Ενημερωτικό δελτίο για τον ψηφιακό μετασχηματισμό

(1ο εξάμηνο 2026)

Έργο: «Κέντρο Καινοτομίας για το Λιανικό Εμπόριο» (κωδικός ΟΠΣ 6002934)

Υποέργο 1: «Σύγχρονες Υπηρεσίες προς τις ΠΜΕ & ΜΜΕ του Εμπορίου»

Πακέτο εργασίας ΠΕ 1.1: «Δράσεις Συστημικής Συμβολής»

Παραδοτέο Π.1.1.2: Ενημερωτικό δελτίο για τον ψηφιακό μετασχηματισμό (1ο εξάμηνο 2026)

Το παρόν ενημερωτικό δελτίο εκπονήθηκε στο πλαίσιο του υποέργου 1 «Σύγχρονες Υπηρεσίες προς τις ΠΜΕ & ΜΜΕ του Εμπορίου» της Πράξης: «Κέντρο Καινοτομίας για το Λιανικό Εμπόριο» (κωδικός ΟΠΣ 6002934), η οποία είναι ενταγμένη στο Πρόγραμμα «Ανταγωνιστικότητα 2021-2027» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (ΕΚΤ+) και από εθνικούς πόρους.

Ενημερωτικό δελτίο για τον ψηφιακό μετασχηματισμό

(1ο εξάμηνο 2026)

Ερευνητική & Συγγραφική ομάδα:

Μεραμβελιωτάκης Γεώργιος

Κεμαχλής Ιωάννης

Παππάς Ιωάννης

Παναγιωτοπούλου Μιλένα

Πλιάτσικας Βασίλειος

Επιμέλεια κειμένου:

Καρρά Μαριλένα

Copyright INEMY © 2026

Πετράκη 8
10563, Αθήνα
Τηλ: 210 3259170
E-mail: info@inemy.gr
URL: www.inemy.gr

Απαγορεύεται η με οποιονδήποτε τρόπο ανατύπωση ή μετάφραση όλου ή μέρους του κειμένου χωρίς την άδεια του εκδότη. Επίσης, η αναδημοσίευση (όλου ή μέρους του) χωρίς αναφορά της πηγής.

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2021-2027

ΠΡΟΓΡΑΜΜΑ ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ 2021 – 2027

Περιεχόμενα

1. Εισαγωγή 2

2. Το οικοσύστημα των ψηφιακών πληρωμών στο λιανικό εμπόριο 7

2.1 Από τη χρήση των μετρητών στις ψηφιακές συναλλαγές: τα στάδια της μετάβασης 7

2.2 Η τυπολογία των ψηφιακών μέσων πληρωμής 9

2.3 Ο ρόλος των ενδιάμεσων: πάροχοι αποδοχής συναλλαγών (acquirers), πάροχοι υπηρεσιών πληρωμών (payment processors) και fintech πλατφόρμες 15

2.4 Ευρωπαϊκά και ελληνικά δεδομένα διείσδυσης των ψηφιακών πληρωμών 17

3. Οι ψηφιακές πληρωμές ως ζήτημα δημόσιας πολιτικής 21

3.1 Το ευρωπαϊκό ρυθμιστικό πλαίσιο: Οδηγίες για τις Υπηρεσίες Πληρωμών (PSD1, PSD2, PSD3) και Κανονισμός για τις Άμεσες Πληρωμές (Instant Payments Regulation) 21

3.2 Ανταγωνιστικό έλλειμα στην αγορά πληρωμών 27

3.3 Ψηφιακό ευρώ: ευκαιρία ή νέα εξάρτηση; 31

3.4 Χρηματοοικονομικός αποκλεισμός και ψηφιακές πληρωμές 34

4. Κυβερνοασφάλεια και λιανικό εμπόριο: το νέο τοπίο των απειλών 38

4.1 Η κυβερνοασφάλεια ως δομικό χαρακτηριστικό της ψηφιακής αγοράς 38

4.2 Η τυπολογία των κυβερνοεπιθέσεων στο λιανικό εμπόριο 41

4.3 Το κόστος των κυβερνοεπιθέσεων 46

5. Το ευρωπαϊκό ρυθμιστικό πλαίσιο κυβερνοασφάλειας 50

5.1 NIS2, DORA και GDPR: υποχρεώσεις για το λιανικό εμπόριο 50

5.2 Το PCI DSS και η τυποποίηση της ασφάλειας των πληρωμών 55

5.3 Το κόστος της κανονιστικής συμμόρφωσης για τις μικρομεσαίες επιχειρήσεις 57

6. Οι μικρομεσαίες επιχειρήσεις του λιανικού εμπορίου απέναντι στις προκλήσεις της κυβερνοασφάλειας 62

6.1 Το «ψηφιακό χάσμα» στην κυβερνοασφάλεια 62

6.2 Εξάρτηση από τρίτους παρόχους και μεταφορά ρίσκου 64

6.3 Εμπιστοσύνη των καταναλωτών ως ανταγωνιστικό πλεονέκτημα 68

7. Συμπεράσματα 71

8. Βιβλιογραφία 75

1. Εισαγωγή

Ο ψηφιακός μετασχηματισμός του λιανικού εμπορίου δεν εξαντλείται και δεν περιορίζεται στην αναδιάρθρωση των καναλιών διανομής και στη διεύρυνση της ηλεκτρονικής κατανάλωσης, αλλά, ταυτόχρονα, επαναπροσδιορίζει, θεμελιακά, την ίδια την υποδομή των εμπορικών συναλλαγών, δηλαδή τον τρόπο με τον οποίον διακινείται και επαληθεύεται η αξία μεταξύ αγοραστή και πωλητή. Η ψηφιοποίηση των πληρωμών αποτελεί, υπό αυτήν την έννοια, έναν από τους πλέον ορατούς και άμεσους τρόπους, με τους οποίους ο ψηφιακός μετασχηματισμός διεισδύει στην τυπική, καθημερινή εμπορική πράξη, μετασχηματίζοντας τους όρους της συναλλαγής, τους ενδιάμεσους που αυτή προϋποθέτει, τη ροή της πληροφορίας που παράγει και τον βαθμό ελέγχου που ασκεί κάθε εμπλεκόμενο υποκείμενο επί της διαδικασίας αυτής.

Τούτων δοθέντων, η σταδιακή μετάβαση από την αποκλειστική χρήση των μετρητών στις ψηφιακές πληρωμές δεν μπορεί να νοηθεί ως μια απλή τεχνολογική αναβάθμιση, αλλά θα πρέπει να εκληφθεί και, ως εκ τούτου, να αναλυθεί ως μια, δομικού τύπου, αναδιάρθρωση του πλέγματος των σχέσεων μεταξύ εμπόρων, καταναλωτών και χρηματοπιστωτικών υποδομών. Το περιεχόμενο της ψηφιακής συναλλαγής υπερβαίνει, κατά πολύ, την αυτονόητη λειτουργία της ως μηχανισμού ανταλλαγής αξίας. Αποτελεί, ταυτόχρονα, ένα γεγονός πλούσιο σε δεδομένα, δεδομένου ότι κάθε συναλλαγή παράγει και αποτυπώνει ένα σύνολο πληροφοριών, τα οποία αφορούν την ταυτότητα του αγοραστή, τη χρονική στιγμή της πραγματοποίησης της αγοράς, το περιεχόμενο του καταναλωτικού καλαθιού και τις επιμέρους επιλογές του, τη γεωγραφική διάσταση της συναλλαγής, καθώς και τον τύπο του μέσου πληρωμής που χρησιμοποιείται. Κατ' αυτόν τον τρόπο, η πληρωμή μετατρέπεται από μια απλή πράξη ολοκλήρωσης της εμπορικής ανταλλαγής σε έναν κρίσιμο μηχανισμό παραγωγής, συλλογής και αξιοποίησης δεδομένων, ενισχύοντας τη σημασία της πληροφορίας ως στρατηγικού πόρου στη λειτουργία του σύγχρονου λιανικού εμπορίου. Επομένως, οι ψηφιακές πληρωμές δεν είναι απλώς μηχανισμοί διευκόλυνσης της συναλλαγής, αλλά υποδομές παραγωγής και συγκέντρωσης δεδομένων, με άμεσες επιπτώσεις στη δομή της αγοράς, στις σχέσεις ισχύος μεταξύ των εμπλεκόμενων φορέων και στις δυνατότητες εποπτείας και ρύθμισης.

Η ταχεία διείσδυση των ψηφιακών πληρωμών στο λιανικό εμπόριο δεν συντελείται σε ένα ουδέτερο και απαλλαγμένο από κινδύνους θεσμικό και τεχνολογικό πεδίο.

Αντιθέτως, εξελίσσεται παράλληλα με την ανάδυση νέων και ολοένα πιο σύνθετων μορφών κυβερνοαπειλών, οι οποίες στρέφονται ακριβώς εκεί όπου συσσωρεύεται η οικονομική αξία και η κρίσιμη πληροφορία, ήτοι στα συστήματα πληρωμών, στις ψηφιακές υποδομές των επιχειρήσεων, στα δεδομένα των καταναλωτών και στις αλυσίδες εφοδιασμού των καταστημάτων λιανικής. Υπό αυτές τις συνθήκες, η κυβερνοασφάλεια παύει να αποτελεί ένα αμιγώς τεχνικό ζήτημα, περιορισμένο στην αρμοδιότητα των εξειδικευμένων τμημάτων Πληροφορικής. Αναδεικνύεται σε στρατηγική διάσταση της επιχειρηματικής λειτουργίας, με άμεσες οικονομικές, ανταγωνιστικές και θεσμικές προεκτάσεις. Η ικανότητα μιας επιχείρησης να διασφαλίζει την ακεραιότητα των συναλλαγών, την προστασία των δεδομένων και την ομαλή διεκπεραίωση των ψηφιακών λειτουργιών της καθίσταται, πλέον, βασική προϋπόθεση για τη διατήρηση της εμπιστοσύνης των καταναλωτών, για την ανθεκτικότητα και τη μακροπρόθεσμη ανταγωνιστικότητά της.

Στο πλαίσιο αυτό, το παρόν δελτίο επιχειρεί να χαρτογραφήσει και να αναλύσει, με τρόπο συστηματικό, δύο αλληλένδετες διαστάσεις του ψηφιακού μετασχηματισμού που συντελείται στο λιανικό εμπόριο, καταρχάς, τις ψηφιακές πληρωμές, ως δομικό χαρακτηριστικό του σύγχρονου εμπορικού οικοσυστήματος και, εν συνεχεία, την κυβερνοασφάλεια, ως αναγκαία προϋπόθεση για τη διασφάλιση της ψηφιακής εμπιστοσύνης και της ασφάλειας των συναλλαγών. Τα δύο αυτά πεδία δεν προσεγγίζονται ως αυτοτελή και αποκλειστικά τεχνολογικά ζητήματα, αλλά ως αλληλένδετες συνιστώσες ενός ευρύτερου μετασχηματισμού, ο οποίος αναδιαμορφώνει, σε βάθος, τη δομή και τη λειτουργία της λιανικής αγοράς.

Αυτός ο, εν εξελίξει, μετασχηματισμός δεν επηρεάζει μόνο τους τρόπους και τις διαδικασίες, μέσω των οποίων πραγματοποιούνται οι συναλλαγές, αλλά αναδιατάσσει ευρύτερα τις σχέσεις ισχύος μεταξύ επιχειρήσεων, καταναλωτών, τραπεζικών και τεχνολογικών υποκειμένων. Ταυτόχρονα, δημιουργεί νέες προκλήσεις για τις μικρομεσαίες επιχειρήσεις, οι οποίες καλούνται να προσαρμοστούν σε ένα πιο σύνθετο και δυσνόητο ψηφιακό περιβάλλον, ενώ, την ίδια στιγμή, καθιστά αναγκαίους παράγοντες τον σχεδιασμό και τη θεσμοθέτηση νέων και αποτελεσματικότερων ρυθμιστικών παρεμβάσεων, σε εθνικό και ευρωπαϊκό επίπεδο.

Η ανάλυση που ακολουθεί αποσκοπεί, αρχικά, στην αποτύπωση της δομής και της δυναμικής του οικοσυστήματος των ψηφιακών πληρωμών, αναδεικνύοντας τα στάδια της ιστορικής του εξέλιξης, την τυπολογία των διαθέσιμων μέσων και τους

μηχανισμούς συγκέντρωσης ισχύος που αναπτύσσονται στο εσωτερικό του. Στη συνέχεια, εξετάζεται το ευρωπαϊκό ρυθμιστικό πλαίσιο, το οποίο διέπει τόσο τις ψηφιακές πληρωμές όσο και την κυβερνοασφάλεια, αναλύοντας την επάρκεια, τα κενά και τις ανισορροπίες που εντοπίζονται σε σχέση με τις πραγματικές ανάγκες των επιχειρήσεων λιανικής, και ιδίως των μικρομεσαίων. Ακολούθως, αναλύεται η σύγχρονη τοπογραφία των κυβερνοαπειλών, με έμφαση στους τύπους επιθέσεων που στοχεύουν τις υποδομές πληρωμών και τις επιχειρηματικές οντότητες του λιανικού εμπορίου, καθώς και το οικονομικό και επιχειρησιακό κόστος που αυτές συνεπάγονται. Ιδιαίτερη βαρύτητα δίνεται στην κατάσταση των μικρομεσαίων επιχειρήσεων, οι οποίες, παρά τη, συχνά, μεγαλύτερη έκθεσή τους σε κινδύνους, διαθέτουν σημαντικά περιορισμένους πόρους ψηφιακής ανθεκτικότητας. Τέλος, το δελτίο ανοίγει τη συζήτηση για τον σχεδιασμό ενός εναλλακτικού υποδείγματος ψηφιακής συναλλακτικής ασφάλειας, το οποίο θα εντάσσει την κυβερνοασφάλεια όχι ως κόστος συμμόρφωσης, αλλά ως συστατικό της επιχειρηματικής αξίας και της δημόσιας εμπιστοσύνης.

Η πραγμάτευση του συγκεκριμένου ζητήματος αποκτά ιδιαίτερη βαρύτητα στο πλαίσιο της ελληνικής οικονομίας, όπου το λιανικό εμπόριο συγκροτείται στην πλειοψηφική βάση των μικρών και πολύ μικρών επιχειρήσεων, οι οποίες διαθέτουν περιορισμένους οικονομικούς, οργανωτικούς και τεχνολογικούς πόρους για την υλοποίηση ενός ολοκληρωμένου ψηφιακού μετασχηματισμού. Παράλληλα, στην Ελλάδα, καταγράφεται ιστορικά υψηλή χρήση μετρητών, σε σχέση με τον ευρωπαϊκό μέσο όρο, γεγονός που καθιστά την ταχεία μετάβαση προς τις ηλεκτρονικές και ψηφιακές πληρωμές έναν ιδιαίτερα σημαντικό μετασχηματισμό για τη δομή και τη λειτουργία της αγοράς.

Η μετάβαση στις ολοκληρωμένες ψηφιακές πληρωμένες διευκολύνεται και, ταυτόχρονα, επιταχύνεται από ένα ευρύτερο πλέγμα ευρωπαϊκών και εθνικών πολιτικών, από τη διευρυμένη εγκατάσταση και χρήση τερματικών POS, καθώς και από την υποχρεωτική αποδοχή ηλεκτρονικών μέσων πληρωμής σε ολοένα και περισσότερες κατηγορίες οικονομικής δραστηριότητας. Ωστόσο, η ταχεία ενσωμάτωση των επιχειρήσεων στο ψηφιακό οικοσύστημα πληρωμών δεν συνοδεύεται πάντα από την αντίστοιχη ενίσχυση των μηχανισμών κυβερνοπροστασίας και της ψηφιακής τους ανθεκτικότητας. Ως εκ τούτου, οι μικρομεσαίες επιχειρήσεις του ελληνικού λιανικού εμπορίου καλούνται να προσαρμοστούν σε ένα ψηφιακό και

κανονιστικό περιβάλλον, το οποίο διέπεται, εν πολλοίς, από περιορισμένους πόρους, ασύμμετρη διαπραγματευτική ισχύ έναντι των μεγάλων τεχνολογικών και χρηματοπιστωτικών φορέων, όπως και από την αυξανόμενη έκθεση στους ποικίλους κινδύνους που φέρουν οι κυβερνοαπειλές.

Ταυτόχρονα, η ΕΕ βρίσκεται σε μια κρίσιμη φάση αναμόρφωσης του κανονιστικού πλαισίου που διέπει τις υπηρεσίες πληρωμών και την ψηφιακή ασφάλεια. Ειδικότερα, η αναθεώρηση του πλαισίου για τις υπηρεσίες πληρωμών, μέσω της PSD3, σε συνδυασμό με τον Κανονισμό για τις Άμεσες Πληρωμές (Instant Payments Regulation) μεταβάλλουν σταδιακά τους όρους λειτουργίας και πρόσβασης στο οικοσύστημα των πληρωμών, ενισχύοντας, παράλληλα, την ασφάλεια, την ταχύτητα και τη διαλειτουργικότητα των συναλλαγών. Την ίδια στιγμή, η Οδηγία NIS2 και ο Κανονισμός DORA συγκροτούν το ευρωπαϊκό θεσμικό πλαίσιο για την κυβερνοασφάλεια και την ψηφιακή επιχειρησιακή ανθεκτικότητα, διευρύνοντας τις πολιτικές διαχείρισης κινδύνων και προστασίας των ψηφιακών υποδομών σε ένα ευρύτερο φάσμα οικονομικών δραστηριοτήτων. Επιπλέον, η προοπτική του ψηφιακού ευρώ ανοίγει μια νέα συζήτηση, σχετικά με τη μελλοντική αρχιτεκτονική των ευρωπαϊκών υποδομών για τις ψηφιακές πληρωμές και, κατ' επέκταση, αναφορικά με τον ρόλο, τις δυνατότητες και τις προσαρμογές που θα απαιτηθούν από τις επιχειρήσεις λιανικής σε αυτό το, υπό διαμόρφωση, νέο περιβάλλον.

Ως εκ τούτου, το παρόν δελτίο φιλοδοξεί να συμβάλει σε μια τεκμηριωμένη, συστηματική και κριτικά προσανατολισμένη προσέγγιση των ψηφιακών πληρωμών και της κυβερνοασφάλειας, ως κρίσιμων ζητημάτων δημόσιας πολιτικής, όσον αφορά το ελληνικό λιανικό εμπόριο. Η ανάλυση δεν περιορίζεται στην καταγραφή των τεχνολογικών εξελίξεων, ούτε στην απλή αποτύπωση των, διαρκώς, μεταβαλλόμενων κανονιστικών απαιτήσεων. Επιδιώκει, αντίθετα, να εξετάσει τις ευρύτερες οικονομικές, θεσμικές και επιχειρηματικές επιπτώσεις του ψηφιακού μετασχηματισμού, αναδεικνύοντας τις δομικές ανισορροπίες και τις ασυμμετρίες ισχύος, οι οποίες διαμορφώνονται στο σύγχρονο οικοσύστημα ψηφιακών πληρωμών. Επιπρόσθετα, το παρόν δελτίο επιχειρεί να αξιολογήσει την επάρκεια και την αποτελεσματικότητα των ήδη ισχυόντων θεσμικών και ρυθμιστικών εργαλείων, δίνοντας αναλυτική προτεραιότητα στις προκλήσεις που αντιμετωπίζουν οι μικρομεσαίες επιχειρήσεις. Στόχο συνιστά η συμβολή στη συζήτηση για τη διαμόρφωση ενός συνεκτικού πλαισίου δημόσιας πολιτικής, το οποίο δεν θα

αντιμετωπίζει την ψηφιοποίηση ως αυτοσκοπό, αλλά θα επιδιώκει να διασφαλίσει την ψηφιακή ανθεκτικότητα και ανταγωνιστικότητα του λιανικού εμπορίου, την ισότιμη πρόσβαση των επιχειρήσεων στις νέες υποδομές και στις σύγχρονες τεχνολογίες, την αποτελεσματική προστασία των καταναλωτών και, ευρύτερα, τη διαμόρφωση μιας συμπεριληπτικής και βιώσιμης ψηφιακής ανάπτυξης.

2. Το οικοσύστημα των ψηφιακών πληρωμών στο λιανικό εμπόριο

2.1 Από τη χρήση των μετρητών στις ψηφιακές συναλλαγές: τα στάδια της μετάβασης

Η ιστορία των μέσων πληρωμής στο λιανικό εμπόριο είναι, κατά βάθος, η ιστορία της σταδιακής αφαίρεσης της φυσικής υλικότητας από τη συναλλακτική σχέση. Η μετάβαση από τα μετρητά στις ψηφιακές πληρωμές δεν αποτελεί μια απλή αλλαγή του διαθέσιμου τεχνολογικού εργαλείου, αλλά μια διαδικασία βαθύτερης μεταβολής της σχέσης αγοραστή και πωλητή, της φύσης της εμπιστοσύνης που αυτή προϋποθέτει και της θεσμικής υποδομής που την υποστηρίζει.

Τα μετρητά, ως μέσον πληρωμής, ενσωματώνουν, εγγενώς, ορισμένες ιδιότητες που τα καθιστούν μοναδικά ως προς το γεγονός ότι η συναλλαγή ολοκληρώνεται αμέσως, δεν αφήνει ίχνος δεδομένων, δεν απαιτεί ενδιάμεσο φορέα και δεν εξαρτάται από κάποιο είδος, έστω και πρωτόλειας, τεχνολογικής υποδομής. Αυτές ακριβώς οι ιδιότητες, οι οποίες, ιστορικά, επιτάχυναν και μεγέθυναν τις εγχρήματες συναλλαγές, μετατράπηκαν σήμερα, στη λογική της ψηφιακής οικονομίας, σε περιορισμούς, υπό την έννοια της αδυναμίας παρακολούθησης των σταδίων της συναλλαγής, της αδυναμίας αυτοματοποίησής τους και της ταυτόχρονης αδυναμίας ενσωμάτωσής τους σε ψηφιακές ροές επεξεργασίας δεδομένων.

Μια από τις πρώτες κρίσιμες καμπές στην ιστορική εξέλιξη των μέσων πληρωμής υπήρξε η εισαγωγή της τραπεζικής κάρτας, κατά τη δεκαετία του 1950, και η σταδιακή διάδοσή της στις διεθνείς συναλλαγές, κατά τις δεκαετίες του 1970 και του 1980. Η τραπεζική κάρτα δεν αποτέλεσε απλώς μια νέα εναλλακτική έναντι των μετρητών, αλλά σηματοδότησε μια βαθύτερη μεταβολή στην ίδια την αρχιτεκτονική της συναλλαγής. Για πρώτη φορά, η ολοκλήρωση της πληρωμής προϋπέθετε, συστηματικά, τη συμμετοχή εξειδικευμένων ενδιάμεσων φορέων, όπως ο εκδότης της κάρτας και οι οργανισμοί επεξεργασίας και εκκαθάρισης των συναλλαγών. Παράλληλα, η χρήση της κάρτας εγκαινίασε μια νέα εποχή καταγραφής και συστηματικής συγκέντρωσης πληροφοριών, σχετικά με τη συναλλακτική συμπεριφορά

των χρηστών, μετατρέποντας, σταδιακά, την πληρωμή από μια στιγμιαία πράξη ανταλλαγής σε πηγή αξιοποιήσιμων δεδομένων (Peneder, 2022).

Η δεκαετία του 1990, με την ανάπτυξη των ηλεκτρονικών δικτύων μεταφοράς κεφαλαίων, και στη συνέχεια η δεκαετία του 2000, με την αλματώδη ανάπτυξη του ηλεκτρονικού εμπορίου και την εμφάνιση των νέων μορφών ψηφιακής πληρωμής, επιτάχυναν ακόμα περισσότερο αυτήν τη μετάβαση. Η εμφάνιση του PayPal, το 1998, και η κατοπινή διάδοση των ψηφιακών πορτοφολιών νοηματοδότησαν τη σταδιακή μετατόπιση από ένα, κυρίως, αναλογικό και τραπεζοκεντρικό σύστημα πληρωμών προς ένα ψηφιακό, διασυνδεδεμένο και περισσότερο βασισμένο στα δεδομένα οικοσύστημα συναλλαγών (Arslanian, 2022). Η εν λόγω εξέλιξη δεν άλλαξε μόνο τον τρόπο με τον οποίον πραγματοποιούνται οι πληρωμές, αλλά και τα υποκείμενα που συμμετέχουν στη συναλλαγή, τα δεδομένα που παράγονται κατά την ολοκλήρωσή της και τις δυνατότητες πρόσβασης, επεξεργασίας και αξιοποίησής τους.

Κατά τη δεκαετία του 2010, οι ψηφιακές πληρωμές επεκτάθηκαν σε εκθετικό βαθμό, σε σχέση με την προηγούμενη περίοδο. . Η ευρεία διάδοση της τεχνολογίας NFC (Near Field Communication) και των ανέπαφων συναλλαγών (contactless), η εισαγωγή υπηρεσιών κινητών πληρωμών, με χαρακτηριστικό παράδειγμα το Apple Pay, το 2014, η ταχεία ανάπτυξη των κωδικών QR, ως μέσου πληρωμής, ιδίως σε αναδυόμενες αγορές, καθώς και η θεσμική κατοχύρωση του open banking, μέσω της Οδηγίας PSD2, η οποία υιοθετήθηκε το 2015 και τέθηκε σε εφαρμογή το 2018, συνέβαλαν στη διαμόρφωση ενός νέου, ταχύτατα αναπτυσσόμενου, οικοσυστήματος πληρωμών (Konovalova et al., 2019). Υπό αυτές τις συνθήκες, η φυσική παρουσία του αγοραστή και η άμεση επαφή μεταξύ των συναλλασσόμενων παύουν σταδιακά να αποτελούν τις αναγκαίες προϋποθέσεις για την ολοκλήρωση μιας εμπορικής συναλλαγής.

Κατά την περίοδο της πανδημίας COVID-19, η αποφυγή της χρήσης μετρητών, λόγω των σχετικών υγειονομικών οδηγιών, η διεύρυνση των ανέπαφων πληρωμών, ακόμα και για συναλλαγές μικρής αξίας, καθώς και η συνακόλουθη απότομη αύξηση του ηλεκτρονικού εμπορίου ενίσχυσαν, σε σημαντικό βαθμό, την υιοθέτηση των ψηφιακών μέσων πληρωμής από καταναλωτές και επιχειρήσεις (Tan & Xue, 2021). Η πανδημία λειτούργησε, επομένως, ως καταλύτης μιας ήδη εξελισσόμενης διαδικασίας ψηφιακού μετασχηματισμού, επισπεύδοντας, μέσα σε σύντομο χρονικό διάστημα, μεταβολές στη συμπεριφορά των καταναλωτών, στις επιχειρηματικές πρακτικές και στις υποδομές

των συναλλαγών, οι οποίες, υπό διαφορετικές συνθήκες, θα απαιτούσαν, πιθανότατα, πολύ μεγαλύτερο χρονικό διάστημα για να εδραιωθούν.

Η εξέλιξη αυτή μπορεί να αποδοθεί αναλυτικά μέσα από ένα τριφασικό υπόδειγμα, αντίστοιχο εκείνου που περιγράφηκε στο προηγούμενο δελτίο σχετικά με τη γενικότερη ψηφιοποίηση του λιανικού εμπορίου. Στην πρώτη φάση, αυτήν της ψηφιοποίησης της πληρωμής (digitization), τα παραδοσιακά μέσα πληρωμής — μετρητά, επιταγές — αντικαθίστανται από ψηφιακά τους ισοδύναμα, χωρίς ουσιαστική μεταβολή στη δομή της συναλλαγής. Στη δεύτερη φάση, δηλ. σ' εκείνην της ψηφιακής ολοκλήρωσης (digitalization), οι πληρωμές ενσωματώνονται σε ευρύτερα ψηφιακά οικοσυστήματα — εφαρμογές, πλατφόρμες, CRM συστήματα — και αρχίζουν να παράγουν δεδομένα που ανατροφοδοτούν επιχειρηματικές αποφάσεις. Στην τρίτη φάση, αυτήν του ψηφιακού μετασχηματισμού των πληρωμών (digital transformation), το ίδιο το επιχειρηματικό μοντέλο αναδιαμορφώνεται αναφορικά με τη ροή των δεδομένων πληρωμής. Κατ' αυτόν τον τρόπο, η πληρωμή παύει να είναι το τέλος της συναλλαγής και μετατρέπεται στο σημείο εκκίνησης νέων εμπορικών, επικοινωνιακών και αναλυτικών διαδικασιών.

Το ελληνικό λιανικό εμπόριο κινείται, σε μεγάλο βαθμό, μεταξύ της πρώτης και της δεύτερης φάσης, με ανομοιογένεια ανάλογη εκείνης που παρατηρείται στη γενικότερη ψηφιακή ωριμότητα των επιχειρήσεων. Η υποχρεωτική αποδοχή ηλεκτρονικών μέσων πληρωμής, η οποία θεσπίστηκε από την ελληνική φορολογική νομοθεσία, σε συνδυασμό με την κρατική επιδότηση της προμήθειας POS τερματικών επιτάχυναν τη διείσδυση της πρώτης φάσης σε ένα ευρύ φάσμα εμπορικών και επαγγελματικών δραστηριοτήτων. Ωστόσο, η ενσωμάτωση των ψηφιακών πληρωμών σε ολοκληρωμένα ψηφιακά συστήματα διαχείρισης και η αξιοποίηση των δεδομένων τους παραμένουν, εν πολλοίς, περιορισμένες.

2.2 Η τυπολογία των ψηφιακών μέσων πληρωμής

Η κατανόηση του σύγχρονου οικοσυστήματος ψηφιακών πληρωμών προϋποθέτει τη συστηματική καταγραφή της τυπολογίας των διαθέσιμων μέσων, η οποία θα αναδείξει όχι μόνον τα τεχνικά χαρακτηριστικά τους, αλλά και τις δομικές επιπτώσεις τους για τις επιχειρήσεις του λιανικού εμπορίου και τους καταναλωτές.

Τραπεζικές κάρτες (debit/credit): συνιστούν το βασικό μέσον της ψηφιακής πληρωμής, τόσο διεθνώς όσο και στην Ελλάδα, με μερίδιο που παραμένει το υψηλότερο στο σύνολο των συναλλαγών, παρά την ανάδυση νέων, πιο τεχνολογικά ανεπτυγμένων, μέσων (Yilmazkuday, 2026). Η αρχιτεκτονική των συστημάτων πληρωμών με κάρτα στηρίζεται, κατά κανόνα, σε ένα τετραμερές σχήμα, στο οποίο συμμετέχουν τέσσερις βασικοί φορείς: η εκδότρια τράπεζα ή ο εκδότης της κάρτας (issuing bank), η αποδέκτρια τράπεζα ή ο πάροχος υπηρεσιών αποδοχής πληρωμών (acquiring bank), το δίκτυο καρτών (card scheme), όπως η Visa και η Mastercard, και ο κάτοχος της κάρτας. Η αλληλεπίδραση όλων αυτών κατά την ολοκλήρωση της κάθε συναλλαγής διαμορφώνει ένα σύνθετο σύστημα χρεώσεων και προμηθειών, στο οποίο περιλαμβάνονται, μεταξύ άλλων, οι διατραπεζικές προμήθειες (interchange fees) και οι προμήθειες των δικτύων καρτών (scheme fees). Οι χρεώσεις αυτές συνιστούν σημαντικό στοιχείο του κόστους αποδοχής των ηλεκτρονικών πληρωμών για τις εμπορικές επιχειρήσεις και επιβαρύνουν, αναλογικά, περισσότερο τις μικρές επιχειρήσεις, οι οποίες διαθέτουν, εκ φύσεως, περιορισμένη διαπραγματευτική ισχύ.

Η επιβολή ανώτατων ορίων στις διατραπεζικές προμήθειες, μέσω του Κανονισμού (ΕΕ) 2015/751 — 0,2% για τις συναλλαγές με χρεωστικές κάρτες και 0,3% για τις συναλλαγές με πιστωτικές κάρτες— αποτέλεσε μια σημαντική ρυθμιστική παρέμβαση για τον περιορισμό του κόστους των πληρωμών με κάρτα. Ωστόσο, η παρέμβαση αυτή δεν εξάλειψε πλήρως τις υφιστάμενες ασυμμετρίες στο οικοσύστημα των καρτών, καθώς άλλες κατηγορίες χρεώσεων, όπως οι προμήθειες των δικτύων καρτών που επιβάλλονται από τα σχετικά δίκτυα, παρέμειναν, σε μεγάλο βαθμό, εκτός της άμεσης ρύθμισης. Το γεγονός αυτό διατηρεί το συνολικό κόστος αποδοχής καρτών σε υψηλότερα επίπεδα από εκείνα που προκύπτουν αποκλειστικά από τις διατραπεζικές προμήθειες, ενώ, παράλληλα, αναδεικνύει τα όρια μιας ρυθμιστικής παρέμβασης που επικεντρώνεται σε μια μόνο συνιστώσα της συνολικής δομής των χρεώσεων[1].

[1] Ο Κανονισμός της ΕΕ 2015/751 επικεντρώθηκε, κυρίως, στις διατραπεζικές προμήθειες, οι οποίες αποτελούν μια μόνο συνιστώσα του συνολικού κόστους αποδοχής μιας συναλλαγής με κάρτα. Η επιβολή ανώτατων ορίων σε αυτές τις προμήθειες περιόρισε ένα σημαντικό μέρος του κόστους, δεν οδήγησε, όμως, σε αντίστοιχη ολοκληρωμένη ρύθμιση όλων των υπόλοιπων χρεώσεων που επιβαρύνουν τις εμπορικές επιχειρήσεις. Ιδιαίτερη σημασία έχουν οι προμήθειες των δικτύων καρτών, οι οποίες επιβάλλονται από τα ίδια τα διεθνή δίκτυα, όπως η Visa και η Mastercard, ως αντάλλαγμα για τη χρήση και τη λειτουργία της υποδομής των συστημάτων πληρωμών. Οι χρεώσεις αυτές παρέμειναν, σε μεγάλο

Κινητές πληρωμές (mobile payments): Η κατηγορία αυτή περιλαμβάνει ένα ευρύ φάσμα τεχνολογιών και υπηρεσιών πληρωμής, οι οποίες αξιοποιούν το κινητό τηλέφωνο ως το βασικό μέσον έναρξης, ταυτοποίησης και ολοκλήρωσης της συναλλαγής. Σε αυτές περιλαμβάνονται οι ανέπαφες πληρωμές, μέσω της τεχνολογίας NFC από smartphones, όπως οι υπηρεσίες Apple Pay, Google Pay και Samsung Pay, οι πληρωμές που πραγματοποιούνται μέσω εφαρμογών των τραπεζών, καθώς και οι υπηρεσίες που προσφέρονται από ψηφιακές και fintech πλατφόρμες, όπως η Revolut και η N26.

Κοινός παρονομαστής αυτών των διαφορετικών μορφών είναι η αξιοποίηση του smartphone, ως μέσου πρόσβασης στο οικοσύστημα των πληρωμών, με αποτέλεσμα η φυσική χρήση της τραπεζικής κάρτας να καθίσταται ολοένα και λιγότερο αναγκαία. Οι κινητές πληρωμές παρουσιάζουν ταχεία ανάπτυξη σε ευρωπαϊκό επίπεδο, με ιδιαίτερα υψηλά ποσοστά υιοθέτησής τους στις βόρειες και ανατολικές ευρωπαϊκές αγορές. Στην Ελλάδα, η διείσδυσή τους παραμένει χαμηλότερη, σε σύγκριση με τον ευρωπαϊκό μέσο όρο, παρουσιάζει, όμως, σταθερή ανοδική πορεία από το 2020 κι ύστερα, αντανακλώντας τη γενικότερη επιτάχυνση της ψηφιοποίησης των συναλλαγών και την αυξανόμενη εξοικείωση των καταναλωτών με τις ανέπαφες και ψηφιακές μεθόδους πληρωμής (ECB, 2024).

βαθμό, εκτός άμεσης ρύθμισης και, ως εκ τούτου, η μείωση των διατραπεζικών προμηθειών δεν συνεπάγεται, κατ' ανάγκην, ανάλογη μείωση του συνολικού κόστους που καταβάλλει ο έμπορος. Παράλληλα, στο τελικό κόστος προστίθεται και η αμοιβή του παρόχου αποδοχής της συναλλαγής (acquirer), ο οποίος αναλαμβάνει την τεχνική και λειτουργική επεξεργασία των πληρωμών και τη συμβατική σχέση με την εμπορική επιχείρηση (https://www.taxheaven.gr/circulars/22855/kanonismos-ee-2015-751).

Κατά συνέπεια, η συνολική επιβάρυνση του εμπόρου για την αποδοχή μιας πληρωμής με κάρτα διαμορφώνεται από περισσότερες της μιας συνιστώσες και δεν μπορεί να αποτυπωθεί αποκλειστικά μέσω της διατραπεζικής προμήθειας. Ενδεικτικά, το συνολικό κόστος μπορεί να προσεγγιστεί ως το άθροισμα της διατραπεζικής προμήθειας, των χρεώσεων των δικτύων καρτών και της αμοιβής του παρόχου αποδοχής, μαζί με τυχόν πρόσθετες χρεώσεις που συνδέονται με την παροχή των σχετικών υπηρεσιών. Επομένως, ακόμα και μετά τη ρύθμιση των διατραπεζικών προμηθειών, οι επιχειρήσεις εξακολουθούν να αντιμετωπίζουν ένα σύνθετο, και όχι πάντα επαρκώς διαφανές, σύστημα χρεώσεων, εντός του οποίου η πραγματική δυνατότητα διαπραγμάτευσης είναι περιορισμένη, ιδίως όσον αφορά τις μικρές και πολύ μικρές επιχειρήσεις.

Ανοιχτή Τραπεζική (open banking) και πληρωμές από λογαριασμό σε λογαριασμό (Account-to-Account – A2A): Η εφαρμογή της σχετικής Οδηγίας PSD2 και η υποχρέωση των τραπεζών να παρέχουν, υπό συγκεκριμένες προϋποθέσεις και με τη συναίνεση του πελάτη, πρόσβαση σε δεδομένα και λειτουργίες του λογαριασμού, μέσω τυποποιημένων διεπαφών προγραμματισμού εφαρμογών (Application Programming Interfaces – APIs), δημιούργησαν τις συνθήκες για την ανάπτυξη ενός νέου μοντέλου πληρωμών. Στο πλαίσιο αυτό, αναπτύχθηκαν οι πληρωμές από λογαριασμό σε λογαριασμό (Account-to-Account – A2A), μέσω των οποίων τα κεφάλαια μεταφέρονται απευθείας από τον τραπεζικό λογαριασμό του πληρωτή στον λογαριασμό του δικαιούχου, χωρίς να απαιτείται η διαμεσολάβηση των παραδοσιακών δικτύων καρτών[2].

Οι υπηρεσίες εκκίνησης πληρωμών (Payment Initiation Services – PIS), οι οποίες παρέχονται από εξειδικευμένους παρόχους υπηρεσιών εκκίνησης πληρωμών (Payment Initiation Service Providers – PISPs), επιτρέπουν την έναρξη της συναλλαγής απευθείας από τον λογαριασμό του καταναλωτή, με την απαιτούμενη συναίνεση και αυθεντικοποίησή του. Το μοντέλο αυτό μπορεί, υπό ορισμένες προϋποθέσεις, να μειώσει το κόστος αποδοχής πληρωμών για τις επιχειρήσεις, καθώς περιορίζει, σε μερικές δε περιπτώσεις εξαλείφει, τη συμμετοχή ορισμένων ενδιάμεσων φορέων, ενώ, ταυτόχρονα, δεν επιβαρύνεται με τις χρεώσεις των δικτύων κρατών και των διατραπεζικών συναλλαγών (Stefanelli & Manta, 2023).

Ωστόσο, η ευρύτερη υιοθέτηση των A2A πληρωμών, στο λιανικό εμπόριο, προϋποθέτει την ανάπτυξη αξιόπιστων και εύχρηστων τεχνολογικών υποδομών, τη διαλειτουργικότητα μεταξύ τραπεζών και παρόχων, καθώς και τη διαθεσιμότητα

[2] Με άλλα λόγια, η ανοικτή τραπεζική (open banking) αναφέρεται σε ένα θεσμικό και τεχνολογικό πλαίσιο, το οποίο επιτρέπει, με τη συναίνεση του πελάτη και υπό την εποπτεία του σχετικού κανονιστικού πλαισίου, την ασφαλή πρόσβαση αδειοδοτημένων τρίτων παρόχων σε συγκεκριμένα τραπεζικά δεδομένα και υπηρεσίες, μέσω τυποποιημένων διεπαφών προγραμματισμού εφαρμογών (APIs). Με αυτόν τον τρόπο, η παροχή χρηματοπιστωτικών υπηρεσιών μετατοπίζεται από ένα αποκλειστικά συγκεντροποιημένο τραπεζοκεντρικό μοντέλο προς ένα πιο ανοικτό και ανταγωνιστικό οικοσύστημα, όπου συμμετέχουν τράπεζες, fintech επιχειρήσεις και εξειδικευμένοι πάροχοι. Στο πεδίο των πληρωμών, η ανοιχτή τραπεζική δημιουργεί, κυρίως, τις προϋποθέσεις για την ανάπτυξη πληρωμών από λογαριασμό σε λογαριασμό (A2A), διευκολύνοντας την πραγματοποίηση συναλλαγών, χωρίς την αναγκαστική προσφυγή στα παραδοσιακά δίκτυα καρτών, και μεταβάλλοντας, κατ' επέκταση, τη δομή του ανταγωνισμού και του κόστους στην αγορά των πληρωμών (Stefanelli & Manta, 2023).

υπηρεσιών που μπορούν να ενσωματωθούν εύκολα στα συστήματα των εμπορικών επιχειρήσεων. Όσον αφορά τις μικρές και μεσαίες επιχειρήσεις, η μετάβαση αυτή ενδέχεται να συνοδεύεται από τεχνικά, οργανωτικά και οικονομικά εμπόδια, καθώς η περιορισμένη τεχνογνωσία και η εξάρτηση από εξωτερικούς παρόχους μπορούν να περιορίσουν τη δυνατότητά τους να αξιοποιήσουν πλήρως τα πιθανά πλεονεκτήματα της ανοιχτής τραπεζικής.

Κωδικοί QR (QR payments): Οι κωδικοί QR έχουν αναδειχθεί σε ένα ιδιαίτερα σημαντικό μέσον ψηφιακών πληρωμών, γνωρίζοντας μαζική διάδοση, κυρίως στις ασιατικές αγορές, και ιδιαίτερα στην Κίνα, όπου η ανάπτυξη οικοσυστημάτων, όπως το Alipay και το WeChat Pay, συνέβαλε στην ευρεία χρήση τους στην καθημερινή οικονομική δραστηριότητα (Klein, 2020). Αντίθετα, η διείσδυσή τους στην ευρωπαϊκή αγορά παραμένει σχετικά περιορισμένη, γεγονός που συνδέεται, μεταξύ άλλων, με την ήδη υψηλή διάδοση των τραπεζικών καρτών και των ανέπαφων πληρωμών, μέσω τεχνολογίας NFC (Górka, 2025). Κατά την περίοδο της πανδημίας, οι κωδικοί QR απέκτησαν ακόμα μεγαλύτερη δυναμική, ενώ, σε ορισμένες ευρωπαϊκές χώρες, ενσωματώθηκαν σταδιακά στα εθνικά συστήματα πληρωμών και στις υποδομές των άμεσων μεταφορών[3]. Στο ευρωπαϊκό πλαίσιο, η European Payments Initiative (EPI) και η υπηρεσία Wero εντάσσονται στην ευρύτερη προσπάθεια ανάπτυξης μιας πιο ολοκληρωμένης ευρωπαϊκής υποδομής ψηφιακών πληρωμών. Η αξιοποίηση κινητών εφαρμογών και τεχνολογιών, όπως οι κωδικοί QR, έχει τη δυνατότητα να διευκολύνει την πραγματοποίηση άμεσων πληρωμών, χωρίς την αποκλειστική εξάρτηση από τα παραδοσιακά διεθνή δίκτυα καρτών.

BNPL — Buy Now, Pay Later («Αγόρασε τώρα, πλήρωσε αργότερα»): Οι υπηρεσίες BNPL αποτελούν μια από τις πλέον δυναμικά αναπτυσσόμενες κατηγορίες χρηματοοικονομικών προϊόντων, στο σύγχρονο λιανικό εμπόριο. Το μοντέλο αυτό επιτρέπει στον καταναλωτή να αποκτήσει άμεσα ένα προϊόν ή μια υπηρεσία και να εξοφλήσει την αξία του σε μεταγενέστερο χρόνο, είτε εφάπαξ είτε μέσω δόσεων. Πάροχοι, όπως η Klarna, η Afterpay και η Affirm, έχουν αποκτήσει σημαντική παρουσία, ιδίως στο ηλεκτρονικό εμπόριο και σε κατηγορίες προϊόντων, όπως ο

[3] Χαρακτηριστικό παράδειγμα συνιστά η Ολλανδία, όπου το εθνικό σύστημα πληρωμών iDEAL ενσωμάτωσε τη χρήση κωδικών QR για την εκκίνηση πληρωμών μέσω των εφαρμογών κινητής τραπεζικής (mobile banking).

ρουχισμός και τα ηλεκτρονικά είδη. Στις εμπορικές επιχειρήσεις, οι υπηρεσίες BNPL μπορούν να λειτουργήσουν ως εργαλείο ενίσχυσης των πωλήσεων, καθώς επιτρέπουν στον καταναλωτή να κατανείμει το κόστος της αγοράς σε μεταγενέστερες δόσεις, περιορίζοντας την άμεση οικονομική επιβάρυνση, την οποίαν συνεπάγεται η καταβολή ολόκληρου του ποσού κατά τον χρόνο της συναλλαγής. Με αυτόν τον τρόπο, το BNPL μπορεί να διευκολύνει την ολοκλήρωση μιας αγοράς, η οποία, σε άλλη περίπτωση, θα μπορούσε να αναβληθεί ή να εγκαταλειφθεί, ενώ, παράλληλα, ενδέχεται να μειώνει τα ποσοστά εγκατάλειψης του ηλεκτρονικού καλαθιού και να αυξάνει τη μέση αξία των αγορών. Η διευκόλυνση αυτή συνδέεται, ωστόσο, με αυξημένο κόστος για τον έμπορο, καθώς οι πάροχοι BNPL χρεώνουν, συνήθως, υψηλότερες προμήθειες, σε σχέση με αρκετά παραδοσιακά μέσα πληρωμής (Guttman-Kenney et al., 2023). Ταυτόχρονα, η ταχεία εξάπλωση των υπηρεσιών BNPL ανέδειξε σημαντικές προκλήσεις ως προς την προστασία των καταναλωτών, καθώς η δυνατότητα αναβολής της πληρωμής μπορεί να λειτουργήσει, στην πράξη, ως μορφή βραχυπρόθεσμης καταναλωτικής πίστωσης. Η ευκολία πρόσβασης σε τέτοιες υπηρεσίες ενδέχεται να ενθαρρύνει την πραγματοποίηση αγορών πέρα από τις άμεσες οικονομικές δυνατότητες του καταναλωτή και να αυξήσει τον κίνδυνο υπερχρέωσης, ιδίως όταν συνδυάζεται με πολλαπλές ταυτόχρονες πιστωτικές υποχρεώσεις. Γι' αυτόν τον λόγο, η ανάπτυξη του BNPL ανέδειξε την ανάγκη προσαρμογής του ευρωπαϊκού πλαισίου καταναλωτικής πίστης στις νέες ψηφιακές μορφές χρηματοδότησης (Kumar et al., 2024). Η αναθεωρημένη Οδηγία για τις Συμβάσεις Καταναλωτικής Πίστης (CCD2), που εκδόθηκε το 2023[4], διευρύνει το πεδίο εφαρμογής των σχετικών κανόνων και εντάσσει, υπό συγκεκριμένες προϋποθέσεις, περισσότερες μορφές βραχυπρόθεσμης και ψηφιακής πίστωσης στο πλαίσιο προστασίας της καταναλωτικής πίστης. Με αυτόν τον τρόπο, επιδιώκεται να διασφαλιστεί ότι η τεχνολογική καινοτομία στις πληρωμές δεν οδηγεί σε αποδυνάμωση των δικαιωμάτων και της προστασίας των καταναλωτών.

Κρυπτονομίσματα και ψηφιακά περιουσιακά στοιχεία: Παρά την εκτενή δημοσιότητα που έχουν αποκτήσει και το ιδιαίτερα υψηλό ύψος της κεφαλαιοποίησης των αγορών τους, τα κρυπτονομίσματα εξακολουθούν να διαδραματίζουν περιορισμένο ρόλο, ως μέσον πληρωμής, στο λιανικό εμπόριο. Η υψηλή μεταβλητότητα της αξίας τους (volatility), η σχετικά περιορισμένη αποδοχή τους από

[4]https://www.stradalex.eu/en/se_src_publ_leg_eur_jo/toc/leg_eur_jo_3_20231030/doc/ojeu_20230222
5

τις εμπορικές επιχειρήσεις, οι τεχνολογικές και λειτουργικές απαιτήσεις, τις οποίες προϋποθέτει η χρήση τους, καθώς και οι αβεβαιότητες που εξακολουθούν να χαρακτηρίζουν ορισμένες πτυχές της προστασίας των καταναλωτών λειτουργούν ως ανασταλτικοί παράγοντες για την ευρεία υιοθέτησή τους στις καθημερινές λιανικές συναλλαγές.

Ιδιαίτερο ενδιαφέρον παρουσιάζουν, ωστόσο, τα λεγόμενα stablecoins, δηλαδή διάφορα ψηφιακά περιουσιακά στοιχεία που φαίνεται να διατηρούν σχετικά σταθερή αξία, μέσω της σύνδεσής τους με παραδοσιακά νομίσματα ή και άλλα περιουσιακά στοιχεία (π.χ. χρυσός). Η μεγαλύτερη σταθερότητα που φαίνεται να διαθέτουν δημιουργεί, δυνητικά, ευνοϊκότερες προϋποθέσεις για τη χρήση τους στις πληρωμές και, κατ' επέκταση, για την ενσωμάτωσή τους σε ψηφιακά οικοσυστήματα λιανικού εμπορίου (Ante et al., 2023). Ωστόσο, η ανάπτυξή τους συνδέεται, πλέον, στενά με το εξελισσόμενο ευρωπαϊκό κανονιστικό πλαίσιο. Ο Κανονισμός MiCA (Markets in Crypto-Assets), που θεσπίστηκε το 2023[5], εισάγει ένα ενιαίο ευρωπαϊκό πλαίσιο για την έκδοση, προσφορά και παροχή υπηρεσιών, οι οποίες σχετίζονται με κρυπτοστοιχεία, συμπεριλαμβανομένων ειδικών κανόνων για τα stablecoins. Η σταδιακή εφαρμογή του πλαισίου αυτού αναμένεται να επηρεάσει σημαντικά τους όρους, υπό τους οποίους τα ψηφιακά περιουσιακά στοιχεία μπορούν να ενσωματωθούν στο ευρωπαϊκό χρηματοπιστωτικό και, ευρύτερα, στο οικοσύστημα των ψηφιακών πληρωμών.

2.3 Ο ρόλος των ενδιάμεσων: πάροχοι αποδοχής συναλλαγών (acquirers), πάροχοι υπηρεσιών πληρωμών (payment processors) και fintech πλατφόρμες

Ένα από τα πλέον σημαντικά — και συχνά παραγνωρισμένα — χαρακτηριστικά του σύγχρονου οικοσυστήματος ψηφιακών πληρωμών είναι η πολυπλοκότητα της αλυσίδας των ενδιάμεσων φορέων που παρεμβάλλεται μεταξύ εμπόρου και καταναλωτή. Η φαινομενικά απλή πράξη της ηλεκτρονικής πληρωμής εμπλέκει, στην

[5] https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

πραγματικότητα, ένα πλέγμα φορέων, καθένας εκ των οποίων έχει διαφορετική λειτουργία, φέρει διαφορετικό κανονιστικό βάρος και καρπούται διαφορετικό μερίδιο της αξίας που παράγεται.

Ο πάροχος αποδοχής συναλλαγών (acquirer) είναι ο χρηματοπιστωτικός οργανισμός ή ο αδειοδοτημένος πάροχος υπηρεσιών πληρωμών, ο οποίος παρέχει στον έμπορο τη δυνατότητα να αποδέχεται πληρωμές, μέσω καρτών και άλλων ηλεκτρονικών μέσων, διαχειρίζεται τη σχέση του με το σύστημα αποδοχής πληρωμών και, ανάλογα με το μοντέλο λειτουργίας, παρέχει ή υποστηρίζει την υποδομή του τερματικού POS. Παράλληλα, διαβιβάζει τις συναλλαγές προς το αντίστοιχο δίκτυο πληρωμών και εξασφαλίζει την πίστωση των σχετικών ποσών στον λογαριασμό του εμπόρου. Το κόστος των υπηρεσιών αποδοχής αποτυπώνεται στη merchant discount rate (MDR), δηλαδή στη συνολική χρέωση, η οποία επιβαρύνει τον έμπορο για την αποδοχή μιας ηλεκτρονικής συναλλαγής και ενσωματώνει διαφορετικές συνιστώσες κόστους, μεταξύ άλλων, τη διατραπεζική χρέωση, τις χρεώσεις του δικτύου της κάρτας και την αμοιβή του παρόχου αποδοχής (Sutherland & Jarrahi, 2018). Στις μικρές και πολύ μικρές επιχειρήσεις λιανικής, η διαπραγματευτική ισχύς έναντι των συγκεκριμένων παρόχων είναι, συνήθως, περιορισμένη, γεγονός που μπορεί να περιορίζει τη δυνατότητά τους να εξασφαλίζουν ευνοϊκότερους όρους τιμολόγησης, σε σχέση με μεγαλύτερες επιχειρήσεις, οι οποίες διαθέτουν υψηλότερο όγκο συναλλαγών και ισχυρότερη διαπραγματευτική θέση.

Ο πάροχος υπηρεσιών πληρωμών (payment processor) είναι ο φορέας που αναλαμβάνει την τεχνική και λειτουργική επεξεργασία μιας ηλεκτρονικής συναλλαγής, υποστηρίζοντας, μεταξύ άλλων, τη διαβίβαση των δεδομένων της συναλλαγής, την επικοινωνία μεταξύ των εμπλεκόμενων φορέων, την εφαρμογή μηχανισμών αυθεντικοποίησης και την ανίχνευση και πρόληψη περιστατικών απάτης. Η επεξεργασία συνδέεται στενά με τις διαδικασίες εκκαθάρισης και διακανονισμού (clearing and settlement), χωρίς, όμως, οι λειτουργίες αυτές να ταυτίζονται, κατ' ανάγκην, με τον ρόλο του συγκεκριμένου παρόχου. Στις περισσότερες περιπτώσεις, οι λειτουργίες τόσο του πάροχου των υπηρεσιών πληρωμών όσο και αυτού της αποδοχής των συναλλαγών, ενσωματώνονται στο ίδιο επιχειρηματικό σχήμα (Hazar & Babuşcu, 2023). Εταιρείες τεχνολογίας χρηματοπιστωτικών υπηρεσιών (fintech), όπως η Stripe, η Adyen και η Worldpay, έχουν αναπτύξει ολοκληρωμένες υποδομές επεξεργασίας και αποδοχής ηλεκτρονικών πληρωμών, προσφέροντας στις επιχειρήσεις υπηρεσίες που

συνδυάζουν τεχνική διασύνδεση, διαχείριση συναλλαγών, μηχανισμούς πρόληψης απάτης και, ανάλογα με το μοντέλο παροχής, υπηρεσίες αποδοχής πληρωμών.

Η ανάδυση των *fintech* πλατφορμών ως νέων ενδιάμεσων στο οικοσύστημα των ψηφιακών πληρωμών αποτελεί παράλληλη εξέλιξη προς εκείνη που παρουσιάστηκε στο προηγούμενο δελτίο, αναφορικά με τις πλατφόρμες ηλεκτρονικού εμπορίου. Και στις δύο περιπτώσεις, η ψηφιοποίηση δεν καταργεί τη διαμεσολάβηση, αλλά μετασχηματίζει τη μορφή και τους φορείς της, δημιουργώντας νέους ψηφιακούς ενδιάμεσους, οι οποίοι διευκολύνουν την πρόσβαση στις αγορές και μειώνουν το κόστος πραγματοποίησης των συναλλαγών, ενώ δημιουργούν, ταυτόχρονα, νέες μορφές εξάρτησης και ασυμμετρίας ισχύος. Η εξάρτηση αυτή συνδέεται, μεταξύ άλλων, με το λεγόμενο κόστος μεταπήδησης (switching costs) και το φαινόμενο του εγκλωβισμού (lock-in effects), καθώς η επιλογή ενός παρόχου πληρωμών δεν αφορά, πλέον, μια απλή, εύκολα αναστρέψιμη εμπορική σχέση, αλλά ενδέχεται να συνδέεται στενά με την ευρύτερη ψηφιακή υποδομή της επιχείρησης (Westermeier, 2020).

Υπό αυτήν την έννοια, η επιλογή παρόχου υπηρεσιών πληρωμών αποκτά, για τον έμπορο, στρατηγικό χαρακτήρα. Η ενσωμάτωση των υπηρεσιών πληρωμών στα λογιστικά και πληροφοριακά συστήματα, στις διαδικασίες τιμολόγησης και συμφωνίας συναλλαγών, στα συστήματα διαχείρισης πελατειακών σχέσεων (CRM), καθώς και στις πλατφόρμες ηλεκτρονικού εμπορίου, επιφέρει σημαντικό τεχνικό και οργανωτικό κόστος μετακίνησης σε έναν εναλλακτικό πάροχο. Κατά συνέπεια, η αρχική επιλογή παρόχου μπορεί να δημιουργήσει μια σχέση τεχνολογικής και επιχειρησιακής εξάρτησης, περιορίζοντας, εκ των υστέρων, τη δυνατότητα του εμπόρου να αλλάξει πάροχο ή να διαπραγματευτεί αποτελεσματικότερα τους όρους της ισχύουσας συνεργασίας. Το ζήτημα αποκτά ιδιαίτερη σημασία για τις μικρές και πολύ μικρές επιχειρήσεις, οι οποίες διαθέτουν περιορισμένους οικονομικούς και τεχνολογικούς πόρους για την αντιμετώπιση του κόστους μιας τέτοιας μετάβασης.

2.4 Ευρωπαϊκά και ελληνικά δεδομένα διείσδυσης των ψηφιακών πληρωμών

Η εμπειρική τεκμηρίωση της διείσδυσης των ψηφιακών πληρωμών στο ευρωπαϊκό και ελληνικό πλαίσιο αποτελεί αναγκαία προϋπόθεση για την αξιολόγηση τόσο των

ευκαιριών όσο και των κινδύνων που αναλύονται στα επόμενα κεφάλαια του παρόντος δελτίου.

Εντός της Ευρωζώνης, τα πλέον πρόσφατα διαθέσιμα στοιχεία της Ευρωπαϊκής Κεντρικής Τράπεζας (ECB, 2024)[6] επιβεβαιώνουν τη συνεχιζόμενη μετατόπιση των καταναλωτών προς τα ψηφιακά μέσα πληρωμής, αν και η χρήση μετρητών παραμένει σημαντική, ιδίως στις συναλλαγές μικρής αξίας. Τα μετρητά εξακολουθούν να αποτελούν το συχνότερα χρησιμοποιούμενο μέσον πληρωμής στα φυσικά σημεία πώλησης, αντιπροσωπεύοντας το 52% των συναλλαγών, έναντι 59%, το 2022, 72%, το 2019, και 79%, το 2016. Αντίθετα, το μερίδιο των πληρωμών με κάρτα αυξήθηκε στο 39%, το 2024, από 34%, το 2022, ενώ οι πληρωμές μέσω κινητών συσκευών ανήλθαν στο 6%, φτάνοντας σχεδόν στο διπλάσιο, σε σχέση με το 2022. Η μετάβαση προς τα ψηφιακά μέσα είναι ακόμα εντονότερη στις ηλεκτρονικές αγορές: το μερίδιο των online πληρωμών, στο σύνολο των καθημερινών συναλλαγών, αυξήθηκε από 7%, το 2019, σε 17%, το 2022, και 21%, το 2024, ενώ, σε όρους αξίας, αντιπροσωπεύει, πλέον, το 36% των σχετικών πληρωμών. Παράλληλα, το 55% των καταναλωτών δήλωσε ότι προτιμά κάρτες ή άλλα ηλεκτρονικά μέσα πληρωμής, όταν πραγματοποιεί αγορές σε φυσικά καταστήματα, έναντι του 22% που εξακολουθεί να προτιμά τα μετρητά. Τα στοιχεία αυτά καταδεικνύουν ότι η ψηφιοποίηση των πληρωμών έχει, πλέον, εδραιωθεί ως βασικό χαρακτηριστικό του ευρωπαϊκού λιανικού εμπορίου, χωρίς, ωστόσο, να συνεπάγεται την άμεση ή πλήρη υποκατάσταση των μετρητών.

Η Ελλάδα παρουσιάζει μια χαρακτηριστική πορεία ταχείας μεταβολής των παραδοσιακών προτύπων πληρωμής, χωρίς, όμως, να έχει ολοκληρωθεί η μετάβαση προς ένα κατεξοχήν ψηφιακό οικοσύστημα συναλλαγών. Ιστορικά, η ελληνική αγορά χαρακτηριζόταν από ιδιαίτερα υψηλή χρήση μετρητών, η οποία συνδεόταν με ένα ευρύτερο πλέγμα οικονομικών, θεσμικών και τεχνολογικών παραγόντων, όπως η εκτεταμένη παραοικονομία, η περιορισμένη εμπιστοσύνη στο τραπεζικό σύστημα, κατά την περίοδο της χρηματοπιστωτικής κρίσης, η χαμηλότερη ψηφιακή ωριμότητα σημαντικού τμήματος των μικρών επιχειρήσεων και η περιορισμένη διάδοση των υποδομών ηλεκτρονικών πληρωμών. Η επιβολή κεφαλαιακών περιορισμών το 2015, σε συνδυασμό με την ενίσχυση των φορολογικών κινήτρων για τη χρήση ηλεκτρονικών

[6]https://www.ecb.europa.eu/stats/ecb_surveys/space/html/ecb.space2024~19d46f0f17.en.html?utm_source

μέσων πληρωμής και τη σταδιακή υποχρεωτική εγκατάσταση και αποδοχή τερματικών POS αποτέλεσαν σημαντικούς θεσμικούς μηχανισμούς επιτάχυνσης της μετάβασης. Η πανδημία COVID-19 λειτούργησε, στη συνέχεια, ως πρόσθετος επιταχυντής, ενισχύοντας την εξοικείωση των καταναλωτών και των επιχειρήσεων με τις ηλεκτρονικές και ανέπαφες πληρωμές.

Τα πλέον πρόσφατα διαθέσιμα στοιχεία της Ευρωπαϊκής Κεντρικής Τράπεζας (ECB, 2024) επιβεβαιώνουν τη σημαντική μεταβολή που έχει συντελεστεί. Το μερίδιο των μετρητών στις συναλλαγές σε φυσικά σημεία πώλησης στην Ελλάδα μειώθηκε στο 54%, από 62%, το 2022, και 80%, το 2019. Παρά τη σημαντική αυτή υποχώρηση, τα μετρητά εξακολουθούν να αποτελούν το συχνότερα χρησιμοποιούμενο μέσον πληρωμής, ενώ οι κάρτες αντιπροσωπεύουν, πλέον, το 37% των συναλλαγών POS και οι πληρωμές μέσω κινητών συσκευών περίπου το 5%. Η ψηφιοποίηση είναι ακόμα εντονότερη στο ηλεκτρονικό εμπόριο, όπου οι κάρτες αποτελούν το κυριότερο μέσον πληρωμής. Παράλληλα, η διεύρυνση της τεχνολογικής υποδομής είναι ιδιαίτερα σημαντική: ο αριθμός των τερματικών POS που παρέχονταν από εγχώριους παρόχους υπηρεσιών πληρωμών ανήλθε σε περίπου 1,325 εκατ., στο τέλος του 2024, και αυξήθηκε ακόμα περισσότερο σε περίπου 1,351 εκατ., κατά το πρώτο εξάμηνο του 2025.

Η εξέλιξη αυτή καταδεικνύει ότι η Ελλάδα έχει διανύσει μια ιδιαίτερα σημαντική απόσταση από το παραδοσιακά μετρητοκεντρικό μοντέλο πληρωμών, μολονότι δεν έχει καταφέρει να συγκλίνει πλήρως προς τα πρότυπα των πλέον ψηφιοποιημένων ευρωπαϊκών αγορών. Η διατήρηση του μεριδίου των μετρητών στο 54% των συναλλαγών POS, σε συνδυασμό με τη σημαντική, πλέον, διείσδυση των καρτών και την αυξανόμενη χρήση των κινητών συναλλαγών αποτυπώνουν μια αγορά σε διαδικασία μετάβασης, όπου διαφορετικά μέσα πληρωμής συνυπάρχουν και ανταγωνίζονται για τη διαμόρφωση των νέων καταναλωτικών και επιχειρηματικών πρακτικών. Η μετάβαση αυτή έχει ιδιαίτερη σημασία για τις μικρές και πολύ μικρές επιχειρήσεις, καθώς η διεύρυνση των ψηφιακών πληρωμών δεν συνεπάγεται μόνον επενδύσεις σε τεχνολογική υποδομή, αλλά και προσαρμογή των λογιστικών, πληροφοριακών και οργανωτικών διαδικασιών τους στο νέο ψηφιακό περιβάλλον.

Η ανάλυση των δεδομένων αναδεικνύει, ωστόσο, μια κρίσιμη διαφοροποίηση μεταξύ της βασικής τεχνολογικής υιοθέτησης και της στρατηγικής αξιοποίησης των ψηφιακών δυνατοτήτων. Η εγκατάσταση POS και η αποδοχή καρτών συνιστούν αναγκαία, αλλά

όχι επαρκή, στοιχεία ψηφιακού μετασχηματισμού. Η ουσιαστική αξιοποίηση των δυνατοτήτων, τις οποίες προσφέρουν οι ψηφιακές πληρωμές, προϋποθέτει την ενσωμάτωση των δεδομένων των συναλλαγών στα πληροφοριακά και λειτουργικά συστήματα της επιχείρησης, τη σύνδεσή τους με συστήματα διαχείρισης πελατειακών σχέσεων (CRM), την αξιοποίησή τους για αναλύσεις καταναλωτικής συμπεριφοράς και τη διασύνδεσή τους με τα ψηφιακά κανάλια πωλήσεων και *marketing*. Η διάκριση αυτή είναι ιδιαίτερα σημαντική στην ελληνική περίπτωση, καθώς η διεύρυνση της χρήσης των ψηφιακών μέσων πληρωμής δεν συνοδεύεται ακόμα από αντίστοιχο επίπεδο συνολικής ψηφιακής ωριμότητας των επιχειρήσεων. Σύμφωνα με τα πλέον πρόσφατα διαθέσιμα στοιχεία, το 2025, μόλις το 55,95% των ελληνικών μικρομεσαίων επιχειρήσεων είχε επιτύχει τουλάχιστον βασικό επίπεδο ψηφιακής έντασης, έναντι 71,39% στην ΕΕ, ενώ η υιοθέτηση προηγμένων τεχνολογιών, όπως η ανάλυση δεδομένων, το *cloud computing* και η Τεχνητή Νοημοσύνη, εξακολουθεί να υπολείπεται σημαντικά των ευρωπαϊκών επιδόσεων (Eurostat, 2026).

Το χάσμα μεταξύ της ψηφιοποίησης της συναλλαγής και της αξιοποίησης της πληροφορίας που αυτή αποφέρει συνιστά μια σημαντική αναπτυξιακή ευκαιρία, αλλά και έναν παράγοντα επιχειρησιακής ευπάθειας. Από τη μια πλευρά, τα δεδομένα των πληρωμών μπορούν να αξιοποιηθούν για την καλύτερη κατανόηση της ζήτησης, τη βελτιστοποίηση του αποθέματος, την εξατομίκευση της επικοινωνίας με τους πελάτες και τη βελτίωση της συνολικής εμπειρίας αγοράς. Από την άλλη, η απλή υιοθέτηση ψηφιακών μέσων πληρωμής, χωρίς την αντίστοιχη ανάπτυξη των οργανωτικών, πληροφοριακών και τεχνολογικών δυνατοτήτων της επιχείρησης, καταλήγει σε μια μορφή ασύμμετρης ψηφιοποίησης. Η επιχείρηση εντάσσεται στο ψηφιακό οικοσύστημα και παράγει ολοένα και περισσότερα δεδομένα, χωρίς να διαθέτει, κατ' ανάγκην, την ικανότητα να τα επεξεργαστεί, να τα αξιοποιήσει στρατηγικά ή να διαχειριστεί αποτελεσματικά τους κινδύνους που συνδέονται με αυτά.

3. Οι ψηφιακές πληρωμές ως ζήτημα δημόσιας πολιτικής

3.1 Το ευρωπαϊκό ρυθμιστικό πλαίσιο: Οδηγίες για τις Υπηρεσίες Πληρωμών (PSD1, PSD2, PSD3) και Κανονισμός για τις Άμεσες Πληρωμές (Instant Payments Regulation)

Το ευρωπαϊκό ρυθμιστικό πλαίσιο στον τομέα των πληρωμών αντανακλά μια διαρκή προσπάθεια εξισορρόπησης μεταξύ διαφορετικών και, σε ορισμένες περιπτώσεις, αντικρουόμενων επιδιώξεων, αφενός, της ενίσχυσης του ανταγωνισμού, της καινοτομίας και της πρόσβασης νέων παρόχων στην αγορά και, αφετέρου, της προστασίας των καταναλωτών, της ασφάλειας των συναλλαγών, της χρηματοπιστωτικής σταθερότητας και της δημιουργίας ενός πραγματικά ενιαίου ευρωπαϊκού χώρου πληρωμών. Το εγχείρημα αυτό δεν έχει λάβει τη μορφή μιας ενιαίας και στατικής ρυθμιστικής παρέμβασης, αλλά μιας διαδοχικής και δυναμικής θεσμικής διαδικασίας, μέσω της οποίας το ευρωπαϊκό πλαίσιο προσαρμόζεται στις τεχνολογικές εξελίξεις και στις μεταβαλλόμενες δομές της αγοράς.

Η εξέλιξη από την πρώτη Οδηγία για τις υπηρεσίες πληρωμών από την PSD1 στην PSD2 και, πλέον, προς την PSD3 και το συνακόλουθο νέο κανονιστικό πλαίσιο για τις υπηρεσίες πληρωμών αποτυπώνουν αυτή τη σταδιακή μετάβαση από ένα σχετικά περιορισμένο πλαίσιο ρύθμισης των παραδοσιακών υπηρεσιών πληρωμών προς ένα πιο ανοικτό, ανταγωνιστικό και τεχνολογικά ουδέτερο οικοσύστημα. Παράλληλα, ο Κανονισμός για τις Άμεσες Πληρωμές (Instant Payments Regulation) εισάγει μια διαφορετική, αλλά συμπληρωματική διάσταση, καθώς επιδιώκει να καταστήσει τις άμεσες μεταφορές χρημάτων ευρύτερα διαθέσιμες, οικονομικά προσβάσιμες και λειτουργικά ενσωματωμένες στην καθημερινή οικονομική δραστηριότητα (Ortino, 2022). Οι εξελίξεις αυτές μεταβάλλουν όχι μόνο τους κανόνες λειτουργίας των παρόχων υπηρεσιών πληρωμών, αλλά και τις συνθήκες, υπό τις οποίες οι εμπορικές επιχειρήσεις και οι καταναλωτές συμμετέχουν στο νέο ψηφιακό οικοσύστημα συναλλαγών.

Υπό αυτήν την έννοια, το ευρωπαϊκό ρυθμιστικό πλαίσιο για τις πληρωμές μπορεί να εννοηθεί ως μια διαδικασία σταδιακής θεσμικής αναδιάρθρωσης της αγοράς, μέσω της οποίας μεταβάλλονται οι ρόλοι των τραπεζών, των παρόχων υπηρεσιών πληρωμών,

των *fintech* επιχειρήσεων και των τεχνολογικών πλατφορμών, ενώ, παράλληλα, επαναπροσδιορίζονται οι όροι πρόσβασης, ανταγωνισμού και κατανομής κινδύνων στο οικοσύστημα των πληρωμών. Όσον αφορά το λιανικό εμπόριο, η εξέλιξη αυτή έχει ιδιαίτερη σημασία, καθώς οι επιχειρήσεις δεν αποτελούν απλώς τελικούς χρήστες των νέων υποδομών, αλλά εντάσσονται σε ένα ολοένα και πιο σύνθετο θεσμικό και τεχνολογικό περιβάλλον, το οποίο επηρεάζει το κόστος των συναλλαγών, τη διαχείριση των δεδομένων, την ασφάλεια των πληρωμών και, εν τέλει, την ίδια τη σχέση τους με τους καταναλωτές και τους παρόχους ψηφιακών υπηρεσιών.

Η αρχική Οδηγία για τις Υπηρεσίες Πληρωμών (PSD1, 2007/64/ΕΚ) αποτέλεσε την πρώτη ολοκληρωμένη προσπάθεια δημιουργίας ενός εναρμονισμένου νομικού πλαισίου για τις υπηρεσίες πληρωμών στην ΕΕ και συνέβαλε στη δυναμική διαμόρφωση μιας ολοκληρωμένης ευρωπαϊκής αγοράς πληρωμών. Η Οδηγία επιδίωξε να εναρμονίσει τους βασικούς κανόνες που διέπουν την παροχή υπηρεσιών πληρωμών, να ενισχύσει τη διαφάνεια ως προς τους όρους και τις χρεώσεις των συναλλαγών, να καθορίσει σαφέστερα τα δικαιώματα και τις υποχρεώσεις των παρόχων και των χρηστών υπηρεσιών πληρωμών και να διευκολύνει την πραγματοποίηση διασυνοριακών πληρωμών εντός της ενιαίας αγοράς. Η PSD1 αποτέλεσε, παράλληλα, σημαντικό θεσμικό συμπλήρωμα της ευρύτερης διαδικασίας δημιουργίας του Ενιαίου Χώρου Πληρωμών σε Ευρώ (SEPA), ο οποίος βασίστηκε σε διακριτό, αλλά συμπληρωματικό κανονιστικό και τεχνικό πλαίσιο (Ortino, 2022).

Ωστόσο, το ρυθμιστικό μοντέλο της PSD1 σχεδιάστηκε σε ένα περιβάλλον, όπου οι ψηφιακές πληρωμές και οι νέες τεχνολογικές μορφές χρηματοπιστωτικής διαμεσολάβησης βρίσκονταν ακόμα σε σχετικά πρώιμο στάδιο. Η ταχεία ανάπτυξη του ηλεκτρονικού εμπορίου, των *fintech* επιχειρήσεων, των ψηφιακών πορτοφολιών και, κυρίως, των υπηρεσιών που βασίζονται στην πρόσβαση σε τραπεζικά δεδομένα ανέδειξε, σταδιακά, τα όρια του ισχύοντος πλαισίου. Η ανάγκη προσαρμογής της ευρωπαϊκής ρύθμισης στις νέες τεχνολογικές και επιχειρηματικές συνθήκες αποτέλεσε, επομένως, έναν από τους βασικούς λόγους που οδήγησαν στην αναθεώρηση της PSD1 και στην υιοθέτηση της PSD2, το 2015.

Η δεύτερη Οδηγία για τις Υπηρεσίες Πληρωμών [PSD2, Οδηγία (ΕΕ) 2015/2366], η οποία άρχισε να εφαρμόζεται το 2018, αναθεώρησε ριζικά το μέχρι τότε υπάρχον ευρωπαϊκό ρυθμιστικό πλαίσιο, καθώς εισήγαγε τρεις, θεμελιακού τύπου, καινοτομίες. Πρώτον, υποχρέωσε τις τράπεζες να παρέχουν, υπό συγκεκριμένες προϋποθέσεις και

με τη ρητή συγκατάθεση του πελάτη, ασφαλή πρόσβαση σε λογαριασμούς και δεδομένα πληρωμών σε αδειοδοτημένους τρίτους παρόχους, μέσω διεπαφών προγραμματισμού εφαρμογών (Application Programming Interfaces – APIs), θέτοντας, έτσι, τα θεμέλια για την ανάπτυξη της ανοιχτής τραπεζικής. Δεύτερον, αναγνώρισε θεσμικά και ρύθμισε δύο νέες κατηγορίες παρόχων, αυτούς των Υπηρεσιών Έναρξης Πληρωμών (Payment Initiation Service Providers – PISPs) και τους Παρόχους Υπηρεσιών Πληροφόρησης Λογαριασμών (Account Information Service Providers – AISPs). Τρίτον, εισήγαγε τη ρήτρα της Ισχυρής Αυθεντικοποίησης Πελάτη (Strong Customer Authentication – SCA), δηλαδή την υποχρέωση χρήσης δύο τουλάχιστον ανεξάρτητων στοιχείων ταυτοποίησης για την πρόσβαση σε ηλεκτρονικές υπηρεσίες και την εκτέλεση ηλεκτρονικών συναλλαγών, με στόχο τον περιορισμό της απάτης και την ενίσχυση της ασφάλειας των ψηφιακών πληρωμών (Gounari et al., 2024). Αυτές οι τρεις καινοτομίες σηματοδότησαν μια ουσιαστική μεταβολή στη δομή του ευρωπαϊκού οικοσυστήματος πληρωμών, μετατοπίζοντάς το από ένα κυρίως τραπεζοκεντρικό μοντέλο προς ένα περισσότερο ανοικτό, ανταγωνιστικό και τεχνολογικά διασυνδεδεμένο περιβάλλον, όπου οι τράπεζες παύουν να αποτελούν τους αποκλειστικούς διαμεσολαβητές της πληρωμής και της χρηματοοικονομικής πληροφορίας.

Η εφαρμογή της PSD2 ανέδειξε, εντούτοις, μια σειρά δομικών αδυναμιών και περιορισμών, οι οποίοι εμπόδισαν την πλήρη αξιοποίηση του μετασχηματιστικού δυναμικού της. Η ανάπτυξη και εφαρμογή των ανοιχτών διεπαφών προγραμματισμού εφαρμογών (APIs) από τα πιστωτικά ιδρύματα υπήρξε ανομοιογενής, με σημαντικές διαφοροποιήσεις ως προς την ποιότητα, τη λειτουργικότητα και την αξιοπιστία των διαθέσιμων υποδομών. Παράλληλα, η εισαγωγή της ρήτρας της Ισχυρής Αυθεντικοποίησης Πελάτη (Strong Customer Authentication – SCA) αποτέλεσε μια σημαντική τομή στην ενίσχυση της ασφάλειας των ηλεκτρονικών συναλλαγών, συνοδεύτηκε, όμως, και από ορισμένες παράπλευρες επιπτώσεις στη διαδικασία πραγματοποίησης της πληρωμής (Peón & Sun, 2025). Η απαίτηση για την επιβεβαίωση της ταυτότητας του χρήστη μέσω περισσότερων του ενός στοιχείων αυθεντικοποίησης πρόσθεσε επιπλέον βήματα και στάδια σε μια διαδικασία που, ιδίως στο ηλεκτρονικό εμπόριο, έχει αποκτήσει ιδιαίτερη σημασία ως προς την ταχύτητα και την ευκολία ολοκλήρωσης. Σε περιπτώσεις όπου η διαδικασία αυθεντικοποίησης αποδεικνύεται σύνθετη, χρονοβόρα ή δεν ολοκληρώνεται επιτυχώς, αυξάνεται

σημαντικά η πιθανότητα εγκατάλειψης της συναλλαγής από τον καταναλωτή. Κατ' αυτόν τον τρόπο, αναδεικνύεται η επιτακτικότητα της επίτευξης της κατάλληλης ισορροπίας μεταξύ της μέγιστης δυνατής ασφάλειας των συναλλαγών και της ανάγκης διατήρησης μιας ομαλής, εύχρηστης και χωρίς περιττές επιβαρύνσεις διαδικασίας πληρωμής.

Ταυτόχρονα, η εφαρμογή της PSD2 ανέδειξε τα όρια μιας ρυθμιστικής προσέγγισης, η οποία σχεδιάστηκε πρωτίστως με βάση τη σχέση μεταξύ τραπεζών, καταναλωτών και αδειοδοτημένων τρίτων παρόχων υπηρεσιών πληρωμών, χωρίς να μπορεί να προβλέψει πλήρως την ταχεία ενίσχυση της παρουσίας των μεγάλων τεχνολογικών πλατφορμών στο οικοσύστημα των πληρωμών. Η ανάπτυξη υπηρεσιών, όπως τα ψηφιακά πορτοφόλια και οι ενσωματωμένες υπηρεσίες πληρωμών, επαναπροσδιορίζουν τη δομή της αγοράς, δεδομένου ότι οι επιχειρήσεις δεν ανταγωνίζονται αποκλειστικά μέσω μιας μεμονωμένης υπηρεσίας πληρωμών, αλλά αξιοποιούν τον έλεγχο που ασκούν σε ευρύτερα ψηφιακά οικοσυστήματα. Η κατοχή και διαχείριση λειτουργικών συστημάτων, ψηφιακών συσκευών, εφαρμογών, πλατφορμών ηλεκτρονικού εμπορίου και μεγάλων βάσεων χρηστών τούς επιτρέπει να ενσωματώνουν τις υπηρεσίες πληρωμών στις ήδη υπάρχουσες ψηφιακές υποδομές τους και να δημιουργούν σημαντικά πλεονεκτήματα κλίμακας και δικτύου.

Η εξέλιξη αυτή δημιουργεί μια διαφορετική μορφή ανταγωνιστικής δυναμικής από εκείνη που επεδίωκε αρχικά να ενισχύσει η PSD2. Η πρόσβαση σε ένα εκτενές δίκτυο χρηστών μπορεί να προσφέρει στις μεγάλες τεχνολογικές πλατφόρμες σημαντικό πλεονέκτημα έναντι μικρότερων παρόχων, ενώ η ενσωμάτωση των υπηρεσιών πληρωμών σε ένα ευρύτερο οικοσύστημα αυξάνει το κόστος μεταπήδησης (switching cost) για επιχειρήσεις και καταναλωτές. Όσο περισσότερες λειτουργίες —όπως πληρωμές, ηλεκτρονικό εμπόριο, διαχείριση δεδομένων, εφαρμογές και υπηρεσίες ταυτοποίησης— συνδέονται μεταξύ τους μέσα στην ίδια την πλατφόρμα, τόσο δυσκολότερη και δαπανηρότερη γίνεται η μετάβαση σε έναν εναλλακτικό πάροχο (Steennot, 2018). Συνεπώς, η ψηφιακή διαμεσολάβηση δεν εξαλείφει, κατ' ανάγκην, τις σχέσεις εξάρτησης που χαρακτήριζαν το παραδοσιακό χρηματοπιστωτικό σύστημα, αλλά τις μετασχηματίζει και τις μεταφέρει σε νέα επίπεδα της ψηφιακής οικονομίας.

Υπό αυτήν την έννοια, η εμπειρία της PSD2 έφερε στην επιφάνεια ένα ευρύτερο ρυθμιστικό δίλημμα, καθώς η ενίσχυση της καινοτομίας και η διευκόλυνση της εισόδου νέων παρόχων στην αγορά δεν αρκούν, εάν δημιουργούνται, παράλληλα, νέες μορφές

συγκέντρωσης οικονομικής και τεχνολογικής ισχύος. Η πρόκληση για το ευρωπαϊκό ρυθμιστικό πλαίσιο δεν αφορά, επομένως, μόνο την προστασία του καταναλωτή και την ασφάλεια των συναλλαγών, αλλά και τη διασφάλιση συνθηκών αποτελεσματικού και διατηρήσιμου ανταγωνισμού σε μια αγορά, όπου η πρόσβαση στα δεδομένα, στις ψηφιακές υποδομές και στα δίκτυα χρηστών αποτελεί πλέον κρίσιμο παράγοντα οικονομικής ισχύος. Οι εν λόγω αδυναμίες της PSD2 συνέβαλαν στην ανάδειξη της ανάγκης για ένα νέο και πιο ολοκληρωμένο κανονιστικό πλαίσιο, ικανό να αντιμετωπίσει όχι μόνο τις τεχνολογικές εξελίξεις στις πληρωμές, αλλά και τις νέες μορφές διαμεσολάβησης, εξάρτησης και συγκέντρωσης ισχύος, οι οποίες αναπτύσσονται στην ψηφιακή οικονομία.

Η τρίτη Οδηγία για τις Υπηρεσίες Πληρωμών (PSD3), σε συνδυασμό με τον προτεινόμενο Κανονισμό για τις Υπηρεσίες Πληρωμών (Payment Services Regulation – PSR) επιχειρούν να αντιμετωπίσουν τις αδυναμίες που ανέδειξε η εφαρμογή της PSD2 και να προσαρμόσουν το ευρωπαϊκό πλαίσιο στις νέες συνθήκες, οι οποίες έχουν διαμορφωθεί στην ψηφιακή αγορά πληρωμών. Σε αντίθεση με την προηγούμενη οδηγία, αυτή η τρίτη, κατά σειρά, ρύθμιση δεν περιορίζεται στην επιπλέον διευκόλυνση της πρόσβασης τρίτων παρόχων στις τραπεζικές υπηρεσίες, αλλά επιχειρεί να αντιμετωπίσει συνολικότερα ζητήματα ανταγωνισμού, ασφάλειας, προστασίας των καταναλωτών και τεχνολογικής διαμεσολάβησης. Μεταξύ των βασικών προτεινόμενων αλλαγών περιλαμβάνονται η ενίσχυση της πρόσβασης και της διαθεσιμότητας δεδομένων στο πλαίσιο της ανοιχτής χρηματοοικονομικής (open finance), η επιπλέον ενίσχυση της ρήτρας της Ισχυρής Αυθεντικοποίησης Πελάτη (SCA), σε συνδυασμό με μέτρα που αποσκοπούν στη μείωση της πιθανότητας εγκατάλειψης της συναλλαγής από τον καταναλωτή, καθώς και η ενδυνάμωση των μηχανισμών πρόληψης και αντιμετώπισης της ηλεκτρονικής απάτης (Kotáb & Martiník, 2025).

Ιδιαίτερη σημασία αποκτά, στο πλαίσιο της τρίτης οδηγίας, η προσπάθεια αντιμετώπισης της αυξανόμενης παρουσίας των μεγάλων τεχνολογικών επιχειρήσεων (BigTech) στην αγορά των πληρωμών. Η οδηγία επιδιώκει να δημιουργήσει πιο ισότιμους όρους ανταγωνισμού μεταξύ τραπεζών, *fintech* επιχειρήσεων και τεχνολογικών πλατφορμών, περιορίζοντας τις δυνατότητες δημιουργίας νέων μορφών συγκέντρωσης και εξάρτησης, οι οποίες προκύπτουν από τον έλεγχο των ψηφιακών υποδομών και οικοσυστημάτων. Παράλληλα, η ενίσχυση της προστασίας των

καταναλωτών έναντι της ηλεκτρονικής απάτης αντανακλά τη μετατόπιση του ρυθμιστικού ενδιαφέροντος από την απλή ασφάλεια της τεχνικής διαδικασίας πληρωμής προς μια ευρύτερη επιδίωξη τόνωσης της ψηφιακής εμπιστοσύνης και της κατανομής των κινδύνων μεταξύ των εμπλεκόμενων φορέων (Kotáb & Martiník, 2025).

Σημαντική θεσμική καινοτομία αποτελεί η επιλογή να συμπληρωθεί η PSD3 από έναν άμεσα εφαρμοστέο Κανονισμό για τις Υπηρεσίες Πληρωμών (Payment Services Regulation - PSR). Η διαφοροποίηση αυτή έχει ιδιαίτερη βαρύτητα, δεδομένου ότι ο συγκεκριμένος Κανονισμός εφαρμόζεται άμεσα και ομοιόμορφα στα κράτη μέλη, περιορίζοντας τις αποκλίσεις που μπορεί να προκύψουν κατά την εθνική μεταφορά μιας Οδηγίας. Κατ' αυτόν τον τρόπο, επιδιώκεται μεγαλύτερη κανονιστική ομοιομορφία και συνεκτικότητα στην Ενιαία Αγορά, μειώνοντας τον κίνδυνο διαφορετικών εθνικών ερμηνειών και εφαρμογών των κανόνων (Wandhöfer, 2025). Η PSD3 και ο PSR συνιστούν, επομένως, όχι απλώς μια τεχνική επικαιροποίηση του ισχύοντος πλαισίου, αλλά μια ευρύτερη προσπάθεια θεσμικής αναδιάρθρωσης της ευρωπαϊκής αγοράς πληρωμών, όπου η ενίσχυση της καινοτομίας και του ανταγωνισμού συνδυάζεται με αυξημένες απαιτήσεις ως προς την ασφάλεια, την προστασία των καταναλωτών και τον περιορισμό νέων μορφών συγκέντρωσης οικονομικής και τεχνολογικής ισχύος.

Τέλος, ο Κανονισμός για τις Άμεσες Πληρωμές (Instant Payments Regulation), Κανονισμός (ΕΕ) 2024/886) αποτελεί μια από τις σπουδαιότερες πρόσφατες ρυθμιστικές εξελίξεις, όσον αφορά το ευρωπαϊκό οικοσύστημα πληρωμών, και παρουσιάζει ιδιαίτερο ενδιαφέρον για το λιανικό εμπόριο. Ο συγκεκριμένος Κανονισμός επιδιώκει να καταστήσει τις άμεσες μεταφορές χρημάτων σε ευρώ ευρύτερα διαθέσιμες, απαιτώντας από τους παρόχους υπηρεσιών πληρωμών που προσφέρουν μεταφορές πίστωσης σε ευρώ να παρέχουν επίσης τη δυνατότητα άμεσων μεταφορών, μέσω των οποίων τα χρήματα καθίστανται διαθέσιμα στον λογαριασμό του δικαιούχου μέσα σε λίγα δευτερόλεπτα, Μάλιστα, ο Κανονισμός προβλέπει ότι η χρέωση για μια άμεση μεταφορά δεν μπορεί να υπερβαίνει τη χρέωση που επιβάλλεται για αντίστοιχη συμβατική μεταφορά πίστωσης (Bruggink, 2026).

Αναφορικά με το λιανικό εμπόριο η ανάπτυξη της δυνατότητας των άμεσων μεταφορών, χωρίς επιπρόσθετο κόστος, ενισχύει και την επέκταση των πληρωμών από λογαριασμό σε λογαριασμό (Account-to-Account – A2A), ως εναλλακτικού

μηχανισμού έναντι των παραδοσιακών πληρωμών με κάρτα. Η δυνατότητα άμεσης μεταφοράς χρημάτων μεταξύ τραπεζικών λογαριασμών επιτρέπει στις επιχειρήσεις να περιορίσουν την εξάρτησή τους από τα παραδοσιακά δίκτυα καρτών και, υπό την προϋπόθεση της ύπαρξης ανταγωνιστικών χρεώσεων από τους παρόχους, να μειώσουν το κόστος αποδοχής ηλεκτρονικών πληρωμών. Η εξέλιξη αυτή καθίσταται, δυνητικά, ιδιαίτερα σημαντική για τις μικρές και πολύ μικρές επιχειρήσεις, στις οποίες ακόμα και σχετικά μικρές προμήθειες ανά συναλλαγή επιφέρουν, λόγω του μεγάλου αριθμού των συναλλαγών, ένα, αθροιστικά, μεγάλο συναλλακτικό κόστος.

Ωστόσο, η αξιοποίηση των δυνατοτήτων που δημιουργεί το νέο πλαίσιο προϋποθέτει την ανάπτυξη των κατάλληλων τεχνολογικών υποδομών, διαλειτουργικών εφαρμογών και εύχρηστων λύσεων, οι οποίες μπορούν να ενσωματωθούν στα πληροφοριακά και εμπορικά συστήματα των επιχειρήσεων. Συνεπώς, η ρυθμιστική διευκόλυνση των άμεσων πληρωμών δεν εξαλείφει από μόνη της τα εμπόδια που συνοδεύουν την υιοθέτηση της ψηφιακής τεχνολογίας. Το ζήτημα της τεχνολογικής και οργανωτικής ικανότητας παραμένει κρίσιμο για τις μικρομεσαίες επιχειρήσεις, καθώς η δυνατότητα αξιοποίησης των νέων υποδομών εξαρτάται, σε σημαντικό βαθμό, από την πρόσβαση σε κατάλληλες και οικονομικά προσιτές ψηφιακές λύσεις.

3.2 Ανταγωνιστικό έλλειμα στην αγορά πληρωμών

Η ανάλυση του ρυθμιστικού πλαισίου δεν μπορεί να αποσυνδεθεί από την εξέταση της ίδιας της δομής της αγοράς πληρωμών, καθώς η αποτελεσματικότητα των ρυθμιστικών παρεμβάσεων εξαρτάται, εν πολλοίς, από τις ανταγωνιστικές συνθήκες, υπό τις οποίες λειτουργούν οι εμπλεκόμενοι φορείς. Παρά τη σταδιακή απελευθέρωση της αγοράς και την είσοδο νέων τραπεζών, *fintech* και τεχνολογικών παρόχων, η αγορά πληρωμών εξακολουθεί να χαρακτηρίζεται από σημαντικές και επίμονες ασυμμετρίες ισχύος. Πρόκειται για μια αγορά, όπου η ύπαρξη μιας, τυπικά, ανοικτής πρόσβασης δεν συνεπάγεται, κατ' ανάγκην, ισότιμους όρους ανταγωνισμού, δεδομένου ότι η οικονομική και τεχνολογική ισχύς κατανέμεται άνισα μεταξύ των διαφορετικών κατηγοριών παρόχων.

Η ιδιαιτερότητα της αγοράς συνδέεται, καταρχάς, με τις εγγενείς ισχυρές εξωτερικές επιδράσεις δικτύου (network effects). Η αξία ενός συστήματος πληρωμών αυξάνεται με τη διεύρυνση του αριθμού των καταναλωτών και των επιχειρήσεων που το

χρησιμοποιούν, καθώς η εκτεταμένη αποδοχή του δημιουργεί πρόσθετα κίνητρα για την ένταξη νέων χρηστών. Η διαδικασία αυτή μπορεί να οδηγήσει σε αυτοενισχυόμενες δυναμικές συγκέντρωσης, με δεδομένο ότι οι ήδη υπάρχοντες πάροχοι διαθέτουν ένα σημαντικό πλεονέκτημα έναντι των νεοεισερχόμενων επιχειρήσεων (Jun, & Yeo,2016). Όσο μεγαλύτερο είναι το δίκτυο ενός παρόχου, τόσο δυσκολότερο καθίσταται για έναν νέο ανταγωνιστή να προσελκύσει, ταυτόχρονα, επαρκή αριθμό καταναλωτών και εμπόρων, ώστε να καταστεί βιώσιμη η εναλλακτική πλατφόρμα του.

Παράλληλα, η αγορά χαρακτηρίζεται από μεγάλα εμπόδια εισόδου, τα οποία δεν περιορίζονται στο αρχικό οικονομικό κόστος ανάπτυξης των υποδομών. Η συμμετοχή στο οικοσύστημα των πληρωμών προϋποθέτει πρόσβαση σε τεχνολογικές υποδομές, κανονιστική συμμόρφωση, μηχανισμούς ασφάλειας και διαχείρισης κινδύνων, όπως και δυνατότητα διασύνδεσης με ένα σύνθετο δίκτυο τραπεζών, παρόχων και τεχνολογικών συστημάτων. Την ίδια στιγμή, η συσσώρευση δεδομένων και η πρόσβαση σε μεγάλες βάσεις χρηστών δημιουργούν πρόσθετα πλεονεκτήματα για τους ήδη εγκατεστημένους παρόχους, ενισχύοντας τη δυνατότητά τους να αναπτύσσουν νέες υπηρεσίες και να διατηρούν τη θέση τους στην αγορά (Bott & Milkau, 2016).

Ιδιαίτερη σημασία έχουν, τέλος, το λεγόμενο κόστος μεταπήδησης (switching costs) και το φαινόμενο του τεχνολογικού εγκλωβισμού (lock-in effects). Σε μια εμπορική επιχείρηση, η επιλογή παρόχου υπηρεσιών πληρωμών ενσωματώνεται, σταδιακά, στις τεχνολογικές, λογιστικές και οργανωτικές διαδικασίες της. Ως εκ τούτου, η αλλαγή παρόχου μπορεί να συνεπάγεται τεχνικές προσαρμογές, κόστος επανεκπαίδευσης, αναδιοργάνωση των πληροφοριακών συστημάτων και, ενδεχομένως, απώλεια της πρόσβασης σε υπηρεσίες ή δεδομένα που συνδέονται με το υπάρχον οικοσύστημα (Staykova & Damsgaard, 2015). Οι παράγοντες αυτοί περιορίζουν την πραγματική δυνατότητα των επιχειρήσεων να μετακινούνται μεταξύ παρόχων και, κατά συνέπεια, μπορούν να αποδυναμώσουν την ανταγωνιστική πίεση, ακόμα και σε μια αγορά όπου, τυπικά, δραστηριοποιούνται πολλοί φορείς.

Το αποτέλεσμα είναι μια αγορά, όπου ο ανταγωνισμός δεν καθορίζεται αποκλειστικά από την τιμή και την ποιότητα της επιμέρους υπηρεσίας πληρωμών, αλλά και από τον έλεγχο των δικτύων, των δεδομένων, των τεχνολογικών υποδομών και των ψηφιακών οικοσυστημάτων. Υπό αυτήν την έννοια, το ανταγωνιστικό έλλειμμα της αγοράς πληρωμών δεν συνίσταται, κατ' ανάγκην, στην απουσία ανταγωνιστών, αλλά στην ύπαρξη δομικών συνθηκών, οι οποίες επιτρέπουν στους ήδη ισχυρούς δρώντες να

διατηρούν και να αναπαράγουν το ανταγωνιστικό τους πλεονέκτημα. Η διάσταση αυτή είναι ιδιαίτερα σημαντική για τις μικρές και πολύ μικρές επιχειρήσεις του λιανικού εμπορίου, οι οποίες, λόγω του περιορισμένου όγκου συναλλαγών, των χαμηλότερων τεχνολογικών δυνατοτήτων και της περιορισμένης διαπραγματευτικής ισχύος τους, είναι πιο εκτεθειμένες στις συνέπειες αυτών των ασυμμετριών.

Σε αυτό το πλαίσιο, η κυριαρχία των δικτύων Visa και Mastercard στην αγορά επεξεργασίας καρτών παραμένει δεσπόζουσα, με το αθροιστικό τους μερίδιο να υπερβαίνει το 90% των συναλλαγών με κάρτα στην ΕΕ (European Court of Auditors, (2025). Αυτή η ολιγοπωλιακή δομή δεν συνιστά απλώς το αποτέλεσμα μιας ανταγωνιστικής υπεροχής, αλλά συνδέεται άρρηκτα με τη φύση της ίδιας της αγοράς, ως αμφίπλευρης πλατφόρμας (two-sided market), καθώς η αξία ενός δικτύου πληρωμών για τον έμπορο εξαρτάται από τον αριθμό των καταναλωτών που το χρησιμοποιούν, δημιουργώντας ισχυρά κίνητρα σύγκλισης γύρω από λίγα επικρατούντα δίκτυα. Όσο περισσότεροι καταναλωτές διαθέτουν και χρησιμοποιούν τις κάρτες ενός συγκεκριμένου δικτύου, τόσο μεγαλύτερο είναι το κίνητρο των εμπόρων να το αποδέχονται. Αντίστοιχα, όσο περισσότερες επιχειρήσεις αποδέχονται το συγκεκριμένο δίκτυο, τόσο μεγαλύτερη γίνεται η χρησιμότητα της κάρτας για τους καταναλωτές.

Η δομή των διατραπεζικών προμηθειών, παρά την επιβολή ανώτατων ορίων, μέσω του Κανονισμού (ΕΕ) 2015/751, εξακολουθεί να αποτελεί σημαντικό πεδίο ασυμμετρίας μεταξύ των επιχειρήσεων που αποδέχονται ηλεκτρονικές πληρωμές. Η ρύθμιση περιόρισε μεν μια βασική συνιστώσα του κόστους των συναλλαγών με κάρτα, δεν εξάλειψε, όμως, τις διαφοροποιήσεις στη διαπραγματευτική θέση των επιχειρήσεων έναντι των παρόχων υπηρεσιών πληρωμών. Οι μεγάλες επιχειρήσεις λιανικής, λόγω του υψηλού όγκου συναλλαγών που πραγματοποιούν και της μεγαλύτερης διαπραγματευτικής ισχύος τους, έχουν τη δυνατότητα να διαπραγματεύονται ευνοϊκότερους εμπορικούς όρους με τους παρόχους υπηρεσιών αποδοχής πληρωμών (acquirers), ενώ οι μικρές και πολύ μικρές επιχειρήσεις αντιμετωπίζουν συχνότερα τυποποιημένα τιμολογιακά σχήματα και διαθέτουν περιορισμένα περιθώρια ουσιαστικής διαπραγμάτευσης. Η διαφορά αυτή δεν αφορά μόνο το ύψος της προμήθειας, αλλά αντανακλά μια ευρύτερη ανισορροπία ως προς τη δυνατότητα των επιχειρήσεων να επηρεάζουν τους όρους, με τους οποίους συμμετέχουν στο οικοσύστημα των ψηφιακών πληρωμών.

Η είσοδος των μεγάλων τεχνολογικών επιχειρήσεων (BigTech) στην αγορά των πληρωμών εισάγει μια νέα διάσταση ανταγωνιστικής ασυμμετρίας, ποιοτικά διαφορετική από εκείνη που χαρακτήριζε τους παραδοσιακούς χρηματοπιστωτικούς και τεχνολογικούς παρόχους. Το συγκριτικό ανταγωνιστικό πλεονέκτημα των *BigTech* αναφέρεται στη δυνατότητά τους να μεταφέρουν την οικονομική, τεχνολογική και πληροφοριακή ισχύ, την οποίαν έχουν ήδη συσσωρεύσει, σε άλλες δραστηριότητες. Εταιρείες, όπως η Apple, η Google, η Amazon και η Meta, διαθέτουν πρόσβαση σε μεγάλες ήδη υπάρχουσες βάσεις χρηστών, εκτεταμένα οικοσυστήματα ψηφιακών υπηρεσιών, σημαντικούς όγκους δεδομένων και υποδομές που τους επιτρέπουν να ενσωματώνουν νέες υπηρεσίες στις ήδη εν ενεργεία πλατφόρμες τους, με ιδιαίτερα χαμηλό οριακό κόστος. Παράλληλα, η δραστηριοποίησή τους σε πολλαπλές αγορές δημιουργεί δυνατότητες αξιοποίησης οικονομιών κλίμακας και φάσματος, καθώς και διασταυρούμενης επιδότησης (cross-subsidization) μεταξύ διαφορετικών επιχειρηματικών δραστηριοτήτων[7]. Κατ' αυτόν τον τρόπο, μια υπηρεσία πληρωμών μπορεί να λειτουργεί όχι μόνον ως αυτοτελής πηγή εσόδων, αλλά και ως μέσον ενίσχυσης της συνολικής θέσης της πλατφόρμας στο ευρύτερο ψηφιακό οικοσύστημα[8].

[7] Η διασταυρούμενη επιδότηση (cross-subsidization) επιτρέπει σε μια μεγάλη τεχνολογική επιχείρηση να χρησιμοποιεί τα έσοδα και τους πόρους που της αποφέρει μια επιχειρηματική δραστηριότητά της για να χρηματοδοτεί, να υποστηρίζει ή να προσφέρει, με ευνοϊκότερους όρους, μια άλλη δραστηριότητά της. Για παράδειγμα, μια *BigTech* μπορεί να διατηρεί χαμηλές ή ακόμα και μηδενικές χρεώσεις σε μια υπηρεσία πληρωμών, επειδή η συγκεκριμένη υπηρεσία ενισχύει την κερδοφορία άλλων δραστηριοτήτων της, όπως η διαφήμιση, το ηλεκτρονικό εμπόριο ή οι υπηρεσίες *cloud*. Με αυτόν τον τρόπο, μια επιχείρηση που δραστηριοποιείται σε πολλές αγορές έχει τη δυνατότητα να ανταγωνιστεί, με πολύ επωφελέστερους όρους, μια τιμολογιακή πολιτική, την οποίαν θα ήταν δυσκολότερο να διατηρήσει ένας εξειδικευμένος πάροχος πληρωμών, δημιουργώντας, έτσι, ένα επιπρόσθετο ανταγωνιστικό πλεονέκτημα.

[8] Χαρακτηριστική είναι η περίπτωση της Apple, η οποία, μέσω του οικοσυστήματος iOS, κατείχε, επί σειρά ετών, ιδιαίτερα ισχυρή θέση ως προς την πρόσβαση στην τεχνολογία NFC που χρησιμοποιείται για τις ανέπαφες πληρωμές. Η δυνατότητα ελέγχου της πρόσβασης στην τεχνολογική υποδομή, η οποία απαιτείται για την πραγματοποίηση μιας πληρωμής μέσω κινητής συσκευής, δημιουργούσε ένα σημαντικό ανταγωνιστικό πλεονέκτημα για την Apple και περιόριζε τη δυνατότητα τρίτων παρόχων να προσφέρουν αντίστοιχες υπηρεσίες στο ίδιο οικοσύστημα (https://ec.europa.eu/commission/presscorner/api/files/document/print/fin/ip_24_3706/IP_24_3706_EN.pdf?utm).

Όσον αφορά τις ελληνικές μικρομεσαίες επιχειρήσεις του λιανικού εμπορίου, αυτές οι ανταγωνιστικές ασυμμετρίες μεταφράζονται σε συγκεκριμένες και, οικονομικά, μετρήσιμες επιβαρύνσεις. Η περιορισμένη διαπραγματευτική ισχύς τους συνεπάγεται υψηλότερο σχετικό κόστος αποδοχής ηλεκτρονικών πληρωμών, περιορισμένη δυνατότητα εξασφάλισης ευνοϊκότερων εμπορικών όρων από τους παρόχους υπηρεσιών αποδοχής πληρωμών (acquirers), όπως και μειωμένη διαπραγματευτική θέση έναντι των παρόχων υπηρεσιών επεξεργασίας πληρωμών (payment processors). Παράλληλα, η αυξανόμενη ενσωμάτωση των πληρωμών στα ευρύτερα πληροφοριακά και τεχνολογικά συστήματα των επιχειρήσεων ενισχύει την εξάρτησή τους από ψηφιακά οικοσυστήματα, των οποίων οι όροι λειτουργίας, τιμολόγησης και πρόσβασης καθορίζονται, σε σημαντικό βαθμό, από ισχυρότερους τεχνολογικούς και χρηματοπιστωτικούς φορείς. Επομένως, το πρόβλημα για τις μικρές επιχειρήσεις δεν αφορά μόνο το άμεσο κόστος των ψηφιακών πληρωμών, αλλά και τη διαμόρφωση μιας σχέσης διαρθρωτικής εξάρτησης από υποδομές και παρόχους που δεν έχουν την οικονομική και τεχνολογική δυνατότητα να επηρεάσουν.

Η κατανόηση αυτών των ασυμμετριών αποτελεί, συνεπώς, αναγκαία προϋπόθεση για τον σχεδιασμό μιας αποτελεσματικής πολιτικής στήριξης των μικρών επιχειρήσεων, στον τομέα των ψηφιακών πληρωμών. Μια τέτοια πολιτική δεν θα πρέπει να περιορίζεται στην ενίσχυση της τεχνολογικής υιοθέτησης, μέσω διαφόρων μορφών επιδότησης για την εγκατάσταση των απαιτούμενων ψηφιακών υποδομών, αλλά να λαμβάνει υπόψη τις συνθήκες ανταγωνισμού και τη διαπραγματευτική θέση των επιχειρήσεων, εντός του ευρύτερου οικοσυστήματος πληρωμών. Η ουσιαστική ψηφιακή μετάβαση αυτών των επιχειρήσεων προϋποθέτει, επομένως, όχι μόνο πρόσβαση στις νέες τεχνολογίες, αλλά και διασφάλιση όρων διαφάνειας, διαλειτουργικότητας και αποτελεσματικού ανταγωνισμού, ώστε η ψηφιοποίηση να μην οδηγεί σε επιπλέον ενίσχυση των ήδη υπαρχουσών οικονομικών και τεχνολογικών εξαρτήσεων.

3.3 Ψηφιακό ευρώ: ευκαιρία ή νέα εξάρτηση;

Μεταξύ των πλέον σημαντικών εξελίξεων στο ευρωπαϊκό τοπίο των πληρωμών συγκαταλέγεται η προώθηση του ψηφιακού ευρώ από την Ευρωπαϊκή Κεντρική Τράπεζα (ΕΚΤ). Το εγχείρημα αυτό, το οποίο βρίσκεται σε διαδικασία θεσμικής και

νομοθετικής διαμόρφωσης, υπερβαίνει τη διάσταση μιας ακόμα τεχνολογικής καινοτομίας στα μέσα πληρωμής. Κατ' ουσίαν, αφορά τον επανασχεδιασμό ενός τμήματος της ίδιας της αρχιτεκτονικής των ευρωπαϊκών πληρωμών και εγείρει θεμελιώδη ερωτήματα σχετικά με το πώς θα οργανωθεί το μελλοντικό οικοσύστημα συναλλαγών, ποιοι φορείς θα ελέγχουν τις κρίσιμες υποδομές του και με ποιους όρους θα αποκτούν πρόσβαση σε αυτές οι επιχειρήσεις και οι καταναλωτές. Στο πλαίσιο αυτό, ιδιαίτερη σημασία αποκτά ο ρόλος που θα διαδραματίσουν οι διαφορετικοί εμπλεκόμενοι φορείς —η ΕΚΤ και οι εθνικές κεντρικές τράπεζες, τα εμπορικά πιστωτικά ιδρύματα, οι πάροχοι υπηρεσιών πληρωμών, οι *fintech* επιχειρήσεις και, κυρίως, οι επιχειρήσεις λιανικής— στη διαμόρφωση και στη λειτουργία του νέου συστήματος.

Η βασική ιδιαιτερότητα του ψηφιακού ευρώ έγκειται στο γεγονός ότι θα αποτελεί ψηφιακή μορφή χρήματος κεντρικής τράπεζας, σε αντίθεση με τα ισχύοντα ηλεκτρονικά μέσα πληρωμής, τα οποία στηρίζονται, κατά κύριο λόγο, σε χρήμα εμπορικών τραπεζών και στις υποδομές ιδιωτικών δικτύων πληρωμών. Υπό αυτήν την έννοια, το ψηφιακό ευρώ μπορεί να περιορίσει την εξάρτηση της ευρωπαϊκής αγοράς από διεθνή σχήματα καρτών και μεγάλες τεχνολογικές πλατφόρμες, δημιουργώντας μια ευρωπαϊκή υποδομή πληρωμών με δημόσιο θεσμικό υπόβαθρο. Η δυνατότητα πραγματοποίησης ψηφιακών συναλλαγών σε ευρώ, χωρίς την αποκλειστική διαμεσολάβηση των ήδη υπαρχόντων ιδιωτικών δικτύων, προβλέπεται ότι θα ενισχύσει τον ανταγωνισμό, θα διευρύνει τις διαθέσιμες επιλογές για τις επιχειρήσεις και τους καταναλωτές και θα συμβάλει στη μείωση του κόστους αποδοχής πληρωμών για τις επιχειρήσεις λιανικής (Cotugno et al., 2024).

Αναφορικά με τις μικρές και πολύ μικρές επιχειρήσεις, η διάσταση αυτή παρουσιάζει ιδιαίτερο ενδιαφέρον. Εάν το ψηφιακό ευρώ συνοδευτεί από ανοικτές, διαλειτουργικές και οικονομικά προσιτές υποδομές, θα μπορούσε να προσφέρει μια εναλλακτική οδό πρόσβασης σε ψηφιακές πληρωμές, περιορίζοντας την εξάρτηση από ιδιωτικά δίκτυα και παρόχους με ισχυρή διαπραγματευτική θέση. Παράλληλα, η δυνατότητα άμεσων πληρωμών από λογαριασμό σε λογαριασμό θα μπορούσε να ενισχύσει ακόμα περσσότερο την ανάπτυξη λύσεων A2A και να δημιουργήσει νέες δυνατότητες ανταγωνισμού έναντι των παραδοσιακών σχημάτων πληρωμών με κάρτα.

Ωστόσο, η εισαγωγή μιας δημόσιας ψηφιακής υποδομής δεν εξαλείφει αυτομάτως τις ισχύουσες σχέσεις εξάρτησης, καθώς ενδέχεται, υπό διαφορετικές θεσμικές συνθήκες,

να δημιουργήσει νέες, εντονότερες ασσυμετρίες ισχύος. Η λειτουργία του ψηφιακού ευρώ θα απαιτεί τη συμμετοχή ενδιάμεσων φορέων, την ανάπτυξη τεχνολογικών υποδομών και την ενσωμάτωσή του στα ήδη υπάρχοντα πληροφοριακά και εμπορικά συστήματα των επιχειρήσεων. Επομένως, κρίσιμο ζήτημα δεν συνιστά μόνο το γεγονός ποιος κατέχει το εκδοτικό προνομιο, αλλά και ποιος ελέγχει τα επίπεδα της τεχνολογικής και εμπορικής υποδομής, μέσω των οποίων αυτό χρησιμοποιείται στην καθημερινή συναλλαγή. Εάν η πρόσβαση των επιχειρήσεων στο νέο σύστημα εξαρτηθεί υπερβολικά από περιορισμένο αριθμό παρόχων τεχνολογικών υπηρεσιών, τραπεζών ή ψηφιακών πλατφορμών, ελλοχεύει το ενδεχόμενο να αναπαραχθούν, υπό διαφορετική μορφή, ορισμένες από τις ασυμμετρίες που χαρακτηρίζουν ήδη την αγορά των ψηφιακών πληρωμών.

Η εξέλιξη αυτή αναδεικνύει, επομένως, ένα κρίσιμο θεσμικό δίλημμα. Το ψηφιακό ευρώ μπορεί να αποτελέσει εργαλείο ενίσχυσης της ευρωπαϊκής στρατηγικής αυτονομίας, της ανταγωνιστικότητας και της ανθεκτικότητας του συστήματος πληρωμών, αλλά η επίτευξη αυτών των στόχων εξαρτάται από τον τρόπο, με τον οποίον θα σχεδιαστεί και θα εφαρμοστεί η σχετική υποδομή. Όσον αφορά τις επιχειρήσεις λιανικής, και ιδιαίτερα τις μικρομεσαίες επιχειρήσεις, το κομβκό ζήτημα συνίσταται στους όρους, υπό τους οποίους θα αποκτούν πρόσβαση σε αυτό, το κόστος αποδοχής του, η διαλειτουργικότητά του με τα ήδη υπάρχοντα συστήματα και η δυνατότητα εναλλαγής μεταξύ διαφορετικών παρόχων, χωρίς σημαντικό κόστος μεταπήδησης. Η θεσμική αρχιτεκτονική του ψηφιακού ευρώ θα καθορίσει, συνεπώς, σε σημαντικό βαθμό, εάν η νέα υποδομή θα λειτουργήσει ως πραγματικό εργαλείο διεύρυνσης του ανταγωνισμού ή εάν θα αποτελέσει, απλώς, ένα νέο επίπεδο διαμεσολάβησης, μέσα σε ένα ήδη συγκεντρωμένο ψηφιακό οικοσύστημα.

Για την ΕΣΕΕ και τις επιχειρήσεις που εκπροσωπεί, η συζήτηση για το ψηφιακό ευρώ δεν θα πρέπει να αποτελεί αποκλειστικά και μόνο μια τεχνολογική και χρηματοπιστωτική εξέλιξη νομοτελειακού τύπου, αλλά ένα κρίσιμο πεδίο θεσμικής και πολιτικής παρέμβασης. Η διαμόρφωση του νέου οικοσυστήματος πληρωμών θα πρέπει να λαμβάνει υπόψη τις ιδιαίτερες δυνατότητες και τους περιορισμούς των μικρών και πολύ μικρών επιχειρήσεων, ώστε η υιοθέτηση του ψηφιακού ευρώ να μην εξελιχθεί σε έναν επιπλέον παράγοντα αύξησης του λειτουργικού και τεχνολογικού τους κόστους. Στο πλαίσιο αυτό, ιδιαίτερη βαρύτητα αποκτούν η διασφάλιση εύλογων και αναλογικών τεχνολογικών απαιτήσεων για την αποδοχή του ψηφιακού ευρώ, η

πρόβλεψη κατάλληλων περιόδων προσαρμογής και, όπου απαιτείται, ειδικών μεταβατικών ρυθμίσεων για τις πολύ μικρές επιχειρήσεις, όπως επίσης και η διαμόρφωση ενός πλαισίου χρεώσεων που θα διασφαλίζει ότι το κόστος των συναλλαγών παραμένει ανταγωνιστικό και αναλογικό προς τις δυνατότητες των επιχειρήσεων.

Από την οπτική αυτή, η συμμετοχή της ΕΣΕΕ στη σχετική ευρωπαϊκή και εθνική διαβούλευση είναι κρίσιμη, καθώς η αρχιτεκτονική του ψηφιακού ευρώ θα επηρεάσει άμεσα τους όρους με τους οποίους οι επιχειρήσεις λιανικής θα εντάσσονται στο νέο σύστημα. Η βασική επιδίωξη δεν θα πρέπει να είναι, απλώς, η καθολική υιοθέτηση μιας νέας τεχνολογίας, αλλά η διασφάλιση ότι αυτή θα πραγματοποιηθεί υπό την προϋπόθεση της οικονομικής βιωσιμότητας, της τεχνολογικής προσβασιμότητας, της διαλειτουργικότητας και του αποτελεσματικού ανταγωνισμού.

3.4 Χρηματοοικονομικός αποκλεισμός και ψηφιακές πληρωμές

Η συζήτηση για την προώθηση των ψηφιακών πληρωμών και τη σταδιακή υποχώρηση της χρήσης των μετρητών συχνά παραβλέπει τον κίνδυνο του ενδεχόμενου χρηματοοικονομικού αποκλεισμού ομάδων του πληθυσμού, οι οποίες δεν διαθέτουν την ίδια δυνατότητα πρόσβασης στις ψηφιακές υποδομές, τις τεχνολογικές δεξιότητες και τους οικονομικούς πόρους που απαιτεί η συμμετοχή στο νέο περιβάλλον των ψηφιακών συναλλαγών. Υπό τις υπάρχουσες συνθήκες της επιταχυνόμενης ψηφιοποίησης, η δυνατότητα πραγματοποίησης μιας καθημερινής εμπορικής συναλλαγής παύει, σταδιακά, να αποτελεί αυτονόητη δυνατότητα για όλους και εξαρτάται ολοένα και περισσότερο από την κατοχή της κατάλληλης συσκευής, την πρόσβαση σε τραπεζικό λογαριασμό, τη σύνδεση στο διαδίκτυο και την ικανότητα χρήσης σύνθετων ψηφιακών εφαρμογών.

Ο κίνδυνος του αποκλεισμού συνιστά δομικό αποτέλεσμα μιας διαδικασίας ψηφιακού μετασχηματισμού, η οποία δεν λαμβάνει επαρκώς υπόψη τις σημαντικές διαφοροποιήσεις που υπάρχουν ως προς την πρόσβαση, τις δεξιότητες και την ικανότητα προσαρμογής των διαφορετικών κοινωνικών ομάδων. Οι ηλικιωμένοι, τα άτομα με χαμηλό εισόδημα, οι κάτοικοι περιοχών με ανεπαρκείς ψηφιακές και

τραπεζικές υποδομές, καθώς και τα πρόσωπα με περιορισμένη ψηφιακή και χρηματοοικονομική παιδεία ενδέχεται να αντιμετωπίσουν δυσανάλογες δυσκολίες συμμετοχής σε ένα σύστημα, όπου οι ηλεκτρονικές συναλλαγές καθίστανται, βαθμιαία, η κυρίαρχη διαθέσιμη μορφή πληρωμής.

Σε αυτό το πλαίσιο, ο χρηματοοικονομικός αποκλεισμός αναφέρεται στην αντικειμενική αδυναμία ενός ατόμου να συμμετέχει ισότιμα στην οικονομική και εμπορική ζωή, επειδή στερείται των τεχνολογικών, οικονομικών και γνωστικών προϋποθέσεων, τις οποίες απαιτεί η χρήση των σύγχρονων μέσων πληρωμής. Η μετάβαση στις ψηφιακές πληρωμές ενδέχεται, επομένως, να διευρύνει τις ήδη υπάρχουσες, κοινωνικές ανισότητες, εάν δεν συνοδεύεται από πολιτικές ψηφιακής και χρηματοοικονομικής ένταξης, καθώς και από τη διατήρηση εναλλακτικών και προσβάσιμων μέσων συναλλαγής.

Η νομική διάσταση του ζητήματος αναδεικνύεται μέσα από την έννοια του «νόμιμου χρήματος» (legal tender). Εφόσον τα τραπεζογραμμάτια και τα νομίσματα σε ευρώ αποτελούν νόμιμο χρήμα, η αποδοχή τους συνδέεται, καταρχήν, με την υποχρέωση εξόφλησης χρηματικών οφειλών, γεγονός που προσδίδει ιδιαίτερη σημασία στην πρακτική των επιχειρήσεων που αρνούνται την πληρωμή με μετρητά. Η αρχή αυτή, ωστόσο, δεν συνεπάγεται ότι η αποδοχή μετρητών είναι απολύτως ανεξαίρετη σε κάθε δυνατή συναλλαγή, καθώς οι περιορισμοί ή οι εξαιρέσεις μπορούν, υπό συγκεκριμένες προϋποθέσεις, να προβλέπονται από το ισχύον νομικό πλαίσιο (Indrawati, 2023).

Η Ευρωπαϊκή Επιτροπή, με τη Σύσταση 2022/C 244/04, η οποία αναγνωρίζει τα μετρητά σε ευρώ ως νόμιμο χρήμα, επιβεβαίωσε την ιδιαίτερη θεσμική σημασία της ιδιότητας αυτής. Ειδικότερα, η απόκλιση από την, καταρχήν, υποχρέωση αποδοχής μετρητών δεν μπορεί να αντιμετωπίζεται ως αυθαίρετη επιχειρηματική επιλογή, αλλά απαιτεί επαρκή νομική βάση και τήρηση των προϋποθέσεων, τις οποίες θέτει το ευρωπαϊκό και το εθνικό δίκαιο. Υπό αυτήν την έννοια, μια γενικευμένη πολιτική άρνησης των μετρητών από επιχειρήσεις, χωρίς σαφές νομικό έρεισμα, εγείρει ζητήματα συμβατότητας με τον θεσμικό ρόλο του ευρώ, ως κοινού νομίσματος και νόμιμου χρήματος της Ευρωζώνης[9].

[9] Η πρακτική εφαρμογή αυτής της αρχής παραμένει, ωστόσο, σύνθετη. Η ταχεία εξάπλωση των ηλεκτρονικών πληρωμών και η αυξανόμενη υιοθέτηση επιχειρηματικών πρακτικών «μηδενικής αποδοχής της χρήσης μετρητών» σε ορισμένους κλάδους δημιουργούν μια προοδευτική απόκλιση

Για τις επιχειρήσεις του λιανικού εμπορίου, η διάσταση αυτή έχει άμεσες επιχειρηματικές προεκτάσεις. Η πλήρης εγκατάλειψη των μετρητών, ως μέσου πληρωμής, μπορεί να οδηγήσει, πρακτικά, στον αποκλεισμό ενός τμήματος της δυνητικής πελατειακής βάσης, περιορίζοντας την πρόσβαση ορισμένων καταναλωτών στην αγορά. Σε κοινωνίες με υψηλό ποσοστό ηλικιωμένων —όπως η ελληνική, η οποία συγκαταλέγεται στις πλέον γηράσκουσες χώρες της ΕΕ—τα μετρητά εξακολουθούν να αποτελούν το οικειότερο, απλούστερο και πλέον προσιτό μέσον συναλλαγής. Επομένως, η διατήρηση της δυνατότητας πληρωμής με μετρητά δεν αποτελεί, απλώς, ζήτημα κοινωνικής ευαισθησίας και κανονιστικής συμμόρφωσης, αλλά συνδέεται επίσης με τη διατήρηση της εμπορικής προσβασιμότητας των επιχειρήσεων σε ένα ευρύτερο φάσμα καταναλωτών. Η αναζήτηση ισορροπίας μεταξύ της ψηφιακής μετάβασης και της κοινωνικής συμπερίληψης συνιστά, υπό αυτήν την έννοια, όχι μόνο ζήτημα δημόσιας πολιτικής, αλλά και μια συγκεκριμένη επιχειρηματική πρόκληση που οι έμποροι καλούνται να διαχειριστούν.

Η ανάλυση των παραπάνω ζητημάτων δημόσιας πολιτικής αναδεικνύει έναν κοινό παρονομαστή: η μετάβαση στις ψηφιακές πληρωμές δεν αποτελεί μια τεχνολογικά ουδέτερη και αμιγώς τεχνική διαδικασία. Αντίθετα, συνιστά μια βαθιά οικονομική, θεσμική και πολιτική μεταβολή με σημαντικές διανεμητικές συνέπειες, οι οποίες αφορούν τη διάρθρωση και τον ανταγωνισμό στην αγορά πληρωμών, τη θέση και τη διαπραγματευτική ισχύ των μικρομεσαίων επιχειρήσεων, την πρόσβαση των καταναλωτών στις βασικές υπηρεσίες συναλλαγών, καθώς και τον βαθμό ελέγχου επί των κρίσιμων ψηφιακών υποδομών. Οι επιλογές που γίνονται ως προς τον σχεδιασμό, τη ρύθμιση και την ανάπτυξη του συστήματος των ψηφιακών πληρωμών καθορίζουν, επομένως, όχι μόνο την αποτελεσματικότητα και την ταχύτητα των συναλλαγών, αλλά και το ποιοι συμμετέχουν, με ποιους όρους και υπό ποιες σχέσεις εξάρτησης στο νέο ψηφιακό οικοσύστημα.

μεταξύ της νομικής κατοχύρωσης των μετρητών και της πραγματικής δυνατότητας χρήσης τους στην καθημερινή οικονομική ζωή. Η εξέλιξη αυτή αποκτά βαρύνουσα σημασία, καθώς ο περιορισμός της αποδοχής μετρητών μπορεί να πλήξει, δυσανάλογα, τα τμήματα του πληθυσμού που εξαρτώνται περισσότερο από αυτά. Επομένως, η διατήρηση της πραγματικής δυνατότητας πληρωμής με μετρητά δεν αποτελεί μόνο ζήτημα προστασίας ενός παραδοσιακού μέσου συναλλαγής, αλλά συνδέεται άμεσα με την πρόληψη του χρηματοοικονομικού αποκλεισμού και τη διασφάλιση της καθολικής πρόσβασης στην οικονομική και εμπορική δραστηριότητα.

Υπό αυτήν την οπτική, η πολιτική για τις ψηφιακές πληρωμές είναι αναπόσπαστα συνδεδεμένη με την ευρύτερη στρατηγική για τον ψηφιακό μετασχηματισμό του λιανικού εμπορίου. Μια επιτυχής μετάβαση δεν μπορεί να αποτιμηθεί αποκλειστικά με βάση την αύξηση του αριθμού των ηλεκτρονικών συναλλαγών ούτε με την ταυτόχρονη υποχώρηση της χρήσης μετρητών. Προϋποθέτει τη διαμόρφωση ενός συστήματος που θα ενισχύει συγχρόνως τον ανταγωνισμό, θα περιορίζει τις ασυμμετρίες ισχύος, θα διασφαλίζει την ισότιμη πρόσβαση των μικρομεσαίων επιχειρήσεων στις νέες υποδομές και θα προστατεύει τους καταναλωτές από νέες μορφές αποκλεισμού. Η ψηφιακή μετάβαση του λιανικού εμπορίου αποκτά, συνεπώς, ουσιαστικό κοινωνικό και αναπτυξιακό περιεχόμενο, μόνον όταν συνδυάζεται με την οικονομική βιωσιμότητα των επιχειρήσεων, την κοινωνική συμπερίληψη και τη διατήρηση της δυνατότητας πραγματικής επιλογής για όλους τους συμμετέχοντες στην αγορά.

4. Κυβερνοασφάλεια και λιανικό εμπόριο: το νέο τοπίο των απειλών

4.1 Η κυβερνοασφάλεια ως δομικό χαρακτηριστικό της ψηφιακής αγοράς

Η κυβερνοασφάλεια δεν αποτελεί, πλέον, ένα παρεπόμενο ζήτημα τεχνικής διαχείρισης, περιορισμένο στην αρμοδιότητα των εξειδικευμένων τμημάτων πληροφορικής. Αντιθέτως, αναδεικνύεται σε μια κρίσιμη διάσταση της επιχειρηματικής στρατηγικής, της κανονιστικής συμμόρφωσης και της εύρυθμης λειτουργίας της ψηφιακής οικονομίας. Η μετατόπιση αυτή δεν είναι ούτε συγκυριακή ούτε τυχαία. Αποτελεί δομική συνέπεια της ίδιας της διαδικασίας του ψηφιακού μετασχηματισμού, η οποία, αφενός, διευρύνει διαρκώς την έκθεση των επιχειρήσεων σε κυβερνοαπειλές και, αφετέρου, αυξάνει την εξάρτηση της οικονομικής και κοινωνικής δραστηριότητας από ψηφιακές υποδομές, πληροφοριακά συστήματα και δικτυακές υπηρεσίες. Καθώς όλο και περισσότερες κρίσιμες λειτουργίες —από τις πληρωμές και την επικοινωνία έως την εφοδιαστική αλυσίδα και τη διαχείριση δεδομένων— μεταφέρονται στο ψηφιακό περιβάλλον, μια κυβερνοεπίθεση μπορεί να υπερβεί το επίπεδο της μεμονωμένης τεχνικής δυσλειτουργίας και να προκαλέσει σοβαρές οικονομικές απώλειες, επιχειρησιακές διακοπές και διατάραξη της εμπιστοσύνης στην ίδια τη λειτουργία της αγοράς.

Το λιανικό εμπόριο κατέχει πρωτεύουσα θέση στο σύγχρονο τοπίο των κυβερνοαπειλών, για λόγους που συνδέονται όχι μόνο με το μέγεθος του κλάδου, αλλά, κυρίως, με τα δομικά χαρακτηριστικά της λειτουργίας του. Ο μεγάλος αριθμός των συναλλαγών, η συνεχής επεξεργασία δεδομένων πληρωμών και των προσωπικών δεδομένων των καταναλωτών, η εκτεταμένη εξάρτηση από πληροφοριακά συστήματα και ψηφιακές υποδομές, καθώς και η διασύνδεση των επιχειρήσεων με πλήθος τρίτων παρόχων τεχνολογικών υπηρεσιών δημιουργούν ένα ιδιαίτερα σύνθετο και εκτεταμένο πεδίο έκθεσης σε κυβερνοκινδύνους (Rajgopal, 2025). Η προσβολή ενός συστήματος λιανικής μπορεί να αποφέρει άμεσο οικονομικό όφελος, μέσω της υποκλοπής στοιχείων πληρωμών, της παράνομης μεταφοράς κεφαλαίων, ακόμα και επιθέσεων εκβιασμού, ενώ, παράλληλα, μπορεί να εξασφαλίσει πρόσβαση σε μεγάλους όγκους

προσωπικών και εμπορικών δεδομένων. Τα δεδομένα αυτά ενδέχεται να αξιοποιηθούν, στη συνέχεια, για την οργάνωση ευρύτερων εκστρατειών ηλεκτρονικής απάτης, κλοπής ταυτότητας, ακόμα και στοχευμένων επιθέσεων κοινωνικής μηχανικής (social engineering), κατά τις οποίες οι επιτιθέμενοι εκμεταλλεύονται προσωπικές ή επιχειρηματικές πληροφορίες, προκειμένου να εξατομικεύσουν την εξαπάτηση και να παρακινήσουν συγκεκριμένα άτομα στην αποκάλυψη ευαίσθητων δεδομένων ή στην εκτέλεση μη ασφαλών ενεργειών (ENISA, 2024). Υπό αυτήν την έννοια, η κυβερνοεπίθεση κατά μιας εμπορικής επιχείρησης δεν αφορά, πλέον, αποκλειστικά την ίδια, αλλά μπορεί να λειτουργήσει ως αφετηρία για την έκθεση καταναλωτών, προμηθευτών και άλλων συνδεδεμένων φορέων σε ευρύτερους κινδύνους, γεγονός που αναδεικνύει τον λιανικό κλάδο σε κρίσιμο κόμβο της συνολικής ψηφιακής ασφάλειας της οικονομίας.

Η σύνδεση μεταξύ των ψηφιακών πληρωμών και της κυβερνοασφάλειας είναι, υπό αυτό το πρίσμα, όχι συμπτωματική, αλλά δομική. Κάθε ψηφιακή συναλλαγή προϋποθέτει τη δημιουργία, διαβίβαση, επεξεργασία και, σε διαφορετικά στάδια, αποθήκευση δεδομένων —δεδομένων πληρωμής, δεδομένων ταυτοποίησης και δεδομένων που μπορούν να αποτυπώνουν τη συναλλακτική και καταναλωτική συμπεριφορά. Σε αυτό το πλαίσιο, η ψηφιακή επέκταση του λιανικού εμπορίου δεν διευρύνει μόνο τις δυνατότητες εξυπηρέτησης των καταναλωτών και πραγματοποίησης των συναλλαγών, αλλά και την επιφάνεια επίθεσης (attack surface), στην οποίαν εκτίθενται οι επιχειρήσεις. Κάθε πρόσθετο ψηφιακό κανάλι, διασυνδεδεμένο πληροφοριακό σύστημα, εφαρμογή, τερματικό ή εξωτερικός πάροχος δημιουργούν ένα νέο σημείο δυνητικής εισόδου για κυβερνοεπιθέσεις, ιδίως, όταν οι διαφορετικές υποδομές συνδέονται μεταξύ τους και διαμορφώνουν σύνθετες αλυσίδες τεχνολογικής εξάρτησης (Rajgopal, 2025). Η σχέση μεταξύ ψηφιοποίησης και κυβερνοκινδύνου δεν είναι, συνεπώς, απλώς ποσοτική, αλλά αφορά την αυξανόμενη πολυπλοκότητα και διασυνδεσιμότητα του ψηφιακού οικοσυστήματος, μέσα στο οποίο πραγματοποιείται η εμπορική συναλλαγή.

Η εξέλιξη των κυβερνοαπειλών, κατά την τελευταία δεκαετία, αποτυπώνει μια θεμελιώδη μεταβολή στη φύση και στην οργάνωση του κυβερνοεγκλήματος, από σχετικά αποσπασματικές και περιορισμένης τεχνικής εμβέλειας επιθέσεις προς ολοένα και περισσότερες οργανωμένες, επαγγελματικές και οικονομικά προσανατολισμένες δραστηριότητες Ο σύγχρονος κυβερνοεγκληματίας που στοχεύει το λιανικό εμπόριο

δεν δρα, κατ' ανάγκην, ως μεμονωμένος, τεχνικά καταρτισμένος δράστης, αλλά, συχνά, εντάσσεται σε ευρύτερα οργανωμένα δίκτυα, όπου η ανάπτυξη, η διάθεση και η εκτέλεση των επιθέσεων πραγματοποιούνται μέσω εξειδικευμένης κατανομής ρόλων. Η εξέλιξη αυτή έχει οδηγήσει στη διαμόρφωση μιας διεθνοποιημένης αγοράς παράνομων ψηφιακών υπηρεσιών, γνωστής ως «Έγκλημα υπό μορφήν Υπηρεσίας» (Crime-as-a-Service – CaaS), μέσω της οποίας διατίθενται σε τρίτους έτοιμα εργαλεία, υποδομές και υπηρεσίες για την πραγματοποίηση κυβερνοεπιθέσεων (Huang et al., 2017).

Η ανάπτυξη αυτού του είδους παράνομων δραστηριοτήτων μεταβάλλει ουσιαστικά τα οικονομικά και τεχνολογικά χαρακτηριστικά του κυβερνοεγκλήματος. Εργαλεία και υπηρεσίες, που, στο παρελθόν, απαιτούσαν σημαντική τεχνική εξειδίκευση, μπορούν, πλέον, να αποκτηθούν έναντι αμοιβής και να χρησιμοποιηθούν από δράστες με περιορισμένες τεχνικές γνώσεις. Η διάθεση *ransomware-as-a-service*, υπηρεσιών υποκλοπής διαπιστευτηρίων, εργαλείων *phishing* και άλλων μορφών κακόβουλου λογισμικού μειώνει το κόστος και τα τεχνικά εμπόδια εισόδου στην παράνομη δραστηριότητα, διευρύνοντας σημαντικά τον αριθμό των δυνητικών δραστών[10]. Παράλληλα, η εξειδίκευση των εγκληματικών δικτύων επιτρέπει την κατανομή της δραστηριότητας σε επιμέρους λειτουργίες, όπως η ανάπτυξη λογισμικού, η απόκτηση πρόσβασης σε πληροφοριακά συστήματα, η κλοπή και εμπορία δεδομένων και η εκβίαση των θυμάτων.

[10] Το *Ransomware-as-a-Service* (RaaS) είναι ένα μοντέλο, όπου ομάδες κυβερνοεγκληματιών αναπτύσσουν το *ransomware* και το διαθέτουν σε άλλους δράστες ως υπηρεσία. Ο «πελάτης» δεν χρειάζεται να γνωρίζει πώς να δημιουργήσει το κακόβουλο λογισμικό, καθώς χρησιμοποιεί την έτοιμη υποδομή, προκειμένου να κρυπτογραφήσει αρχεία και να αποκτήσει πρόσβαση σε συστήματα. Οι υπηρεσίες υποκλοπής διαπιστευτηρίων αφορούν εργαλεία που χρησιμοποιούνται για την κλοπή κωδικών πρόσβασης, στοιχείων σύνδεσης και άλλων δεδομένων ταυτοποίησης, τα οποία μπορούν, στη συνέχεια, να χρησιμοποιηθούν για παράνομη πρόσβαση σε λογαριασμούς και πληροφοριακά συστήματα. Τα εργαλεία *phishing* είναι έτοιμες εφαρμογές και υποδομές, οι οποίες διευκολύνουν την εξαπάτηση χρηστών, συνήθως, μέσω πλαστών μηνυμάτων, ιστοσελίδων ή ηλεκτρονικών επικοινωνιών που εμφανίζονται ως νόμιμες, με σκοπό την απόκτηση ευαίσθητων πληροφοριών. Το κοινό χαρακτηριστικό όλων αυτών είναι ότι μετατρέπουν το κυβερνοέγκλημα σε υπηρεσία, η οποία μπορεί να αγοραστεί, μειώνοντας σημαντικά το τεχνικό και οικονομικό κόστος εισόδου για νέους δράστες (Rajgopal, 2025) .

Όσον αφορά το λιανικό εμπόριο, η εξέλιξη αυτή είναι εξαιρετικά σημαντική, καθώς οι επιχειρήσεις διαθέτουν ένα ευρύ σύνολο ψηφιακών σημείων, τα οποία μπορούν να αποτελέσουν στόχο, από τα συστήματα ηλεκτρονικών πληρωμών και τα πληροφοριακά συστήματα έως τις πλατφόρμες ηλεκτρονικού εμπορίου, τα τερματικά POS και τις συνδεδεμένες υποδομές τρίτων παρόχων. Η επαγγελματοποίηση του κυβερνοεγκλήματος σημαίνει, συνεπώς, ότι η έκθεση μιας επιχείρησης σε κυβερνοεπίθεση δεν εξαρτάται, πλέον, αποκλειστικά από το εάν αποτελεί έναν «ελκυστικό» μεμονωμένο στόχο. Η επίθεση μπορεί να πραγματοποιείται αυτοματοποιημένα και μαζικά, με τη χρήση κοινών εργαλείων και υπηρεσιών που επιτρέπουν στους δράστες να στοχοποιούν, ταυτόχρονα, μεγάλο αριθμό επιχειρήσεων.

Συνεπώς, η κυβερνοασφάλεια δεν αφορά, πλέον, μόνο την προστασία μιας επιχείρησης από μεμονωμένες επιθέσεις, αλλά την ικανότητά της να λειτουργεί σε ένα περιβάλλον, όπου η πρόσβαση σε τεχνολογικά εργαλεία επίθεσης είναι ευκολότερη, φθηνότερη και ευρύτερα διαθέσιμη. Η εξέλιξη αυτή καθιστά την πρόληψη, την έγκαιρη ανίχνευση, την επιχειρησιακή συνέχεια και την ταχεία ανάκαμψη από περιστατικά κυβερνοασφάλειας αναπόσπαστα στοιχεία της συνολικής επιχειρηματικής ανθεκτικότητας.

4.2 Η τυπολογία των κυβερνοεπιθέσεων στο λιανικό εμπόριο

Η κατανόηση του τοπίου κυβερνοαπειλών, στον κλάδο του λιανικού εμπορίου, προϋποθέτει τη συστηματική τυπολογία των κύριων μορφών επίθεσης, οι οποίες πρέπει να αναλυθούν ως προς τον τρόπο λειτουργίας τους, τους στόχους τους και τις επιπτώσεις τους στις επιχειρήσεις.

Ηλεκτρονικό ψάρεμα (Phishing): Το *phishing* αποτελεί, διαχρονικά, μια από τις πλέον διαδεδομένες μορφές κυβερνοεπίθεσης, τόσο λόγω της σχετικά χαμηλής τεχνικής πολυπλοκότητάς του όσο και εξαιτίας της υψηλής αποτελεσματικότητάς του. Βασίζεται στην εξαπάτηση των χρηστών, με στόχο να αποκαλύψουν διαπιστευτήρια πρόσβασης, οικονομικά δεδομένα ή άλλες εμπιστευτικές πληροφορίες, μέσω πλαστών και παραπλανητικά διαμορφωμένων επικοινωνιών —όπως ηλεκτρονικά μηνύματα, ιστοτόπους ή μηνύματα κειμένου— που εμφανίζονται ως προερχόμενες από αξιόπιστες και νόμιμες πηγές. Στο λιανικό εμπόριο, οι επιθέσεις *phishing* μπορούν να στοχεύουν

τόσο τους εργαζομένους των επιχειρήσεων, με σκοπό την απόκτηση πρόσβασης σε εσωτερικά πληροφοριακά συστήματα, πλατφόρμες πληρωμών και υποδομές POS, όσο και απευθείας τους καταναλωτές, μέσω πλαστών ηλεκτρονικών καταστημάτων, ψευδών ειδοποιήσεων για την αποστολή ή παράδοση δεμάτων και εξατομικευμένων εκστρατειών *spear phishing*, οι οποίες αξιοποιούν διαθέσιμα προσωπικά ή συναλλακτικά δεδομένα. Η ταχεία ανάπτυξη της Τεχνητής Νοημοσύνης ενισχύει ακόμα περισσότερο αυτή την απειλή, καθώς παρέχει στους κυβερνοεγκληματίες τη δυνατότητα δημιουργίας ιδιαίτερα ρεαλιστικών, γλωσσικά άρτιων και εξατομικευμένων μηνυμάτων εξαπάτησης σε μεγάλη κλίμακα (Joshi & Akhilesh, 2019). Κατά συνέπεια, η διάκριση μεταξύ νόμιμης και κακόβουλης επικοινωνίας καθίσταται ολοένα και δυσκολότερη, περιορίζοντας την αποτελεσματικότητα των παραδοσιακών πρακτικών αναγνώρισης του *phishing* και καθιστώντας αναγκαία την ενίσχυση τόσο των τεχνολογικών μηχανισμών προστασίας όσο και της ψηφιακής και οργανωσιακής εγρήγορσης των επιχειρήσεων και των χρηστών.

Κακόβουλο λογισμικό εκβιασμού (Ransomware): Το *ransomware* αποτελεί μια από τις σοβαρότερες μορφές κυβερνοεπίθεσης για τις επιχειρήσεις λιανικής, καθώς μπορεί να προκαλέσει, ταυτόχρονα, άμεσες οικονομικές απώλειες, διακοπή της επιχειρησιακής λειτουργίας και σημαντικές επιπτώσεις στη φήμη του καταστήματος και στην εμπιστοσύνη των πελατών. Η επίθεση βασίζεται στην απόκτηση μη εξουσιοδοτημένης πρόσβασης σε πληροφοριακά συστήματα, στην κρυπτογράφηση δεδομένων και στην παρεμπόδιση της πρόσβασης σε κρίσιμες επιχειρησιακές λειτουργίες, με τους δράστες να απαιτούν, στη συνέχεια, την καταβολή λύτρων για την αποκατάσταση της πρόσβασης. Στη σύγχρονη μορφή του, το *ransomware* ακολουθεί, συχνά, το μοντέλο του «διπλού εκβιασμού» (double extortion), όπου οι δράστες δεν περιορίζονται στην κρυπτογράφηση των δεδομένων, αλλά, προηγουμένως, τα εξάγουν και απειλούν με δημοσιοποίησή τους, ασκώντας πρόσθετη πίεση στο θύμα, ακόμα και στην περίπτωση που διαθέτει αντίγραφα ασφαλείας και έχει τη δυνατότητα να αποκαταστήσει τα συστήματά του. Στο λιανικό εμπόριο, μια επιτυχημένη επίθεση *ransomware* μπορεί να οδηγήσει σε αδυναμία επεξεργασίας πληρωμών, διακοπή της λειτουργίας φυσικών καταστημάτων, αναστολή ή περιορισμό των ηλεκτρονικών πωλήσεων και έκθεση προσωπικών και εμπορικών δεδομένων (Saleh et al.,2026). Οι επιπτώσεις αυτές καθίστανται ιδιαίτερα σοβαρές στην περίπτωση των μικρών και πολύ μικρών επιχειρήσεων, οι οποίες, πολλές φορές, διαθέτουν περιορισμένες

δυνατότητες δημιουργίας και ασφαλούς διατήρησης αντιγράφων ασφαλείας, καθώς και ανεπαρκή σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από περιστατικά κυβερνοασφάλειας. Υπό αυτήν την έννοια, η προστασία από το *ransomware* δεν αφορά μόνο την πρόληψη μιας κυβερνοεπίθεσης, αλλά και την ικανότητα της επιχείρησης να διατηρεί κρίσιμες λειτουργίες, να περιορίζει τις επιπτώσεις μιας παραβίασης και να επαναφέρει ταχέως τη λειτουργία της, μετά από ένα περιστατικό.

Υποκλοπή δεδομένων πληρωμής (Card Skimming & Formjacking): Η υποκλοπή δεδομένων πληρωμής αποτελεί μια εξαιρετικά κρίσιμη κατηγορία κυβερνοεπιθέσεων, καθώς στοχεύει άμεσα στα δεδομένα που απαιτούνται για την πραγματοποίηση και την εξουσιοδότηση μιας χρηματοοικονομικής συναλλαγής. Στο φυσικό περιβάλλον, πραγματοποιείται μέσω της εγκατάστασης παράνομων συσκευών ή άλλων μηχανισμών σε τερματικά POS και ATM, με σκοπό την παράνομη αντιγραφή των δεδομένων της κάρτας. Σε ορισμένες περιπτώσεις, η υποκλοπή των δεδομένων της κάρτας συνδυάζεται με τεχνικές που αποσκοπούν στην απόκτηση του PIN, επιτρέποντας στους δράστες να αξιοποιήσουν τα κλεμμένα στοιχεία για την πραγματοποίηση μη εξουσιοδοτημένων συναλλαγών. Στο ηλεκτρονικό περιβάλλον, αφορά την εισαγωγή κακόβουλου κώδικα σε σελίδες ολοκλήρωσης αγορών ηλεκτρονικών καταστημάτων, με αποτέλεσμα τα δεδομένα πληρωμής που εισάγει ο καταναλωτής να υποκλέπτονται, κατά τη διαδικασία της συναλλαγής, και να διαβιβάζονται στους δράστες. Ιδιαίτερα γνωστές είναι οι επιθέσεις *Magecart*, ένας όρος που χρησιμοποιείται για να περιγράψει ένα ευρύτερο σύνολο κυβερνοεγκληματικών εκστρατειών και τεχνικών, οι οποίες έχουν ως στόχο τις διαδικασίες ηλεκτρονικών πληρωμών, συχνά μέσω της παραβίασης ή της κακόβουλης τροποποίησης τρίτων *scripts*, *plugins* και άλλων στοιχείων λογισμικού, τα οποία ενσωματώνονται στις πλατφόρμες ηλεκτρονικού εμπορίου (Dharmavaram, 2021). Η αυξημένη επικινδυνότητα αυτών των επιθέσεων, στην περίπτωση του λιανικού εμπορίου, έγκειται στο γεγονός ότι μπορούν να πραγματοποιούνται χωρίς εμφανή διακοπή της λειτουργίας του ηλεκτρονικού καταστήματος, επιτρέποντας την παράλληλη συνέχιση των συναλλαγών και, κατά συνέπεια, τη μαζική συλλογή δεδομένων πληρωμής από μεγάλο αριθμό καταναλωτών. Η αντιμετώπιση αυτού του κινδύνου εκ μέρους των επιχειρήσεων προϋποθέτει, επομένως, όχι μόνο την προστασία των δικών τους πληροφοριακών συστημάτων, αλλά και τον συστηματικό έλεγχο των τρίτων στοιχείων λογισμικού και των εξωτερικών παρόχων που ενσωματώνονται στην ψηφιακή υποδομή τους.

Παραβιάσεις δεδομένων (Data Breaches): Η μαζική υποκλοπή των δεδομένων που τηρούνται στα πληροφοριακά συστήματα των επιχειρήσεων συνιστά μια από τις σοβαρότερες μορφές κυβερνοασφάλειας, τις οποίες αντιμετωπίζει ο λιανικός κλάδος. Η συγκέντρωση αυτών των δεδομένων σε μεγάλες βάσεις καθιστά τις επιχειρήσεις ελκυστικούς στόχους για κυβερνοεγκληματικές ομάδες, καθώς αυτά μπορούν να αξιοποιηθούν για οικονομική απάτη, κλοπή ταυτότητας, στοχευμένες εκστρατείες *phishing* και άλλες μορφές παράνομης δραστηριότητας. Ιδιαίτερη σημασία έχει, επίσης, η δυνατότητα συνδυασμού διαφορετικών κατηγοριών δεδομένων, καθώς η συσχέτιση στοιχείων ταυτοποίησης, συναλλακτικού ιστορικού και καταναλωτικών προτιμήσεων μπορεί να αυξήσει σημαντικά την αξία τους για τους δράστες και να επιτρέψει πιο εξατομικευμένες μορφές εξαπάτησης (Hemphill & Longstreet, 2016).

Επιθέσεις σε αλυσίδες εφοδιασμού (Supply Chain Attacks): Οι επιθέσεις στην αλυσίδα εφοδιασμού αποτελούν μια από τις πλέον σύνθετες και δύσκολα ανιχνεύσιμες μορφές κυβερνοεπίθεσης, δεδομένου ότι αξιοποιούν τις τεχνολογικές και οργανωτικές αλληλεξαρτήσεις, οι οποίες χαρακτηρίζουν τη σύγχρονη ψηφιακή οικονομία. Αντί να στοχεύουν άμεσα την πληροφοριακή υποδομή της επιχείρησης-στόχου, οι δράστες επιχειρούν να παραβιάσουν έναν αξιόπιστο τρίτο φορέα —όπως πάροχο λογισμικού, πάροχο υπηρεσιών πληρωμών, πάροχο υπολογιστικού νέφους (cloud services) ή πάροχο συστημάτων POS— και να αξιοποιήσουν την υπάρχουσα σχέση εμπιστοσύνης και διασύνδεσης, προκειμένου να αποκτήσουν πρόσβαση στα συστήματα ή στα δεδομένα της επιχείρησης. Η συγκεκριμένη μορφή επίθεσης είναι ιδιαιτέρως επικίνδυνη, επειδή η κακόβουλη δραστηριότητα μπορεί να εισέλθει στο πληροφοριακό περιβάλλον μιας επιχείρησης, μέσω ενός, κατά τα άλλα, νόμιμου και έμπιστου τεχνολογικού καναλιού, καθιστώντας την έγκαιρη ανίχνευσή της σημαντικά δυσκολότερη (Simon & Omar, 2020). Όσον αφορά το λιανικό εμπόριο, ο κίνδυνος αυτός αποκτά βαρύνουσα σημασία, λόγω της εκτεταμένης εξάρτησης των επιχειρήσεων από τρίτους τεχνολογικούς και χρηματοπιστωτικούς παρόχους. Συστήματα POS, υπηρεσίες επεξεργασίας και αποδοχής πληρωμών, πλατφόρμες ηλεκτρονικού εμπορίου, υπηρεσίες *cloud*, λογισμικό διαχείρισης αποθεμάτων και πελατειακών σχέσεων, καθώς και μια σειρά από εξωτερικά *plugins* και εφαρμογές συνθέτουν ένα σύνθετο δίκτυο τεχνολογικών αλληλεξαρτήσεων

Επιθέσεις Κατανεμημένης Άρνησης Υπηρεσίας (DDoS): Οι επιθέσεις Κατανεμημένης Άρνησης Υπηρεσίας (Distributed Denial of Service – DDoS)

στοχεύουν στη διατάραξη και στην προσωρινή διακοπή της διαθεσιμότητας των ψηφιακών υπηρεσιών και των πληροφοριακών υποδομών, προκαλώντας την ταυτόχρονη αποστολή εξαιρετικά μεγάλου όγκου αιτημάτων προς έναν συγκεκριμένο στόχο. Αυτό έχει ως αποτέλεσμα ο όγκος της εισερχόμενης κίνησης να υπερβαίνει τη δυνατότητα διαχείρισης της ψηφιακής υποδομής, η λειτουργία της υπηρεσίας να επιβραδύνεται σημαντικά, με ενδεχόμενο ακόμα και να διακοπεί προσωρινά, καθιστώντας την απρόσιτη στους νόμιμους χρήστες (Zkik et al., 2024). Στην περίπτωση του ηλεκτρονικού εμπορίου, μια επιτυχημένη DDoS επίθεση, σε κρίσιμες εμπορικές περιόδους —όπως εορταστικές περίοδοι, μεγάλες εκπτωτικές εκστρατείες ή άλλα χρονικά διαστήματα αυξημένης ζήτησης— επιφέρει σημαντικές απώλειες εσόδων, διαταραχή της λειτουργίας του ηλεκτρονικού καταστήματος και υποβάθμιση της εμπιστοσύνης των καταναλωτών. Η οικονομική επίπτωση μπορεί να είναι ιδιαίτερα υψηλή, όταν η επίθεση συμπίπτει με χρονικά περιορισμένες εμπορικές ευκαιρίες, κατά τις οποίες η επιχείρηση εξαρτάται, σε μεγάλο βαθμό, από τη συνεχή διαθεσιμότητα των ψηφιακών καναλιών της.

Εσωτερικές απειλές (Insider Threats): Μια κατηγορία κυβερνοκινδύνου, η οποία συχνά υποτιμάται, αφορά τις απειλές που προέρχονται από άτομα, τα οποία διαθέτουν νόμιμη πρόσβαση στα πληροφοριακά συστήματα και στις ψηφιακές υποδομές μιας επιχείρησης. Η απειλή μπορεί να είναι σκόπιμη, όταν ένας εργαζόμενος ή συνεργάτης αξιοποιεί την πρόσβασή του για υποκλοπή δεδομένων, πρόκληση ζημίας ή εξυπηρέτηση οικονομικών ή άλλων κινήτρων, αλλά και ακούσια, όταν η παραβίαση προκύπτει από ανθρώπινο λάθος, όπως το άνοιγμα ενός κακόβουλου συνδέσμου *phishing*, η χρήση ανεπαρκώς ασφαλών κωδικών πρόσβασης ή η μη ασφαλής αποθήκευση και διαβίβαση επιχειρησιακών δεδομένων. Η ιδιαιτερότητα των εσωτερικών απειλών έγκειται στο γεγονός ότι ο δράστης διαθέτει ήδη ένα επίπεδο πρόσβασης και εμπιστοσύνης, με αποτέλεσμα ο εντοπισμός της κακόβουλης ή επικίνδυνης δραστηριότητας να είναι συχνά δυσκολότερος, σε σχέση με μια εξωτερική επίθεση (Omotoye & Chen, 2025).

Το ζήτημα αποκτά ιδιαίτερη σημασία στο λιανικό εμπόριο, όπου η υψηλή κινητικότητα του προσωπικού, η απασχόληση μεγάλου αριθμού εργαζομένων σε διαφορετικά σημεία και βάρδιες, καθώς και η πρόσβαση σε συστήματα POS, δεδομένα πελατών και πληροφοριακές υποδομές δημιουργούν ένα σύνθετο περιβάλλον διαχείρισης δικαιωμάτων πρόσβασης. Στις μικρές και πολύ μικρές επιχειρήσεις, ο κίνδυνος μπορεί

να εντείνεται από την περιορισμένη εκπαίδευση του προσωπικού και την απουσία τυποποιημένων διαδικασιών για τη χορήγηση, τον περιορισμό και την άμεση ανάκληση δικαιωμάτων πρόσβασης, όταν ένας εργαζόμενος αποχωρεί ή αλλάζει θέση. Η αντιμετώπιση των εσωτερικών απειλών απαιτεί, επομένως, συνδυασμό τεχνικών και οργανωτικών μέτρων, όπως η αρχή της ελάχιστης αναγκαίας πρόσβασης (least privilege), η τακτική επανεξέταση των δικαιωμάτων χρηστών, η πολυπαραγοντική αυθεντικοποίηση, η καταγραφή και παρακολούθηση κρίσιμων ενεργειών και, κυρίως, η συστηματική εκπαίδευση του προσωπικού σε ζητήματα κυβερνοασφάλειας (Omotoye & Chen, 2025).

4.3 Το κόστος των κυβερνοεπιθέσεων

Η ποσοτικοποίηση του κόστους των κυβερνοεπιθέσεων αποτελεί αναγκαίο, έστω και αν χαρακτηρίζεται ως, εγγενώς, ατελές, εγχείρημα για την κατανόηση της βαρύτητας του εν λόγω ζητήματος. Η ατέλεια είναι διπλή, καθώς, αφενός, σημαντικό ποσοστό των συμβάντων δεν καταγγέλλεται ή δεν ανακαλύπτεται, αφετέρου, το πραγματικό κόστος ενσωματώνει μη ποσοτικοποιήσιμες παραμέτρους —ζημία φήμης, διάβρωση εμπιστοσύνης, απώλεια ανταγωνιστικής θέσης— οι οποίες υπερβαίνουν τις άμεσες οικονομικές απώλειες.

Η αυξανόμενη ένταση και πολυπλοκότητα των κυβερνοαπειλών μεταφράζεται σε σημαντικές οικονομικές επιπτώσεις για τις επιχειρήσεις, οι οποίες δεν περιορίζονται στο άμεσο κόστος αποκατάστασης της παραβίασης, αλλά εκτείνονται στη διακοπή της επιχειρηματικής δραστηριότητας, στην απώλεια εσόδων, στο κόστος κανονιστικής συμμόρφωσης, στις νομικές υποχρεώσεις, στην αποκατάσταση των πληροφοριακών συστημάτων και, κυρίως, στην απώλεια εμπιστοσύνης των πελατών. Σύμφωνα με την έκθεση *Cost of a Data Breach Report 2024* της IBM[11], το μέσο παγκόσμιο κόστος μιας παραβίασης δεδομένων ανήλθε σε 4,88 εκατ. δολάρια, το 2024, σημειώνοντας αύξηση κατά 10%, σε σχέση με το 2023, και καταγράφοντας το υψηλότερο επίπεδο από την έναρξη της συγκεκριμένης σειράς ερευνών. Στον κλάδο του λιανικού εμπορίου, το αντίστοιχο μέσο κόστος ανήλθε σε 3,48 εκατ. δολάρια, έναντι 2,96 εκατ. Δολαρίων, το προηγούμενο έτος, καταγράφοντας αύξηση περίπου 18%. Παρά το γεγονός ότι το

[11] https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry

κόστος αυτό υπολείπεται του μέσου όρου σε παγκόσμια κλίμακα, η εξέλιξή του καταδεικνύει ότι οι κυβερνοπαραβιάσεις αποτελούν, πλέον, σημαντικό παράγοντα οικονομικού κινδύνου και για τις επιχειρήσεις του λιανικού εμπορίου.

Η οικονομική διάσταση του κυβερνοκινδύνου είναι, ωστόσο, ευρύτερη από την άμεση χρηματοοικονομική ζημία που προκαλεί μια παραβίαση. Το κόστος μιας κυβερνοεπίθεσης προκύπτει από την προσωρινή αδυναμία λειτουργίας των ηλεκτρονικών καταστημάτων, τη διακοπή των συστημάτων πληρωμών, την αναστολή της λειτουργίας φυσικών καταστημάτων, την απώλεια συναλλαγών, καθώς και από τις δαπάνες διερεύνησης και αποκατάστασης του περιστατικού. Παράλληλα, η επιχείρηση μπορεί να αντιμετωπίσει αυξημένες υποχρεώσεις ενημέρωσης και υποστήριξης των πελατών, νομικές αξιώσεις, διοικητικές κυρώσεις και σημαντικές δαπάνες για την αποκατάσταση της αξιοπιστίας της (Cashell et al., 2004). Η ιδιαίτερη σημασία της επιχειρησιακής διακοπής έγκειται στο γεγονός ότι οι οικονομικές απώλειες μπορούν να συνεχίζονται ακόμη και μετά την τεχνική αποκατάσταση της παραβίασης, καθώς η επιχείρηση ενδέχεται να χρειάζεται σημαντικό χρονικό διάστημα για να επαναφέρει πλήρως τις λειτουργίες της και να αποκαταστήσει την εμπιστοσύνη των καταναλωτών.

Τα διαθέσιμα στοιχεία επιβεβαιώνουν ότι το λιανικό εμπόριο αποτελεί έναν ολοένα σημαντικότερο στόχο των κυβερνοεγκλημάτων. Σύμφωνα με την *2025 Data Breach Investigations Report* της Verizon[12], τα περιστατικά κυβερνοασφάλειας στον κλάδο του λιανικού εμπορίου αυξήθηκαν κατά 15% σε σχέση με την προηγούμενη περίοδο. Παράλληλα, παρατηρείται μετατόπιση του ενδιαφέροντος των δραστών από τα παραδοσιακά δεδομένα πληρωμών προς διαπιστευτήρια χρηστών, δεδομένα πελατών, επιχειρησιακές πληροφορίες και άλλα στοιχεία που μπορούν να αξιοποιηθούν για οικονομική απάτη ή περαιτέρω επιθέσεις. Η εξέλιξη αυτή είναι ιδιαίτερα σημαντική για το λιανικό εμπόριο, καθώς αναδεικνύει ότι η προστασία των συστημάτων πληρωμών, μολονότι παραμένει κρίσιμη, δεν επαρκεί πλέον για την αντιμετώπιση του συνολικού κυβερνοκινδύνου που αντιμετωπίζει μια σύγχρονη εμπορική επιχείρηση.

Ιδιαίτερη ανησυχία προκαλεί η διάδοση του ransomware και η δυσανάλογη έκθεση των μικρών και μεσαίων επιχειρήσεων. Σύμφωνα με τα στοιχεία από την έκθεση της Verizon για το 2025, το ransomware συνδεόταν με το 44% των παραβιάσεων που καταγράφηκαν συνολικά, ενώ στις μικρές και μεσαίες επιχειρήσεις το αντίστοιχο

[12] https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

ποσοστό ανήλθε στο 88%, έναντι 39% στις μεγαλύτερες επιχειρήσεις. Η σημαντική αυτή διαφοροποίηση αναδεικνύει μια θεμελιώδη ασυμμετρία του κυβερνοκινδύνου. Από τη μία μεριά, οι μικρομεσαίες επιχειρήσεις δεν διαθέτουν μόνο μικρότερες δυνατότητες επένδυσης σε τεχνολογίες προστασίας, αλλά είναι και περισσότερο εκτεθειμένες σε επιθέσεις που προκαλούν άμεση διακοπή της λειτουργίας τους. Για μια μεγάλη επιχείρηση, μια κυβερνοεπίθεση αποτελεί ένα σοβαρό, αλλά, παρόλα αυτά, διαχειρίσιμο περιστατικό στο πλαίσιο μιας ευρύτερης δομής διαχείρισης κινδύνων. Για μια μικρή εμπορική επιχείρηση, αντίθετα, μια παρατεταμένη διακοπή λειτουργίας, η απώλεια δεδομένων και η αδυναμία πραγματοποίησης συναλλαγών μπορεί να απειλήσει άμεσα την ίδια τη βιωσιμότητά της.

Η διάσταση αυτή αποκτά ιδιαίτερη σημασία στο λιανικό εμπόριο, καθώς η ψηφιοποίηση των επιχειρήσεων πραγματοποιείται σε μεγάλο βαθμό μέσω εξωτερικών παρόχων τεχνολογίας. POS, payment gateways, υπηρεσίες επεξεργασίας πληρωμών, πλατφόρμες ηλεκτρονικού εμπορίου, υπηρεσίες υπολογιστικού νέφους, εφαρμογές διαχείρισης πελατειακών σχέσεων και εξωτερικά plugins αποτελούν πλέον αναπόσπαστα στοιχεία της ψηφιακής υποδομής ακόμη και μιας μικρής εμπορικής επιχείρησης. Ως αποτέλεσμα, η ασφάλεια της επιχείρησης εξαρτάται σε σημαντικό βαθμό από την ασφάλεια των συστημάτων και των διαδικασιών των τρίτων παρόχων. Η Verizon καταγράφει ότι η συμμετοχή τρίτων μερών στις παραβιάσεις αυξήθηκε σημαντικά και ανήλθε στο 30% των breaches το 2025. Η εξέλιξη αυτή ενισχύει το επιχείρημα ότι η κυβερνοασφάλεια δεν μπορεί να αντιμετωπίζεται πλέον αποκλειστικά ως εσωτερική λειτουργία της επιχείρησης, αλλά πρέπει να προσεγγίζεται ως ζήτημα διαχείρισης ενός ευρύτερου δικτύου τεχνολογικών και επιχειρησιακών αλληλεξαρτήσεων.

Παράλληλα, το οικονομικό κόστος της κυβερνοπαραβίασης επηρεάζεται σημαντικά από την ταχύτητα με την οποία αυτή εντοπίζεται και περιορίζεται. Όσο μεγαλύτερο είναι το χρονικό διάστημα κατά το οποίο ένας μη εξουσιοδοτημένος δράστης παραμένει εντός των πληροφοριακών συστημάτων μιας επιχείρησης, τόσο αυξάνεται η πιθανότητα πρόσβασης σε μεγαλύτερο όγκο δεδομένων και κρίσιμων λειτουργιών και, κατ' επέκταση, το δυνητικό κόστος του περιστατικού (Cashell et al., 2004). .

Η οικονομική διάσταση του κυβερνοκινδύνου συνδέεται, τέλος, με ένα ευρύτερο πρόβλημα επενδυτικής ανεπάρκειας. Η EuroCommerce έχει επισημάνει την ανάγκη για σημαντικές επενδύσεις στον ψηφιακό μετασχηματισμό του ευρωπαϊκού λιανικού και

χονδρικού εμπορίου, συμπεριλαμβανομένων των υποδομών κυβερνοασφάλειας[13]. Οι απαιτούμενες επενδύσεις δεν αφορούν μόνο την εγκατάσταση βασικών τεχνολογικών συστημάτων, αλλά και τη δημιουργία δυνατοτήτων συνεχούς παρακολούθησης, πρόληψης, ανίχνευσης και αντιμετώπισης κυβερνοαπειλών. Το πρόβλημα είναι ότι η ανάγκη αυτή συνυπάρχει με σημαντικούς περιορισμούς χρηματοδότησης και ανθρώπινου δυναμικού, ιδιαίτερα στις μικρές επιχειρήσεις.

Από την οπτική αυτή, η κυβερνοασφάλεια θα πρέπει να αντιμετωπίζεται ως στοιχείο της συνολικής οικονομικής ανθεκτικότητας του λιανικού εμπορίου και όχι ως απλή δαπάνη τεχνολογικής υποδομής. Η προστασία των πληροφοριακών συστημάτων, των δεδομένων και των ψηφιακών συναλλαγών θα πρέπει να αποτελεί προϋπόθεση για τη διασφάλιση της επιχειρησιακής συνέχειας, της εμπιστοσύνης των καταναλωτών και της ανταγωνιστικότητας των επιχειρήσεων.

[13] https://www.eurocommerce.eu/app/uploads/2022/10/2022.10.25-Transforming-the-EU-retail-and-wholesale-sector.pdf?utm

5. Το ευρωπαϊκό ρυθμιστικό πλαίσιο κυβερνοασφάλειας

5.1 NIS2, DORA και GDPR: υποχρεώσεις για το λιανικό εμπόριο

Η ευρωπαϊκή ρυθμιστική αρχιτεκτονική στον τομέα της κυβερνοασφάλειας έχει εξελιχθεί, κατά την τελευταία δεκαετία, σε ένα πολυεπίπεδο και διαρκώς διευρυνόμενο σύστημα αλληλοσυμπληρούμενων κανόνων, το οποίο επιχειρεί να ανταποκριθεί στην αυξανόμενη πολυπλοκότητα και ετερογένεια των κυβερνοαπειλών μέσω του συνδυασμού οριζόντιων και τομεακών ρυθμίσεων. Στον πυρήνα του θεσμικού αυτού πλαισίου βρίσκονται, μεταξύ άλλων, η Οδηγία NIS2, ο Κανονισμός DORA και ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR), οι οποίοι, παρά τις διαφορετικές αφετηρίες, στόχους και πεδία εφαρμογής τους, διαμορφώνουν ένα ολοένα πιο απαιτητικό κανονιστικό περιβάλλον για τις επιχειρήσεις.

Για το λιανικό εμπόριο, η πλοήγηση στο περιβάλλον αυτό αποτελεί αφ' εαυτής σημαντική επιχειρησιακή και οργανωτική πρόκληση. Οι υποχρεώσεις που απορρέουν από τα επιμέρους νομοθετικά κείμενα δεν εφαρμόζονται πάντοτε κατά τρόπο πλήρως διακριτό, αλλά σε ορισμένες περιπτώσεις αλληλοεπικαλύπτονται ή λειτουργούν συμπληρωματικά. Παράλληλα, η εφαρμογή τους συνεπάγεται διαφορετικές απαιτήσεις ως προς την αξιολόγηση και διαχείριση κινδύνων, την τεκμηρίωση των μέτρων ασφαλείας, την αναφορά περιστατικών, την προστασία προσωπικών δεδομένων και τη διαχείριση των σχέσεων με τρίτους παρόχους. Η πολυπλοκότητα αυτή είναι ιδιαίτερα αισθητή για τις μικρές και μεσαίες εμπορικές επιχειρήσεις, οι οποίες συχνά στερούνται εξειδικευμένων νομικών και τεχνικών δομών ικανών να παρακολουθούν συστηματικά τις κανονιστικές εξελίξεις και να εξασφαλίζουν τη συνεχή συμμόρφωσή τους με αυτές.

Η κατανόηση του πεδίου εφαρμογής και των διαφορών μεταξύ των τριών αυτών κανονιστικών πλαισίων είναι, επομένως, κρίσιμη προκειμένου να προσδιοριστούν με μεγαλύτερη ακρίβεια οι πραγματικές υποχρεώσεις των επιχειρήσεων λιανικής. Η NIS2 επικεντρώνεται πρωτίστως στην ενίσχυση της κυβερνοανθεκτικότητας κρίσιμων και σημαντικών τομέων της οικονομίας, ο DORA στη λειτουργική ψηφιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα, ενώ ο GDPR ρυθμίζει την προστασία των δεδομένων

προσωπικού χαρακτήρα και επιβάλλει συγκεκριμένες υποχρεώσεις ασφαλείας και γνωστοποίησης παραβιάσεων. Κατά συνέπεια, οι τρεις αυτές ρυθμίσεις δεν πρέπει να αντιμετωπίζονται ως ένα ενιαίο και ομοιογενές σύστημα υποχρεώσεων, αλλά ως διακριτά — και ταυτόχρονα αλληλοσυνδεόμενα — κανονιστικά επίπεδα, των οποίων η σημασία για κάθε εμπορική επιχείρηση εξαρτάται από το μέγεθος, τη δραστηριότητα, τη θέση της στην αλυσίδα εφοδιασμού και τον βαθμό ψηφιοποίησης των λειτουργιών της.

Η Οδηγία NIS2 (Οδηγία (ΕΕ) 2022/2555), η οποία αντικατέστησε την αρχική Οδηγία NIS του 2016, αποτελεί το κεντρικό ευρωπαϊκό νομοθετικό πλαίσιο για την ενίσχυση της κυβερνοασφάλειας κρίσιμων και σημαντικών οντοτήτων εκτός του ειδικότερου πεδίου των χρηματοπιστωτικών υπηρεσιών. Τα κράτη-μέλη όφειλαν να μεταφέρουν τις διατάξεις της στο εθνικό τους δίκαιο έως τις 17 Οκτωβρίου 2024. Σε σχέση με την προκάτοχό της, η NIS2 διευρύνει σημαντικά το πεδίο εφαρμογής της, εντάσσοντας νέους τομείς και κατηγορίες οντοτήτων, ενώ διακρίνει τις υπαγόμενες επιχειρήσεις σε «ουσιώδεις» (essential) και «σημαντικές» (important) οντότητες, με διαφοροποιημένο καθεστώς εποπτείας και ελέγχου. Παράλληλα, ενισχύει τις υποχρεώσεις διαχείρισης των κυβερνοκινδύνων, δίνοντας ιδιαίτερη έμφαση στην ασφάλεια της αλυσίδας εφοδιασμού και των σχέσεων με τρίτους παρόχους, καθιερώνει αυστηρότερα και εναρμονισμένα χρονικά πλαίσια για την αναφορά σημαντικών κυβερνοσυμβάντων — συμπεριλαμβανομένης της έγκαιρης προειδοποίησης εντός 24 ωρών και της κοινοποίησης συμβάντος εντός 72 ωρών — και ενισχύει τη λογοδοσία των διοικητικών οργάνων, στα οποία ανατίθεται ρητά η ευθύνη έγκρισης και εποπτείας των μέτρων διαχείρισης κυβερνοκινδύνων (Gaie & Mueck, 2025).

Η εφαρμογή της NIS2 στο λιανικό εμπόριο απαιτεί, συνεπώς, προσεκτική ερμηνεία του πεδίου εφαρμογής της. Το λιανικό εμπόριο, ως γενική οικονομική δραστηριότητα, δεν περιλαμβάνεται στους τομείς υψηλής κρισιμότητας που κατονομάζονται ρητά στα Παραρτήματα Ι και ΙΙ της Οδηγίας. Κατά συνέπεια, η πλειονότητα των μικρών και μεσαίων επιχειρήσεων λιανικής δεν υπάγεται αυτομάτως στις άμεσες υποχρεώσεις της NIS2. Υπαγωγή μπορεί να προκύψει, ωστόσο, όταν μια επιχείρηση ασκεί παράλληλα δραστηριότητα που εντάσσεται σε συγκεκριμένο τομέα ή κατηγορία οντοτήτων του κανονιστικού πεδίου της Οδηγίας — για παράδειγμα, όταν παρέχει ορισμένες υπηρεσίες ψηφιακής υποδομής ή άλλες ρητά καλυπτόμενες υπηρεσίες — και πληροί τις σχετικές προϋποθέσεις μεγέθους και δραστηριότητας.

Η σημασία της NIS2 για τον λιανικό κλάδο δεν περιορίζεται, ωστόσο, στις επιχειρήσεις που υπάγονται άμεσα στις διατάξεις της. Για παράδειγμα, ένας λιανοπωλητής που συνεργάζεται με οργανισμούς ή επιχειρήσεις οι οποίες υπάγονται στη NIS2 — όπως φορείς του τομέα της υγείας ή άλλες κρίσιμες οντότητες — ενδέχεται να κληθεί να αποδείξει ότι διαθέτει στοιχειώδεις διαδικασίες κυβερνοασφάλειας, μηχανισμούς διαχείρισης περιστατικών και κατάλληλα μέτρα προστασίας των πληροφοριακών του συστημάτων. Η απαίτηση αυτή δεν συνεπάγεται αυτοτελή νομική υπαγωγή του στη NIS2, αλλά αποτελεί έμμεση συνέπεια της αυξημένης κανονιστικής ευθύνης του ρυθμιζόμενου αντισυμβαλλομένου του. Υπό αυτή την έννοια, η NIS2 λειτουργεί και ως μηχανισμός διάχυσης προτύπων κυβερνοασφάλειας σε ευρύτερα επιχειρηματικά δίκτυα.

Για τις επιχειρήσεις λιανικής, ιδίως τις μικρές και πολύ μικρές επιχειρήσεις, η εξέλιξη αυτή έχει ιδιαίτερη σημασία, καθώς η κυβερνοασφάλεια μετατρέπεται σταδιακά από ζήτημα εσωτερικής τεχνικής προστασίας σε παράγοντα εμπορικής αξιοπιστίας και πρόσβασης σε επιχειρηματικές συνεργασίες. Επιχειρήσεις που δεν θα είναι σε θέση να τεκμηριώσουν ένα βασικό επίπεδο ψηφιακής ασφάλειας ενδέχεται να αντιμετωπίσουν αυξανόμενες δυσκολίες στη συνεργασία τους με μεγάλους οργανισμούς και επιχειρήσεις που υπάγονται σε αυστηρότερα κανονιστικά καθεστώτα. Επομένως, ακόμη και στις περιπτώσεις όπου η NIS2 δεν δημιουργεί άμεση νομική υποχρέωση για τον έμπορο, οι αρχές και τα πρότυπα που εισάγει αναμένεται να επηρεάσουν σταδιακά τη λειτουργία και τις απαιτήσεις ολόκληρης της αλυσίδας αξίας.

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ/GDPR, Κανονισμός (ΕΕ) 2016/679), μολονότι δεν αποτελεί νομοθέτημα κυβερνοασφάλειας με τη στενή έννοια του όρου, διαμορφώνει ένα ιδιαίτερα σημαντικό πλαίσιο υποχρεώσεων ασφάλειας για κάθε επιχείρηση που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα. Στην κατηγορία αυτή εντάσσεται η συντριπτική πλειονότητα των επιχειρήσεων λιανικής, οι οποίες συλλέγουν και διαχειρίζονται δεδομένα πελατών μέσω των συστημάτων πληρωμών, του ηλεκτρονικού εμπορίου, των προγραμμάτων επιβράβευσης, των εφαρμογών διαχείρισης πελατειακών σχέσεων και των λοιπών ψηφιακών καναλιών επικοινωνίας.

Ιδιαίτερη σημασία παρουσιάζουν το άρθρο 25, το οποίο καθιερώνει τις αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού (*data protection by design and by default*), και το άρθρο 32, το οποίο υποχρεώνει τον υπεύθυνο

επεξεργασίας και τον εκτελούντα την επεξεργασία να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση επιπέδου ασφάλειας ανάλογου προς τον εκάστοτε κίνδυνο. Ο Κανονισμός δεν καθορίζει εξαντλητικά ποια συγκεκριμένα τεχνολογικά μέτρα πρέπει να εφαρμόζει κάθε επιχείρηση, αλλά ακολουθεί μία προσέγγιση βασισμένη στον κίνδυνο, σύμφωνα με την οποία η επάρκεια των μέτρων αξιολογείται λαμβάνοντας υπόψη τη φύση, το εύρος, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τη σοβαρότητα των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Η ευελιξία αυτή επιτρέπει την προσαρμογή των υποχρεώσεων στα ιδιαίτερα χαρακτηριστικά κάθε επιχείρησης, δημιουργεί όμως ταυτόχρονα δυσκολίες ερμηνείας, ιδίως για τις μικρές επιχειρήσεις που δεν διαθέτουν εξειδικευμένη νομική και τεχνική υποστήριξη.

Η αυστηρότητα του πλαισίου ενισχύεται από το σύστημα κυρώσεων του ΓΚΠΔ. Για ορισμένες κατηγορίες παραβάσεων, ο Κανονισμός προβλέπει διοικητικά πρόστιμα που μπορούν να φθάσουν έως τα 20 εκατ. ευρώ ή, στην περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, αναλόγως με το ποιο ποσό είναι υψηλότερο. Ωστόσο, η επιβολή των κυρώσεων διέπεται από την αρχή της αναλογικότητας και απαιτεί την εξατομικευμένη αξιολόγηση κάθε περίπτωσης. Το μέγεθος της επιχείρησης, η φύση και η σοβαρότητα της παράβασης, ο βαθμός υπαιτιότητας, τα μέτρα που ελήφθησαν για τον περιορισμό της ζημίας και ο βαθμός συνεργασίας με την εποπτική αρχή αποτελούν παράγοντες που λαμβάνονται υπόψη κατά την επιβολή κυρώσεων.

Ο Κανονισμός DORA (Digital Operational Resilience Act, Κανονισμός (ΕΕ) 2022/2554), ο οποίος εφαρμόζεται από τις 17 Ιανουαρίου 2025, συνιστά βασικό στοιχείο της νέας ευρωπαϊκής αρχιτεκτονικής για την κυβερνοασφάλεια και την ψηφιακή ανθεκτικότητα. Ο DORA απευθύνεται πρωτίστως στις χρηματοπιστωτικές οντότητες και δεν επιβάλλει, κατά κανόνα, άμεσες υποχρεώσεις στις επιχειρήσεις λιανικού εμπορίου. Στο πεδίο εφαρμογής του περιλαμβάνονται, μεταξύ άλλων, τα πιστωτικά ιδρύματα, τα ιδρύματα πληρωμών, οι πάροχοι υπηρεσιών πληροφόρησης λογαριασμού, τα ιδρύματα ηλεκτρονικού χρήματος, οι ασφαλιστικές επιχειρήσεις, οι επενδυτικές επιχειρήσεις και άλλοι φορείς του χρηματοπιστωτικού τομέα, ενώ ο Κανονισμός καλύπτει επίσης, υπό συγκεκριμένες προϋποθέσεις, τους τρίτους παρόχους υπηρεσιών ΤΠΕ που υποστηρίζουν τις λειτουργίες αυτών των οντοτήτων. Σκοπός του είναι η διασφάλιση υψηλού επιπέδου ψηφιακής λειτουργικής ανθεκτικότητας μέσω

ενιαίων απαιτήσεων για τη διαχείριση κινδύνων ΤΠΕ, την αναφορά σημαντικών περιστατικών, τη διενέργεια δοκιμών ανθεκτικότητας και τη διαχείριση των κινδύνων που συνδέονται με την εξάρτηση από τρίτους τεχνολογικούς παρόχους.

Η σημασία του DORA για το λιανικό εμπόριο είναι, ωστόσο, ουσιαστική, καθώς μεγάλο μέρος της καθημερινής λειτουργίας των εμπορικών επιχειρήσεων εξαρτάται από χρηματοπιστωτικές και ψηφιακές υποδομές που υπάγονται στο κανονιστικό του περιβάλλον. Οι acquirers, οι αδειοδοτημένοι πάροχοι υπηρεσιών πληρωμών, οι πάροχοι υπηρεσιών BNPL και άλλοι φορείς του ευρύτερου οικοσυστήματος πληρωμών καλούνται, εφόσον εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού, να ενισχύσουν τη διαχείριση των κινδύνων ΤΠΕ και την επιχειρησιακή τους ανθεκτικότητα. Η εξέλιξη αυτή μπορεί να επηρεάσει έμμεσα τους εμπόρους, κυρίως μέσω της μεγαλύτερης ασφάλειας και αξιοπιστίας των υπηρεσιών πληρωμών από τις οποίες εξαρτώνται, αλλά και μέσω αυστηρότερων διαδικασιών συνεργασίας, ελέγχου κινδύνου και διαχείρισης περιστατικών.

Για τις επιχειρήσεις λιανικής, η επίδραση του DORA πρέπει, επομένως, να γίνει κατανοητή πρωτίστως ως έμμεση και οικοσυστημική. Ο έμπορος δεν μετατρέπεται σε ρυθμιζόμενη χρηματοπιστωτική οντότητα επειδή δέχεται πληρωμές με κάρτα ή συνεργάζεται με έναν πάροχο πληρωμών. Εντούτοις, όσο περισσότερο οι υπηρεσίες πληρωμών, το ηλεκτρονικό εμπόριο και οι συναφείς ψηφιακές υποδομές εντάσσονται σε περιβάλλον αυστηρότερης εποπτείας και διαχείρισης κινδύνου, τόσο το πιθανότερο είναι να αυξάνονται οι πρακτικές απαιτήσεις που συνοδεύουν τη συνεργασία με τους αντίστοιχους παρόχους. Οι επιχειρήσεις μπορεί, για παράδειγμα, να κληθούν να εφαρμόζουν ασφαλέστερες διαδικασίες διαχείρισης λογαριασμών και πρόσβασης, να ανταποκρίνονται αποτελεσματικότερα σε περιστατικά ασφαλείας ή να συμμορφώνονται με αυστηρότερα πρωτόκολλα που θέτουν οι πάροχοι των ψηφιακών και χρηματοπιστωτικών υπηρεσιών τους.

Υπό αυτή την έννοια, ο DORA συμβάλλει στη σταδιακή αναδιαμόρφωση του ευρύτερου περιβάλλοντος μέσα στο οποίο λειτουργεί το λιανικό εμπόριο. Η επίδρασή του στις μικρομεσαίες επιχειρήσεις δεν συνίσταται στην αυτόματη δημιουργία άμεσων κανονιστικών υποχρεώσεων, αλλά στην αυξανόμενη ενσωμάτωση υψηλότερων προτύπων ασφάλειας στις υποδομές και τις υπηρεσίες από τις οποίες εξαρτώνται. Το γεγονός αυτό μπορεί να λειτουργήσει θετικά, ενισχύοντας τη συνολική ασφάλεια και ανθεκτικότητα του οικοσυστήματος πληρωμών, δημιουργεί όμως ταυτόχρονα την

ανάγκη οι μικρές επιχειρήσεις να αναπτύξουν μεγαλύτερη κατανόηση των ψηφιακών εξαρτήσεων και των κυβερνοκινδύνων που συνοδεύουν τη λειτουργία τους.

5.2 Το PCI DSS και η τυποποίηση της ασφάλειας των πληρωμών

Παράλληλα με το δημόσιο ρυθμιστικό πλαίσιο, το λιανικό εμπόριο υπόκειται, στον τομέα της ασφάλειας των πληρωμών με κάρτα, σε ένα ιδιαίτερα σημαντικό ιδιωτικό πρότυπο, το λεγόμενο Payment Card Industry Data Security Standard (PCI DSS). Το PCI DSS αποτελεί ένα διεθνώς αναγνωρισμένο πλαίσιο τεχνικών και οργανωτικών απαιτήσεων για την προστασία των δεδομένων καρτών πληρωμής, αναπτύσσεται και συντηρείται από το Payment Card Industry Security Standards Council (PCI SSC)[14]. Το εν λόγω Συμβούλιο ιδρύθηκε το 2006 από τους πέντε μεγάλους διεθνείς οργανισμούς καρτών —Visa, Mastercard, American Express, Discover και JCB— με σκοπό τη διαμόρφωση κοινών προτύπων ασφάλειας για το οικοσύστημα των πληρωμών με κάρτα. Το PCI DSS δεν αποτελεί νομοθετική πράξη, ούτε επιβάλλεται αυτοτελώς από το ευρωπαϊκό και το εθνικό δίκαιο. Η εφαρμογή του προκύπτει κυρίως από τους κανόνες και τις συμβατικές απαιτήσεις των δικτύων καρτών και των φορέων που συμμετέχουν στο οικοσύστημα πληρωμών.

Η σημασία του PCI DSS για το λιανικό εμπόριο είναι σημαντική, καθώς το πρότυπο καλύπτει ένα ευρύ φάσμα απαιτήσεων που αφορούν την ασφαλή διαχείριση των δεδομένων των καρτών σε ολόκληρο τον κύκλο ζωής μιας συναλλαγής. Οι απαιτήσεις του αφορούν, μεταξύ άλλων, την προστασία των συστημάτων και των δικτύων, τον έλεγχο της πρόσβασης στα δεδομένα, την κρυπτογράφηση και ασφαλή διαχείριση των πληροφοριών πληρωμής, τη συνεχή παρακολούθηση και καταγραφή των σχετικών συστημάτων, καθώς και την τακτική αξιολόγηση της ασφάλειας των πληροφοριακών υποδομών. Με τον τρόπο αυτό, το PCI DSS επιχειρεί να περιορίσει την πιθανότητα υποκλοπής, μη εξουσιοδοτημένης πρόσβασης και κατάχρησης των δεδομένων καρτών, τα οποία αποτελούν έναν από τους πλέον κρίσιμους στόχους των κυβερνοεπιθέσεων στο λιανικό εμπόριο.

[14] https://www.pcisecuritystandards.org/standards/

Ιδιαίτερο ενδιαφέρον παρουσιάζει, ωστόσο, η σχέση του PCI DSS με τις δημόσιες ρυθμίσεις που εξετάστηκαν προηγουμένως. Το πρότυπο λειτουργεί συμπληρωματικά προς το GDPR, τη NIS2 και, έμμεσα, το DORA, χωρίς να τα υποκαθιστά. Ενώ ο GDPR επικεντρώνεται στην προστασία των προσωπικών δεδομένων, η NIS2 στη διαχείριση των κυβερνοκινδύνων και την ανθεκτικότητα συγκεκριμένων κατηγοριών οντοτήτων και ο DORA στην ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα, το PCI DSS επικεντρώνεται ειδικότερα στην ασφάλεια των δεδομένων που συνδέονται με τις πληρωμές με κάρτα. Μία εμπορική επιχείρηση μπορεί, επομένως, να βρίσκεται ταυτόχρονα αντιμέτωπη με διαφορετικά επίπεδα κανονιστικών και συμβατικών απαιτήσεων, τα οποία αλληλοσυμπληρώνονται, αλλά δεν ταυτίζονται ως προς το αντικείμενο, τη νομική τους βάση και τους μηχανισμούς επιβολής.

Η διάσταση αυτή αποκτά ιδιαίτερη σημασία για τις μικρομεσαίες του λιανικού εμπορίου. Η συμμόρφωση με ένα σύνθετο σύνολο τεχνικών απαιτήσεων μπορεί να συνεπάγεται κόστος για την αναβάθμιση των πληροφοριακών συστημάτων, την ασφαλή διαχείριση των τερματικών POS, την εκπαίδευση του προσωπικού, τη διενέργεια ελέγχων και την παρακολούθηση των συστημάτων. Για μια μεγάλη επιχείρηση, οι απαιτήσεις αυτές μπορούν να ενσωματωθούν σε ένα οργανωμένο σύστημα διακυβέρνησης της ασφάλειας πληροφοριών. Για μια μικρή επιχείρηση, αντίθετα, μπορεί να αποτελούν σημαντική οικονομική και οργανωτική επιβάρυνση, ιδιαίτερα όταν δεν διαθέτει εξειδικευμένο προσωπικό κυβερνοασφάλειας, αναδεικνύοντας την ανάγκη της αναλογικής προσέγγισης στην κυβερνοασφάλεια των μικρών και πολύ μικρών επιχειρήσεων, καθώς η θέσπιση ολοένα αυστηρότερων απαιτήσεων δεν εξασφαλίζει από μόνη της αποτελεσματικότερη προστασία εάν οι μικρές επιχειρήσεις δεν διαθέτουν τους αναγκαίους πόρους και την τεχνογνωσία για την εφαρμογή τους.

Το PCI DSS αναδεικνύει, τέλος, μία ευρύτερη ιδιαιτερότητα του σύγχρονου οικοσυστήματος ψηφιακών πληρωμών, ότι η ασφάλεια δεν διαμορφώνεται αποκλειστικά μέσω δημόσιας ρύθμισης, αλλά και μέσω των ιδιωτικών προτύπων που αναπτύσσονται από τους ίδιους τους φορείς της αγοράς. Η συνύπαρξη δημόσιων κανόνων και ιδιωτικών προτύπων μπορεί να ενισχύσει το επίπεδο προστασίας, δημιουργεί όμως ταυτόχρονα ένα περισσότερο σύνθετο περιβάλλον συμμόρφωσης για τις επιχειρήσεις.

5.3 Το κόστος της κανονιστικής συμμόρφωσης για τις μικρομεσαίες επιχειρήσεις

Η ανάλυση του ευρωπαϊκού ρυθμιστικού πλαισίου για την κυβερνοασφάλεια αναδεικνύει ένα κρίσιμο ζήτημα πολιτικής, αυτό της αναλογικότητας του κανονιστικού κόστους σε σχέση με τις οικονομικές, οργανωτικές και τεχνολογικές δυνατότητες των επιχειρήσεων. Παρότι η ευρωπαϊκή νομοθεσία υιοθετεί σε σημαντικό βαθμό μια προσέγγιση βασισμένη στον κίνδυνο και, ιδίως στην περίπτωση της NIS2, διαφοροποιεί τις υποχρεώσεις ανάλογα με το μέγεθος και τη σημασία των οντοτήτων, η πρακτική εφαρμογή των απαιτήσεων κυβερνοασφάλειας μπορεί να δημιουργεί δυσανάλογες επιβαρύνσεις για τις μικρές και πολύ μικρές επιχειρήσεις. Η διαφορά αυτή δεν προκύπτει κατ' ανάγκην από την επιβολή υψηλότερων τυπικών υποχρεώσεων σε αυτές, αλλά από το γεγονός ότι το σταθερό κόστος συμμόρφωσης κατανέμεται σε πολύ μικρότερη οικονομική βάση και, συνεπώς, αντιπροσωπεύει αναλογικά μεγαλύτερο μέρος των διαθέσιμων πόρων τους. Δημιουργείται, κατά αυτόν τον τρόπο ,μια σημαντική ασυμμετρία μεταξύ επιχειρήσεων διαφορετικού μεγέθους: ενώ οι μεγάλες επιχειρήσεις μπορούν να κατανείμουν το κόστος της συμμόρφωσης σε μεγαλύτερο κύκλο εργασιών και να αξιοποιήσουν οικονομίες κλίμακας, οι μικρότερες αντιμετωπίζουν συχνά το ίδιο ή παρόμοιο σύνολο τεχνικών, οργανωτικών και διοικητικών προκλήσεων με πολύ περιορισμένες εσωτερικές δυνατότητες και πόρους.

Το άμεσο οικονομικό κόστος της κανονιστικής συμμόρφωσης στον τομέα της κυβερνοασφάλειας περιλαμβάνει πολλαπλές και αλληλοσυνδεόμενες παραμέτρους. Σε αυτές περιλαμβάνονται η αρχική αξιολόγηση της υφιστάμενης κατάστασης ασφάλειας και ο εντοπισμός αποκλίσεων από τις απαιτήσεις (*gap analysis*), η εγκατάσταση ή αναβάθμιση τεχνικών συστημάτων προστασίας, η εφαρμογή διαδικασιών διαχείρισης κινδύνων, η εκπαίδευση του προσωπικού, η σύνταξη και επικαιροποίηση πολιτικών και διαδικασιών, καθώς και η διαρκής παρακολούθηση και τεκμηρίωση της συμμόρφωσης. Στις δαπάνες αυτές προστίθεται το κόστος των περιοδικών ελέγχων, των αξιολογήσεων και των δοκιμών, καθώς και το κόστος προσαρμογής στις μεταβαλλόμενες τεχνολογικές και κανονιστικές απαιτήσεις Schmidt et al., 2007). Για μια μεγάλη επιχείρηση, σημαντικό μέρος αυτών των δαπανών μπορεί να ενσωματωθεί στις υφιστάμενες δομές της εταιρικής διακυβέρνησης και της διαχείρισης κινδύνων. Αντίθετα, για μια μικρότερη, ακόμη και σχετικά πολύ μικρές δαπάνες

αντιπροσωπεύουν σημαντικό ποσοστό του διαθέσιμου λειτουργικού της προϋπολογισμού.

Το πρόβλημα γίνεται ακόμη εντονότερο όταν η συμμόρφωση απαιτεί εξειδικευμένο ανθρώπινο δυναμικό. Η κυβερνοασφάλεια αποτελεί έναν τομέα στον οποίο η ζήτηση για εξειδικευμένες δεξιότητες υπερβαίνει σημαντικά τη διαθέσιμη προσφορά, γεγονός που αυξάνει το κόστος πρόσληψης και διατήρησης του κατάλληλου προσωπικού. Για τις περισσότερες μικρές επιχειρήσεις λιανικής, η δημιουργία ενός εσωτερικού τμήματος κυβερνοασφάλειας δεν αποτελεί ρεαλιστική οργανωτική επιλογή. Η εξωτερική ανάθεση λειτουργιών σε εξειδικευμένους παρόχους, όπως οι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας (*Managed Security Service Providers – MSSPs*), μπορεί να αποτελέσει, ενδεχομένως, την αποτελεσματικότερη και οικονομικά αποδοτικότερη λύση (Aiyer et al., 2021). Ωστόσο, η εξωτερική ανάθεση δεν εξαλείφει την ανάγκη της εσωτερικής εποπτείας, καθώς η επιχείρηση εξακολουθεί να πρέπει να είναι σε θέση να αξιολογεί την καταλληλότητα του παρόχου, να κατανοεί τους κινδύνους που συνδέονται με την παρεχόμενη υπηρεσία, να καθορίζει σαφώς τις συμβατικές ευθύνες και να παρακολουθεί την ποιότητα και την αποτελεσματικότητα των μέτρων ασφαλείας. Συνεπώς, ακόμη και όταν η τεχνική εξειδίκευση αγοράζεται (out of house), απαιτείται ένα ελάχιστο επίπεδο εσωτερικής οργανωτικής ικανότητας προκειμένου η εξωτερική ανάθεση να μην μετατραπεί σε νέα μορφή τεχνολογικής εξάρτησης.

Σημαντική παράμετρος αποτελεί επίσης η πρόσβαση των μικρομεσαίων επιχειρήσεων σε χρηματοδοτικά εργαλεία για την πραγματοποίηση των απαιτούμενων επενδύσεων. Σε ευρωπαϊκό επίπεδο, προγράμματα όπως το *Digital Europe Programme*[15], έχουν συμβάλει στη δημιουργία δυνατοτήτων χρηματοδότησης για την ανάπτυξη ψηφιακών και κυβερνοασφαλών υποδομών. Ωστόσο, η διαθεσιμότητα των χρηματοδοτικών πόρων δεν συνεπάγεται αυτομάτως και την ουσιαστική πρόσβαση των μικρών επιχειρήσεων σε αυτούς. Η συμμετοχή σε ανταγωνιστικά προγράμματα απαιτεί συχνά διοικητική επάρκεια, τεχνική τεκμηρίωση, ικανότητα προετοιμασίας προτάσεων και, σε αρκετές περιπτώσεις, δυνατότητα συγχρηματοδότησης. Οι απαιτήσεις αυτές

[15] https://www.ese-hormones.org/what-we-do/research/european-research-funding/funding-programmes/digital-europe/?gad_source=1&gad_campaignid=20039600869&gbraid=0AAAAAoxFtxB_Uh3ozaxys4Dm6rAPtXyeX&gclid=EAIaIQobChMIlqq53qXalgMVIJ9oCR1HJRN3EAAYASAAEgIc0PD_BwE

μπορούν να λειτουργήσουν ως πρόσθετο εμπόδιο για τις πολύ μικρές επιχειρήσεις, οι οποίες δεν διαθέτουν εξειδικευμένα στελέχη ή διοικητικές δομές για την αξιοποίηση σύνθετων χρηματοδοτικών εργαλείων.

Το ζήτημα αποκτά ιδιαίτερη σημασία υπό το πρίσμα των θέσεων που έχουν διατυπωθεί από τους ευρωπαϊκούς φορείς εκπροσώπησης των μικρομεσαίων επιχειρήσεων. Για παράδειγμα, η SMEunited (2024) έχει επισημάνει ότι σχεδόν δύο στις τρεις επιχειρήσεις αυτού του μεγέθους αντιμετωπίζουν δυσκολίες στη διασφάλιση του επαρκούς επιπέδου κυβερνοασφάλειας, με την έλλειψη δεξιοτήτων και το οικονομικό κόστος να συγκαταλέγονται μεταξύ των σημαντικότερων εμποδίων. Η διαπίστωση αυτή είναι ιδιαίτερα κρίσιμη, καθώς καταδεικνύει ότι το πρόβλημα δεν αφορά απλώς την προθυμία των επιχειρήσεων να επενδύσουν στην κυβερνοασφάλεια, αλλά την πραγματική τους ικανότητα να ανταποκριθούν στις απαιτήσεις ενός ολοένα και πιο σύνθετου τεχνολογικού και κανονιστικού περιβάλλοντος. Αντίστοιχα, η EuroCommerce (2024) έχει αναδείξει την ανάγκη για σημαντικές επενδύσεις στον ψηφιακό μετασχηματισμό του λιανικού και χονδρικού εμπορίου, συμπεριλαμβανομένης της κυβερνοασφάλειας, υπογραμμίζοντας ότι η ψηφιακή μετάβαση του κλάδου απαιτεί σημαντικούς οικονομικούς και τεχνολογικούς πόρους. Η διάσταση αυτή είναι ιδιαίτερα σημαντική για τον ελληνικό λιανικό κλάδο, όπου η μεγάλη παρουσία πολύ μικρών επιχειρήσεων περιορίζει τις δυνατότητες αξιοποίησης οικονομιών κλίμακας και δημιουργεί μεγαλύτερη εξάρτηση από εξωτερικούς τεχνολογικούς παρόχους.

Για το ελληνικό λιανικό εμπόριο, η πρόκληση συνδέεται και με την ανάγκη μετάβασης από μια προσέγγιση που επικεντρώνεται κυρίως στην τυπική συμμόρφωση προς μια περισσότερο υποστηρικτική και πρακτικά προσανατολισμένη πολιτική κυβερνοασφάλειας. Η ενσωμάτωση των ευρωπαϊκών απαιτήσεων στο εθνικό δίκαιο αυξάνει τη σημασία της ενημέρωσης, της καθοδήγησης και της ανάπτυξης κατάλληλων εργαλείων για τις επιχειρήσεις που δεν διαθέτουν εξειδικευμένη τεχνική και νομική υποστήριξη. Για τις μικρές και πολύ μικρές επιχειρήσεις η πρόσβαση σε απλές και κατανοητές κατευθύνσεις, πρότυπες διαδικασίες, εργαλεία αυτοαξιολόγησης και οικονομικά προσιτές υπηρεσίες κυβερνοασφάλειας μπορεί να είναι εξίσου σημαντική με την ίδια τη θέσπιση των κανονιστικών απαιτήσεων. Η αποτελεσματικότητα της ρύθμισης εξαρτάται, επομένως, όχι μόνο από την αυστηρότητα των υποχρεώσεων,

αλλά και από την ικανότητα των επιχειρήσεων να τις κατανοήσουν και να τις εφαρμόσουν στην πράξη.

Υπό αυτή την οπτική, αναδεικνύεται ο κίνδυνος δημιουργίας ενός νέου τύπου «ψηφιακού χάσματος», όχι πλέον αποκλειστικά ως προς την πρόσβαση στις ψηφιακές τεχνολογίες, αλλά ως προς την ικανότητα της ασφαλούς και κανονιστικά συμβατής αξιοποίησής τους. Μια επιχείρηση μπορεί να διαθέτει POS, ηλεκτρονικό κατάστημα, ψηφιακές πληρωμές και συστήματα διαχείρισης δεδομένων και, παρ' όλα αυτά, να μην διαθέτει τις αναγκαίες οργανωτικές και τεχνικές δυνατότητες για την αποτελεσματική προστασία αυτών των υποδομών. Η ψηφιακή υιοθέτηση, συνεπώς, δεν ταυτίζεται με την ψηφιακή ανθεκτικότητα. Εάν το κανονιστικό κόστος και οι απαιτήσεις κυβερνοασφάλειας αυξηθούν ταχύτερα από την ικανότητα των μικρομεσαίων επιχειρήσεων να επενδύσουν σε τεχνολογία, δεξιότητες και οργανωτικές διαδικασίες, είναι πιθανό να δημιουργηθούν νέες μορφές εξάρτησης από εξωτερικούς παρόχους, ακόμη και να περιοριστεί η δυνατότητα ορισμένων επιχειρήσεων να συμμετέχουν ισότιμα στο ψηφιακό οικοσύστημα.

Συνεπώς, η αποτελεσματική πολιτική κυβερνοασφάλειας για το λιανικό εμπόριο δεν θα πρέπει να εξαντλείται στην τυπική μεταφορά των κανονιστικών απαιτήσεων από το ευρωπαϊκό στο εθνικό επίπεδο. Θα πρέπει να συνοδεύεται από μηχανισμούς που μειώνουν το κόστος συμμόρφωσης, ενισχύουν την πρόσβαση των μικρομεσαίων επιχειρήσεων σε τεχνογνωσία και χρηματοδότηση και επιτρέπουν την αξιοποίηση κοινών ή επιμερισμένων υπηρεσιών κυβερνοασφάλειας. Ιδιαίτερη σημασία έχουν η ανάπτυξη απλών προτύπων και εργαλείων αυτοαξιολόγησης, η παροχή πρακτικής τεχνικής καθοδήγησης, η ενίσχυση προγραμμάτων κατάρτισης και η δημιουργία οικονομικά προσιτών υπηρεσιών κυβερνοασφάλειας προσαρμοσμένων στις ανάγκες των μικρών επιχειρήσεων. Στο πλαίσιο αυτό, η ΕΣΕΕ μπορεί να διαδραματίσει σημαντικό ρόλο ως ενδιάμεσος θεσμός μεταξύ των επιχειρήσεων και των δημόσιων και ευρωπαϊκών φορέων, συμβάλλοντας τόσο στη διάχυση της σχετικής τεχνογνωσίας, όσο και στη διαμόρφωση ενός περισσότερο αναλογικού και εφαρμόσιμου θεσμικού και κανονιστικού πλαισίου. Η αναλογικότητα, η τεχνική, η χρηματοδοτική υποστήριξη και η πρόσβαση σε οικονομικά προσιτές λύσεις δεν θα πρέπει, συνεπώς, να θεωρούνται εξαιρέσεις από το κανονιστικό πλαίσιο, αλλά αναγκαίες προϋποθέσεις για την αποτελεσματική εφαρμογή του. Μόνον υπό αυτές τις συνθήκες η ενίσχυση των απαιτήσεων κυβερνοασφάλειας μπορεί να λειτουργήσει ως παράγοντας ψηφιακής

ανθεκτικότητας και ανταγωνιστικότητας και όχι ως πρόσθετο εμπόδιο για τη συμμετοχή των μικρών και πολύ μικρών επιχειρήσεων στο ψηφιακό οικοσύστημα του σύγχρονου λιανικού εμπορίου.

6. Οι μικρομεσαίες επιχειρήσεις του λιανικού εμπορίου απέναντι στις προκλήσεις της κυβερνοασφάλειας

6.1 Το «ψηφιακό χάσμα» στην κυβερνοασφάλεια

Η έννοια του «ψηφιακού χάσματος» —η οποία αρχικά χρησιμοποιήθηκε για να περιγράψει τις ανισότητες ως προς την πρόσβαση στις ψηφιακές τεχνολογίες μεταξύ διαφορετικών κοινωνικών ομάδων, γεωγραφικών περιοχών και κατηγοριών επιχειρήσεων— αποκτά πλέον μια νέα και εξίσου κρίσιμη διάσταση: το χάσμα κυβερνοασφάλειας μεταξύ των μεγάλων και των μικρομεσαίων επιχειρήσεων. Η διάσταση αυτή δεν αφορά πλέον πρωτίστως την πρόσβαση στην τεχνολογία, αλλά την άνιση ικανότητα ασφαλούς αξιοποίησής της και την αποτελεσματική προστασία από τους κινδύνους που η ίδια η ψηφιοποίηση δημιουργεί. Πρόκειται, συνεπώς, για μια μορφή ανισότητας που αφορά το αν μια επιχείρηση διαθέτει τους οικονομικούς, τεχνολογικούς, οργανωτικούς και ανθρώπινους πόρους που απαιτούνται για την προστασία της

Το χάσμα αυτό είναι πολυδιάστατο και δεν ανάγεται απλώς στην ανισότητα ως προς τους διαθέσιμους οικονομικούς πόρους. Περιλαμβάνει και ανισότητες ως προς την εξειδικευμένη γνώση και τις δεξιότητες κυβερνοασφάλειας, ως προς την ικανότητα αξιολόγησης του κυβερνοκινδύνου και σχεδιασμού στρατηγικής αντιμετώπισής του, ως προς την πρόσβαση σε αξιόπιστη πληροφόρηση και τεχνική καθοδήγηση, ως προς τη δυνατότητα ανάκαμψης μετά από ένα κυβερνοσυμβάν και ως προς την ικανότητα παρακολούθησης της συνεχώς εξελισσόμενης απειλητικής τοπογραφίας. Κάθε μία από αυτές τις ανισότητες αποτελεί από μόνη της σημαντικό παράγοντα διαφοροποίησης, ενώ στο σύνολό τους συνιστούν ένα δομικό μειονέκτημα των μικρομεσαίων επιχειρήσεων.

Σύμφωνα με έκθεση *State of Cybersecurity in the Union 2024*, της ENISA[16], το 83% των μεγάλων επιχειρήσεων στην ΕΕ είχε υιοθετήσει το 2022 τουλάχιστον ένα μέτρο ασφάλειας ΤΠΕ (Τεχνολογίες Πληροφορικής & Επικοινωνιών), έναντι μόλις 49% των

[16] https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

αντίστοιχων μικρομεσαίων. Ακόμη μεγαλύτερο αποδεικνύεται το χάσμα ως προς την ολοκληρωμένη εφαρμογή των μέτρων ασφάλειας, καθώς ενώ το 17% των μεγάλων επιχειρήσεων εφάρμοζε το σύνολο των εξεταζόμενων μέτρων, το αντίστοιχο ποσοστό για τις μικρές επιχειρήσεις περιοριζόταν μόλις στο 4%. Αντίστοιχα, το 80% των μεγάλων επιχειρήσεων διέθετε τεκμηριωμένα μέτρα, πρακτικές και διαδικασίες κυβερνοασφάλειας, έναντι 36% των μικρομεσαίων, ενώ το 58% των μεγάλων επιχειρήσεων είχε ορίσει και επανεξετάσει πολιτική ασφάλειας ΤΠΕ κατά τους προηγούμενους 12 μήνες, έναντι μόλις 23% των μικρότερων επιχειρήσεων. Η διαφορά είναι ακόμη εντονότερη στη συστηματική αξιολόγηση κινδύνων, καθώς το 72% των μεγάλων επιχειρήσεων πραγματοποιούσε αξιολογήσεις κινδύνου για περιστατικά ασφάλειας ΤΠΕ, ενώ στις μικρομεσαίες το αντίστοιχο ποσοστό ανερχόταν μόλις στο 31%.

Η υστέρηση των μικρομεσαίων επιχειρήσεων δεν αφορά μόνο τις τεχνικές υποδομές, αλλά και τη δυνατότητα ανάπτυξης και διατήρησης της αναγκαίας οργανωτικής και ανθρώπινης ικανότητας. Η νεότερη έκθεση της ENISA, *NIS Investments 2025*[17]*,* καταγράφει ότι το 94% των μικρομεσαίων που συμμετείχαν στην έρευνα αντιμετωπίζει δυσκολίες στην προσέλκυση προσωπικού κυβερνοασφάλειας και το 90% δυσκολίες στη διατήρησή του, έναντι 83% και 80%, αντίστοιχα, των μεγάλων επιχειρήσεων. Παράλληλα, η ENISA επισημαίνει ότι οι μικρότερες επιχειρήσεις είναι λιγότερο πιθανό να διαθέτουν εξειδικευμένο προσωπικό και τυποποιημένες διαδικασίες για τη διαχείριση κυβερνοκινδύνων.

Στο ελληνικό πλαίσιο, το ψηφιακό χάσμα της κυβερνοασφάλειας λαμβάνει ιδιαίτερη βαρύτητα λόγω της δομής της επιχειρηματικής βάσης. Η ελληνική οικονομία χαρακτηρίζεται από εξαιρετικά υψηλή συγκέντρωση πολύ μικρών επιχειρήσεων (μέχρι 9 εργαζόμενους), οι οποίες αποτελούν τη συντριπτική πλειονότητα των επιχειρήσεων λιανικής. Οι οντότητες αυτές λειτουργούν κατά κανόνα χωρίς εξειδικευμένο τεχνικό προσωπικό, βασίζονται σε ετερογενείς, συχνά απαρχαιωμένες τεχνολογικές υποδομές και στερούνται της οργανωτικής ικανότητας για συστηματική διαχείριση κινδύνου. Η ψηφιοποίηση των πληρωμών τους — επιταχυνόμενη από θεσμικές ρυθμίσεις και φορολογικά κίνητρα — ενίσχυσε την έκθεσή τους σε κυβερνοαπειλές χωρίς να

[17] https://www.enisa.europa.eu/publications/nis-investments-2025

συνοδευτεί από ανάλογη ενίσχυση της ικανότητάς τους να τις αντιμετωπίσουν αποτελεσματικά.

Η υστέρηση των ελληνικών μικρομεσαίων επιχειρήσεων δεν περιορίζεται, ωστόσο, στις ειδικές πρακτικές κυβερνοασφάλειας, αλλά εντάσσεται σε ένα ευρύτερο έλλειμμα ψηφιακής ωριμότητας. Οι δείκτες που χρησιμοποιούνται από την Ευρωπαϊκή Επιτροπή στο πλαίσιο του Digital Decade, καθώς και ο Δείκτης Ψηφιακής Έντασης (Digital Intensity Index – DII), καταγράφουν διαχρονικά σημαντική απόσταση μεταξύ των ελληνικών μικρομεσαίων επιχειρήσεων και του ευρωπαϊκού μέσου όρου ως προς την υιοθέτηση και αξιοποίηση των ψηφιακών τεχνολογιών. Σύμφωνα με τα πλέον πρόσφατα διαθέσιμα στοιχεία, το 2024 μόλις το 55,95% των ελληνικών μικρομεσαίων επιχειρήσεων διέθετε τουλάχιστον το βασικό επίπεδο ψηφιακής έντασης, έναντι 71,39% στην ΕΕ . Η απόσταση είναι ακόμη μεγαλύτερη ως προς την υιοθέτηση των προηγμένων ψηφιακών τεχνολογιών, με την Ελλάδα να υπολείπεται του ευρωπαϊκού μέσου όρου σε τομείς όπως η τεχνητή νοημοσύνη, το υπολογιστικό νέφος και η αξιοποίηση δεδομένων (European Commission, 2025).

6.2 Εξάρτηση από τρίτους παρόχους και μεταφορά ρίσκου

Μία από τις πλέον χαρακτηριστικές ιδιαιτερότητες της επιχειρησιακής πραγματικότητας των μικρομεσαίων επιχειρήσεων στον τομέα της κυβερνοασφάλειας είναι η αυξανόμενη εξάρτησή τους από τρίτους παρόχους τεχνολογίας και ψηφιακών υπηρεσιών. Η εξάρτηση αυτή είναι ιδιαίτερα έντονη στο λιανικό εμπόριο, όπου οι μικρές και πολύ μικρές επιχειρήσεις διαθέτουν συνήθως περιορισμένες εσωτερικές τεχνολογικές και οργανωτικές δυνατότητες και, ως εκ τούτου, προσφεύγουν σε εξωτερικούς παρόχους για την ανάπτυξη, λειτουργία και υποστήριξη σημαντικού μέρους της ψηφιακής τους υποδομής. Η καθημερινή λειτουργία μιας σύγχρονης εμπορικής επιχείρησης μπορεί να εξαρτάται ταυτόχρονα από τερματικά POS και το σχετικό λογισμικό, παρόχους υπηρεσιών αποδοχής και επεξεργασίας πληρωμών, payment gateways, πλατφόρμες ηλεκτρονικού εμπορίου, συστήματα διαχείρισης αποθεμάτων και πελατειακών σχέσεων, υπηρεσίες υπολογιστικού νέφους (cloud), καθώς και τηλεπικοινωνιακές και άλλες ψηφιακές υπηρεσίες.

Η εκτεταμένη αυτή εξάρτηση μεταβάλλει ουσιαστικά και τη φύση του κυβερνοκινδύνου που αντιμετωπίζει η επιχείρηση. Η ασφάλεια των πληροφοριακών

της συστημάτων δεν εξαρτάται πλέον αποκλειστικά από τα μέτρα που εφαρμόζει στο εσωτερικό της, αλλά επηρεάζεται άμεσα από το επίπεδο ασφάλειας, τις διαδικασίες διαχείρισης κινδύνων και την επιχειρησιακή ανθεκτικότητα των τρίτων παρόχων από τους οποίους εξαρτάται. Μία ευπάθεια σε έναν πάροχο υπηρεσιών πληρωμών, έναν προμηθευτή λογισμικού ή έναν πάροχο cloud μπορεί, υπό συγκεκριμένες συνθήκες, να μετατραπεί σε έμμεσο κίνδυνο για μεγάλο αριθμό επιχειρήσεων που χρησιμοποιούν την ίδια υποδομή. Η σχέση αυτή δημιουργεί ένα σύνθετο πρόβλημα διαχείρισης κινδύνων τρίτων μερών (third-party risk management), καθώς η επιχείρηση καλείται να διαχειριστεί κινδύνους τους οποίους δεν μπορεί να ελέγξει πλήρως και συχνά δεν διαθέτει την τεχνική ή διαπραγματευτική ισχύ για να αξιολογήσει σε βάθος.

Η εξάρτηση από τρίτους παρόχους δημιουργεί ένα ιδιαίτερα κρίσιμο παράδοξο κυβερνοκινδύνου, καθώς η επιχείρηση μπορεί να μεταβιβάζει στην πράξη σημαντικό μέρος της τεχνολογικής διαχείρισης σε εξωτερικούς φορείς, χωρίς όμως να μεταβιβάζει αυτομάτως και το σύνολο των κανονιστικών της υποχρεώσεων. Η ανάθεση μιας ψηφιακής λειτουργίας σε τρίτο πάροχο δεν εξαλείφει την ευθύνη της επιχείρησης για την ορθή διακυβέρνηση των δεδομένων και των πληροφοριακών της υποδομών, αλλά καθιστά αναγκαία τη σαφή κατανομή ρόλων, ευθυνών και υποχρεώσεων μεταξύ των εμπλεκόμενων μερών. Η διάσταση αυτή είναι ιδιαίτερα εμφανής στο πλαίσιο του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ/GDPR). Όταν μια επιχείρηση ενεργεί ως υπεύθυνος επεξεργασίας (data controller) και αναθέτει την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε τρίτο πάροχο, ο πάροχος ενεργεί, υπό τις προϋποθέσεις του Κανονισμού, ως εκτελών την επεξεργασία (data processor). Η ανάθεση αυτή δεν απαλλάσσει τον υπεύθυνο επεξεργασίας από τις υποχρεώσεις του έναντι του ΓΚΠΔ, καθώς εξακολουθεί να οφείλει να επιλέγει κατάλληλους εκτελούντες την επεξεργασία, να διασφαλίζει ότι παρέχουν επαρκείς εγγυήσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων και να καθορίζει τη μεταξύ τους σχέση μέσω κατάλληλης σύμβασης. Παράλληλα, ο ίδιος ο εκτελών την επεξεργασία υπέχει αυτοτελείς υποχρεώσεις βάσει του ΓΚΠΔ και μπορεί να υπέχει ευθύνη για παραβάσεις που εμπίπτουν στο δικό του πεδίο υποχρεώσεων.

Η αντίφαση είναι ιδιαίτερα έντονη στην περίπτωση των μικρών επιχειρήσεων λιανικής, καθώς οι τελευταίες καλούνται να αξιολογήσουν και να διαχειριστούν κινδύνους που συνδέονται με παρόχους —όπως τράπεζες, πάροχοι υπηρεσιών πληρωμών, payment processors και πάροχοι υπολογιστικού νέφους— οι οποίοι διαθέτουν κατά κανόνα

σημαντικά μεγαλύτερους οικονομικούς, τεχνολογικούς και ανθρώπινους πόρους, καθώς και πολύ υψηλότερο επίπεδο εξειδίκευσης στον τομέα της κυβερνοασφάλειας. Η σχέση αυτή δημιουργεί μια εγγενή ασυμμετρία πληροφόρησης και διαπραγματευτικής ισχύος, η μικρή επιχείρηση δεν διαθέτει πάντοτε την τεχνική ικανότητα να αξιολογήσει σε βάθος την ασφάλεια μιας σύνθετης ψηφιακής υπηρεσίας ούτε τη διαπραγματευτική ισχύ που θα της επέτρεπε να απαιτήσει εξατομικευμένους όρους προστασίας, ελέγχου και διαχείρισης περιστατικών.

Ταυτόχρονα, η εξάρτηση από τρίτους παρόχους δημιουργεί ένα δεύτερο, συναφές με τη δομή της αγοράς, παράδοξο, καθώς οι μικρομεσαίες είναι εκ των πραγμάτων αναγκασμένες να εμπιστεύονται παρόχους τους οποίους συχνά δεν διαθέτουν την τεχνική και οργανωτική ικανότητα να αξιολογήσουν επαρκώς, σε έναν τομέα όπου η ασύμμετρη πληροφόρηση (information asymmetry) είναι ιδιαίτερα έντονη (Westerlund, 2020). Η ποιότητα της κυβερνοασφάλειας αποτελεί, άλλωστε, ένα χαρακτηριστικό υπηρεσίας που είναι δύσκολο να παρατηρηθεί και να αξιολογηθεί από τον πελάτη, ιδίως πριν από την πραγματοποίηση της συναλλαγής και ακόμη περισσότερο πριν από την εκδήλωση ενός περιστατικού. Μια επιχείρηση μπορεί να γνωρίζει το κόστος μιας υπηρεσίας, τη φήμη του παρόχου, χωρίς να είναι σε θέση να εκτιμήσει με ακρίβεια την πραγματική ανθεκτικότητα των συστημάτων του, την επάρκεια των μηχανισμών ανίχνευσης και απόκρισης ή την αποτελεσματικότητα των διαδικασιών διαχείρισης περιστατικών.

Υπό αυτές τις συνθήκες, η αδυναμία άμεσης αξιολόγησης της ποιότητας της κυβερνοασφάλειας μπορεί να οδηγήσει τις επιχειρήσεις στην υιοθέτηση υποκατάστατων κριτηρίων επιλογής, όπως η χαμηλότερη τιμή, η αναγνωρισιμότητα του παρόχου, η προηγούμενη εμπειρία συνεργασίας ή η γενικότερη φήμη του στην αγορά. Τα κριτήρια αυτά μπορεί να είναι χρήσιμα για τη λήψη επιχειρηματικών αποφάσεων, δεν αποτελούν όμως κατ' ανάγκην αξιόπιστους δείκτες της πραγματικής ικανότητας ενός παρόχου να προλαμβάνει, να ανιχνεύει και να αντιμετωπίζει κυβερνοαπειλές (Blatz et al., 2018). Η αδυναμία αυτή δημιουργεί τον κίνδυνο η ποιότητα της ασφάλειας να υποτιμάται κατά τη διαδικασία επιλογής παρόχου, καθώς η επιχείρηση δεν είναι σε θέση να παρατηρήσει άμεσα το επίπεδο προστασίας που αγοράζει.

Το πρόβλημα αποκτά ακόμη μεγαλύτερη σημασία όταν η σχέση αφορά κρίσιμες ψηφιακές λειτουργίες, όπως οι πληρωμές, η φιλοξενία δεδομένων ή η λειτουργία ενός

ηλεκτρονικού καταστήματος. Σε αυτές τις περιπτώσεις, η πραγματική ποιότητα της υπηρεσίας ως προς την κυβερνοασφάλεια μπορεί να αποκαλυφθεί μόνο εκ των υστέρων, όταν εκδηλωθεί ένα περιστατικό ή όταν προκύψει σοβαρή διακοπή της υπηρεσίας. Δημιουργείται έτσι ένα χαρακτηριστικό πρόβλημα πληροφοριακής ασυμμετρίας και ατελούς συμβολαιοποίησης, σύμφωνα με το οποίο ο πάροχος διαθέτει περισσότερες πληροφορίες σχετικά με τις πραγματικές δυνατότητες και τους περιορισμούς της υποδομής του από ό,τι η επιχείρηση-πελάτης, ενώ δεν είναι πάντοτε δυνατό να προβλεφθούν και να αποτυπωθούν συμβατικά όλες οι μελλοντικές μορφές κυβερνοκινδύνου.

Η διαχείριση της εξάρτησης από τρίτους παρόχους δεν μπορεί να επαφίεται αποκλειστικά στις ατομικές επιλογές και στις εσωτερικές δυνατότητες κάθε μικρομεσαίας επιχείρησης. Η ένταση της πληροφοριακής ασυμμετρίας, το υψηλό κόστος αξιολόγησης των παρόχων και η περιορισμένη διαπραγματευτική ισχύς των μικρών επιχειρήσεων καθιστούν αναγκαία την ανάπτυξη θεσμικών μηχανισμών που θα μειώνουν το κόστος πληροφόρησης και θα ενισχύουν τη δυνατότητα των μικρότερων επιχειρήσεων να διαχειρίζονται αποτελεσματικά τους σχετικούς κινδύνους. Στο πλαίσιο αυτό, ιδιαίτερη σημασία έχει η θέσπιση σαφών και αναλογικών, ελάχιστων, προτύπων κυβερνοασφάλειας για τους παρόχους κρίσιμων ψηφιακών υπηρεσιών που εξυπηρετούν μικρές επιχειρήσεις, καθώς και η ανάπτυξη απλών και συγκρίσιμων εργαλείων αξιολόγησης μέσω των οποίων μια μικρή επιχείρηση θα μπορεί να εκτιμά το επίπεδο ασφάλειας ενός παρόχου χωρίς να απαιτείται εξειδικευμένη τεχνική τεχνογνωσία.

Παράλληλα, απαιτείται ενίσχυση των μηχανισμών συλλογικής δράσης και εκπροσώπησης των μικρομεσαίων επιχειρήσεων. Η ατομική διαπραγμάτευση μιας μικρής επιχείρησης με μια μεγάλη τράπεζα, έναν πάροχο υπηρεσιών πληρωμών ή μια πολυεθνική εταιρεία τεχνολογίας πραγματοποιείται υπό συνθήκες σημαντικής ασυμμετρίας οικονομικής και πληροφοριακής ισχύος. Η συλλογική εκπροσώπηση μπορεί, υπό προϋποθέσεις, να περιορίσει αυτή την ασυμμετρία, επιτρέποντας στις επιχειρήσεις να διαπραγματεύονται από ισχυρότερη θέση και να διαμορφώνουν κοινά αποδεκτούς όρους σχετικά με την ασφάλεια, τη διαχείριση περιστατικών, την πρόσβαση και φορητότητα των δεδομένων, τη διαφάνεια και την επιχειρησιακή συνέχεια. Ενώσεις όπως η ΕΣΕΕ μπορούν να διαδραματίσουν, συνεπώς, έναν ουσιαστικό ρόλο ως συλλογικοί θεσμικοί διαμεσολαβητές, όχι μόνο εκπροσωπώντας

τα συμφέροντα των επιχειρήσεων έναντι των παρόχων και των δημόσιων αρχών, αλλά και αναπτύσσοντας κοινά εργαλεία αξιολόγησης, πρότυπα συμβατικών όρων, οδηγούς κυβερνοασφάλειας και μηχανισμούς διάχυσης τεχνογνωσίας.

Η προσέγγιση αυτή μετατοπίζει τη συζήτηση από την ατομική «ευθύνη» της κάθε επιχείρησης για την κυβερνοασφάλειά της, προς μια περισσότερο οικοσυστημική αντίληψη της ψηφιακής ανθεκτικότητας. Όταν οι μικρές επιχειρήσεις εξαρτώνται από κοινές ψηφιακές υποδομές και παρόχους, η ασφάλεια του κάθε επιμέρους χρήστη επηρεάζεται από την ασφάλεια του συνολικού οικοσυστήματος. Η δημόσια πολιτική θα πρέπει, επομένως, να επιδιώκει όχι μόνο την ενίσχυση των εσωτερικών δυνατοτήτων των μικρομεσαίων επιχειρήσεων, αλλά και τη δημιουργία ενός περιβάλλοντος στο οποίο οι πάροχοι κρίσιμων ψηφιακών υπηρεσιών υπόκεινται σε επαρκείς απαιτήσεις ασφάλειας, οι όροι συνεργασίας είναι διαφανείς και οι μικρές επιχειρήσεις διαθέτουν συλλογικά μέσα για να περιορίζουν την πληροφοριακή και διαπραγματευτική ασυμμετρία.

6.3 Εμπιστοσύνη των καταναλωτών ως ανταγωνιστικό πλεονέκτημα

Η κυβερνοασφάλεια τείνει να αντιμετωπίζεται στον επιχειρηματικό διάλογο πρωτίστως ως ένα στοιχείο κόστους, το οποίο εξειδικεύεται σε κόστος τεχνολογικής υποδομής, κόστος κανονιστικής συμμόρφωσης, κόστος εξειδικευμένου προσωπικού και υπηρεσιών, κόστος ασφάλισης και, κυρίως, κόστος αντιμετώπισης και ανάκαμψης από ένα περιστατικό κυβερνοασφάλειας. Η μονοδιάστατη αυτή προσέγγιση, ωστόσο, παραβλέπει μια κρίσιμη διάσταση του σύγχρονου ανταγωνισμού στο λιανικό εμπόριο. Η κυβερνοασφάλεια λειτουργεί ως παραγωγικό περιουσιακό στοιχείο της επιχείρησης, μέσω της ενίσχυσης της εμπιστοσύνης των καταναλωτών και της αξιοπιστίας της εμπορικής σχέσης. Σε ένα περιβάλλον όπου οι συναλλαγές πραγματοποιούνται ολοένα περισσότερο μέσω ψηφιακών καναλιών και όπου οι επιχειρήσεις συλλέγουν και επεξεργάζονται σημαντικούς όγκους προσωπικών και συναλλακτικών δεδομένων, η αντίληψη του καταναλωτή ότι τα δεδομένα και οι οικονομικές του συναλλαγές προστατεύονται αποτελεσματικά, ενισχύει την επιθυμία του να πραγματοποιήσει και να επαναλάβει μια αγορά.

Υπό αυτή την έννοια, η κυβερνοασφάλεια μπορεί να δημιουργήσει ανταγωνιστική αξία όχι μόνο επειδή μειώνει την πιθανότητα μιας ζημιογόνου επίθεσης, αλλά κυρίως εφόσον ενισχύει ένα άυλο περιουσιακό στοιχείο ιδιαίτερης σημασίας για το σύγχρονο λιανικό εμπόριο: την ψηφιακή εμπιστοσύνη, η οποία αποτυπώνεται σε υψηλότερη προθυμία ολοκλήρωσης μιας ηλεκτρονικής αγοράς, μεγαλύτερη διατήρηση και αφοσίωση της πελατειακής βάσης και ισχυρότερη μακροχρόνια σχέση μεταξύ επιχείρησης και καταναλωτή (Kosutic & Pigni, 2022) . Η κυβερνοασφάλεια μετατρέπεται, συνεπώς, από ένα είδος «αμυντικής» δαπάνης, σε δυνητικό παράγοντα διαφοροποίησης, ιδίως σε αγορές όπου οι καταναλωτές έχουν τη δυνατότητα να συγκρίνουν όχι μόνο τιμές και προϊόντα, αλλά και την αξιοπιστία, την ασφάλεια και τη συνολική ποιότητα της ψηφιακής εμπειρίας.

Η προστασία των δεδομένων, η ασφαλής πραγματοποίηση των πληρωμών και η διαφανής αντιμετώπιση περιστατικών κυβερνοασφάλειας μπορούν, υπό αυτή την έννοια, να αποτελέσουν στοιχεία διαφοροποίησης και να ενισχύσουν την αξιοπιστία μιας μικρής επιχείρησης έναντι των πελατών της. Η επένδυση στην κυβερνοασφάλεια δεν θα πρέπει, επομένως, να αξιολογείται αποκλειστικά με βάση το κόστος που αποφεύγεται σε περίπτωση επίθεσης, αλλά και με βάση την αξία που δημιουργείται μέσω της ενίσχυσης της εμπιστοσύνης, της επιχειρησιακής συνέχειας και της μακροχρόνιας σχέσης με τον καταναλωτή. Υπό αυτή την οπτική, η κυβερνοασφάλεια αποτελεί μέρος όχι μόνο της διαχείρισης κινδύνων, αλλά και της ευρύτερης στρατηγικής ανταγωνιστικότητας του σύγχρονου λιανικού εμπορίου.

Στο σημείο αυτό θα πρέπει να επισημανθεί ότι η σχέση μεταξύ κυβερνοασφάλειας και εμπιστοσύνης των καταναλωτών χαρακτηρίζεται από μια σημαντική ασυμμετρία, καθώς η απουσία ενός περιστατικού κυβερνοασφάλειας δεν μετατρέπεται αυτομάτως σε θετικό σήμα για τον καταναλωτή. Μια επιχείρηση δεν «κερδίζει» κατ' ανάγκη εμπιστοσύνη απλώς και μόνο επειδή δεν έχει υποστεί παραβίαση. Η οικοδόμηση ψηφιακής εμπιστοσύνης απαιτεί τη δημιουργία αξιόπιστων και ορατών σημάτων ασφάλειας, τα οποία μειώνουν την αβεβαιότητα του καταναλωτή ως προς την προστασία των δεδομένων και των συναλλαγών του. Τέτοια σήματα μπορεί να είναι η ύπαρξη αναγνωρισμένων πιστοποιήσεων και προτύπων ασφάλειας, η διαφάνεια ως προς τον τρόπο συλλογής και επεξεργασίας των δεδομένων, οι σαφείς και κατανοητές πολιτικές απορρήτου, η χρήση αξιόπιστων μηχανισμών αυθεντικοποίησης και η παροχή ασφαλών και εύχρηστων διαδικασιών πληρωμής (Chang et al., 2026).

Αντίθετα, ένα περιστατικό παραβίασης μπορεί να λειτουργήσει ως ιδιαίτερα ισχυρό αρνητικό σήμα, καθώς καθιστά ορατό έναν κίνδυνο ο οποίος προηγουμένως παρέμενε σε μεγάλο βαθμό μη παρατηρήσιμος. Η επίδραση στην εμπιστοσύνη εξαρτάται, ωστόσο, όχι μόνο από τη σοβαρότητα του περιστατικού, αλλά και από τον τρόπο με τον οποίο η επιχείρηση ανταποκρίνεται σε αυτό. Η έγκαιρη αναγνώριση του προβλήματος, η διαφάνεια ως προς την έκταση και τις συνέπειες της παραβίασης, η άμεση ενημέρωση των επηρεαζόμενων καταναλωτών και η λήψη συγκεκριμένων μέτρων περιορισμού και αποκατάστασης μπορούν να συμβάλουν στον περιορισμό της απώλειας εμπιστοσύνης. Αντίθετα, καθυστερημένη αντίδραση, ανεπαρκής ενημέρωση ή προσπάθεια υποβάθμισης του περιστατικού μπορούν να εντείνουν την αρνητική αντίληψη και να μετατρέψουν ένα τεχνικό συμβάν σε ευρύτερη κρίση αξιοπιστίας Bastian, 2023).

Συνεπώς, η μετατόπιση της αντίληψης για την κυβερνοασφάλεια — από κόστος συμμόρφωσης σε επένδυση ανταγωνιστικής διαφοροποίησης — συνιστά κεντρικό στρατηγικό ζήτημα στρατηγικής για τις μικρομεσαίες επιχειρήσεις του λιανικού εμπορίου. Η επένδυση σε βασικά μέτρα κυβερνοασφάλειας, η συστηματική αξιολόγηση και παρακολούθηση των τρίτων παρόχων, η εκπαίδευση του προσωπικού και η σαφής επικοινωνία της δέσμευσης της επιχείρησης για την ασφαλή διαχείριση των δεδομένων δεν θα πρέπει να αποτελούν απλές κανονιστικές υποχρεώσεις, αλλά θα πρέπει να λειτουργήσουν ως επενδύσεις στη σχέση εμπιστοσύνης με τον καταναλωτή. Η αξία της εμπιστοσύνης αυτής υπερβαίνει το άμεσο κόστος της πρόληψης και της συμμόρφωσης, καθώς συνδέεται με την αξιοπιστία της επιχείρησης, τη διατήρηση της πελατειακής βάσης και την προθυμία των καταναλωτών να συνεχίσουν να συναλλάσσονται μαζί της στο ψηφιακό περιβάλλον. Υπό αυτή την έννοια, η κυβερνοασφάλεια δεν θα πρέπει να αντιμετωπίζεται αποκλειστικά ως αμυντική δαπάνη, αλλά ως δυνητικός παράγοντας δημιουργίας αξίας και ανταγωνιστικής διαφοροποίησης, ιδιαίτερα για τις μικρότερες επιχειρήσεις που αναζητούν εναλλακτικές μορφές ανταγωνισμού πέρα από την κλίμακα, την τιμή και τις μεγάλες τεχνολογικές επενδύσεις.

7. Συμπεράσματα

Η ανάλυση που προηγήθηκε κατέδειξε ότι ο ψηφιακός μετασχηματισμός του λιανικού εμπορίου δεν συνιστά μια μεμονωμένη τεχνολογική μεταβολή, αλλά μια πολυδιάστατη διαδικασία αναδιάρθρωσης των όρων υπό τους οποίους πραγματοποιείται η εμπορική συναλλαγή, παράγεται και αξιοποιείται η πληροφορία και κατανέμεται ο κίνδυνος μεταξύ των εμπλεκόμενων φορέων. Η σταδιακή μετάβαση από την αποκλειστική χρήση των μετρητών στις ψηφιακές πληρωμές και η ταυτόχρονη ανάδυση ενός ολοένα πιο σύνθετου τοπίου κυβερνοαπειλών δεν αποτελούν δύο παράλληλα και ανεξάρτητα ζητήματα, αλλά δύο όψεις της ίδιας δομικής μεταβολής: όσο η αξία και η πληροφορία συγκεντρώνονται σε ψηφιακές υποδομές, τόσο αυξάνεται η στρατηγική σημασία της προστασίας τους, με αποτέλεσμα η κυβερνοασφάλεια να αναδεικνύεται σε αναπόσπαστο συστατικό στοιχείο της ίδιας της ψηφιοποίησης και όχι σε παρεπόμενο ζήτημα τεχνικής φύσεως.

Η εξέταση του οικοσυστήματος των ψηφιακών πληρωμών ανέδειξε ότι η ιστορική μετάβαση από τα μετρητά στις κάρτες, τις κινητές πληρωμές, την ανοιχτή τραπεζική και, πλέον, στις άμεσες πληρωμές δεν συνιστά απλή τεχνολογική εξέλιξη, αλλά διαδικασία η οποία αναδιατάσσει τους ρόλους των εμπλεκόμενων φορέων και μεταθέτει σταδιακά το κέντρο βάρους της συναλλαγής από την απλή ολοκλήρωση της πληρωμής στη διαχείριση των δεδομένων που αυτή παράγει. Το ελληνικό λιανικό εμπόριο, καθηλωμένο σε μεγάλο βαθμό στα πρώτα στάδια αυτής της εξέλιξης, καλείται να διαχειριστεί ταυτόχρονα την επιτάχυνση της ψηφιοποίησης, που προήλθε σε σημαντικό βαθμό από θεσμικές και φορολογικές παρεμβάσεις, και την υστέρηση στην ουσιαστική ενσωμάτωση των ψηφιακών εργαλείων σε ολοκληρωμένα συστήματα αξιοποίησης δεδομένων και διαχείρισης κινδύνου.

Στο επίπεδο της δημόσιας πολιτικής, η ανάλυση της διαδοχής PSD1–PSD2–PSD3 και του Κανονισμού για τις Άμεσες Πληρωμές κατέδειξε ότι η ευρωπαϊκή ρυθμιστική προσπάθεια, παρά τη σταδιακή της βελτίωση, εξακολουθεί να αντιμετωπίζει δυσκολίες στην πλήρη εξισορρόπηση μεταξύ καινοτομίας, ανταγωνισμού και ασφάλειας. Η εμπειρία της PSD2 ανέδειξε ιδίως ότι η διευκόλυνση της πρόσβασης νέων παρόχων δεν εξαλείφει αφ’ εαυτής τις ασυμμετρίες ισχύος, καθώς η ανάδυση των μεγάλων τεχνολογικών πλατφορμών δημιούργησε νέες μορφές συγκέντρωσης, ποιοτικά διαφορετικές από εκείνες του παραδοσιακού τραπεζοκεντρικού μοντέλου. Παράλληλα,

η ανάλυση του ανταγωνιστικού ελλείμματος στην αγορά πληρωμών, η συζήτηση για το ψηφιακό ευρώ ως δυνητικό εργαλείο στρατηγικής αυτονομίας και ο κίνδυνος χρηματοοικονομικού αποκλεισμού συγκλίνουν στη διαπίστωση ότι η ψηφιοποίηση των πληρωμών φέρει σημαντικές διανεμητικές συνέπειες, οι οποίες, αν δεν αντιμετωπιστούν συνειδητά μέσω κατάλληλα σχεδιασμένης ρύθμισης, ενδέχεται να αναπαράγουν, ακόμα και να εντείνουν τις υφιστάμενες ασυμμετρίες μεταξύ μεγάλων και μικρών επιχειρήσεων, καθώς και μεταξύ των διαφορετικών κατηγοριών καταναλωτών.

Η εξέταση του τοπίου των κυβερνοαπειλών ανέδειξε τη δομική —και όχι συγκυριακή— σύνδεση μεταξύ ψηφιοποίησης των πληρωμών και έκθεσης σε κυβερνοκίνδυνο, καθώς κάθε πρόσθετο ψηφιακό κανάλι διευρύνει ταυτόχρονα τις δυνατότητες εξυπηρέτησης του καταναλωτή και την επιφάνεια επίθεσης της επιχείρησης. Η επαγγελματοποίηση του κυβερνοεγκλήματος μέσω μοντέλων τύπου «Έγκλημα ως Υπηρεσία», η διάδοση του ransomware και η αυξανόμενη συμμετοχή τρίτων παρόχων στις παραβιάσεις καταδεικνύουν ότι η κυβερνοασφάλεια μιας επιχείρησης λιανικής δεν εξαρτάται πλέον αποκλειστικά από τα δικά της μέτρα προστασίας, αλλά από την ασφάλεια ενός ευρύτερου δικτύου τεχνολογικών αλληλεξαρτήσεων. Η ανισομερής κατανομή του κόστους των κυβερνοεπιθέσεων, με τις μικρομεσαίες επιχειρήσεις να πλήττονται δυσανάλογα από το ransomware και να διαθέτουν συγκριτικά περιορισμένες δυνατότητες ανάκαμψης, επιβεβαίωσε ότι ο κυβερνοκίνδυνος δεν κατανέμεται ουδέτερα στο εσωτερικό του κλάδου, αλλά ακολουθεί σε μεγάλο βαθμό τις προϋπάρχουσες ανισότητες πόρων και τεχνογνωσίας.

Η ανάλυση του ευρωπαϊκού ρυθμιστικού πλαισίου κυβερνοασφάλειας —NIS2, DORA, ΓΚΠΔ και, συμπληρωματικά, PCI DSS— ανέδειξε μια εγγενή αντίφαση, η οποία διατρέχει το σύνολο του δελτίου: ένα πλαίσιο σχεδιασμένο πρωτίστως με γνώμονα τις δυνατότητες μεγάλων οργανισμών εφαρμόζεται σε μια αγορά όπου κυριαρχούν πολύ μικρές επιχειρήσεις, με αποτέλεσμα το σταθερό κόστος συμμόρφωσης να επιβαρύνει αναλογικά περισσότερο εκείνους που διαθέτουν τους λιγότερους πόρους αντιμετώπισής του. Η έμμεση, οικοσυστημική επίδραση κανονιστικών πλαισίων όπως ο DORA, μέσω της μεταφοράς αυστηρότερων απαιτήσεων από τους χρηματοπιστωτικούς φορείς προς τους εμπόρους με τους οποίους συνεργάζονται, καταδεικνύει ότι η ουσιαστική έκθεση των επιχειρήσεων λιανικής σε

κανονιστικές υποχρεώσεις υπερβαίνει κατά πολύ το τυπικό πεδίο εφαρμογής της κάθε ρύθμισης ξεχωριστά.

Η συστηματική εξέταση της θέσης των μικρομεσαίων επιχειρήσεων απέναντι σε αυτές τις προκλήσεις κατέδειξε ότι το «ψηφιακό χάσμα» της κυβερνοασφάλειας αποτελεί σήμερα εξίσου κρίσιμη μορφή ανισότητας με το παραδοσιακό ψηφιακό χάσμα πρόσβασης σε τεχνολογία, με τα διαθέσιμα ευρωπαϊκά στοιχεία να επιβεβαιώνουν εκτεταμένες αποκλίσεις μεταξύ μεγάλων και μικρών επιχειρήσεων ως προς την υιοθέτηση μέτρων ασφάλειας, τη διαθεσιμότητα εξειδικευμένου προσωπικού και την ικανότητα συστηματικής αξιολόγησης κινδύνου. Η αυξανόμενη εξάρτηση των μικρών επιχειρήσεων λιανικής από τρίτους τεχνολογικούς παρόχους δημιουργεί ένα πρόσθετο παράδοξο, καθώς η ανάθεση της τεχνολογικής διαχείρισης δεν συνοδεύεται από αντίστοιχη μεταβίβαση της κανονιστικής ευθύνης, ενώ η ασυμμετρία πληροφόρησης καθιστά δυσχερή την ουσιαστική αξιολόγηση της ποιότητας ασφάλειας που προσφέρει ο εκάστοτε πάροχος. Παράλληλα, η ανάδειξη της κυβερνοασφάλειας ως στοιχείου ενίσχυσης της εμπιστοσύνης των καταναλωτών, και όχι απλώς ως αμυντικής δαπάνης, προσέφερε μια εναλλακτική, θετική οπτική, σύμφωνα με την οποία η επένδυση στην ψηφιακή προστασία μπορεί να λειτουργήσει ως παράγοντας ανταγωνιστικής διαφοροποίησης, ιδίως για τις μικρότερες επιχειρήσεις που αδυνατούν να ανταγωνιστούν μέσω κλίμακας ή τιμής.

Από το σύνολο της ανάλυσης προκύπτει ότι η αντιμετώπιση των προκλήσεων του ψηφιακού μετασχηματισμού για το ελληνικό λιανικό εμπόριο δεν μπορεί να στηριχθεί αποκλειστικά στη μεταφορά ευρωπαϊκών κανόνων στο εθνικό δίκαιο, ούτε στην ατομική προσπάθεια προσαρμογής κάθε επιχείρησης χωριστά. Απαιτείται μια πολιτική προσέγγιση η οποία θα συνδυάζει την αναλογικότητα του κανονιστικού βάρους με ουσιαστική τεχνική και χρηματοδοτική στήριξη, θα ενισχύει τη διαφάνεια και τη συγκρισιμότητα των παρόχων κρίσιμων ψηφιακών υπηρεσιών και θα αξιοποιεί μηχανισμούς συλλογικής δράσης για τον περιορισμό της πληροφοριακής και διαπραγματευτικής ασυμμετρίας που χαρακτηρίζει τη σχέση των μικρών επιχειρήσεων με τους μεγάλους τεχνολογικούς και χρηματοπιστωτικούς φορείς. Υπό αυτή την έννοια, θεσμοί συλλογικής εκπροσώπησης όπως η ΕΣΕΕ καλούνται να αναλάβουν έναν ενισχυμένο ρόλο, όχι μόνο ως φορείς διαμεσολάβησης έναντι δημόσιων αρχών και ιδιωτικών παρόχων, αλλά και ως παραγωγοί πρακτικής τεχνογνωσίας, προτύπων

αυτοαξιολόγησης και εργαλείων υποστήριξης, προσαρμοσμένων στις ιδιαίτερες ανάγκες και δυνατότητες των μικρών και πολύ μικρών επιχειρήσεων.

Συμπερασματικά, ο ψηφιακός μετασχηματισμός του λιανικού εμπορίου δεν θα πρέπει να αξιολογείται με αποκλειστικό κριτήριο την ταχύτητα υιοθέτησης νέων τεχνολογιών πληρωμών και τον βαθμό τυπικής κανονιστικής συμμόρφωσης, αλλά με βάση τη δυνατότητά του να συνδυάζει την ανταγωνιστικότητα, την ασφάλεια και την κοινωνική συμπερίληψη σε ένα ενιαίο πλαίσιο πολιτικής. Η διασφάλιση ότι οι μικρομεσαίες επιχειρήσεις του ελληνικού λιανικού εμπορίου θα συμμετέχουν ισότιμα στο νέο ψηφιακό οικοσύστημα πληρωμών και θα διαθέτουν την ανθεκτικότητα να αντιμετωπίζουν τις κυβερνοαπειλές που αυτό συνεπάγεται συνιστά, ως εκ τούτου, όχι απλώς τεχνική αναγκαιότητα, αλλά κεντρικό ζήτημα οικονομικής και κοινωνικής πολιτικής, με άμεσες προεκτάσεις για τη μακροπρόθεσμη βιωσιμότητα, την ανταγωνιστικότητα και τη συνοχή του κλάδου.

8. Βιβλιογραφία

Ante, L., Fiedler, I., Willruth, J. M., & Steinmetz, F. (2023). A systematic literature review of empirical research on stablecoins. *FinTech*, *2*(1), 34-47.

Arslanian, H. (2022). The history of money. In *The Book of Crypto: The Complete Guide to Understanding Bitcoin, Cryptocurrencies and Digital Assets* (pp. 1-43). Cham: Springer International Publishing.

Aiyer, B., Anant, V., & Di Mattia, D. (2021). Securing small and medium-size enterprises: What's next?. *McKinsey & Company*, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Securing%20small%20and%20medium%20size%20enterprises%20Whats%20next/Securing-small-and-medium-size-enterprises-Whats-next-vF.pdf

Bastian, N. D. (2023). Gaining Competitive Advantages in Cyberspace. *The Cyber Defense Review*, *8*(1), 55-66.

Blatz, F., Bulander, R., & Dietel, M. (2018). Maturity model of digitization for SMEs. In *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)* (pp. 1-9). IEEE.

Bott, J., & Milkau, U. (2016). A market for payments—Payment choice in the 21st century digital economy. In *Transforming Payment Systems in Europe* (pp. 1-27). London: Palgrave Macmillan.

Bruggink, D. (2026). A tale of transactions: An analysis of retail payments in the euro area. *Journal of Payments Strategy & Systems*, *20*(1), 102-116.

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. *Congressional research service documents, CRS RL32331 (Washington DC)*, *2*.

Chang, Y. Y., Lin, Y. M., Hu, Q., Chiang, F. Y., Hung, T. M., & Dai, S. (2026). Securing Strategic Advantage: The Role of Cybersecurity Actions and Government Support in Enhancing Digital Platform Capabilities. *Canadian Journal of Administrative Sciences/Revue Canadienne des Sciences de l'Administration*, *43*(2), e70033.

Cotugno, M., Manta, F., Perdichizzi, S., & Stefanelli, V. (2024). Ready for a digital Euro? Insights from a research agenda. *Research in International Business and Finance*, *67*, 102117.

Dharmavaram, V. G. (2021). Formjacking attack: Are we safe?. *Journal of Financial Crime*, *28*(2), 607-612.

ENISA (2024). *ENISA threat landscape 2024*,

https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf?utm

European Central Bank (ECB). (2024). *Digital payments continue to rise, albeit at a slower pace; cash remains a key payment method*. European Central Bank, https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr241219~172b929461.en.html.

EuroCommerce. (2024). *EuroCommerce manifesto 2024–2029: Delivering a dynamic Single Market and sustainable growth*. EuroCommerce, https://www.eurocommerce.eu/eurocommerce-manifesto-2024-2029/?utm_

European Commission. (2025). *Greece 2025 Digital Decade Country Report*. European Commission. https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2025?utm

European Court of Auditors. (2025). *Digital payments in the EU* (Special Report 01/2025). Publications Office of the European Union, https://www.eca.europa.eu/ECAPublications/SR-2025-01/SR-2025-01_EN.pdf?utm_

Eurostat. (2026). *Digitalisation in Europe – 2026 edition*. European Commission. Digitalisation in Europe – 2026 edition, https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2026?utm_

Hazar, A., & Babuşcu, Ş. (2023). Financial technologies: Digital payment systems and digital banking. today's dynamics. *Journal of Research. Innovation and Technologies*, *2*(4), 162-178.

Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the US retail economy: Restoring confidence in information technology security standards. *Technology in Society*, *44*, 30-38.

Huang, K., Siegel, M., & Madnick, S. (2017). Cybercrime-as-a-service: identifying control points to disrupt. *Massachusetts Institute of Technology (MIT), Tech. Rep*.

Indrawati, F. A. (2023). An ideal legal tender for the digital era. *Journal of Central Banking Law and Institutions*, *2*(3), 373-400.

Gaie, C., & Mueck, M. (2025). Introduction to the Networks and Information Systems 2 (NIS2) Directive. In *European Digital Regulations* (pp. 161-180). Cham: Springer Nature Switzerland.

Górka, J. (2025). The rise of instant payments: a cross-country comparison. *Central European Management Journal*, *33*(4), 575-589.

Gounari, M., Stergiopoulos, G., Pipyros, K., & Gritzalis, D. (2024). Harmonizing open banking in the European Union: An analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards. *International Cybersecurity Law Review*, *5*(1), 79-120.

Guttman-Kenney, B., Firth, C., & Gathergood, J. (2023). Buy now, pay later (BNPL)... on your credit card. *Journal of Behavioral and Experimental Finance*, *37*, 100788.

Joshi, K., & Akhilesh, K. B. (2019). Role of cyber security in retail. In *Smart Technologies: Scope and Applications* (pp. 233-247). Singapore: Springer.

Jun, J., & Yeo, E. (2016). Entry of FinTech firms and competition in the retail payments market. *Asia-Pacific Journal of Financial Studies*, *45*(2), 159-184.

Klein, A. (2020). China's digital payments revolution. *Brookings Institution, Washington*.

Konovalova, M. E., Kuzmina, O. Y., & Salomatina, S. Y. (2019). Transformation of the institution of money in the digital epoch. In *Digital transformation of the economy: challenges, trends and new opportunities* (pp. 315-328). Cham: Springer International Publishing.

Kosutic, D., & Pigni, F. (2022). Cybersecurity: investing for competitive outcomes. *Journal of Business Strategy*, *43*(1), 28-36.

Kotáb, P., & Martiník, P. (2025). Strong Customer Authentication under PSD3 and PSR and Financial Inclusion: Two Steps Forward or One Step Back?. *European Business Law Review*, *36*(5).

Kumar, A., Salo, J., & Bezawada, R. (2024). The effects of buy now, pay later (BNPL) on customers' online purchase behavior. *Journal of Retailing*, *100*(4), 602-617.

Omotoye, S., & Chen, W. (2025). Development of a Comprehensive Framework for Detecting Insider Threats. In *International Conference on Information and Communication Technology for Intelligent Systems* (pp. 379-389). Singapore: Springer Nature Singapore.

Ortino, M. (2022). The functions of law and of digital platforms in the payment system. *European Business Law Review*, *33*(7).

Peón, D., & Sun, Y. (2025). The impact of PSD2 regulation on the financial performance of non-bank payment service providers: the case of Spain. *Journal of Banking Regulation*, *26*(2), 214-231.

Peneder, M. (2022). Digitization and the evolution of money as a social technology of account. *Journal of Evolutionary Economics*, *32*(1), 175-203.

Rajgopal, P. R. (2025). Cybersecurity risk management and zero trust transformation in retail and supply chain sectors. *American Academic Journal*, 2764-2788.

Saleh, N. H. M., Hussin, N. A. A., Kumar, M. S., & Zolkipli, M. F. (2026). Cybersecurity risk management for digital retail: Strategies, frameworks and implementation. *Journal of Applied Computer and Information Technology*, *1*(1), 33-48.

Schmidt, R. Ä., Bennison, D., Bainbridge, S., & Hallsworth, A. (2007). Legislation and SME retailers–compliance costs and consequences. *International Journal of Retail & Distribution Management*, *35*(4), 256-270.

Simon, J., & Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research*, *282*(1), 161-171.

SMEunited. (2024). *Cybersecurity and data protection for SMEs*. SMEunited, https://www.smeunited.eu/admin/storage/smeunited/smeunited-position-paper-on-security-defence-and-preparedness.pdf?utm

Staykova, K. S., & Damsgaard, J. (2015). The race to dominate the mobile payments platform: Entry and expansion strategies. *Electronic Commerce Research and Applications*, *14*(5), 319-330.

Steennot, R. (2018). Reduced payer's liability for unauthorized payment transactions under the second Payment Services Directive (PSD2). *Computer Law & Security Review*, *34*(4), 954-964.

Stefanelli, V., & Manta, F. (2023). Digital financial services and open banking innovation: are banks becoming 'invisible'?. *Global Business Review*, 09721509231151491.

Sutherland, W., & Jarrahi, M. H. (2018). The sharing economy and digital platforms: A review and research agenda. *International journal of information management*, *43*, 328-341.

Tan, L., & Xue, L. (2021). Research on the Development of Digital Currencies under the COVID-19 Epidemic. *Procedia Computer Science*, *187*, 89-96.

Wandhöfer, R. (2025). From the second payment services directive to the payment services regulation and the third payment services directive: a critical assessment of the implications for European Fintechs. *European Business Law Review*, *36*(5).

Westerlund, M. (2020). Digitalization, internationalization and scaling of online SMEs. *Technology Innovation Management Review*, *10*(4).

Westermeier, C. (2020). Money is data–the platformization of financial transactions. *Information, Communication & Society*, *23*(14), 2047-2063.

Yilmazkuday, H. (2026). Drivers of credit and debit card transactions. *Review of Financial Economics*, *44*(1), e70029.

Zkik, K., Belhadi, A., Kamble, S., Venkatesh, M., Oudani, M., & Sebbar, A. (2024). Cyber resilience framework for online retail using explainable deep learning approaches and blockchain-based consensus protocol. *Decision Support Systems*, *182*, 114253.