίπτωση μη εγκεκριμένης συναλλαγής, θεωρείτε ότι η τράπεζα θα σας αποζημιώσει χωρίς δυσκολία;
- ☐ Ναι

☐ Όχι

☐ Δεν είμαι σίγουρος/η

17. Θεωρείτε ότι, σε περίπτωση απάτης, η ευθύνη μετακυλίεται τελικά στον καταναλωτή;

☐ Ναι

☐ Όχι

☐ Εν μέρει

18. Πιστεύετε ότι χρειάζεται περισσότερη ενημέρωση των καταναλωτών για το phishing;

☐ Ναι

☐ Όχι

19. Πιστεύετε ότι τα μέτρα ασφάλειας στις ηλεκτρονικές πληρωμές είναι επαρκή;

☐ Ναι

☐ Όχι

☐ Χρειάζονται βελτίωση

20. Θα αποφεύγατε τη χρήση ηλεκτρονικών πληρωμών λόγω φόβου απάτης;

☐ Ναι

☐ Όχι

☐ Ενδεχομένως