ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΟΙΚΟΝΟΜΙΚΗΣ ΕΠΙΣΤΗΜΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΣΤΗΝ ΟΙΚΟΝΟΜΙΚΗ & ΕΠΙΧΕΙΡΗΣΙΑΚΗ

ΣΤΡΑΤΗΓΙΚΗ

Προστασία καταναλωτή & επιχειρηματική ανάπτυξη: προσωπικά δεδομένα, δικαιώματα & σύγχρονες προκλήσεις

Ραφαέλλα – Σοφία Πυργιώτη

Επιβλέπων Καθηγητής: Γιάννης Α. Πολλάλης

Διπλωματική Εργασία υποβληθείσα στο Τμήμα Οικονομικών Επιστημών του Πανεπιστημίου Πειραιώς ως μέρους των απαιτήσεων για την απόκτηση Μεταπτυχιακού Διπλώματος Ειδίκευσης στην Οικονομική και Επιχειρησιακή Στρατηγική

Πειραιάς, Ιούλιος 2026

UNIVERSITY OF PIRAEUS

DEPARTMENT OF ECONOMICS

MASTER PROGRAM IN
ECONOMIC AND BUSINESS STRATEGY

Consumer Protection and Business Growth: GDPR, Data Rights and Emerging Challenges

by

Raphaella – Sophia Pyrgioti

Supervisor Professor: Yannis A. Pollalis

Master Thesis submitted to the Department of Economics of the University of Piraeus in partial fulfillment of the requirements for the degree of Master of Science in Economic and Business Strategy

Piraeus, Greece, July 2026

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

«Δηλώνω υπεύθυνα ότι το έργο που εκπονήθηκε και παρουσιάζεται στην υποβαλλόμενη διπλωματική εργασία, για τη λήψη του μεταπτυχιακού τίτλου σπουδών, στην «ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΤΡΑΤΗΓΙΚΗ» με τίτλο:

«Προστασία καταναλωτή & επιχειρηματική ανάπτυξη: προσωπικά δεδομένα, δικαιώματα & σύγχρονες προκλήσεις» έχει γραφτεί από εμένα αποκλειστικά στο σύνολό της.

Δεν έχει υποβληθεί ούτε εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας αναφέρονται στο σύνολό τους, κάνοντάς πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου.»

Στην οικογένειά μου

ΕΥΧΑΡΙΣΤΙΕΣ

Με την ολοκλήρωση της παρούσας διπλωματικής εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες προς τον επιβλέποντα καθηγητή μου, κ. Ιωάννη Πολλάλη, τόσο για την πολύτιμη επιστημονική του καθοδήγηση, όσο και για τη συνεχή του υποστήριξη, καθ' όλη τη διάρκεια εκπόνησης της εργασίας. Η συμβολή του υπήρξε καθοριστική για την ολοκλήρωση της παρούσας και η συνεργασία μας αποτέλεσε για μένα μια ιδιαίτερα σημαντική ακαδημαϊκή εμπειρία.

Ιδιαίτερες ευχαριστίες οφείλω και στην οικογένειά μου, καθώς και τους ανθρώπους που στάθηκαν δίπλα μου, σε όλη τη διάρκεια των σπουδών μου, προσφέροντας μου αμέριστη στήριξη, κατανόηση και ενθάρρυνση.

Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει τη σχέση ανάμεσα στην προστασία του καταναλωτή και στην επιχειρηματική ανάπτυξη μέσα από το πρίσμα της προστασίας προσωπικών δεδομένων, των δικαιωμάτων ιδιωτικότητας και των σύγχρονων ρυθμιστικών προκλήσεων. Σκοπός της μελέτης είναι να αναδείξει τον τρόπο με τον οποίο η προστασία δεδομένων λειτουργεί ταυτόχρονα ως μηχανισμός θεσμικής προστασίας του καταναλωτή και ως παράγοντας στρατηγικής αξίας για τις επιχειρήσεις της ψηφιακής οικονομίας. Η μεθοδολογία βασίστηκε σε βιβλιογραφική ανάλυση επιστημονικών άρθρων, ευρωπαϊκών και ελληνικών νομικών κειμένων, κανονιστικών πράξεων, εκθέσεων εποπτικών αρχών και σύγχρονων εμπειρικών μελετών. Η ανάλυση έδειξε ότι η έννοια των προσωπικών δεδομένων έχει αποκτήσει δυναμικό, πολυεπίπεδο και οικονομικά κρίσιμο χαρακτήρα, ενώ ο GDPR διαμόρφωσε ένα συνεκτικό σύστημα δικαιωμάτων, υποχρεώσεων και μηχανισμών λογοδοσίας. Παράλληλα, η έρευνα ανέδειξε ότι η ψηφιακή εμπιστοσύνη των καταναλωτών ενισχύεται μέσω της διαφάνειας, της ασφάλειας, της υπεύθυνης διαχείρισης δεδομένων και της αποτελεσματικής εταιρικής επικοινωνίας. Επιπλέον, προέκυψε ότι η συμμόρφωση δημιουργεί κόστη, αλλά ταυτόχρονα στηρίζει τη φήμη, την ανθεκτικότητα, την καινοτομία και τη μακροπρόθεσμη ανταγωνιστικότητα. Συμπερασματικά, η προστασία δεδομένων αναδεικνύεται ως θεμέλιο βιώσιμης, αξιόπιστης και κοινωνικά υπεύθυνης επιχειρηματικής ανάπτυξης. Η μελέτη προτείνει ενίσχυση της διακυβέρνησης δεδομένων, ενεργότερο ρόλο των DPO, επένδυση στη data literacy και στενότερη συνεργασία επιχειρήσεων και ρυθμιστικών φορέων σε ευρωπαϊκό επίπεδο.

Abstract

This thesis examines the relationship between consumer protection and business development through the lens of personal data protection, privacy rights and regulatory challenges. Its purpose is to explain how data protection operates both as a mechanism for safeguarding consumers and as a strategic resource for firms in the digital economy. The study employed a literature-based methodology built on the analysis of academic articles, European and Greek legal texts, regulatory instruments, supervisory reports, and recent empirical studies. The findings show that personal data have evolved from a narrow legal category into a dynamic, multilayered, and economically valuable resource shaped by Big Data, artificial intelligence, connected devices, and predictive analytics. The analysis also showed that the GDPR created a more coherent framework of rights, obligations, accountability, and enforcement, while complementary European instruments expanded privacy governance into broader fields of digital regulation. In addition, the study found that consumer trust grows through transparency, security, responsible data management, and effective corporate communication. Compliance generates economic pressures, especially for smaller firms, yet it also supports reputation, resilience, innovation, and long-term competitiveness. Overall, the thesis concludes that data protection functions as a foundation of sustainable, credible and responsible business development in contemporary digital markets.

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Γραφημάτων

Γλωσσάρι

Το γλωσσάρι συγκεντρώνει τις βασικές συντομογραφίες, τις κανονιστικές πράξεις και τους τεχνικούς όρους που χρησιμοποιούνται στην εργασία. Οι ορισμοί αποδίδουν τη σημασία των όρων στο πεδίο της προστασίας προσωπικών δεδομένων, της ψηφιακής οικονομίας και της επιχειρηματικής ανάπτυξης.

Πίνακας 1: Κανονιστικές πράξεις

Συντομογραφίες	Ονομασία/ περιγραφή
AI	Artificial Intelligence, Τεχνητή Νοημοσύνη. Περιγράφει υπολογιστικά συστήματα που εκτελούν λειτουργίες όπως πρόβλεψη, ταξινόμηση, παραγωγή περιεχομένου και υποστήριξη αποφάσεων.
AI Act ή EU AI Act	Ο Κανονισμός της Ευρωπαϊκής Ένωσης 2024/1689 για την τεχνητή νοημοσύνη. Εφαρμόζει προσέγγιση βάσει κινδύνου και καθορίζει υποχρεώσεις για παρόχους, φορείς εφαρμογής και χρήστες συστημάτων AI.
ΑΠΔ ή ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Αποτελεί την ανεξάρτητη ελληνική εποπτική αρχή για την εφαρμογή του ΓΚΠΔ και της εθνικής νομοθεσίας προστασίας δεδομένων.
B2B	Business to Business. Αναφέρεται σε συναλλαγές, συνεργασίες και σχέσεις ανταλλαγής δεδομένων μεταξύ επιχειρήσεων.
CSR ή ΕΚΕ	Corporate Social Responsibility, Εταιρική Κοινωνική Ευθύνη. Εκφράζει την οργανωμένη ευθύνη μιας επιχείρησης απέναντι στην κοινωνία, στους εργαζομένους, στους καταναλωτές και στο περιβάλλον.
DGA	Data Governance Act, Κανονισμός της Ευρωπαϊκής Ένωσης 2022/868. Ρυθμίζει την επαναχρησιμοποίηση ορισμένων δεδομένων του δημόσιου τομέα, τις υπηρεσίες διαμεσολάβησης δεδομένων και τον αλτρουισμό δεδομένων.
DMA	Digital Markets Act, Κανονισμός της Ευρωπαϊκής Ένωσης 2022/1925. Στοχεύει στη διαμόρφωση δίκαιων και διεκδικήσιμων ψηφιακών αγορών και επιβάλλει ειδικές υποχρεώσεις στις μεγάλες πλατφόρμες που χαρακτηρίζονται ως πυλωροί.

Συντομογραφίες	Ονομασία/ περιγραφή
DPO	Data Protection Officer, Υπεύθυνος Προστασίας Δεδομένων. Ενημερώνει και συμβουλεύει τον οργανισμό, παρακολουθεί τη συμμόρφωση, υποστηρίζει τις εκτιμήσεις αντικτύπου και λειτουργεί ως σημείο επικοινωνίας με την εποπτική αρχή.
DPIA	Data Protection Impact Assessment, Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων. Αποτελεί οργανωμένη αξιολόγηση των κινδύνων μιας επεξεργασίας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.
DORA	Digital Operational Resilience Act, Κανονισμός της Ευρωπαϊκής Ένωσης 2022/2554. Ενισχύει την ψηφιακή επιχειρησιακή ανθεκτικότητα των χρηματοοικονομικών οντοτήτων και τη διαχείριση κινδύνων τεχνολογιών πληροφορικής.
DSA	Digital Services Act, Κανονισμός της Ευρωπαϊκής Ένωσης 2022/2065. Καθορίζει υποχρεώσεις επιμέλειας, διαφάνειας και λογοδοσίας για ενδιάμεσες ψηφιακές υπηρεσίες, πλατφόρμες και μηχανές αναζήτησης.
ePrivacy	Ευρωπαϊκό πλαίσιο προστασίας της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, με βασικό κείμενο την Οδηγία 2002/58/ΕΚ. Καλύπτει την εμπιστευτικότητα επικοινωνιών, τα cookies και τις ανεπιθύμητες ηλεκτρονικές επικοινωνίες.
ΕΕ	Ευρωπαϊκή Ένωση. Αποτελεί το θεσμικό και κανονιστικό πλαίσιο εντός του οποίου εφαρμόζονται ο ΓΚΠΔ και οι συμπληρωματικές πράξεις της ψηφιακής νομοθεσίας.
ΕΚ	Ευρωπαϊκή Κοινότητα. Η συντομογραφία εμφανίζεται στην αρίθμηση παλαιότερων ευρωπαϊκών οδηγιών και κανονιστικών πράξεων.
EUR Lex	Η επίσημη διαδικτυακή πύλη πρόσβασης στο δίκαιο της Ευρωπαϊκής Ένωσης, στις συνθήκες, στις νομοθετικές πράξεις, στη νομολογία και στα συναφή θεσμικά έγγραφα.

Συντομογραφίες	Ονομασία/ περιγραφή
GDPR ή ΓΚΠΔ	General Data Protection Regulation, Γενικός Κανονισμός Προστασίας Δεδομένων. Πρόκειται για τον Κανονισμό της Ευρωπαϊκής Ένωσης 2016/679, ο οποίος καθορίζει αρχές επεξεργασίας, δικαιώματα των υποκειμένων, υποχρεώσεις οργανισμών και μηχανισμούς εποπτείας.
IoT	Internet of Things, Διαδίκτυο των Πραγμάτων. Περιγράφει δίκτυα συνδεδεμένων συσκευών και αισθητήρων που συλλέγουν, ανταλλάσσουν και επεξεργάζονται δεδομένα.
ΜΜΕ	Μικρές και Μεσαίες Επιχειρήσεις. Στην εργασία ο όρος αφορά επιχειρήσεις μικρού και μεσαίου μεγέθους και τις ιδιαίτερες οργανωτικές και οικονομικές απαιτήσεις συμμόρφωσής τους.

Πίνακας 2: Βασική ορολογία

Συντομογραφίες	Ονομασία/ περιγραφή
Αλγοριθμική διαφάνεια	Η παροχή κατανοητών πληροφοριών για τη λειτουργία, τα κριτήρια, τα δεδομένα και τις συνέπειες ενός αλγοριθμικού συστήματος ή μιας αυτοματοποιημένης απόφασης.
Αλτρουισμός δεδομένων	Η εθελοντική διάθεση δεδομένων για σκοπούς γενικού συμφέροντος, όπως η επιστημονική έρευνα, η δημόσια υγεία και η βελτίωση δημόσιων υπηρεσιών, μέσα σε θεσμικά οργανωμένο πλαίσιο.
Ανωνυμοποίηση	Η επεξεργασία δεδομένων με τρόπο που απομακρύνει οριστικά τη δυνατότητα σύνδεσής τους με συγκεκριμένο φυσικό πρόσωπο, με βάση τα διαθέσιμα και εύλογα μέσα αναγνώρισης.
Αυτοματοποιημένη λήψη αποφάσεων	Η λήψη απόφασης μέσω αυτοματοποιημένης επεξεργασίας δεδομένων, με δυνατότητα παραγωγής νομικών ή παρόμοια σημαντικών συνεπειών για ένα φυσικό πρόσωπο.
Ανάλυση Μεγάλων Δεδομένων, Big Data analytics	Η επεξεργασία μεγάλου όγκου, υψηλής ταχύτητας και ποικιλίας δεδομένων με σκοπό την αναγνώριση προτύπων, τη δημιουργία προβλέψεων και την υποστήριξη επιχειρηματικών ή διοικητικών αποφάσεων.

Συντομογραφίες	Ονομασία/ περιγραφή
Διακυβέρνηση δεδομένων, data governance	Το σύνολο πολιτικών, ρόλων, διαδικασιών και μηχανισμών ελέγχου που ρυθμίζουν την ποιότητα, την πρόσβαση, την ασφάλεια, τη χρήση και τη λογοδοσία σε ολόκληρο τον κύκλο ζωής των δεδομένων.
Διακυβέρνηση ιδιωτικότητας, privacy governance	Η οργανωτική δομή μέσω της οποίας ένας φορέας ενσωματώνει την προστασία της ιδιωτικής ζωής στη στρατηγική, στη λήψη αποφάσεων, στη συμμόρφωση και στις καθημερινές λειτουργίες.
Διασυνοριακή μεταφορά δεδομένων	Η διαβίβαση προσωπικών δεδομένων από τον Ευρωπαϊκό Οικονομικό Χώρο προς τρίτη χώρα ή διεθνή οργανισμό, με εφαρμογή των προβλεπόμενων εγγυήσεων προστασίας.
Δικαίωμα στη λήθη	Η ειδική μορφή του δικαιώματος διαγραφής που επιτρέπει στο υποκείμενο να ζητήσει την απομάκρυνση προσωπικών δεδομένων όταν συντρέχουν οι προϋποθέσεις του ΓΚΠΔ.
Ειδικές κατηγορίες προσωπικών δεδομένων	Δεδομένα που αφορούν, μεταξύ άλλων, τη φυλετική ή εθνοτική καταγωγή, τις πολιτικές απόψεις, τις θρησκευτικές πεποιθήσεις, την υγεία, τη σεξουαλική ζωή, τα γενετικά και τα βιομετρικά χαρακτηριστικά και απολαμβάνουν αυξημένο επίπεδο προστασίας.
Εκτελών την επεξεργασία	Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή ή ο φορέας που επεξεργάζεται προσωπικά δεδομένα για λογαριασμό και σύμφωνα με τις τεκμηριωμένες οδηγίες του υπευθύνου επεξεργασίας.
Ελαχιστοποίηση δεδομένων	Η αρχή σύμφωνα με την οποία τα προσωπικά δεδομένα παραμένουν κατάλληλα, συναφή και περιορισμένα στην έκταση που απαιτεί ο συγκεκριμένος σκοπός επεξεργασίας.
Εποπτική αρχή	Η ανεξάρτητη δημόσια αρχή που παρακολουθεί την εφαρμογή της νομοθεσίας προστασίας δεδομένων, εξετάζει καταγγελίες, παρέχει καθοδήγηση και ασκεί ερευνητικές και διορθωτικές εξουσίες.
Ηθική δεδομένων, data ethics	Το σύνολο αρχών που κατευθύνουν τη δίκαιη, υπεύθυνη και κοινωνικά αποδεκτή συλλογή, ανάλυση, κοινοποίηση και αξιοποίηση δεδομένων πέρα από την τυπική νομική συμμόρφωση.

Συντομογραφίες	Ονομασία/ περιγραφή
Κατάρτιση προφίλ, profiling	Η αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων για την αξιολόγηση ή πρόβλεψη χαρακτηριστικών ενός προσώπου, όπως οι προτιμήσεις, η συμπεριφορά, η οικονομική κατάσταση και τα ενδιαφέροντά του.
Κρυπτογράφηση	Η τεχνική μετατροπής δεδομένων σε μορφή που γίνεται κατανοητή μόνο με τη χρήση κατάλληλου κλειδιού, ενισχύοντας την εμπιστευτικότητα και την ασφάλεια.
Λογοδοσία	Η αρχή που απαιτεί από τον υπεύθυνο επεξεργασίας να εφαρμόζει κατάλληλα μέτρα συμμόρφωσης και να διαθέτει τεκμηρίωση που αποδεικνύει την τήρηση του ΓΚΠΔ.
Παραβίαση δεδομένων προσωπικού χαρακτήρα, data breach	Περιστατικό ασφάλειας που οδηγεί σε καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη γνωστοποίηση ή πρόσβαση σε προσωπικά δεδομένα.
Προγνωστική ιδιωτικότητα, predictive privacy	Η προστασία απέναντι στην εξαγωγή ή πρόβλεψη προσωπικών χαρακτηριστικών μέσω αλγορίθμων που αξιοποιούν δεδομένα του ίδιου προσώπου ή ευρύτερων πληθυσμιακών ομάδων.
Προσωπικά δεδομένα	Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, άμεσα ή έμμεσα, μέσω στοιχείων όπως το όνομα, ο αριθμός ταυτότητας, τα δεδομένα θέσης και οι διαδικτυακοί αναγνωριστικοί δείκτες.
Προστασία δεδομένων από τον σχεδιασμό, Privacy by Design	Η ενσωμάτωση αρχών και εγγυήσεων προστασίας δεδομένων από τα πρώτα στάδια σχεδιασμού ενός προϊόντος, μιας υπηρεσίας, μιας διαδικασίας ή ενός πληροφοριακού συστήματος.
Προστασία δεδομένων εξ ορισμού, Privacy by Default	Η διαμόρφωση των προεπιλεγμένων ρυθμίσεων ώστε κάθε επεξεργασία να περιορίζεται στα δεδομένα, στους αποδέκτες, στη διάρκεια και στην προσβασιμότητα που απαιτεί ο δηλωμένος σκοπός.
Πυλωρός, gatekeeper	Μεγάλη ψηφιακή πλατφόρμα με ισχυρή και σταθερή θέση που λειτουργεί ως κρίσιμο σημείο πρόσβασης ανάμεσα σε επιχειρηματικούς χρήστες και τελικούς χρήστες στο πλαίσιο του DMA.

Συντομογραφίες	Ονομασία/ περιγραφή
Συγκατάθεση	Ελεύθερη, συγκεκριμένη, ενημερωμένη και σαφής δήλωση βούλησης μέσω της οποίας το υποκείμενο αποδέχεται την επεξεργασία των προσωπικών δεδομένων του για καθορισμένο σκοπό.
Υπεύθυνος επεξεργασίας	Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή ή ο φορέας που καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας προσωπικών δεδομένων.
Υποκείμενο των δεδομένων	Το φυσικό πρόσωπο στο οποίο αναφέρονται τα προσωπικά δεδομένα και το οποίο διαθέτει τα δικαιώματα που κατοχυρώνει ο ΓΚΠΔ.
Υπολογιστικό νέφος, cloud computing	Μοντέλο παροχής υπολογιστικών πόρων, αποθήκευσης, λογισμικού και επεξεργαστικής ισχύος μέσω δικτύου, με δυνατότητα κλιμάκωσης και απομακρυσμένης πρόσβασης.
Φορητότητα δεδομένων, data portability	Το δικαίωμα λήψης προσωπικών δεδομένων σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο και διαβίβασής τους σε άλλον υπεύθυνο επεξεργασίας.
Γραμματισμός δεδομένων, data literacy	Η ικανότητα κατανόησης, αξιολόγησης, διαχείρισης, ανάλυσης και υπεύθυνης επικοινωνίας δεδομένων με επίγνωση των νομικών, τεχνικών και ηθικών συνεπειών τους.
Cookies	Μικρά αρχεία ή αναγνωριστικά που αποθηκεύονται στη συσκευή του χρήστη και υποστηρίζουν λειτουργίες όπως η διατήρηση προτιμήσεων, η μέτρηση επισκεψιμότητας και η εξατομίκευση υπηρεσιών.
Ψευδωνυμοποίηση	Η επεξεργασία προσωπικών δεδομένων κατά τρόπο που απαιτεί πρόσθετες πληροφορίες για τη σύνδεσή τους με συγκεκριμένο πρόσωπο, με χωριστή και ασφαλή τήρηση των πρόσθετων πληροφοριών.
Ψηφιακή εμπιστοσύνη	Η πεποίθηση ότι ένας ψηφιακός οργανισμός ή μια υπηρεσία λειτουργεί με ασφάλεια, διαφάνεια, συνέπεια και υπεύθυνη διαχείριση δεδομένων.
Ψηφιακή ταυτότητα	Το σύνολο αναγνωριστικών στοιχείων, διαπιστευτηρίων και ψηφιακών χαρακτηριστικών που επιτρέπουν την ασφαλή ταυτοποίηση και πρόσβαση ενός προσώπου σε ψηφιακές υπηρεσίες.

1. Εισαγωγή

1.1 Αντικείμενο και σκοπός της εργασίας

Η παρούσα διπλωματική εργασία εξετάζει τη σχέση ανάμεσα στην προστασία των προσωπικών δεδομένων, στην προστασία του καταναλωτή και στην ανάπτυξη των επιχειρήσεων στην ψηφιακή οικονομία. Το αντικείμενό της επικεντρώνεται στον τρόπο με τον οποίο το ευρωπαϊκό και το ελληνικό κανονιστικό πλαίσιο διαμορφώνουν δικαιώματα για τους καταναλωτές και υποχρεώσεις λογοδοσίας για τις επιχειρήσεις, καθώς και στον τρόπο με τον οποίο οι πρακτικές διακυβέρνησης δεδομένων επηρεάζουν την εμπιστοσύνη, τη φήμη, την καινοτομία και την οργανωτική ανθεκτικότητα. Η προστασία δεδομένων προσεγγίζεται ως θεσμική εγγύηση δημόσιου συμφέροντος και ως λειτουργική διάσταση της επιχειρηματικής στρατηγικής, ιδιαίτερα σε περιβάλλοντα εξατομίκευσης, αυτοματοποιημένης λήψης αποφάσεων και ψηφιακών συναλλαγών (Hoofnagle et al., 2019; Quinn & Malgieri, 2021).

Σκοπός της εργασίας είναι η κριτική σύνθεση του νομικού πλαισίου και της εμπειρικής βιβλιογραφίας, ώστε να αποσαφηνιστούν οι μηχανισμοί μέσω των οποίων η προστασία των προσωπικών δεδομένων ενισχύει τα δικαιώματα των καταναλωτών και υποστηρίζει βιώσιμες επιχειρηματικές πρακτικές. Η ανάλυση οργανώνεται γύρω από τρεις συνδεδεμένους άξονες, οι οποίοι αφορούν την αποτελεσματικότητα της κανονιστικής προστασίας, τη διαμόρφωση της ψηφιακής εμπιστοσύνης και τις συνέπειες της συμμόρφωσης για την επιχειρηματική ανάπτυξη. Με αυτόν τον προσανατολισμό, η εργασία επιδιώκει να καταλήξει σε τεκμηριωμένες κατευθύνσεις για επιχειρήσεις και ρυθμιστικούς φορείς, συνδέοντας τα τυπικά δικαιώματα με παρατηρήσιμες πρακτικές εφαρμογής και αποτελέσματα αγοράς (Chang et al., 2018; van der Merwe & Al Achkar, 2022).

1.2 Ερευνητικά ερωτήματα και στόχοι της μελέτης

Η μελέτη καθοδηγείται από τρία ερευνητικά ερωτήματα, τα οποία αντιστοιχούν σε σαφείς διαστάσεις ανάλυσης και επιτρέπουν τη συστηματική αντιπαραβολή νομικών κειμένων, θεσμικών δεδομένων και ερευνητικών ευρημάτων.

Ερευνητικό ερώτημα 1. Ποιοι μηχανισμοί του ευρωπαϊκού και του ελληνικού κανονιστικού πλαισίου ενισχύουν την προστασία των προσωπικών δεδομένων και των δικαιωμάτων του καταναλωτή, όπως αποτυπώνονται στα κατοχυρωμένα

δικαιώματα, στις υποχρεώσεις των επιχειρήσεων, στους εποπτικούς μηχανισμούς και στις πράξεις επιβολής;

Ερευνητικό ερώτημα 2. Σε ποιον βαθμό οι πρακτικές προστασίας δεδομένων συνδέονται με την ψηφιακή εμπιστοσύνη των καταναλωτών, όπως αξιολογείται μέσα από τη διαφάνεια, τον αντιληπτό έλεγχο, την ασφάλεια, την άσκηση δικαιωμάτων, τον χρόνο απόκρισης και την επίλυση παραπόνων;

Ερευνητικό ερώτημα 3. Ποια κόστη και ποια οφέλη δημιουργεί η συμμόρφωση με το πλαίσιο προστασίας δεδομένων για την επιχειρηματική ανάπτυξη, όπως αποτυπώνονται στη φήμη, στην αφοσίωση των πελατών, στην καινοτομία, στην ανταγωνιστικότητα και στην οργανωτική ανθεκτικότητα;

Οι στόχοι της μελέτης αντιστοιχούν άμεσα στα τρία ερευνητικά ερωτήματα. Πρώτος στόχος είναι η συστηματική παρουσίαση των νομικών και θεσμικών μηχανισμών προστασίας. Δεύτερος στόχος είναι η αξιολόγηση της σχέσης ανάμεσα στις πρακτικές διακυβέρνησης δεδομένων και στην εμπιστοσύνη του καταναλωτή. Τρίτος στόχος είναι η αποτίμηση των επιχειρηματικών συνεπειών της συμμόρφωσης. Η σύνθεση των τριών αξόνων υποστηρίζει τη διατύπωση εφαρμοσμένων προτάσεων για επιχειρήσεις και ρυθμιστικές αρχές.

1.3 Συνεισφορά και σημασία της εργασίας

Η πρωτότυπη συνεισφορά της εργασίας έγκειται στη σύνδεση τεσσάρων πεδίων που συχνά εξετάζονται χωριστά, δηλαδή του δικαίου προστασίας προσωπικών δεδομένων, της προστασίας του καταναλωτή, της έρευνας για την ψηφιακή εμπιστοσύνη και της επιχειρηματικής στρατηγικής. Το ενιαίο αυτό πλαίσιο επιτρέπει τη διάκριση ανάμεσα στην τυπική κανονιστική συμμόρφωση και στην ουσιαστική συμμόρφωση που γίνεται αντιληπτή από τον καταναλωτή μέσα από κατανοητές πληροφορίες, λειτουργικά δικαιώματα, έγκαιρη απόκριση και υπεύθυνη διαχείριση περιστατικών. Παράλληλα, συνδέει τη νομική προστασία με παρατηρήσιμα αποτελέσματα της αγοράς, όπως η εμπιστοσύνη, η φήμη, η διατήρηση πελατών και η οργανωτική προσαρμοστικότητα.

Η πρακτική και κοινωνικοοικονομική σημασία της μελέτης απορρέει από την ανάπτυξη ενός πλαισίου αξιολόγησης που μπορεί να αξιοποιηθεί από επιχειρήσεις, καταναλωτές και εποπτικούς φορείς. Η εργασία συγκεντρώνει ενδεικτικές μετρικές, όπως το ποσοστό άσκησης δικαιωμάτων, ο χρόνος απόκρισης, η επίλυση καταγγελιών

και η μεταβολή της εμπιστοσύνης μετά από περιστατικά. Με αυτόν τον τρόπο, η προστασία δεδομένων αποκτά μετρήσιμη οργανωτική διάσταση και συνδέεται με τη λογοδοσία, τη βελτίωση των υπηρεσιών και τη βιώσιμη ανάπτυξη των ψηφιακών επιχειρήσεων.

1.4 Μεθοδολογική προσέγγιση

Η εργασία υιοθετεί μια μεθοδολογική προσέγγιση βασισμένη στην υπάρχουσα βιβλιογραφία. Βασίζεται σε συστηματική και κριτική ανάλυση ακαδημαϊκών άρθρων, νομικών κειμένων, κανονιστικού υλικού και θεσμικών εγγράφων σχετικών με την προστασία δεδομένων στην Ευρώπη και την Ελλάδα. Η μέθοδος έχει ποιοτικό και ερμηνευτικό προσανατολισμό. Σκοπός της είναι να συνθέσει επιχειρήματα, να συγκρίνει ευρήματα, να εντοπίσει συγκλίσεις και διαφοροποιήσεις και να αναπτύξει μια συνεκτική αναλυτική αφήγηση γύρω από τη σχέση μεταξύ προστασίας της ιδιωτικής ζωής και ανάπτυξης επιχειρήσεων.

1.5 Δομή της διπλωματικής εργασίας

Η εργασία οργανώνεται σε έξι κεφάλαια. Εκτός από το παρόν εισαγωγικό κεφάλαιο, το Κεφάλαιο 2 παρουσιάζει το θεωρητικό και νομοθετικό πλαίσιο της προστασίας των προσωπικών δεδομένων. Το Κεφάλαιο 3 εξετάζει την προστασία των καταναλωτών και την ψηφιακή εμπιστοσύνη. Το Κεφάλαιο 4 αναλύει την ανάπτυξη των επιχειρήσεων και τη διαχείριση δεδομένων. Το Κεφάλαιο 5 διερευνά τις σύγχρονες προκλήσεις και τις μελλοντικές προοπτικές και το Κεφάλαιο 6 παρουσιάζει συμπεράσματα, προτάσεις πολιτικής, ερευνητικούς περιορισμούς και μελλοντικές κατευθύνσεις.

2. Θεωρητικό και νομοθετικό πλαίσιο προστασίας προσωπικών δεδομένων

2.1 Νομικό πλαίσιο προστασίας προσωπικών δεδομένων

2.1.1 Ιστορική εξέλιξη της προστασίας δεδομένων στην Ευρώπη και την Ελλάδα

Η ιστορική εξέλιξη της προστασίας δεδομένων προσωπικού χαρακτήρα στην Ευρώπη και στην Ελλάδα αποτυπώνει τη μετάβαση από ένα πλαίσιο ελάχιστης εναρμόνισης σε ένα σύστημα ενιαίας, άμεσα εφαρμοστέας και θεσμικά ενισχυμένης προστασίας. Η διαδρομή αυτή συνδέεται με την αυξανόμενη ψηφιοποίηση της οικονομίας, με τη διασυνοριακή κυκλοφορία πληροφοριών και με την ανάγκη να εξασφαλιστεί ότι η επεξεργασία δεδομένων υπηρετεί την ελεύθερη κίνηση πληροφοριών χωρίς να υποβαθμίζει τα δικαιώματα των φυσικών προσώπων. Σε ευρωπαϊκό επίπεδο, η αφετηρία του σύγχρονου πλαισίου βρίσκεται στην Οδηγία 95/46/ΕΚ, ενώ η ώριμη φάση του αποτυπώνεται στον Γενικό Κανονισμό για την Προστασία Δεδομένων, δηλαδή στον Κανονισμό 2016/679. Στην ελληνική έννομη τάξη, η προσαρμογή στο νέο καθεστώς πραγματοποιήθηκε κυρίως με τον Ν. 4624/2019, ο οποίος αναδιοργάνωσε το εθνικό πλαίσιο και επανακαθόρισε θεσμικά τον ρόλο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 1995; Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016).

Η Οδηγία 95/46/ΕΚ αποτέλεσε το βασικό σημείο εκκίνησης της ευρωπαϊκής προστασίας δεδομένων προσωπικού χαρακτήρα. Σύμφωνα με τη σύνοψη του EUR Lex, η Οδηγία συνιστούσε το κείμενο αναφοράς σε ευρωπαϊκό επίπεδο και είχε ως στόχο τη δημιουργία ρυθμιστικού πλαισίου που να προστατεύει τα θεμελιώδη δικαιώματα και τις ελευθερίες των προσώπων, ιδίως το δικαίωμα στην ιδιωτική ζωή, σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Παράλληλα, επιδίωκε να διευκολύνει την ελεύθερη κυκλοφορία των δεδομένων μεταξύ κρατών μελών, στοιχείο ιδιαίτερα σημαντικό για την εσωτερική αγορά. Ωστόσο, η μορφή της οδηγίας άφηνε ευρύ περιθώριο εθνικής μεταφοράς, γεγονός που οδήγησε σε αποκλίσεις ως προς την εφαρμογή, την ερμηνεία και την εποπτεία. Η πολυμορφία αυτή κατέστη περισσότερο αισθητή όσο αναπτύσσονταν οι ψηφιακές υπηρεσίες, οι διαδικτυακές

πλατφόρμες και οι διασυνοριακές ροές δεδομένων (EUR Lex, χ.χ. a; Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 1995).

Ο Κανονισμός 2016/679 εκδόθηκε στις 27 Απριλίου 2016 και τέθηκε σε εφαρμογή στις 25 Μαΐου 2018 ως άμεσα εφαρμοστέο δίκαιο σε όλα τα κράτη μέλη. Η επιλογή του κανονισμού, αντί νέας οδηγίας, αποσκοπούσε ακριβώς στην ενίσχυση της ομοιομορφίας και στη μείωση του κατακερματισμού. Η επίσημη σύνοψη του EUR Lex επισημαίνει ότι ο GDPR ενίσχυσε τα δικαιώματα των υποκειμένων, καθιέρωσε αυξημένες υποχρεώσεις λογοδοσίας για τους υπευθύνους επεξεργασίας και διαμόρφωσε ενιαίο επίπεδο προστασίας στην Ένωση. Η μετάβαση αυτή σήμαινε αλλαγή όχι μόνο τεχνική αλλά και φιλοσοφική. Η προστασία δεδομένων έπαψε να αντιμετωπίζεται κυρίως ως ζήτημα εθνικής συμμόρφωσης και αναδείχθηκε σε κεντρικό μηχανισμό ρύθμισης της ψηφιακής οικονομίας, της διοικητικής δράσης και της εταιρικής διακυβέρνησης. Έτσι, ο GDPR κατέστη το νέο θεσμικό υπόβαθρο πάνω στο οποίο εδράζεται η σημερινή έννοια της νόμιμης, διαφανούς και υπεύθυνης επεξεργασίας προσωπικών δεδομένων (EUR Lex, χ.χ. a; EUR Lex, χ.χ. b; Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016).

Στην Ελλάδα, η προσαρμογή στο νέο ευρωπαϊκό καθεστώς πραγματοποιήθηκε με τον Ν. 4624/2019. Όπως προβλέπει ρητά το άρθρο 1 του νόμου, σκοπός του ήταν αφενός η αντικατάσταση του νομοθετικού πλαισίου που διέπει την ίδρυση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και αφετέρου η λήψη μέτρων για την εφαρμογή του Κανονισμού 2016/679 στην ελληνική έννομη τάξη. Η σημασία του νόμου είναι διπλή. Πρώτον, επιβεβαίωσε ότι η άμεση εφαρμογή του GDPR απαιτούσε εθνικές ρυθμίσεις σε επιμέρους ζητήματα που ο ίδιος ο Κανονισμός αφήνει στη διακριτική ευχέρεια των κρατών μελών. Δεύτερον, διαμόρφωσε το θεσμικό πλαίσιο μέσα στο οποίο η ελληνική διοίκηση, οι επιχειρήσεις και οι δημόσιοι φορείς όφειλαν να οργανώσουν την κανονιστική τους συμμόρφωση (Αρχή Προστασίας Δεδομένων, 2019).

Η ΑΠΔ παρουσιάζει στο θεσμικό της πλαίσιο ότι η ελληνική νομοθεσία για τα προσωπικά δεδομένα συγκροτείται σήμερα από τον GDPR, τον Ν. 4624/2019, τον Ν. 3471/2006 για την προστασία δεδομένων στις ηλεκτρονικές επικοινωνίες, καθώς και από τμήματα του παλαιότερου Ν. 2472/1997 που διατηρήθηκαν όπου αυτό προβλέφθηκε. Η επισήμανση αυτή δείχνει ότι η ελληνική προσαρμογή δεν υπήρξε

απλή κατάργηση του παλαιού πλαισίου, αλλά ανασύνθεση της εθνικής έννομης τάξης γύρω από τον ευρωπαϊκό κανονιστικό πυρήνα. Επιπλέον, η περίληψη της ετήσιας έκθεσης 2022 της ΑΠΔΠΧ σημειώνει ότι από τις 29 Αυγούστου 2019 ο Ν. 4624/2019 λειτουργεί ως το κεντρικό εθνικό κείμενο εφαρμογής του GDPR στην Ελλάδα. Κατά συνέπεια, η ελληνική προσαρμογή πρέπει να ιδωθεί ως διαδικασία ενσωμάτωσης ενός ενιαίου ευρωπαϊκού κανόνα σε ένα διοικητικό και δικαιικό περιβάλλον με ήδη διαμορφωμένες θεσμικές δομές (Αρχή Προστασίας Δεδομένων, 2019; Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 2024).

Καθοριστικός στην ιστορική αυτή εξέλιξη είναι ο ρόλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Σύμφωνα με την επίσημη ιστοσελίδα της, η Αρχή είναι συνταγματικά κατοχυρωμένη ανεξάρτητη δημόσια αρχή με αποστολή την εποπτεία της εφαρμογής του GDPR, του Ν. 4624/2019, του Ν. 3471/2006 και κάθε άλλης ρύθμισης που αφορά την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων. Η σημασία της Αρχής έγκειται στο ότι λειτουργεί ως θεσμικός εγγυητής της νομιμότητας, της διαφάνειας και της αποτελεσματικότητας του συστήματος προστασίας. Δεν περιορίζεται μόνο στην επιβολή κυρώσεων, αλλά παρέχει ενημέρωση, κανονιστική καθοδήγηση, εξέταση καταγγελιών και συνεργασία με άλλες εποπτικές αρχές της Ευρωπαϊκής Ένωσης σε διασυνοριακές υποθέσεις. Η σχετική σελίδα για τις καταγγελίες αναφέρει ρητά ότι η ΑΠΔ είναι αρμόδια να χειρίζεται καταγγελίες και να διερευνά εικαζόμενες παραβιάσεις, εφόσον χρειάζεται και σε συνεργασία με αρχές άλλων κρατών μελών.

Η ενίσχυση του ρόλου της Αρχής μετά τον GDPR συνδέεται άμεσα με την ευρωπαϊκή λογική της συνεκτικής εποπτείας. Σε αντίθεση με το παλαιότερο καθεστώς, στο οποίο η προστασία δεδομένων εξαρτιόταν σε μεγαλύτερο βαθμό από εθνικές επιλογές μεταφοράς της οδηγίας, το ισχύον πλαίσιο αναθέτει στις ανεξάρτητες αρχές κρίσιμο ρόλο στην ερμηνεία, εφαρμογή και πρακτική επιβολή ενός κοινού κανονισμού. Η ελληνική Αρχή, μέσα από τις ετήσιες εκθέσεις, τις γνωμοδοτήσεις, τις αποφάσεις και τις δράσεις ενημέρωσης, συμβάλλει στην επιβολή του δικαίου και στη διαμόρφωση κουλτούρας προστασίας δεδομένων. Επομένως, η ιστορική εξέλιξη από την Οδηγία 95/46/ΕΚ έως τον GDPR και τον Ν. 4624/2019 ολοκληρώνεται θεσμικά μέσα από την αναβάθμιση της ΑΠΔ σε κεντρικό πυλώνα της ελληνικής εφαρμογής του ευρωπαϊκού δικαίου προστασίας δεδομένων. Η εξέλιξη αυτή αποδεικνύει ότι η προστασία

δεδομένων στην Ευρώπη και στην Ελλάδα ακολούθησε πορεία θεσμικής εμβάθυνσης. Από ένα πλαίσιο γενικών κανόνων και εθνικών αποκλίσεων, το σύστημα μετακινήθηκε σε καθεστώς άμεσης εφαρμογής, ενισχυμένων δικαιωμάτων, ειδικών εθνικών συμπληρώσεων και διαρκούς εποπτείας. Για τον λόγο αυτό, η ιστορική προσέγγιση του ζητήματος αποτελεί μια ουσιώδη προϋπόθεση κατανόησης του σημερινού κανονιστικού και διοικητικού περιβάλλοντος με συνέπειες για πολίτες, κράτος και επιχειρήσεις (Αρχή Προστασίας Δεδομένων, 2024).

2.1.2 Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

Ο Γενικός Κανονισμός Προστασίας Δεδομένων συγκροτεί το βασικό πλαίσιο της Ευρωπαϊκής Ένωσης για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και, ταυτόχρονα, για τη διασφάλιση της ελεύθερης κυκλοφορίας των δεδομένων αυτών εντός της Ένωσης. Στο άρθρο 1 ο Κανονισμός ορίζει ρητά ότι υπηρετεί δύο αλληλένδετους στόχους, δηλαδή την προστασία θεμελιωδών δικαιωμάτων και ελευθεριών, με ιδιαίτερη έμφαση στο δικαίωμα προστασίας δεδομένων προσωπικού χαρακτήρα, και τη διατήρηση της ελεύθερης κυκλοφορίας των δεδομένων στην ενιαία αγορά. Με αυτόν τον τρόπο, ο GDPR εντάσσει την προστασία δεδομένων στον πυρήνα της ευρωπαϊκής έννομης τάξης και της ψηφιακής οικονομίας.

Οι θεμελιώδεις αρχές της επεξεργασίας αποτυπώνονται στο άρθρο 5. Πρώτη είναι η αρχή της νομιμότητας, της αντικειμενικότητας και της διαφάνειας, σύμφωνα με την οποία τα δεδομένα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με τρόπο διαφανή ως προς το υποκείμενο των δεδομένων. Η διάταξη αυτή προσδίδει ιδιαίτερη βαρύτητα στην υποχρέωση του υπευθύνου επεξεργασίας να στηρίζει κάθε πράξη επεξεργασίας σε νόμιμη βάση και να καθιστά σαφείς προς το υποκείμενο τους σκοπούς και τις συνθήκες της επεξεργασίας. Δεύτερη είναι η αρχή του περιορισμού του σκοπού, κατά την οποία τα δεδομένα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς. Τρίτη είναι η αρχή της ελαχιστοποίησης, που απαιτεί τα δεδομένα να είναι κατάλληλα, συναφή και περιορισμένα στο αναγκαίο μέτρο σε σχέση με τους σκοπούς της επεξεργασίας. Τέταρτη είναι η αρχή της ακρίβειας, η οποία επιβάλλει τη λήψη εύλογων μέτρων για τη διόρθωση ή διαγραφή ανακριβών δεδομένων. Πέμπτη είναι η αρχή του περιορισμού της περιόδου αποθήκευσης, σύμφωνα με την οποία τα δεδομένα τηρούνται μόνο για όσο χρονικό διάστημα εξυπηρετούν τον σκοπό της επεξεργασίας.

Έκτη είναι η αρχή της ακεραιότητας και εμπιστευτικότητας, δηλαδή η επεξεργασία με τρόπο που εξασφαλίζει την κατάλληλη ασφάλεια των δεδομένων, περιλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή φθορά. Το άρθρο 5 ολοκληρώνεται με την αρχή της λογοδοσίας, αφού ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και οφείλει να είναι σε θέση να αποδείξει τη συμμόρφωσή του με όλες τις παραπάνω αρχές. Το κανονιστικό αυτό σχήμα ενισχύεται από το άρθρο 32, το οποίο απαιτεί την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων ασφαλείας, με γνώμονα την κατάσταση της τεχνολογίας, το κόστος εφαρμογής, τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τη σοβαρότητα των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Ο GDPR αναγνωρίζει ένα εκτεταμένο πλέγμα δικαιωμάτων στα υποκείμενα των δεδομένων. Τα άρθρα 12 έως 14 ρυθμίζουν το δικαίωμα ενημέρωσης και πληροφόρησης, απαιτώντας οι πληροφορίες να παρέχονται με συνοπτικό, διαφανή, κατανοητό και εύκολα προσβάσιμο τρόπο. Το δικαίωμα πρόσβασης κατοχυρώνεται στο άρθρο 15 και επιτρέπει στο υποκείμενο να λαμβάνει επιβεβαίωση για το αν δεδομένα που το αφορούν υφίστανται επεξεργασία, καθώς και πρόσβαση σε ουσιώδη στοιχεία της επεξεργασίας, όπως οι σκοποί, οι κατηγορίες δεδομένων, οι αποδέκτες και η περίοδος αποθήκευσης. Το άρθρο 16 θεσπίζει το δικαίωμα διόρθωσης ανακριβών δεδομένων, ενώ το άρθρο 17 κατοχυρώνει το δικαίωμα διαγραφής, γνωστό και ως δικαίωμα στη λήθη, υπό τις προϋποθέσεις που ο Κανονισμός ορίζει. Το άρθρο 18 προβλέπει το δικαίωμα περιορισμού της επεξεργασίας και το άρθρο 20 το δικαίωμα φορητότητας, δηλαδή το δικαίωμα του υποκειμένου να λαμβάνει τα δεδομένα του σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο και να τα διαβιβάζει σε άλλον υπεύθυνο επεξεργασίας. Παράλληλα, το άρθρο 21 κατοχυρώνει το δικαίωμα εναντίωσης και το άρθρο 22 προσφέρει ειδική προστασία έναντι αποφάσεων που λαμβάνονται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, περιλαμβανομένης της κατάρτισης προφίλ. Συνολικά, τα δικαιώματα αυτά ενισχύουν τη θέση του υποκειμένου και μετατρέπουν τη διαφάνεια και τον έλεγχο σε ενεργά στοιχεία του καθεστώτος προστασίας.

Οι υποχρεώσεις των επιχειρήσεων και γενικότερα των υπευθύνων επεξεργασίας δομούνται γύρω από την αρχή της λογοδοσίας και της συμμόρφωσης ήδη

από τον σχεδιασμό της επεξεργασίας. Το άρθρο 24 απαιτεί από τον υπεύθυνο επεξεργασίας να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα και να είναι σε θέση να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον Κανονισμό. Το άρθρο 25 εξειδικεύει αυτή τη λογική μέσω της προστασίας δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, ενώ το άρθρο 30 εισάγει την τήρηση αρχείων δραστηριοτήτων επεξεργασίας. Το άρθρο 33 ρυθμίζει τη γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή και το άρθρο 34 την ανακοίνωση της παραβίασης στο υποκείμενο, όταν αυτή ενδέχεται να επιφέρει υψηλό κίνδυνο. Ιδιαίτερα σημαντικός είναι ο θεσμός του Υπευθύνου Προστασίας Δεδομένων. Στα άρθρα 37 έως 39 ο Κανονισμός προβλέπει τις περιπτώσεις υποχρεωτικού ορισμού DPO, ιδίως όταν η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, όταν απαιτείται τακτική και συστηματική παρακολούθηση υποκειμένων σε μεγάλη κλίμακα ή όταν πραγματοποιείται μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα. Ο DPO ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, παρακολουθεί τη συμμόρφωση, παρέχει συμβουλές για την εκτίμηση αντικτύπου και λειτουργεί ως σημείο επικοινωνίας με την εποπτική αρχή. Πρόκειται συνεπώς για κρίσιμο μηχανισμό εσωτερικής κανονιστικής οργάνωσης και διαρκούς συμμόρφωσης.

Το σύστημα εποπτείας του GDPR στηρίζεται στις ανεξάρτητες εποπτικές αρχές, οι οποίες ρυθμίζονται στα άρθρα 51 και επόμενα. Το άρθρο 51 ορίζει ότι κάθε κράτος μέλος προβλέπει μία ή περισσότερες ανεξάρτητες δημόσιες αρχές επιφορτισμένες με την παρακολούθηση της εφαρμογής του Κανονισμού. Το άρθρο 57 απαριθμεί τα καθήκοντα των αρχών, όπως η παρακολούθηση και επιβολή της εφαρμογής του Κανονισμού, η ευαισθητοποίηση του κοινού, η εξέταση καταγγελιών και η συνεργασία με άλλες εποπτικές αρχές. Το άρθρο 58 προβλέπει εκτεταμένες ερευνητικές, διορθωτικές, εγκριτικές και συμβουλευτικές εξουσίες, όπως η δυνατότητα προειδοποίησης, επίπληξης, επιβολής συμμόρφωσης, προσωρινού ή οριστικού περιορισμού της επεξεργασίας και επιβολής διοικητικών προστίμων.

Το άρθρο 83 ρυθμίζει ειδικά τα διοικητικά πρόστιμα και καθορίζει ότι αυτά πρέπει να είναι αποτελεσματικά, αναλογικά και αποτρεπτικά. Ο Κανονισμός διακρίνει δύο βασικά ανώτατα επίπεδα, έως 10 εκατομμύρια ευρώ ή 2% του συνολικού ετήσιου

κύκλου εργασιών για ορισμένες παραβάσεις, και έως 20 εκατομμύρια ευρώ ή 4% του συνολικού ετήσιου κύκλου εργασιών για βαρύτερες παραβάσεις, με κριτήριο το υψηλότερο ποσό σε κάθε περίπτωση. Κατά την επιμέτρηση του προστίμου συνεκτιμώνται, μεταξύ άλλων, η φύση, η βαρύτητα και η διάρκεια της παράβασης, ο βαθμός υπαιτιότητας, τα μέτρα περιορισμού της ζημίας, η συνεργασία με την εποπτική αρχή και τυχόν προηγούμενες παραβάσεις. Με αυτό το πλέγμα εποπτείας και κυρώσεων, ο GDPR συνδέει τα δικαιώματα των υποκειμένων με έναν ισχυρό μηχανισμό εφαρμογής, ο οποίος αποσκοπεί τόσο στην πρόληψη όσο και στην ουσιαστική συμμόρφωση των οργανισμών.

2.1.3 Συμπληρωματικό ευρωπαϊκό ρυθμιστικό πλαίσιο

Η προστασία δεδομένων στην Ευρωπαϊκή Ένωση δεν εξαντλείται στον Γενικό Κανονισμό Προστασίας Δεδομένων, αλλά πλαισιώνεται από ένα ευρύτερο ρυθμιστικό πλαίσιο που απαντά στις απαιτήσεις της ψηφιακής οικονομίας, της πλατφορμοποίησης των αγορών, της διαμεσολάβησης των υπηρεσιών και της ανάπτυξης της τεχνητής νοημοσύνης. Το συμπληρωματικό αυτό πλαίσιο έχει ιδιαίτερη σημασία, επειδή εξειδικεύει την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, οργανώνει τις υποχρεώσεις των ψηφιακών μεσαζόντων, αντιμετωπίζει τις ανισορροπίες ισχύος στις ψηφιακές αγορές και δημιουργεί κανόνες για την αξιόπιστη διακυβέρνηση δεδομένων και την ασφαλή ανάπτυξη συστημάτων τεχνητής νοημοσύνης. Κατά συνέπεια, η κατανόηση της προστασίας δεδομένων απαιτεί συνδυαστική προσέγγιση του GDPR με το ePrivacy πλαίσιο, τον Κανονισμό για τις Ψηφιακές Υπηρεσίες, τον Κανονισμό για τις Ψηφιακές Αγορές, τον Κανονισμό για τη Διακυβέρνηση Δεδομένων και τον Κανονισμό για την Τεχνητή Νοημοσύνη.

Η Οδηγία 2002/58/ΕΚ, γνωστή ως ePrivacy Directive, αποτελεί την ειδική ρύθμιση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Σύμφωνα με τη σχετική σύνοψη του EUR-Lex, η Οδηγία εφαρμόζεται στην επεξεργασία δεδομένων σε συνάρτηση με την παροχή δημόσια διαθέσιμων υπηρεσιών ηλεκτρονικών επικοινωνιών και διασφαλίζει την εμπιστευτικότητα των επικοινωνιών, την ασφάλεια της επεξεργασίας, τη ρύθμιση των cookies, την προστασία από ανεπιθύμητες επικοινωνίες και τις υποχρεώσεις γνωστοποίησης παραβιάσεων δεδομένων. Η λογική της είναι συμπληρωματική προς το γενικό πλαίσιο προστασίας δεδομένων, επειδή

επικεντρώνεται όχι απλώς στην επεξεργασία προσωπικών δεδομένων, αλλά ειδικότερα στο απόρρητο των ηλεκτρονικών επικοινωνιών και στη χρήση συναφών τεχνολογιών (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2002).

Η Ευρωπαϊκή Επιτροπή πρότεινε το 2017 νέο Κανονισμό ePrivacy, με στόχο να αντικαταστήσει την Οδηγία και να ευθυγραμμίσει το σχετικό πλαίσιο με τον GDPR. Στην πρόταση αυτή αναφέρεται ότι ο νέος κανονισμός αποσκοπεί στην ενίσχυση της προστασίας της ιδιωτικής ζωής και της εμπιστευτικότητας των ηλεκτρονικών επικοινωνιών, στην εναρμόνιση των κανόνων σε όλη την Ένωση και στην προσαρμογή της νομοθεσίας στο μεταβαλλόμενο τεχνολογικό περιβάλλον, το οποίο περιλαμβάνει υπηρεσίες επιγραμμικής επικοινωνίας, μεταδεδομένα, νέες μορφές ιχνηλάτησης και διευρυμένες διασυνδέσεις συσκευών. Η μετάβαση από οδηγία σε κανονισμό θα ενίσχυε, σε θεσμικό επίπεδο, την ομοιομορφία και την ασφάλεια δικαίου, ακριβώς όπως συνέβη και με τον GDPR (Ευρωπαϊκή Επιτροπή, 2017).

Ο Κανονισμός 2022/2065, γνωστός ως Digital Services Act, θεσπίζει ενιαίο πλαίσιο για τις ενδιάμεσες ψηφιακές υπηρεσίες στην εσωτερική αγορά και επιδιώκει ασφαλέστερο περιβάλλον, μεγαλύτερη λογοδοσία των παρόχων και ισχυρότερη προστασία των χρηστών. Η επίσημη σύνοψη του EUR-Lex επισημαίνει ότι ο DSA εισάγει υποχρεώσεις επιμέλειας, διαφάνειας και λογοδοσίας για παρόχους υπηρεσιών όπως οι υπηρεσίες πρόσβασης στο διαδίκτυο, η φιλοξενία περιεχομένου, οι πλατφόρμες και οι μηχανές αναζήτησης. Για την προστασία δεδομένων, ο DSA έχει σημασία επειδή συνδέει τη διακυβέρνηση περιεχομένου με υποχρεώσεις διαφάνειας ως προς τα συστήματα σύστασης, την διαφήμιση και τους κινδύνους που δημιουργούν οι πλατφόρμες για τα θεμελιώδη δικαιώματα. Έτσι, παρότι δεν αντικαθιστά τον GDPR, λειτουργεί συμπληρωματικά ως κανονισμός θεσμικής ευθύνης των παρόχων (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022α).

Ο Κανονισμός 2022/1925, δηλαδή ο Digital Markets Act, συμπληρώνει το πλαίσιο αυτό από την οπτική της αγοράς. Σύμφωνα με τη σχετική σύνοψη του EUR-Lex, ο DMA επιδιώκει να εξασφαλίσει δίκαιες και διεκδικήσιμες αγορές στον ψηφιακό τομέα, ιδίως απέναντι σε μεγάλες πλατφόρμες που λειτουργούν ως πυλωροί. Η λογική του δεν αφορά μόνο τον ανταγωνισμό με στενή οικονομική έννοια, αλλά και τις συνθήκες πρόσβασης, επιλογής και ελέγχου που έχουν οι επιχειρηματικοί χρήστες και οι τελικοί χρήστες. Για τα δεδομένα, ο DMA αποκτά ιδιαίτερη σημασία επειδή

περιορίζει ορισμένες πρακτικές συνδυασμού δεδομένων, ενισχύει τη δυνατότητα των χρηστών να επιλέγουν υπηρεσίες και λειτουργεί αποτρεπτικά απέναντι σε στρατηγικές συσσώρευσης ισχύος που βασίζονται σε οικοσυστήματα δεδομένων. Ως εκ τούτου, ο DMA συμπληρώνει την προστασία δεδομένων μέσω της ρύθμισης της δομής της αγοράς (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022β).

Ο Κανονισμός 2022/868, δηλαδή ο Data Governance Act, συνιστά κρίσιμο βήμα για την ευρωπαϊκή διακυβέρνηση δεδομένων. Η επίσημη σύνοψη του EUR-Lex αναφέρει ότι αποσκοπεί στην ενίσχυση της διαθεσιμότητας δεδομένων για χρήση, με αύξηση της εμπιστοσύνης στους μηχανισμούς διαμοιρασμού δεδομένων, με θέσπιση κανόνων για την επαναχρησιμοποίηση ορισμένων κατηγοριών δεδομένων του δημόσιου τομέα, με ρύθμιση υπηρεσιών διαμεσολάβησης δεδομένων και με τη δημιουργία πλαισίου για τον αλτρουισμό δεδομένων. Η σημασία του έγκειται στο ότι συνδέει την οικονομική αξιοποίηση των δεδομένων με θεσμικές εγγυήσεις εμπιστοσύνης, διαφάνειας και ελέγχου, στοιχείο ιδιαίτερα σημαντικό για την ευρωπαϊκή στρατηγική δεδομένων (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022γ).

Αντίστοιχα, ο Κανονισμός 2024/1689, γνωστός ως EU AI Act, εισάγει εναρμονισμένους κανόνες για την τεχνητή νοημοσύνη στην Ένωση. Η επίσημη σύνοψη του EUR-Lex υπογραμμίζει ότι σκοπός του είναι να προωθήσει την ανάπτυξη και υιοθέτηση ασφαλών και αξιόπιστων συστημάτων τεχνητής νοημοσύνης, διασφαλίζοντας παράλληλα υψηλό επίπεδο προστασίας της υγείας, της ασφάλειας και των θεμελιωδών δικαιωμάτων. Ο Κανονισμός ακολουθεί προσέγγιση βασισμένη στον κίνδυνο, απαγορεύει ορισμένες πρακτικές, επιβάλλει αυστηρές απαιτήσεις για συστήματα υψηλού κινδύνου και εισάγει ειδικές υποχρεώσεις διαφάνειας για ορισμένες εφαρμογές. Η σχέση του με την προστασία δεδομένων είναι άμεση, επειδή η εκπαίδευση, η ανάπτυξη και η λειτουργία συστημάτων τεχνητής νοημοσύνης συχνά στηρίζονται σε μεγάλους όγκους δεδομένων, ενώ οι αποφάσεις που παράγουν μπορούν να επηρεάσουν βαθιά τα δικαιώματα των προσώπων. Συνεπώς, το συμπληρωματικό αυτό ευρωπαϊκό πλαίσιο δείχνει ότι η προστασία δεδομένων εξελίσσεται σε μέρος ενός ευρύτερου καθεστώτος ψηφιακής συνταγματικότητας, στο οποίο η ιδιωτικότητα, η διαφάνεια, η ασφάλεια, η θεμιτή αγορά και η αξιόπιστη καινοτομία συνυφαίνονται σε

ενιαία ρυθμιστική λογική (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2024).

Η συμπληρωματικότητα αυτών των πράξεων είναι ουσιώδης. Το ePrivacy πλαίσιο εξειδικεύει το απόρρητο των επικοινωνιών. Ο DSA οργανώνει τη συστημική ευθύνη των ενδιάμεσων υπηρεσιών. Ο DMA αντιμετωπίζει τη συγκέντρωση ψηφιακής ισχύος που ενισχύεται μέσω δεδομένων και οικοσυστημάτων πλατφορμών. Ο Data Governance Act επιχειρεί να καταστήσει τη διαθεσιμότητα δεδομένων συμβατή με την εμπιστοσύνη και τη θεσμική εποπτεία. Ο AI Act διαμορφώνει το κανονιστικό περιβάλλον μέσα στο οποίο η χρήση δεδομένων για αλγοριθμικές εφαρμογές συνδέεται με αξιολόγηση κινδύνου και προστασία θεμελιωδών δικαιωμάτων. Συνεπώς, η ευρωπαϊκή ρύθμιση εγκαταλείπει την αποσπασματικότητα και διαμορφώνει ένα πολυεπίπεδο σύστημα, όπου η προστασία δεδομένων λειτουργεί μαζί με κανόνες αγοράς, πλατφορμών, επικοινωνιών και τεχνητής νοημοσύνης, ενισχύοντας τόσο την ασφάλεια δικαίου όσο και την εμπιστοσύνη πολιτών και επιχειρήσεων. Με αυτή τη θεσμική εξέλιξη, η Ένωση επιδιώκει ψηφιακή ανάπτυξη που να στηρίζεται ταυτόχρονα στην καινοτομία, στη λογοδοσία και στην προστασία δικαιωμάτων

Πίνακας 3: Σύγκριση βασικών ευρωπαϊκών ρυθμίσεων για την ψηφιακή οικονομία

Ρύθμιση	Στόχος	Επιπτώσεις στις επιχειρήσεις	Απαιτήσεις διαφάνειας
GDPR	Προστασία των φυσικών προσώπων κατά την επεξεργασία προσωπικών δεδομένων και ελεύθερη κυκλοφορία των δεδομένων στην Ευρωπαϊκή Ένωση.	Λογοδοσία, προστασία ήδη από τον σχεδιασμό και εξ ορισμού, αρχεία επεξεργασίας, ασφάλεια, γνωστοποίηση παραβιάσεων, DPO και διοικητικές κυρώσεις.	Συνοπτική, διαφανής και κατανοητή ενημέρωση για σκοπούς, νομικές βάσεις, αποδέκτες, χρόνο τήρησης και δικαιώματα των υποκειμένων.
ePrivacy	Προστασία της εμπιστευτικότητας των ηλεκτρονικών επικοινωνιών και ρύθμιση των cookies, της ιχνηλάτησης και των ανεπιθύμητων επικοινωνιών.	Διαχείριση συγκατάθεσης, ασφάλεια επικοινωνιών, ρυθμίσεις cookies και προσαρμογή των πρακτικών άμεσης εμπορικής επικοινωνίας.	Σαφής πληροφόρηση για cookies, τεχνολογίες παρακολούθησης, μεταδεδομένα και σκοπούς επεξεργασίας στις ηλεκτρονικές επικοινωνίες.
DSA	Δημιουργία ασφαλέστερου ψηφιακού περιβάλλοντος και ενίσχυση της λογοδοσίας των	Υποχρεώσεις επιμέλειας, αξιολόγηση συστημικών κινδύνων, μηχανισμοί αναφοράς,	Διαφάνεια για διαφημίσεις, συστήματα συστάσεων, πρακτικές εποπτείας

Ρύθμιση	Στόχος	Επιπτώσεις στις επιχειρήσεις	Απαιτήσεις διαφάνειας
	ενδιάμεσων υπηρεσιών και πλατφορμών.	εποπτεία περιεχομένου και πρόσθετες απαιτήσεις για μεγάλες πλατφόρμες.	περιεχομένου, όρους χρήσης και εκθέσεις συστημικών κινδύνων.
DMA	Διασφάλιση δίκαιων και διεκδικήσιμων ψηφιακών αγορών μέσω κανόνων για τις μεγάλες πλατφόρμες που λειτουργούν ως πυλωροί.	Περιορισμοί στον συνδυασμό δεδομένων, ενίσχυση επιλογής χρηστών, κανόνες πρόσβασης και προστασία επιχειρηματικών χρηστών από καταχρηστικές πρακτικές.	Υποχρεώσεις αναφοράς συμμόρφωσης και πληροφόρηση για πρακτικές δεδομένων, διαφημιστικές υπηρεσίες και όρους πρόσβασης στο οικοσύστημα του πυλωρού.
AI Act	Προώθηση ασφαλών και αξιόπιστων συστημάτων τεχνητής νοημοσύνης με προστασία της υγείας, της ασφάλειας και των θεμελιωδών δικαιωμάτων.	Κατηγοριοποίηση κινδύνου, διακυβέρνηση δεδομένων, τεχνική τεκμηρίωση, ανθρώπινη εποπτεία, αξιολόγηση συμμόρφωσης και απαιτήσεις για συστήματα υψηλού κινδύνου.	Ενημέρωση για αλληλεπίδραση με συστήματα τεχνητής νοημοσύνης, διαφάνεια συγκεκριμένων εφαρμογών και παροχή κατάλληλων πληροφοριών για συστήματα υψηλού κινδύνου.

2.1.4 Νομολογία και πρόσφατες υποθέσεις εφαρμογής GDPR

Η πρόσφατη εφαρμογή του GDPR δείχνει ότι ο Κανονισμός έχει εξελιχθεί από ένα κανονιστικό πλαίσιο σε ένα ώριμο καθεστώς συμμόρφωσης που διαμορφώνεται από την εποπτική πρακτική, τη δικαστική ερμηνεία και τις μετρήσιμες οικονομικές συνέπειες. Η εικόνα σε όλη την Ευρώπη χαρακτηρίζεται από μια σταδιακή ενοποίηση των προτεραιοτήτων εφαρμογής γύρω από τις βασικές υποχρεώσεις του GDPR και ιδίως τη νομιμότητα, τη διαφάνεια, τη λογοδοσία και την ασφάλεια. Συγκριτικές μελέτες δείχνουν ότι οι εθνικές αρχές προστασίας δεδομένων δεν έχουν εφαρμόσει τον Κανονισμό ομοιόμορφα, ωστόσο έχουν δημιουργήσει ένα σύνολο πρακτικών που διευκρινίζει ποιες παραβάσεις επισύρουν κυρώσεις και πώς εφαρμόζονται οι κανονιστικές προτεραιότητες (Ruohonen & Hjerppe, 2022; Wolff & Atallah, 2021; Daigle & Khan, 2020). Μέσα σε αυτό το ευρύτερο ευρωπαϊκό τοπίο, η Ελληνική Αρχή Προστασίας Δεδομένων δηλώνει την παρουσία της μέσω ετήσιων εκθέσεων και στοχευμένων αποφάσεων, συμπεριλαμβανομένων υποθέσεων σχετικά με την επεξεργασία δεδομένων στον χώρο εργασίας και βιομετρικών δεδομένων (Αρχή Προστασίας Δεδομένων- ΑΠΔ, 2024a, 2024b, 2019).

Ένα πρώτο σημαντικό θέμα στη βιβλιογραφία αφορά το θέμα των προστίμων του GDPR. Οι Ruohonen και Hjerppe (2022) δείχνουν ότι οι αποφάσεις επιβολής του νόμου αναφέρονται συχνότερα σε διατάξεις που σχετίζονται με γενικές αρχές, νομιμότητα και ασφάλεια πληροφοριών. Η ανάλυσή τους καταδεικνύει ότι η επιβολή του νόμου δεν είναι τυχαία. Οι εποπτικές αρχές επιστρέφουν επανειλημμένα στις θεμελιώδεις υποχρεώσεις του GDPR, γεγονός που υποδηλώνει ότι οι πιο σοβαρές αποτυχίες συμμόρφωσης είναι συχνά διαρθρωτικές παρά τεχνικές. Οι Wolff και Atallah (2021), εξετάζοντας τους πρώτους είκοσι τέσσερις μήνες της δημόσιας επιβολής του νόμου, διαπιστώνουν ομοίως ότι μόνο ένα μέρος των διατάξεων περί κυρώσεων είχε ακόμη χρησιμοποιηθεί στην πράξη και ότι τα περισσότερα πρόστιμα παρέμειναν σχετικά μικρά στην αρχική περίοδο. Τονίζουν επίσης ότι τα μεγαλύτερα πρόστιμα συνήθως συνδέονταν με περιστατικά ασφάλειας, παρόλο που πολλές ενέργειες επιβολής του νόμου αφορούσαν συνολικά παραβιάσεις που σχετίζονται με την ιδιωτικότητα. Οι Daigle και Khan (2020) συμπληρώνουν αυτά τα ευρήματα δείχνοντας ότι η επιβολή του νόμου έγινε πιο δυναμική μετά την αρχική φάση εφαρμογής και ότι οι σημαντικές ενέργειες επικεντρώθηκαν ιδιαίτερα στις δυτικοευρωπαϊκές δικαιοδοσίες.

Πιο πρόσφατη ακαδημαϊκή έρευνα προσθέτει μια νέα διάσταση σε αυτήν την εικόνα. Ο Orlando (2025) αναλύει πάνω από 1.900 περιλήψεις αποφάσεων επιβολής του νόμου και επιβεβαιώνει σημαντικές ανισότητες μεταξύ των κρατών μελών. Η μελέτη διαπιστώνει επίσης ότι οι χρηματικές ποινές δεν αντιστοιχούν πάντα στη σοβαρότητα της παράβασης, καθώς οι σοβαρές παραβιάσεις μπορεί να επισύρουν σχετικά χαμηλά πρόστιμα όταν διαπράττονται από μικρότερους φορείς. Αυτή η διαπίστωση υποδηλώνει ότι η αυστηρότητα της επιβολής του GDPR εξαρτάται όχι μόνο από την τυπική σοβαρότητα μιας παράβασης, αλλά και από το θεσμικό πλαίσιο, τον τύπο του φορέα και την εθνική πρακτική. Οι Pichlak και Gaczoł (2023), μέσω μιας εμπειρικής μελέτης της εποπτικής δραστηριότητας στην Πολωνία, υποστηρίζουν ότι η επιβολή του GDPR έχει ενσωματώσει μόνο μερικές μορφές αναστοχαστικής ρύθμισης. Τα ευρήματά τους υποδηλώνουν ότι οι εποπτικές αρχές συχνά ανταποκρίνονται κατά περίπτωση, αλλά δεν αναπτύσσουν πάντα αρχές και συνεκτικές μορφές κανονιστικής μάθησης. Σε διακρατικό επίπεδο, οι Gentile και Lynskey (2022) εντοπίζουν δομικές αδυναμίες στον σχεδιασμό της διασυνοριακής επιβολής του GDPR, ενώ οι Brito Bastos και Pałka (2023) υποστηρίζουν ότι η πιο κεντρική επιβολή μπορεί να καταστεί

συνταγματικά απαραίτητη σε περιπτώσεις κοινού ευρωπαϊκού ενδιαφέροντος. Μαζί, αυτές οι μελέτες δείχνουν ότι η επιβολή του GDPR είναι ενεργή, αλλά εξακολουθεί να είναι θεσμικά άνιση.

Αυτές οι ευρύτερες συζητήσεις βοηθούν στην καλύτερη κατανόηση της ελληνικής πραγματικότητας. Σύμφωνα με την Ετήσια Έκθεση της Αρχής Προστασίας Δεδομένων (ΑΠΔ) για το 2024, η Αρχή αντιμετώπισε σημαντικά ζητήματα κατά τη διάρκεια του 2024, εξέδωσε 46 αποφάσεις για παραβάσεις, έλαβε 1.820 καταγγελίες, διεκπεραίωσε 1.422 από αυτές και επέβαλε πρόστιμα συνολικού ύψους 4.301.249 ευρώ (ΑΠΔ, 2024a). Συνεπώς, η δραστηριότητά της ήταν σημαντική. Αυτά τα στοιχεία δείχνουν επίσης ότι η επιβολή του νόμου στην Ελλάδα καλύπτει φορείς τόσο του ιδιωτικού όσο και του δημόσιου τομέα. Η έκθεση αναφέρεται, για παράδειγμα, σε αποφάσεις που αφορούν παράνομες κλήσεις άμεσου μάρκετινγκ, παραβιάσεις δεδομένων που επηρεάζουν υπουργεία και δημόσιους φορείς, σε ελλείψεις συνεργασίας με την Αρχή, σε ελλείψεις στις εκτιμήσεις επιπτώσεων και σε ελλείψεις στην παροχή γενικών πληροφοριών στα υποκείμενα των δεδομένων (ΑΠΔ, 2024a). Από αυτή την άποψη, η ελληνική εμπειρία ευθυγραμμίζεται με την ευρύτερη ευρωπαϊκή βιβλιογραφία, η οποία επανειλημμένα προσδιορίζει τη νομιμότητα, τη διαφάνεια και την ασφάλεια ως κύρια εναύσματα επιβολής του νόμου.

Δύο ελληνικές αποφάσεις είναι ιδιαίτερα χρήσιμες για να δείξουν πώς οι αρχές του GDPR μεταφράζονται σε συγκεκριμένα ευρήματα. Η πρώτη είναι η Απόφαση 26/2019, σχετικά με την επεξεργασία προσωπικών δεδομένων εργαζομένων από ιδιωτική συμβουλευτική εταιρεία. Στην περίληψή της, η Αρχή Προστασίας Δεδομένων (ΑΠΔ) καθιστά σαφές ότι η συγκατάθεση στη σχέση εργασίας δεν μπορεί κανονικά να θεωρηθεί ότι δίνεται ελεύθερα λόγω της ανισορροπίας μεταξύ εργοδότη και εργαζομένου (ΑΠΔ, 2019). Η Αρχή διαπίστωσε ότι η εταιρεία είχε επιλέξει ακατάλληλη νομική βάση, δημιούργησε την εσφαλμένη εντύπωση ότι η επεξεργασία βασιζόταν στη συγκατάθεση και δεν ικανοποίησε τις απαιτήσεις διαφάνειας και λογοδοσίας. Η υπόθεση είναι ιδιαίτερα σημαντική επειδή δείχνει ότι η νομική βάση για την επεξεργασία δεν είναι τυπικό ζήτημα. Επηρεάζει τη δικαιοσύνη, τη διαφάνεια και το εύρος των δικαιωμάτων των εργαζομένων βάσει των άρθρων 5 και 6 του GDPR. Η Αρχή τόνισε επίσης ότι ο υπεύθυνος επεξεργασίας πρέπει να επιλύει τις αμφιβολίες σχετικά με τη νομιμότητα πριν από την έναρξη της επεξεργασίας και δεν μπορεί να

μεταθέσει το βάρος της συμμόρφωσης στους ίδιους τους εργαζομένους (ΑΠΔ, 2019). Η απόφαση αυτή αποτελεί επομένως ένα ισχυρό παράδειγμα του πώς η ελληνική επιβολή του νόμου εσωτερικεύει τις βασικές αρχές του GDPR στο πλαίσιο της απασχόλησης. Ένα δεύτερο παράδειγμα είναι η Απόφαση 42/2024, η οποία επισημαίνεται στην Ετήσια Έκθεση ως υπόθεση που αφορά βιομετρικά δεδομένα (ΑΠΔ, 2024a; ΑΠΔ, 2024b). Η συμπερίληψή της στην έκθεση είναι αναλυτικά σημαντική, επειδή η βιομετρική επεξεργασία αντιπροσωπεύει έναν ευαίσθητο τομέα της εφαρμογής του GDPR. Η απόφαση σηματοδοτεί ότι η ελληνική αρχή αντιμετωπίζει τις μορφές επεξεργασίας δεδομένων υψηλού κινδύνου ως ξεχωριστή προτεραιότητα επιβολής.

Η πρόσφατη νομολογία και η επιβολή έχουν επίσης σημασία, επειδή οι κυρώσεις επηρεάζουν τους οργανισμούς πέρα από την άμεση νομική κύρωση. Οι Ford et al. (2023) καταδεικνύουν ότι οι ανακοινώσεις προστίμων του GDPR μπορούν να μειώσουν την αγοραία αξία των εισηγμένων στο χρηματιστήριο εταιρειών, με αρνητικές επιπτώσεις αποτίμησης που συχνά υπερβαίνουν την χρηματική αξία του ίδιου του προστίμου. Η επιβολή του GDPR διαμορφώνει επομένως τις αντιλήψεις των επενδυτών, τη φήμη τους και τις προτεραιότητες εταιρικής διακυβέρνησης. Οι Kareklas et al. (2024), εστιάζοντας στις ελληνικές εταιρείες, δείχνουν ομοίως ότι η εφαρμογή συνεπάγεται σημαντικό οργανωτικό και τεχνολογικό κόστος, αλλά υπογραμμίζει επίσης τη σημασία της καθοδήγησης από τις αρμόδιες αρχές και τον ρόλο του Υπεύθυνου Προστασίας Δεδομένων. Τέλος, η συζήτηση της υπόθεσης C-300/21 από τον Li (2023) προσθέτει μια δικαστική διάσταση, διευκρινίζοντας ότι η αποζημίωση για ηθική βλάβη βάσει του άρθρου 82 του GDPR απαιτεί απόδειξη πραγματικής ζημίας, αν και δεν απαιτείται όριο σοβαρότητας. Συνολικά, η σχετική βιβλιογραφία δείχνει ότι η επιβολή του GDPR έχει γίνει ένα πολυδιάστατο σύστημα που συνδυάζει διοικητικές κυρώσεις, θεσμική μάθηση και οικονομικές συνέπειες.

2.2 Θεωρητικές προσεγγίσεις

2.2.1 Η έννοια, η κατηγοριοποίηση και η ευαισθησία των προσωπικών δεδομένων

Τα προσωπικά δεδομένα αποτελούν το κεντρικό αντικείμενο του σύγχρονου δικαίου προστασίας δεδομένων, επειδή καθορίζουν πότε εφαρμόζονται οι νομικές εγγυήσεις, τα οργανωτικά καθήκοντα και τα δικαιώματα των καταναλωτών. Εντός της

Ευρωπαϊκής Ένωσης, ο GDPR (Γενικός Κανονισμός Προστασίας Δεδομένων) καθιέρωσε ένα δομημένο καθεστώς για τη διακυβέρνηση των προσωπικών πληροφοριών. Οι Hoofnagle et al. (2019) παρουσιάζουν τον Κανονισμό ως συνέχεια της Οδηγίας για την Προστασία Δεδομένων του 1995 και ως ρυθμιστική αλλαγή που ενσωματώνει τα προσωπικά δεδομένα σε ένα πλαίσιο λογοδοσίας, διακυβέρνησης πληροφοριών και ανθρώπινης εποπτείας. Η ανάλυσή τους δείχνει ότι ο GDPR περιορίζει την κακή χρήση και αναδιοργανώνει τον τρόπο με τον οποίο οι οργανισμοί συλλέγουν, διαχειρίζονται και δικαιολογούν τις πρακτικές τους σχετικά με τα δεδομένα που διαχειρίζονται. Αυτή η ευρύτερη προσέγγιση έχει σημασία για την προστασία των καταναλωτών, επειδή τα προσωπικά δεδομένα συνδέονται με τη συμπεριφορά της αγοράς, το εμπορικό πλεονέκτημα και τη νομιμότητα των ψηφιακών επιχειρηματικών μοντέλων. Οποιαδήποτε συζήτηση για τα δικαιώματα των καταναλωτών στην ψηφιακή οικονομία απαιτεί επομένως μια ακριβή κατανόηση του τι είναι τα προσωπικά δεδομένα και γιατί έχει σημασία η νομική τους ταξινόμηση.

Ο Wong (2019) υποστηρίζει ότι η οριοθέτηση των προσωπικών δεδομένων είναι κρίσιμη επειδή καθορίζει το ουσιαστικό πεδίο εφαρμογής των υποχρεώσεων προστασίας δεδομένων. Το βασικό όριο είναι το εάν οι πληροφορίες αφορούν ένα άτομο. Αυτή η απαίτηση είναι καθοριστική επειδή η νομοθεσία περί προστασίας δεδομένων δεν καλύπτει κάθε πληροφορία, αλλά μόνο πληροφορίες που συνδέονται επαρκώς με ένα φυσικό πρόσωπο. Ο Wong (2019) δείχνει επίσης ότι τα δικαστήρια στο Ηνωμένο Βασίλειο και την Ευρωπαϊκή Ένωση δυσκολεύονται να ερμηνεύσουν αυτήν την απαίτηση με συνέπεια. Αυτές οι δυσκολίες επηρεάζουν το εάν οι υπεύθυνοι επεξεργασίας εμπίπτουν στον GDPR, εάν τα άτομα μπορούν να επικαλεστούν δικαιώματα και εάν ορισμένες πρακτικές δεδομένων παραμένουν ρυθμιζόμενες. Οι Hoofnagle et al. (2019) ενισχύουν αυτό το σημείο δείχνοντας ότι ο GDPR εντάσσει τα προσωπικά δεδομένα σε ένα λεπτομερές καθεστώς που επηρεάζει τη χρήση δεδομένων παγκοσμίως. Για αυτόν τον λόγο, ο ορισμός των προσωπικών δεδομένων έχει άμεσες συνέπειες για τη συμμόρφωση, την επιβολή και την ισορροπία μεταξύ καινοτομίας και προστασίας.

Το δεύτερο ζήτημα αφορά τις κατηγορίες δεδομένων και την πρακτική σημασία του ελέγχου. Οι Van Ooijen και Vrabec (2019) αναλύουν εάν ο GDPR ενισχύει τον έλεγχο των καταναλωτών επί των προσωπικών δεδομένων και καταλήγουν στο

συμπέρασμα ότι ο Κανονισμός ενισχύει τον ατομικό έλεγχο, αλλά μόνο εν μέρει. Η οπτική τους είναι χρήσιμη επειδή αποκαλύπτει ότι η νομική προστασία συχνά βασίζεται σε υποθέσεις σχετικά με τη λήψη ανθρώπινων αποφάσεων που είναι αδύναμες στην πράξη. Διακρίνουν τρία στάδια στην οικονομία δεδομένων, δηλαδή τη λήψη πληροφοριών, την έγκριση της κύριας χρήσης και την αντιμετώπιση της δευτερογενούς χρήσης ή επαναχρησιμοποίησης. Σε κάθε στάδιο, τα άτομα αντιμετωπίζουν γνωστικούς και συμπεριφορικούς περιορισμούς που μειώνουν την ικανότητά τους να ασκούν ουσιαστικό έλεγχο. Αυτό έχει σημασία για την κατηγοριοποίηση, επειδή τα νόμιμα δικαιώματα ασκούνται σε περιβάλλοντα λήψης αποφάσεων που διαμορφώνονται από πολυπλοκότητα και ασυμμετρία. Έτσι, τα προσωπικά δεδομένα θα πρέπει να νοούνται όχι μόνο ως πληροφορίες που σχετίζονται με ένα άτομο, αλλά και ως πληροφορίες ενσωματωμένες σε συστήματα ειδοποίησης, έγκρισης και επαναχρησιμοποίησης.

Ένα ξεχωριστό επίπεδο προστασίας ισχύει για ειδικές κατηγορίες προσωπικών δεδομένων, που συχνά ονομάζονται ευαίσθητα δεδομένα. Οι Quinn και Malgieri (2021) εξηγούν ότι αυτές οι κατηγορίες παραδοσιακά λάμβαναν ισχυρότερη προστασία επειδή η επεξεργασία τους δημιουργεί μεγαλύτερο κίνδυνο διακρίσεων και σχετικών βλαβών, ειδικά για ευάλωτες ομάδες. Το άρθρο τους δείχνει ότι τα ευαίσθητα δεδομένα παραμένουν εξαιρετικά σχετικά στο πλαίσιο του GDPR, ωστόσο ο ορισμός τους έχει γίνει πιο δύσκολος στα σύγχρονα τεχνολογικά περιβάλλοντα. Η πιο ισχυρή υπολογιστική, η ευρύτερη διαδικτυακή διαθεσιμότητα δεδομένων και οι ολοένα και πιο πολύπλοκοι αλγόριθμοι σημαίνουν ότι οι πληροφορίες που αρχικά φαίνονται συνηθισμένες μπορεί να παράγουν ευαίσθητα συμπεράσματα όταν συνδυάζονται με άλλα δεδομένα. Σε αυτή τη βάση, οι Quinn και Malgieri (2021) υποστηρίζουν ότι η ευαισθησία δεν μπορεί να γίνει κατανοητή μόνο μέσω στατικών κατηγοριών. Προτείνουν ένα υβριδικό ερμηνευτικό μοντέλο στο οποίο ο σκοπός έχει μεγαλύτερο ρόλο, ενώ το πλαίσιο και η εύλογη προβλεψιμότητα λειτουργούν ως δικλείδες ασφαλείας.

2.2.2 Εμπιστοσύνη και πληροφοριακός έλεγχος

Στο θεωρητικό επίπεδο, η εμπιστοσύνη συνδέεται με την αντίληψη ότι η συλλογή και η χρήση προσωπικών δεδομένων πραγματοποιούνται με προβλέψιμο, ασφαλή και υπεύθυνο τρόπο. Ο ουσιαστικός πληροφοριακός έλεγχος, η κατανοητή

ενημέρωση, η διαφάνεια των τεχνολογικών λειτουργιών και η ορατή λογοδοσία περιορίζουν την αβεβαιότητα των χρηστών και ενισχύουν την αξιοπιστία των οργανισμών. Η προσέγγιση αυτή συνδέει τις παρατηρήσεις των Van Ooijen και Vrabec (2019) για τον ατομικό έλεγχο με το μοντέλο διαφάνειας της Wachter (2018) και με τα ευρήματα των Haddara et al. (2023) για την ενίσχυση της ασφάλειας και της εμπιστοσύνης των πελατών μέσω της συμμόρφωσης με τον GDPR.

2.2.3 Διακυβέρνηση δεδομένων σε τεχνολογικά περιβάλλοντα

Η ψηφιακή εποχή έχει εντείνει αυτά τα ζητήματα μέσω της ανόδου του Διαδικτύου των Πραγμάτων και της επέκτασης της παραγωγής δεδομένων. Η Wachter (2018) δείχνει ότι τα συστήματα IoT βασίζονται στη διάχυτη συλλογή και σύνδεση δεδομένων χρηστών, προκειμένου να παρέχουν εξατομικευμένες και προσαρμοσμένες στο περιβάλλον υπηρεσίες. Τέτοια συστήματα απαιτούν την αναγνώριση χρηστών και συσκευών, γεγονός που καθιστά τη συλλογή δεδομένων επίμονη και συχνά δύσκολη στην παρατήρηση από τα άτομα. Η Wachter (2018) υποστηρίζει ότι, παρόλο που ο GDPR περιέχει αρκετές σχετικές προστασίες, αυτές μπορεί να μην επαρκούν για να διασφαλίσουν μια δίκαιη ισορροπία μεταξύ χρηστών και προγραμματιστών. Το μοντέλο διαφάνειας τριών βημάτων της συμπληρώνει επομένως το νομικό πλαίσιο με ηθικές οδηγίες για την επικοινωνία της λειτουργικότητας και των κινδύνων του IoT. Αυτή η συμβολή δείχνει ότι τα προσωπικά δεδομένα σε περιβάλλοντα IoT είναι ενσωματωμένα σε υποδομές που συλλέγουν, συνδέουν και ερμηνεύουν συνεχώς πληροφορίες.

Η ανάλυση των Μεγάλων Δεδομένων (Big Data analytics) εμβαθύνει αυτές τις ανησυχίες επειδή αυξάνει την κλίμακα, την ετερογένεια και την επαναχρησιμοποίηση των πληροφοριών. Οι Georgiadis και Poels (2022), μέσω μιας συστηματικής ανασκόπησης της βιβλιογραφίας, εντοπίζουν τους κινδύνους απορρήτου και προστασίας δεδομένων που αφορούν ειδικά την ανάλυση των Μεγάλων Δεδομένων και τους οργανώνουν σε εννέα Σημεία Επαφής για την Ιδιωτικότητα (Privacy Touch Points). Τα ευρήματά τους δείχνουν ότι τα παραδοσιακά εργαλεία αξιολόγησης της ιδιωτικότητας δεν επαρκούν για αυτά τα περιβάλλοντα και ότι απαιτούνται πιο εξειδικευμένες μεθοδολογίες αξιολόγησης επιπτώσεων στο πλαίσιο του GDPR. Οι Rhahla et al. (2021) τονίζουν ομοίως ότι η συμμόρφωση με τον GDPR στα συστήματα Μεγάλων Δεδομένων παραμένει δύσκολη επειδή τα δεδομένα κινούνται μέσα από

πολύπλοκους κύκλους ζωής που περιλαμβάνουν συλλογή, απορρόφηση, αποθήκευση και ανάλυση. Το πλαίσιό τους αντιστοιχίζει τις νομικές απαιτήσεις στις τεχνικές απαιτήσεις σχεδιασμού και προτείνει καθοδήγηση για επαλήθευση και εφαρμογή.

Η τεχνητή νοημοσύνη δημιουργεί μια περαιτέρω πρόκληση. Ο Mühlhoff (2023) υποστηρίζει ότι η Τεχνητή Νοημοσύνη και τα Μεγάλα Δεδομένα επιτρέπουν την πρόβλεψη προσωπικών πληροφοριών για άτομα από τα δεδομένα πολλών άλλων, δημιουργώντας το πρόβλημα της προγνωστικής ιδιωτικότητας. Ο Brkan (2017) προσθέτει ότι η αυτοματοποιημένη λήψη αποφάσεων στο πλαίσιο του GDPR εγείρει ανεπίλυτα ερωτήματα σχετικά με τη διαφάνεια, την επεξηγησιμότητα και την αμφισβήτηση. Συνολικά, αυτές οι μελέτες δείχνουν ότι τα προσωπικά δεδομένα περιλαμβάνουν πλέον πληροφορίες που συλλέγονται άμεσα, αλλά και εξαγόμενα και προγνωστικά αποτελέσματα.

Οι Hoofnagle et al. (2019) επισημαίνουν ότι ο GDPR αφενός θέτει σημαντικούς περιορισμούς σε επιχειρηματικά μοντέλα που βασίζονται σε εντατική συλλογή και αξιοποίηση πληροφοριών, αφετέρου ενισχύει τη σημασία της εσωτερικής διακυβέρνησης δεδομένων και της ανάπτυξης πιο άμεσων και αξιόπιστων σχέσεων με τους καταναλωτές. Οι Haddara et al. (2023) παρέχουν εμπειρική υποστήριξη για αυτήν την παρατήρηση μέσω συνεντεύξεων με επαγγελματίες του ηλεκτρονικού εμπορίου. Τα ευρήματά τους δείχνουν ότι η συμμόρφωση με τον GDPR δημιούργησε πρόσθετο κόστος για τις εταιρείες, αλλά και βελτίωσε την ασφάλεια, αύξησε την εμπιστοσύνη των πελατών και άλλαξε τις πρακτικές ανάλυσης. Συνολικά, η βιβλιογραφία δείχνει ότι η έννοια των προσωπικών δεδομένων πρέπει να γίνει κατανοητή μέσω του ορισμού, της κατηγοριοποίησης, της ευαισθησίας και του τεχνολογικού μετασχηματισμού. Στην εποχή των Μεγάλων Δεδομένων, του Διαδικτύου των Πραγμάτων και της Τεχνητής Νοημοσύνης, τα προσωπικά δεδομένα αποκτούν μεγαλύτερη πολυπλοκότητα, παράγουν νέα πληροφορία μέσω συνδυαστικής και προβλεπτικής επεξεργασίας και αναδεικνύονται σε κρίσιμο πόρο για τη σύγχρονη οικονομία, γεγονός που καθιστά τη νομική οριοθέτηση και τη θεσμική τους διακυβέρνηση αναγκαία τόσο για την προστασία των καταναλωτών όσο και για τη βιώσιμη ανάπτυξη των επιχειρήσεων.

3. Προστασία του καταναλωτή και ψηφιακή εμπιστοσύνη

3.1 Δικαιώματα του καταναλωτή και στατιστική αποτύπωση στην Ελλάδα και στην Ευρωπαϊκή Ένωση

3.1.1 Η έννοια του καταναλωτή και τα δικαιώματά του στην Ευρωπαϊκή Ένωση

Στο δίκαιο της Ευρωπαϊκής Ένωσης, ο καταναλωτής ορίζεται ως κάθε φυσικό πρόσωπο που ενεργεί για σκοπούς οι οποίοι βρίσκονται εκτός της εμπορικής, επιχειρηματικής, βιοτεχνικής ή επαγγελματικής του δραστηριότητας. Ο ορισμός αυτός, που αποτυπώνεται στην Οδηγία 2011/83/ΕΕ, έχει ιδιαίτερη σημασία, επειδή καθορίζει το υποκείμενο στο οποίο απονέμονται ειδικά δικαιώματα πληροφόρησης, υπαναχώρησης και προστασίας στις συναλλαγές με επαγγελματίες, ιδίως στο πεδίο των εξ αποστάσεως και εκτός εμπορικού καταστήματος συμβάσεων (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2011).

Παράλληλα, η έννοια του καταναλωτή στην ΕΕ συνδέεται στενά με το δικαίωμα στην ιδιωτικότητα και στην προστασία των προσωπικών δεδομένων. Ο Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης κατοχυρώνει αφενός το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής και αφετέρου το αυτοτελές δικαίωμα προστασίας δεδομένων προσωπικού χαρακτήρα στα άρθρα 7 και 8 αντίστοιχα. Στο σύγχρονο ψηφιακό περιβάλλον, τα δικαιώματα αυτά αποκτούν ιδιαίτερη πρακτική αξία, καθώς ο καταναλωτής συμμετέχει σε αγορές όπου η συλλογή, η αποθήκευση και η επεξεργασία δεδομένων συνδέονται άμεσα με την εμπορική στόχευση, τη διαφήμιση και την εξατομίκευση υπηρεσιών (Ευρωπαϊκή Ένωση, 2012).

Εξίσου κρίσιμη είναι η προστασία του καταναλωτή από αθέμιτες εμπορικές πρακτικές. Η Οδηγία 2005/29/ΕΚ καθιερώνει κοινό ευρωπαϊκό πλαίσιο κατά των πρακτικών που στρεβλώνουν ουσιωδώς την οικονομική συμπεριφορά του καταναλωτή. Το κανονιστικό αυτό πλαίσιο καλύπτει ιδίως παραπλανητικές και επιθετικές πρακτικές, πριν, κατά τη διάρκεια και μετά την εμπορική συναλλαγή. Με αυτόν τον τρόπο, η προστασία του καταναλωτή στην ΕΕ αποκτά πολυδιάστατο χαρακτήρα, συνδυάζοντας συμβατικά δικαιώματα, προστασία ιδιωτικότητας και διασφάλιση δίκαιης εμπορικής συμπεριφοράς στην εσωτερική αγορά (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2005).

Η πολιτική προστασίας του καταναλωτή απέκτησε ευρύτερο στρατηγικό προσανατολισμό μέσω του νέου θεματολογίου της Ευρωπαϊκής Ένωσης για την περίοδο 2020 έως 2025. Οι βασικοί άξονες αφορούσαν την πράσινη μετάβαση, τον ψηφιακό μετασχηματισμό, την αποτελεσματική επιβολή των δικαιωμάτων, την ειδική μέριμνα για ευάλωτες ομάδες καταναλωτών και τη διεθνή συνεργασία. Το ενημερωτικό υλικό του Ευρωπαϊκού Κοινοβουλίου, το οποίο αναδημοσιεύθηκε από το Lawspot, αποδίδει οπτικά τη σύνδεση ανάμεσα στη ρύθμιση της ψηφιακής οικονομίας, στην ασφάλεια των προϊόντων, στην εγκυρότητα των περιβαλλοντικών ισχυρισμών και στην προστασία του δικαιώματος του καταναλωτή να ασκεί πραγματική επιλογή (Lawspot, 2021; Ευρωπαϊκό Κοινοβούλιο, 2021).

Γράφημα 1: Κατευθύνσεις ενίσχυσης της προστασίας των καταναλωτών στην Ευρωπαϊκή Ένωση

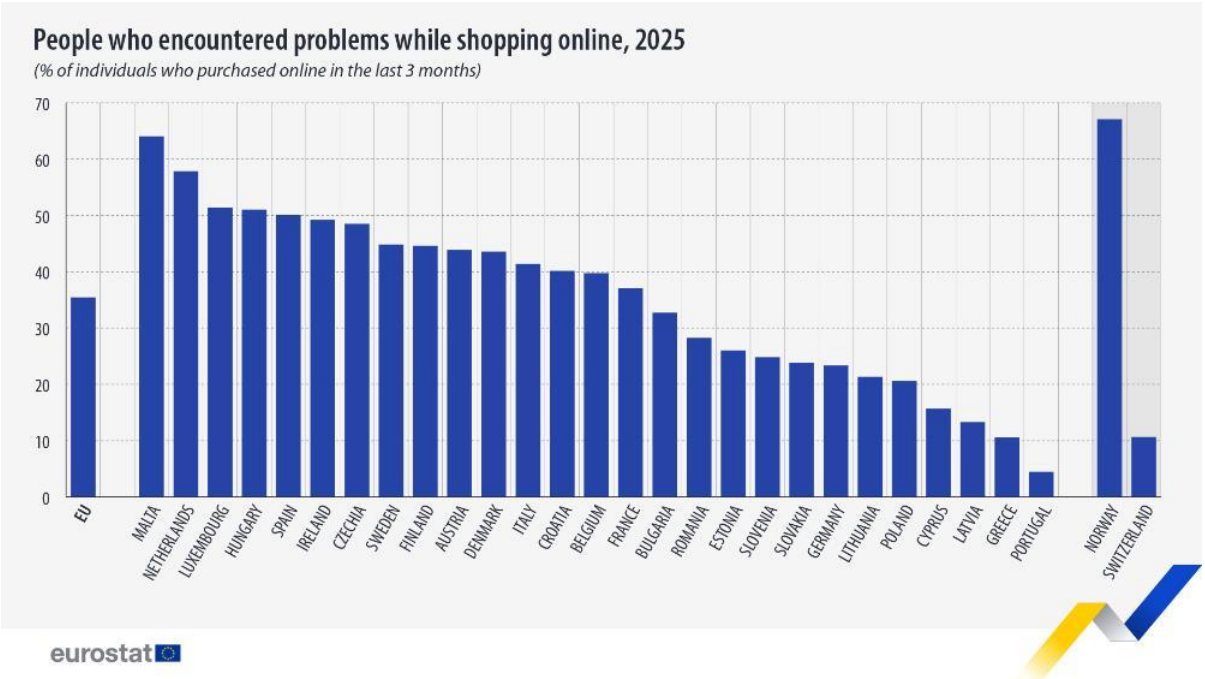
Πηγή: Lawspot, 2021, Ευρωπαϊκό Κοινοβούλιο

3.1.2 Στατιστική αποτύπωση της προστασίας του καταναλωτή στην Ελλάδα και στην Ευρωπαϊκή Ένωση

Η στατιστική εικόνα αναδεικνύει την έκταση και τη μορφή των προβλημάτων που συνοδεύουν τις ηλεκτρονικές αγορές. Στην έρευνα χρήσης τεχνολογιών πληροφορίας και επικοινωνιών του 2025, το 35,4% των ηλεκτρονικών αγοραστών στην Ευρωπαϊκή Ένωση ανέφερε κάποιο πρόβλημα κατά την αγορά μέσω ιστοσελίδας ή εφαρμογής. Για

την Ελλάδα το αντίστοιχο ποσοστό διαμορφώθηκε σε 10,6%. Ο δείκτης αφορά άτομα ηλικίας 16 έως 74 ετών που πραγματοποίησαν ηλεκτρονική αγορά κατά τους τρεις μήνες πριν από την έρευνα και προσφέρει ένα συγκρίσιμο μέτρο εμπειρίας καταναλωτή μεταξύ των κρατών μελών (Eurostat, 2026).

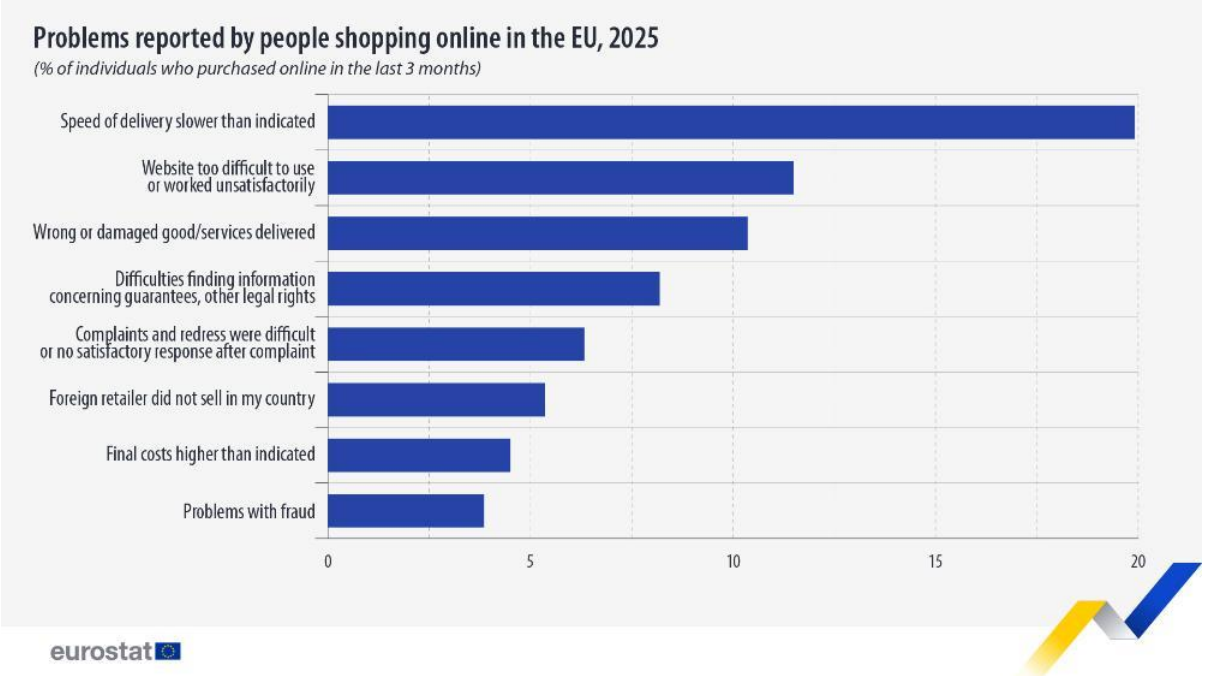
Γράφημα 2: Ηλεκτρονικοί αγοραστές που αντιμετώπισαν προβλήματα στην Ευρωπαϊκή Ένωση το 2025.



Πηγή: Eurostat, 2026

Η καθυστέρηση παράδοσης αποτέλεσε το συχνότερο πρόβλημα και αφορούσε το 19,9% των ηλεκτρονικών αγοραστών στην Ευρωπαϊκή Ένωση. Ακολούθησαν η δυσκολία χρήσης ή η προβληματική λειτουργία της ιστοσελίδας με 11,5% και η παράδοση λανθασμένων ή κατεστραμμένων αγαθών και υπηρεσιών με 10,4%. Η κατανομή αυτή συνδέει την προστασία του καταναλωτή με την ποιότητα των ψηφιακών διεπαφών, την αξιοπιστία των πληροφοριών και την αποτελεσματική διαχείριση της εφοδιαστικής αλυσίδας (Eurostat, 2026).

Γράφημα 3: Συχνότερα προβλήματα κατά τις ηλεκτρονικές αγορές στην Ευρωπαϊκή Ένωση το 2025



Πηγή: Eurostat, 2026

Η ελληνική εμπειρία παρουσιάζει έντονη μεταβολή κατά την περίοδο της ταχείας ανάπτυξης του ηλεκτρονικού εμπορίου. Το ποσοστό των χρηστών που πραγματοποιούσαν αγορές μέσω ηλεκτρονικών καταστημάτων αυξήθηκε από 21% στα τέλη του 2019 σε 50% έως το καλοκαίρι του 2020. Παράλληλα, το μερίδιο των αναφορών προς τον Συνήγορο του Καταναλωτή που αφορούσε το ηλεκτρονικό εμπόριο αυξήθηκε από 12% τον Δεκέμβριο του 2019 σε 25% τον Οκτώβριο του 2020. Τα στοιχεία αυτά αποτυπώνουν τη στενή σχέση ανάμεσα στην επέκταση της ψηφιακής αγοράς και στην ανάγκη ενισχυμένων μηχανισμών εποπτείας και επίλυσης διαφορών (Τσότσου, 2020).

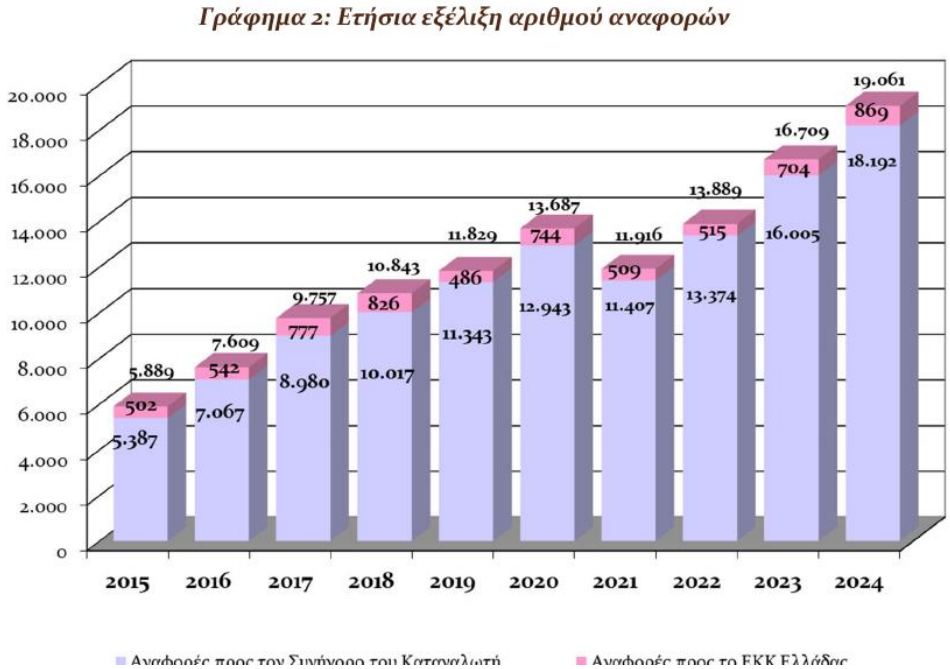
Πίνακας 4: Ενδεικτικοί δείκτες εξέλιξης του ηλεκτρονικού εμπορίου και προστασίας του καταναλωτή στην Ελλάδα

Δείκτης	Περίοδος αναφοράς	Τιμή	Αναλυτική σημασία
Χρήστες ηλεκτρονικών καταστημάτων	Τέλη 2019 και καλοκαίρι 2020	21% και 50%	Ταχεία διεύρυνση της συμμετοχής στην ψηφιακή αγορά
Αναφορές σχετικές με ηλεκτρονικό εμπόριο	Δεκέμβριος 2019 και Οκτώβριος 2020	12% και 25% του συνόλου	Αύξηση της ζήτησης για θεσμική προστασία
Αναφορές προς τον Συνήγορο του Καταναλωτή	2023 και 2024	16.005 και 18.192	Ετήσια αύξηση 13,7%
Επίλυση αναφορών	2024	Σχεδόν 80%	67,46% υπέρ καταναλωτή και 12,22% υπέρ προμηθευτή
Μέσος χρόνος επίλυσης	2024	95 ημέρες	Λειτουργικός δείκτης ταχύτητας θεσμικής απόκρισης

Πηγή: Τσότσου, 2020 και Συνήγορος του Καταναλωτή, 2026

Η Ετήσια Έκθεση 2024 του Συνηγόρου του Καταναλωτή καταγράφει 18.192 αναφορές έναντι 16.005 το 2023 και ετήσια αύξηση 13,7%. Με τη συνεκτίμηση των αναφορών προς το Ευρωπαϊκό Κέντρο Καταναλωτή Ελλάδας, το συνολικό μέγεθος ανήλθε από 16.709 σε 19.061 αναφορές. Η Αρχή επιλύει περίπου οκτώ στις δέκα υποθέσεις μέσα σε μέσο χρονικό διάστημα 95 ημερών. Η εξέλιξη του αριθμού των αναφορών λειτουργεί ως δείκτης έντασης των καταναλωτικών διαφορών, ενώ το ποσοστό και ο χρόνος επίλυσης λειτουργούν ως δείκτες αποτελεσματικότητας της θεσμικής προστασίας (Συνήγορος του Καταναλωτή, 2026).

Γράφημα 4: Ετήσια εξέλιξη του αριθμού αναφορών προς τον Συνήγορο του Καταναλωτή και το Ευρωπαϊκό Κέντρο Καταναλωτή Ελλάδας



Πηγή: Συνήγορος του Καταναλωτή, 2026, Ετήσια Έκθεση 2024

Οι περιπτώσεις επιβολής της νομοθεσίας δείχνουν τρεις συμπληρωματικές μορφές εποπτείας. Η πρώτη αφορά την επιβολή οικονομικών κυρώσεων για παραπλανητικές προσφορές. Η δεύτερη αφορά τη διορθωτική εποπτεία με συστάσεις και επανέλεγχο. Η τρίτη αφορά τον συνδυασμό προστίμου και προσωρινού περιορισμού ψηφιακής πρόσβασης όταν οι παραβάσεις εμφανίζουν σοβαρό και επαναλαμβανόμενο χαρακτήρα. Η συγκριτική παρουσίαση αποτυπώνει τη μετάβαση από την καταγγελία στην έρευνα, στη διοικητική αντίδραση και στην αποκατάσταση της συμμόρφωσης.

Πίνακας 5: Ενδεικτικές περιπτώσεις εφαρμογής της νομοθεσίας προστασίας καταναλωτή

Έτος και χώρα	Περίπτωση	Εύρημα και μέτρο	Σημασία για την εμπιστοσύνη
2024 Ελλάδα	Έλεγχος έντεκα επιχειρήσεων	Πλασματικές εκπτώσεις, προσφορές και πλημμελής εφαρμογή της καταναλωτικής νομοθεσίας. Συνολικά πρόστιμα 1.480.000 ευρώ	Η δημοσιοποίηση και η οικονομική κύρωση ενισχύουν τη διαφάνεια των τιμών
2025 Κύπρος	Έλεγχος 150 καταστημάτων σχολικών ειδών	Πλήρης αρχική συμμόρφωση σε 140 καταστήματα. Γραπτές συστάσεις σε 10 καταστήματα, ποσοστό 6,67%, και πλήρης συμμόρφωση στους επανελέγχους	Ο επανέλεγχος μετατρέπει τη σύσταση σε επαληθεύσιμο αποτέλεσμα συμμόρφωσης
2026 Ελλάδα	Ηλεκτρονικό κατάστημα PCRAMA	Παράλειψη παράδοσης πληρωμένων προϊόντων, εκκρεμείς επιστροφές χρημάτων και ανακριβής πληροφόρηση διαθεσιμότητας. Πρόστιμο 150.000 ευρώ και προσωρινή απαγόρευση πρόσβασης	Ο συνδυασμός κύρωσης και περιορισμού πρόσβασης προστατεύει άμεσα τους συναλλασσόμενους

Πηγή: Υπουργείο Ανάπτυξης, 2024, Υπηρεσία Προστασίας Καταναλωτή Κύπρου, 2025 και Newmoney, 2026

3.2 Ψηφιακή εμπιστοσύνη και εταιρική υπευθυνότητα

Η εμπιστοσύνη αποτελεί βασική προϋπόθεση για τη νομιμότητα των επιχειρήσεων στις αγορές που χρησιμοποιούν την τεχνολογία, επειδή οι καταναλωτές αξιολογούν τις εταιρείες από τον τρόπο με τον οποίο συλλέγουν, εξηγούν, προστατεύουν και χρησιμοποιούν προσωπικά δεδομένα. Σε ψηφιακά περιβάλλοντα, η εμπιστοσύνη διαμορφώνεται από ένα μείγμα θεσμικών διαβεβαιώσεων, αντιληπτής διαφάνειας, προσδοκιών απορρήτου και ηθικών αξιολογήσεων της εταιρικής συμπεριφοράς. Η βιβλιογραφία που αναλύεται σε αυτήν την ενότητα δείχνει ότι η ψηφιακή εμπιστοσύνη δεν μπορεί να περιοριστεί μόνο στην εμπιστοσύνη στην τεχνική ασφάλεια, καθώς αντικατοπτρίζει επίσης τις πεποιθήσεις για τη δικαιοσύνη, την κατανοησιμότητα, την υπευθυνότητα και την υπεύθυνη εταιρική συμπεριφορά. Για το λόγο αυτό, η σχέση μεταξύ εμπιστοσύνης και επιχειρηματικής ανάπτυξης είναι στενά συνδεδεμένη με τη διακυβέρνηση δεδομένων, τις πρακτικές επικοινωνίας και την

εταιρική ευθύνη. Η ακόλουθη ανάλυση εξετάζει αυτή τη σχέση μέσω τριών αλληλένδετων διαστάσεων, δηλαδή το πλαίσιο εμπιστοσύνης του ψηφιακού μετασχηματισμού, τη σύνδεση μεταξύ εμπιστοσύνης, διαφάνειας και αφοσίωσης πελατών και τη σύνδεση μεταξύ εταιρικής κοινωνικής ευθύνης και προστασίας δεδομένων (Chang et al., 2018; van der Merwe & Al Achkar, 2022).

3.2.1 Το πλαίσιο εμπιστοσύνης στον ψηφιακό μετασχηματισμό

Ο ψηφιακός μετασχηματισμός διευρύνει τις ευκαιρίες για εξατομίκευση, αυτοματοποίηση και δέσμευση πελατών, αλλά εντείνει επίσης την αβεβαιότητα σχετικά με την επιτήρηση και την κακή χρήση πληροφοριών. Σε αυτό το πλαίσιο, η εμπιστοσύνη λειτουργεί ως μηχανισμός που μειώνει την αντιληπτή ευπάθεια και επιτρέπει στους καταναλωτές να ασχολούνται με ψηφιακές υπηρεσίες παρά την ελλιπή γνώση των οργανωτικών διαδικασιών. Οι Chang et al. (2018) δείχνουν ότι η αντιληπτή αποτελεσματικότητα της πολιτικής απορρήτου επηρεάζει σημαντικά τον έλεγχο της ιδιωτικότητας, τον κίνδυνο απορρήτου, την εμπιστοσύνη και τη συνολική αντιληπτή ιδιωτικότητα. Τα ευρήματά τους δείχνουν ότι η ειδοποίηση, η πρόσβαση, η ασφάλεια και η επιβολή δεν είναι τυπικά νομικά χαρακτηριστικά, αλλά πρακτικά στοιχεία οικοδόμησης εμπιστοσύνης. Οι καταναλωτές συμπεραίνουν από αυτά τα στοιχεία εάν μια εταιρεία σέβεται τα πληροφοριακά όρια και εάν το ψηφιακό περιβάλλον είναι διαχειρίσιμο.

Μια συμπληρωματική διάσταση δίνεται από τους Montecchi et al. (2024), οι οποίοι αντιλαμβάνονται την αντιληπτή διαφάνεια της επωνυμίας μέσω τριών διαστάσεων: παρατηρησιμότητα, κατανοησιμότητα και σκοπιμότητα. Αυτό το πλαίσιο είναι πολύτιμο επειδή διευκρινίζει ότι η ψηφιακή εμπιστοσύνη εξαρτάται από την ορατότητα των πληροφοριών και από το εάν οι πληροφορίες μπορούν να γίνουν κατανοητές και εάν η αποκάλυψη φαίνεται ειλικρινής παρά στρατηγική. Επομένως, η διαφάνεια λειτουργεί ως μια ένδειξη ποιότητας επικοινωνίας που βοηθά τους καταναλωτές να ερμηνεύουν τα οργανωτικά κίνητρα. Στον ψηφιακό μετασχηματισμό, αυτό είναι ιδιαίτερα σημαντικό επειδή οι εταιρείες βασίζονται συχνά σε αδιαφανείς υποδομές δεδομένων που είναι δύσκολο να αξιολογηθούν άμεσα από τους απλούς χρήστες.

Η εμπιστοσύνη επηρεάζεται επίσης από την παρουσία συγκεκριμένων μηχανισμών διασφάλισης. Οι Saxena και Thakur (2024) διαπιστώνουν ότι οι μηχανισμοί διασφάλισης, συμπεριλαμβανομένων των ασφαλών συστημάτων πληρωμών, των σφραγίδων εμπιστοσύνης και των μέτρων προστασίας δεδομένων, επηρεάζουν σημαντικά την πρόθεση αγοράς, ενώ οι ανησυχίες για την εμπιστοσύνη και την ιδιωτικότητα μεσολαβούν εν μέρει σε αυτή τη σχέση. Τα στοιχεία τους δείχνουν ότι οι τεχνικές και συμβολικές διαβεβαιώσεις είναι εξίσου σημαντικές, καθώς αφενός προστατεύουν τις συναλλαγές και αφετέρου, διαμορφώνουν τις ψυχολογικές συνθήκες υπό τις οποίες οι καταναλωτές κρίνουν μια εταιρεία ως αξιόπιστη. Ομοίως, οι Alzaidi και Agag (2022) καταδεικνύουν ότι οι ανησυχίες για την εμπιστοσύνη και την ιδιωτικότητα επηρεάζουν έντονα τη συμπεριφορά αγοράς σε υπηρεσίες ηλεκτρονικού λιανικού εμπορίου που βασίζονται στα μέσα κοινωνικής δικτύωσης, ενώ η ποιότητα των πληροφοριών, οι ανησυχίες για την ασφάλεια, η ευκολία χρήσης, οι σφραγίδες διασφάλισης και η πιστοποίηση τρίτων λειτουργούν ως σημαντικοί παράγοντες. Η ψηφιακή εμπιστοσύνη, επομένως, γίνεται καλύτερα κατανοητή ως μια πολυδιάστατη έννοια που παράγεται από μηχανισμούς διακυβέρνησης, επικοινωνιακή σαφήνεια και προσδοκίες που σχετίζονται με την ιδιωτικότητα.

3.2.2 Η σχέση μεταξύ εμπιστοσύνης, διαφάνειας και αφοσίωσης πελατών

Η δεύτερη διάσταση αφορά τη σχέση μεταξύ εμπιστοσύνης, διαφάνειας και αφοσίωσης πελατών. Στις ψηφιακές αγορές, η εμπιστοσύνη έχει στρατηγική σημασία επειδή υποστηρίζει τη συνέχεια της αλληλεπίδρασης, την προθυμία αποκάλυψης πληροφοριών και τη μακροπρόθεσμη δέσμευση. Οι Cardoso et al. (2022) δείχνουν ότι η εμπιστοσύνη και η αφοσίωση συμβάλλουν από κοινού στην οικοδόμηση βιώσιμων σχέσεων με την επωνυμία και ότι η ικανοποίηση και η ποιότητα της σχέσης ενισχύουν αυτή τη διαδικασία. Η μελέτη τους επιβεβαιώνει ότι η εμπιστοσύνη δεν είναι μόνο ένας αρχικός παράγοντας υιοθέτησης, αλλά αποτελεί θεμέλιο για την σταθερή προσκόλληση του πελάτη με την πάροδο του χρόνου.

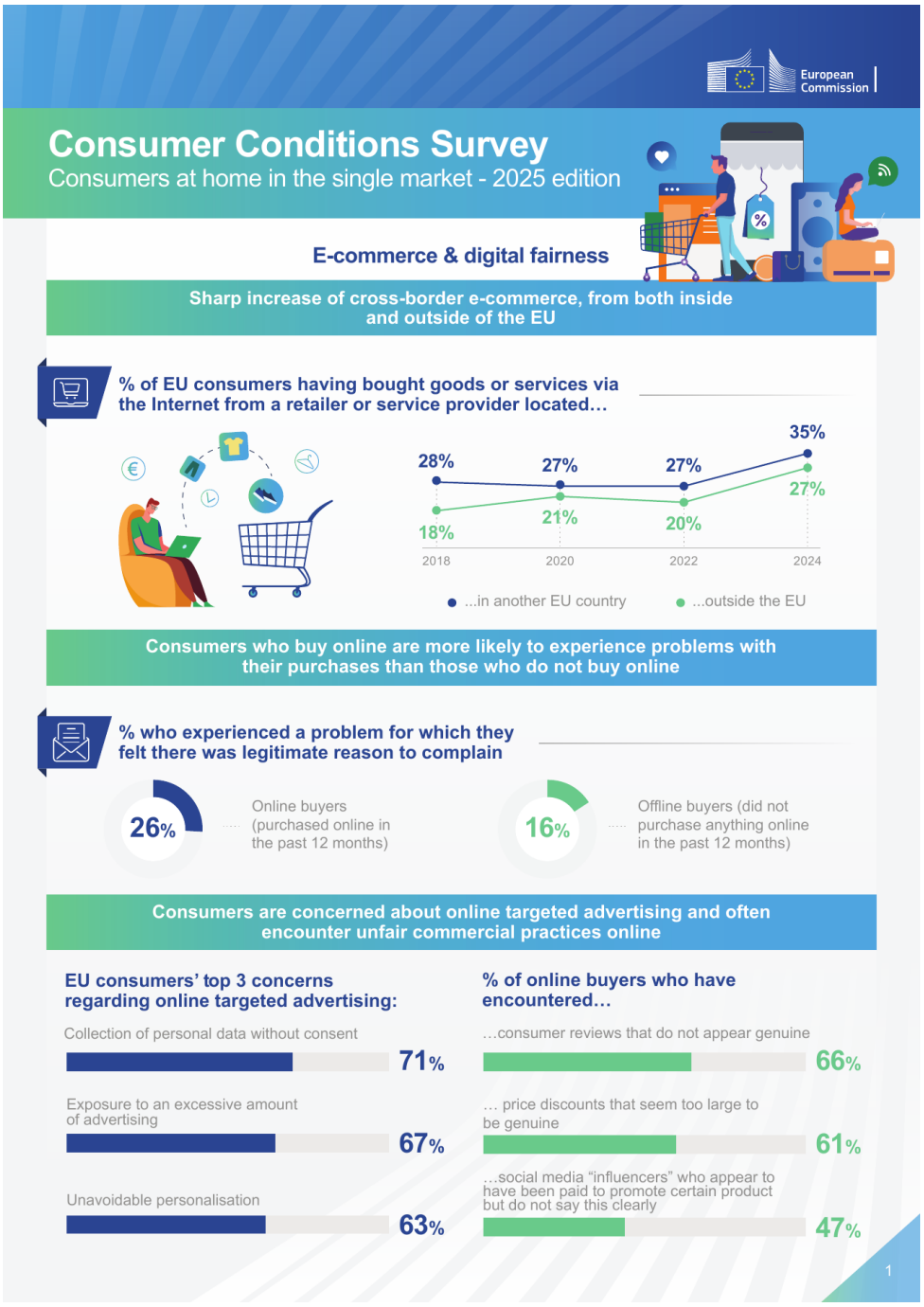
Η διαφάνεια παίζει κρίσιμο ρόλο σε αυτή τη δυναμική. Οι Chang et al. (2018) δείχνουν ότι ο έλεγχος της ιδιωτικότητας επηρεάζει σημαντικά την εμπιστοσύνη και την αντιληπτή ιδιωτικότητα, ενώ οι Montecchi et al. (2024) τονίζουν ότι η διαφάνεια μπορεί να ενισχύσει τις αξιολογήσεις της επωνυμίας όταν είναι κατανοητή και στοχευμένη. Αυτό υποδηλώνει ότι οι εταιρείες κερδίζουν αφοσίωση όχι

αποκαλύπτοντας τα πάντα αδιακρίτως, αλλά δημιουργώντας ουσιαστική διαφάνεια που επιτρέπει στους πελάτες να κατανοήσουν πώς χειρίζονται τα δεδομένα τους και γιατί συμβαίνουν ορισμένες πρακτικές. Με αυτήν την έννοια, η εμπιστοσύνη προκύπτει όταν η διαφάνεια μειώνει την ασάφεια αντί να αυξάνει την υπερφόρτωση πληροφοριών.

Ταυτόχρονα, η σχέση αυτή δεν είναι γραμμική. Οι Canhoto et al. (2024) εξετάζουν την εξατομίκευση με την τεχνητή νοημοσύνη στο φυσικό λιανικό εμπόριο και δείχνουν ότι οι καταναλωτές εκτιμούν τις σχετικές προσφορές και τις βελτιωμένες εμπειρίες αγορών, ωστόσο δυσανασχετούν με τις διακοπές, τη γενική στόχευση και την παρακολούθηση που παρεμβαίνει στην ιδιωτικότητα. Η ανάλυσή τους για το παράδοξο της εξατομίκευσης και της ιδιωτικότητας αποκαλύπτει ότι οι πελάτες αναζητούν ταυτόχρονα την ευκολία και τον έλεγχο. Αυτό σημαίνει ότι οι εταιρείες δεν μπορούν να υποθέσουν ότι η περισσότερη εξατομίκευση ενισχύει αυτόματα την αφοσίωση. Αντίθετα, η αφοσίωση εξαρτάται από το αν η εξατομίκευση βιώνεται ως σεβαστή και χρήσιμη. Οι Alzaidi και Agag (2022) υποστηρίζουν αυτό το συμπέρασμα δείχνοντας ότι οι ανησυχίες για την ιδιωτικότητα παραμένουν κεντρικές ακόμη και όταν αυξάνονται οι ψηφιακές αγορές. Η εμπιστοσύνη γίνεται επομένως ο μηχανισμός εξισορρόπησης, μέσω του οποίου οι εταιρείες μπορούν να μετατρέψουν την αλληλεπίδραση που βασίζεται στα δεδομένα σε διαρκείς σχέσεις με τους πελάτες.

Τα ευρωπαϊκά δεδομένα παρέχουν πληροφόρηση για τη σύνδεση ανάμεσα στη διαφάνεια και στην εμπιστοσύνη. Επτά στους δέκα καταναλωτές θεωρούν ότι οι έμποροι και οι πάροχοι υπηρεσιών σέβονται τα δικαιώματά τους και το 61% εκφράζει εμπιστοσύνη στους δημόσιους οργανισμούς προστασίας. Παράλληλα, το 93% των ηλεκτρονικών αγοραστών εκφράζει ανησυχία για τη στοχευμένη διαδικτυακή διαφήμιση και το 45% των καταναλωτών έχει συναντήσει διαδικτυακές απάτες κατά το προηγούμενο έτος. Η συνύπαρξη θεσμικής εμπιστοσύνης και υψηλής έκθεσης σε ψηφιακούς κινδύνους δείχνει ότι η εμπιστοσύνη αποτελεί δυναμικό μέγεθος που απαιτεί συνεχή επαλήθευση μέσω της εμπειρίας χρήσης και της αποτελεσματικής επιβολής (Ευρωπαϊκή Επιτροπή, 2025).

Γράφημα 5: Ηλεκτρονικό εμπόριο και ψηφιακή δικαιοσύνη στην Ευρωπαϊκή Ένωση



Πηγή: Ευρωπαϊκή Επιτροπή, 2025, Consumer Conditions Survey

Πίνακας 6: Ευρωπαϊκές μετρικές εμπιστοσύνης και ψηφιακού κινδύνου

Μετρική	Ποσοστό	Ερμηνεία
Σεβασμός δικαιωμάτων από επιχειρήσεις	70%	Αντίληψη αξιοπιστίας των εμπορικών φορέων

Μετρική	Ποσοστό	Ερμηνεία
Εμπιστοσύνη στους δημόσιους φορείς προστασίας	61%	Αντίληψη αποτελεσματικότητας της θεσμικής προστασίας
Ανησυχία για στοχευμένη διαδικτυακή διαφήμιση	93%	Ένταση αντιλαμβανόμενου κινδύνου ιδιωτικότητας
Συνάντηση με διαδικτυακή απάτη κατά το προηγούμενο έτος	45%	Πραγματική έκθεση σε ψηφιακό κίνδυνο

Πηγή: Ευρωπαϊκή Επιτροπή, 2025

3.2.3 Εταιρική κοινωνική ευθύνη και προστασία δεδομένων

Η τρίτη διάσταση αφορά τη σχέση μεταξύ εταιρικής κοινωνικής ευθύνης και προστασίας δεδομένων. Σε αυτό το θέμα η βιβλιογραφία κινείται πέρα από την συναλλακτική εμπιστοσύνη σε μια ευρύτερη αξιολόγηση του εταιρικού σκοπού και της ευθύνης. Οι Van der Merwe και Al Achkar (2022) υποστηρίζουν ότι η υπεύθυνη χρήση δεδομένων πρέπει να αναλυθεί μέσω των συνδεδεμένων ιδεών της εταιρικής κοινωνικής ευθύνης, της εταιρικής ψηφιακής ευθύνης και της ευθύνης δεδομένων. Η συμβολή τους είναι σημαντική επειδή παρουσιάζει τις πρακτικές δεδομένων ως ηθικά και κοινωνικά ζητήματα και όχι απλώς ως λειτουργικά ή νομικά ζητήματα. Υπό αυτή την οπτική γωνία, η υπεύθυνη χρήση των δεδομένων γίνεται μέρος του τρόπου με τον οποίο οι εταιρείες ασκούν την εξουσία τους στην ψηφιακή κοινωνία.

Ο Pollach (2011) προσφέρει μια προηγούμενη εμπειρική βάση για αυτόν τον ισχυρισμό, δείχνοντας ότι το διαδικτυακό απόρρητο είχε εισέλθει στην ατζέντα της ΕΚΕ άνισα. Πολλές μεγάλες εταιρείες αντιμετώπισαν το απόρρητο κυρίως μέσω μέτρων συμμόρφωσης, ενώ ο διάλογος με τα ενδιαφερόμενα μέρη και οι ευρύτερες σχεσιακές δεσμεύσεις παρέμειναν περιορισμένες. Αυτό το εύρημα υποδηλώνει ότι οι εταιρείες συχνά αναγνώριζαν το απόρρητο ως ζήτημα χωρίς να το ενσωματώνουν πλήρως στις στρατηγικές κοινωνικής ευθύνης τους. Ο Steele (2022) προωθεί τη συζήτηση συνδέοντας ρητά την προστασία δεδομένων με την εταιρική λογοδοσία και το δικαίωμα στην ιδιωτικότητα. Το άρθρο αυτό υποστηρίζει ότι η προστασία δεδομένων θα πρέπει να αντιμετωπίζεται ως ουσιαστική ευθύνη των επιχειρήσεων και όχι απλώς ως τεχνική υποχρέωση συμμόρφωσης.

Σύγχρονα έρευνες ενισχύουν αυτή τη θέση. Οι Alhumud et al. (2025) δείχνουν ότι η ψηφιακή γνωστοποίηση ΕΚΕ σχετικά με την προστασία των καταναλωτών, την ευημερία των εργαζομένων, τις φιλικές προς το περιβάλλον πρακτικές και τη συμμετοχή της κοινότητας επηρεάζει θετικά την εμπιστοσύνη των καταναλωτών, η οποία με τη σειρά της ενισχύει την δέσμευση των πελατών. Τα ευρήματά τους δείχνουν ότι η υπεύθυνη γνωστοποίηση έχει συνέπειες στη φήμη και στις σχέσεις, ειδικά μεταξύ των καταναλωτών που χαρακτηρίζονται από ισχυρότερους δεοντολογικούς προσανατολισμούς και υπακοή στο νόμο. Συνολικά, αυτές οι μελέτες δείχνουν ότι η προστασία δεδομένων έχει γίνει ένα σημαντικό συστατικό της εταιρικής ευθύνης. Οι εταιρείες που ευθυγραμμίζουν τη διαφάνεια, τις διασφαλίσεις απορρήτου και την ηθική γνωστοποίηση είναι πιο πιθανό να εμπνέουν εμπιστοσύνη, να διατηρούν τη συμμετοχή και να ενισχύουν τη νομιμότητα στις ψηφιακές αγορές.

3.3 Ψυχολογικοί και κοινωνικοί παράγοντες

3.3.1 Αντιλήψεις καταναλωτών για την ιδιωτικότητα

Η εμπιστοσύνη των καταναλωτών στις ψηφιακές αγορές ξεκινά με τον τρόπο που τα άτομα αντιλαμβάνονται την ιδιωτικότητα, την ασφάλεια και τον έλεγχο των προσωπικών πληροφοριών. Τα πρώιμα στοιχεία από το ηλεκτρονικό εμπόριο έδειξαν ότι οι κίνδυνοι για την ιδιωτικότητα και την ασφάλεια ήταν ήδη κεντρικά εμπόδια στη συμπεριφορά των καταναλωτών στις ψηφιακές αγορές. Οι Miyazaki και Fernandez (2001) διαπίστωσαν ότι οι αντιλήψεις για την ιδιωτικότητα και τον κίνδυνο ασφάλειας στο Διαδίκτυο ποικίλλουν ανάλογα με την εμπειρία στο Διαδίκτυο και συνδέονται ουσιαστικά με τη δραστηριότητα ηλεκτρονικών αγορών. Η μελέτη τους διαπίστωσε ότι οι ανησυχίες για την ιδιωτικότητα δεν είναι αφηρημένες στάσεις, αλλά πρακτικές κρίσεις που διαμορφώνουν την προθυμία για συναλλαγές. Αυτή η γνώση παραμένει θεμελιώδης επειδή μεταγενέστερη έρευνα επιβεβαιώνει ότι οι αντιλήψεις για την ιδιωτικότητα αναπτύσσονται μέσω γνωστικών αξιολογήσεων του κινδύνου, του ελέγχου και των θεσμικών διασφαλίσεων και όχι μόνο μέσω της χρήσης της τεχνολογίας.

Οι Xu et al. (2011) εμβαθύνουν αυτήν την προοπτική συνδέοντας τις ατομικές ανησυχίες για την ιδιωτικότητα με τις θεσμικές διασφαλίσεις για την ιδιωτικότητα. Βασιζόμενοι στη θεωρία της Διαχείρισης της Ιδιωτικότητας των Επικοινωνιών,

δείχνουν ότι οι ανησυχίες για την ιδιωτικότητα διαμορφώνονται μέσω μιας διαδικασίας αξιολόγησης που περιλαμβάνει τον αντιληπτό κίνδυνο για την ιδιωτικότητα, τον έλεγχο της ιδιωτικότητας και την ατομική προδιάθεση να εκτιμά κανείς την σημασία της ιδιωτικότητας. Είναι σημαντικό ότι η μελέτη τους καταδεικνύει ότι οι πολιτικές απορρήτου και η αυτορρύθμιση του κλάδου μπορούν να μειώσουν τις ανησυχίες για την ιδιωτικότητα όταν θεωρούνται αποτελεσματικές. Αυτό σημαίνει ότι η εμπιστοσύνη είναι εν μέρει ψυχολογική και εν μέρει θεσμική.

Μια παρόμοια λογική εμφανίζεται σε περιβάλλοντα κοινωνικής δικτύωσης. Ο Shin (2010) δείχνει ότι η αντιληπτή ιδιωτικότητα, η αντιληπτή ασφάλεια και η εμπιστοσύνη είναι ξεχωριστές αλλά συνδεδεμένες έννοιες που επηρεάζουν την υιοθέτηση των κοινωνικών δικτύων. Η μελέτη διαπιστώνει επίσης ότι η αντιληπτή ασφάλεια μετριάζει την επίδραση της αντιληπτής ιδιωτικότητας στην εμπιστοσύνη. Έτσι, οι αντιλήψεις για την ιδιωτικότητα δεν λειτουργούν μεμονωμένα, καθώς στην πράξη αλληλεπιδρούν με τις πεποιθήσεις σχετικά με την τεχνική και οργανωτική ικανότητα των πλατφορμών να προστατεύουν τους χρήστες. Οι Gupta και Dhami (2015) υποστηρίζουν περαιτέρω αυτό το επιχείρημα δείχνοντας ότι η ασφάλεια, η εμπιστοσύνη και η ιδιωτικότητα επηρεάζουν σημαντικά την πρόθεση συμπεριφοράς των χρηστών να μοιράζονται πληροφορίες σε ιστότοπους κοινωνικής δικτύωσης. Μαζί, αυτές οι μελέτες υποδηλώνουν ότι η ψυχολογία της εμπιστοσύνης βασίζεται σε μια αλληλεπίδραση μεταξύ ευπάθειας και διασφάλισης, όπου οι χρήστες λαμβάνουν υπόψιν τους τα αναμενόμενα κοινωνικά ή συναλλακτικά οφέλη έναντι της πιθανότητας κακής χρήσης.

Το ίδιο μοτίβο είναι ορατό σε περιβάλλοντα λιανικής πώλησης. Οι Mohr και Walter (2019) υποστηρίζουν ότι, στο πλαίσιο των ηλεκτρονικών αγορών, η αντίληψη των καταναλωτών για την ασφάλεια των πληροφοριών δεν διαμορφώνεται πάντοτε μέσω αυτόνομης αξιολόγησης των τεχνικών μέτρων προστασίας. Αντίθετα, συχνά απορρέει από τη γενικότερη εμπιστοσύνη που έχουν προς τον ηλεκτρονικό λιανοπωλητή, η οποία μεταφέρεται και στην εκτίμησή τους ότι τα προσωπικά τους δεδομένα προστατεύονται επαρκώς. Αυτό βοηθά να εξηγηθεί γιατί οι καταναλωτές μπορεί να εκφράζουν ανησυχία σε έρευνες, αλλά να συμπεριφέρονται λιγότερο προσεκτικά στην πράξη. Οι Evans et al. (2023) προσθέτουν μια άλλη σημαντική διάσταση δείχνοντας ότι οι ανησυχίες για την προστασία της ιδιωτικής ζωής

επηρεάζονται από παράγοντες όπως η αξία της εξατομίκευσης, ο αντιληπτός έλεγχος από τους καταναλωτές, η οργανωσιακή εμπιστοσύνη και η διαφάνεια των δεδομένων, αν και δεν μειώνουν όλοι αυτοί οι παράγοντες την ανησυχία με τον ίδιο τρόπο. Τα ευρήματά τους αναδεικνύουν ότι η ψυχολογία της εμπιστοσύνης περιλαμβάνει κάτι πιο σημαντικό από την απλή αποφόρτιση της ανησυχίας. Οι καταναλωτές συχνά αναγνωρίζουν την αξία της εξατομίκευσης, ενώ παράλληλα αποδίδουν ιδιαίτερη σημασία στη διατήρηση του ουσιαστικού ελέγχου επί των προσωπικών τους δεδομένων. Ως εκ τούτου, οι αντιλήψεις για την ιδιωτικότητα εμφανίζουν μεταβλητό χαρακτήρα, εξαρτώνται από το εκάστοτε πλαίσιο και συνδέονται στενά με ευρύτερες προσδοκίες περί δικαιοσύνης, διαφάνειας και ατομικής αυτονομίας.

3.3.2 Ο αντίκτυπος των παραβιάσεων δεδομένων ή της κακής χρήσης δεδομένων

Εάν οι αντιλήψεις για την προστασία της ιδιωτικής ζωής διαμορφώνουν την αρχική εμπιστοσύνη, οι παραβιάσεις δεδομένων και η κακή χρήση δεδομένων ελέγχουν εάν αυτή η εμπιστοσύνη μπορεί να επιβιώσει από την οργανωτική αποτυχία. Πρόσφατες μελέτες δείχνουν ότι τα περιστατικά παραβίασης έχουν άμεσες και διαρκείς συνέπειες στις σχέσεις. Οι Swani et al. (2024), εξετάζοντας σχέσεις μεταξύ επιχειρήσεων, διαπιστώνουν ότι η παραβίαση τόσο των προσωπικών δεδομένων των στελεχών ή εκπροσώπων της επιχείρησης πελάτη όσο και των εταιρικών πληροφοριών που αφορούν την ίδια την επιχείρηση περιορίζει την εμπιστοσύνη, ενισχύει τη δυσαρέσκεια και οδηγεί στην υιοθέτηση προστατευτικών συμπεριφορών ή στην αναζήτηση διαφορετικού προμηθευτή. Η ανάλυσή τους είναι ιδιαίτερα σημαντική επειδή καταδεικνύει ότι οι επιπτώσεις της παραβίασης μεταδίδονται από το ζημιωθέν μέρος σε ευρύτερα αποτελέσματα σχέσεων, συμπεριλαμβανομένης της δέσμευσης και της φήμης του προμηθευτή. Η εμπιστοσύνη, επομένως, λειτουργεί ως ένα εύθραυστο πλεονέκτημα που μπορεί να επιδεινωθεί γρήγορα όταν η προστασία δεδομένων αποτύχει.

Ο Nikkhah (2025) προσεγγίζει το ζήτημα από την οπτική γωνία της οργανωτικής αντίδρασης μετά από μια παραβίαση. Χρησιμοποιώντας ένα πείραμα πεδίου που περιλαμβάνει πραγματικά θύματα, η μελέτη δείχνει ότι η αποζημίωση μπορεί να μειώσει τις άμεσες αρνητικές αντιδράσεις, αλλά δεν επιδιορθώνει τις μακροπρόθεσμες πεποιθήσεις. Αυτή η διάκριση είναι κρίσιμη για την ψυχολογική κατανόηση της εμπιστοσύνης. Ο βραχυπρόθεσμος κατευνασμός και η μακροπρόθεσμη

αποκατάσταση δεν είναι ισοδύναμες. Ένας καταναλωτής μπορεί να δεχτεί αποζημίωση ενώ συνεχίζει να πιστεύει ότι ο οργανισμός είναι αναξιόπιστος, αδιαφανής ή ηθικά ανεπαρκής. Συνεπώς, τα γεγονότα παραβίασης αλλοιώνουν όχι μόνο την ικανοποίηση αλλά και τις βαθύτερες πεποιθήσεις που υποστηρίζουν τη μελλοντική εμπιστοσύνη. Σε κοινωνικούς όρους, μπορούν επίσης να επηρεάσουν τη φήμη μέσω της προφορικής ενημέρωσης, της δημόσιας κριτικής και του συλλογικού σκεπτικισμού απέναντι στις πρακτικές ψηφιακών δεδομένων γενικότερα.

Εξάλλου, οι πραγματικές υποθέσεις παραβίασης επιτρέπουν την εφαρμογή των θεωρητικών συμπερασμάτων σε συγκεκριμένα γεγονότα. Η έκταση των επηρεαζόμενων αρχείων, η ταχύτητα γνωστοποίησης, το ύψος της κύρωσης και η ποιότητα των διορθωτικών ενεργειών λειτουργούν ως ορατά σήματα λογοδοσίας. Η θεσμική και οργανωτική αντίδραση διαμορφώνει τη δυνατότητα αποκατάστασης της εμπιστοσύνης, ιδιαίτερα όταν συνδυάζει ενημέρωση, τεχνική ενίσχυση, υποστήριξη των επηρεαζόμενων προσώπων και αναθεώρηση της εταιρικής διακυβέρνησης.

Πίνακας 7: Συγκριτική παρουσίαση περιστατικών παραβίασης και επιπτώσεων στην εμπιστοσύνη

Περίπτωση	Περιστατικό και έκταση	Θεσμική και οργανωτική αντίδραση	Διάσταση εμπιστοσύνης
Facebook και Cambridge Analytica	Παραπλανητική συλλογή δεδομένων από δεκάδες εκατομμύρια χρήστες για κατάρτιση προφίλ και πολιτική στόχευση	Η Cambridge Analytica οδηγήθηκε σε πτώχευση το 2018. Η Ομοσπονδιακή Επιτροπή Εμπορίου επέβαλε στο Facebook κύρωση 5 δισεκατομμυρίων δολαρίων και νέους μηχανισμούς λογοδοσίας	Η υπόθεση ανέδειξε τη σύνδεση ανάμεσα στη συγκατάθεση, στην εμπορική αξιοποίηση δεδομένων και στη δημόσια νομιμοποίηση της πλατφόρμας
British Airways	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα περίπου 429.612 προσώπων, συμπεριλαμβανομένων στοιχείων καρτών και λογαριασμών	Η εταιρεία ενημέρωσε πελάτες και εποπτικές αρχές, περιόρισε την ευπάθεια και ενίσχυσε τα τεχνικά μέτρα. Η αρμόδια αρχή επέβαλε πρόστιμο 20 εκατομμυρίων λιρών	Η άμεση ενημέρωση και η τεχνική αποκατάσταση λειτουργούν ως πρώτα βήματα, ενώ η κύρωση αποτυπώνει τη σοβαρότητα του περιστατικού

Περίπτωση	Περιστατικό και έκταση	Θεσμική και οργανωτική αντίδραση	Διάσταση εμπιστοσύνης
Marriott International	Παραβίαση του συστήματος Starwood με εκτιμώμενη επίδραση σε 339 εκατομμύρια αρχεία επισκεπτών, από τα οποία 30,1 εκατομμύρια αφορούσαν τον Ευρωπαϊκό Οικονομικό Χώρο	Η εταιρεία δημιούργησε ειδική ιστοσελίδα και τηλεφωνικό κέντρο, ανέπτυξε πρόγραμμα αποκατάστασης άνω των 50 εκατομμυρίων δολαρίων και έλαβε πρόστιμο 18,4 εκατομμυρίων λιρών	Η υπόθεση ανέδειξε τη σημασία του ελέγχου κυβερνοασφάλειας κατά τις εταιρικές εξαγορές και της συνεχούς παρακολούθησης παλαιών συστημάτων

Πηγή: Federal Trade Commission, 2019 και Information Commissioner's Office, 2020α, 2020β

3.3.3 Στρατηγικές επικοινωνίας για την ενίσχυση της εμπιστοσύνης

Επειδή η εμπιστοσύνη διαμορφώνεται τόσο από τις αντιλήψεις όσο και από την τεχνική απόδοση, οι στρατηγικές επικοινωνίας είναι κεντρικές για την οικοδόμηση εταιρικής εμπιστοσύνης. Οι Flavián και Guinalíu (2006) δείχνουν ότι η εμπιστοσύνη των καταναλωτών, η αντιλαμβανόμενη ασφάλεια και η πολιτική απορρήτου είναι τρία βασικά στοιχεία της αφοσίωσης σε έναν ιστότοπο. Τα αποτελέσματά τους δείχνουν ότι η εμπιστοσύνη επηρεάζει την πρόθεση αγοράς και την αποτελεσματική αγοραστική συμπεριφορά, συμπεριλαμβανομένης της προτίμησης, της συχνότητας επισκέψεων και της κερδοφορίας. Οι Wu et al. (2012) διαπιστώνουν ομοίως ότι το περιεχόμενο των πολιτικών απορρήτου στο διαδίκτυο επηρεάζει σημαντικά την ανησυχία για την προστασία της ιδιωτικής ζωής, την εμπιστοσύνη και την προθυμία παροχής προσωπικών πληροφοριών, με τις διαπολιτισμικές διαφορές να μετριάζουν αυτές τις σχέσεις. Αυτές οι μελέτες καταδεικνύουν ότι η επικοινωνία περί απορρήτου είναι ένα στρατηγικό μέσο μέσω του οποίου οι εταιρείες διαμορφώνουν τον τρόπο με τον οποίο οι καταναλωτές ερμηνεύουν τον κίνδυνο.

Οι Milne και Culnan (2004) παρέχουν μια πιο λεπτομερή εικόνα από άποψη συμπεριφοράς, εξετάζοντας γιατί οι καταναλωτές διαβάζουν ή δεν διαβάζουν τις ειδοποιήσεις απορρήτου. Διαπιστώνουν ότι η ανάγνωση σχετίζεται με την ανησυχία για την προστασία της ιδιωτικής ζωής, τις αντιλήψεις για την κατανόηση της ειδοποίησης και την εμπιστοσύνη στην ίδια την ειδοποίηση. Οι αποτελεσματικές ειδοποιήσεις, επομένως, εξυπηρετούν μια ουσιαστική λειτουργία μείωσης του

κινδύνου, αλλά μόνο όταν οι καταναλωτές μπορούν να τις κατανοήσουν και να τις χρησιμοποιήσουν. Οι Thomas et al. (2022) επεκτείνουν αυτό το επιχείρημα στην έρευνά τους για την ευθύνη για την προστασία της ιδιωτικής ζωής και την ασφάλεια, η οποία τονίζει ότι η επικοινωνία μετά από μια παραβίαση θα πρέπει να αντικατοπτρίζει την υπεύθυνη διαχείριση δεδομένων καθώς και την υπεύθυνη απεικόνιση του περιστατικού. Αυτό σημαίνει ότι η εταιρική επικοινωνία θα πρέπει να αποδεικνύει την ευθύνη, να εξηγεί τα προστατευτικά μέτρα και να δείχνει σεβασμό στα επηρεαζόμενα άτομα. Σε αυτές τις μελέτες τελικά, η αποτελεσματική επικοινωνία ενισχύει την εμπιστοσύνη όταν είναι σαφής, αξιόπιστη, κατανοητή και ευθυγραμμισμένη με την ορατή οργανωτική ευθύνη.

Συνολικά, η βιβλιογραφία δείχνει ότι η εμπιστοσύνη των καταναλωτών απέναντι στην ιδιωτικότητα διαμορφώνεται μέσα από έναν συνδυασμό προσωπικής εμπειρίας, κοινωνικών προσδοκιών και εταιρικών πρακτικών. Οι άνθρωποι αξιολογούν τον τρόπο με τον οποίο μια επιχείρηση διαχειρίζεται τα προσωπικά δεδομένα τους με βάση όσα έχουν ζήσει στο παρελθόν, όσα θεωρούν θεμιτά στο κοινωνικό τους περιβάλλον, αλλά και όσα αντιλαμβάνονται από τις πολιτικές, τα μηνύματα και τις ενέργειες της ίδιας της εταιρείας. Η εμπιστοσύνη ενισχύεται όταν οι οργανισμοί προσφέρουν σαφείς πληροφορίες, εύκολα κατανοητές πολιτικές απορρήτου, ορατά μέτρα ασφάλειας και σταθερή επικοινωνία με σεβασμό προς τον χρήστη. Οι μελέτες που παρουσιάστηκαν σε αυτήν την ενότητα επιπλέον, αναδεικνύουν ότι η εμπιστοσύνη αναπτύσσεται σταδιακά και αποκτά βάθος μέσα στον χρόνο. Κάθε συνεπής και προσεκτική πρακτική, όπως μια ευανάγνωστη ενημέρωση, μια ξεκάθαρη πολιτική χρήσης δεδομένων ή μια υπεύθυνη διαχείριση ενός περιστατικού, συμβάλλει στη δημιουργία μιας πιο σταθερής σχέσης ανάμεσα στην επιχείρηση και τον καταναλωτή. Για τις επιχειρήσεις, αυτό σημαίνει ότι η εμπιστοσύνη αποτελεί αποτέλεσμα καλής διακυβέρνησης, σωστού σχεδιασμού και ποιοτικής επικοινωνίας. Για την παρούσα έρευνα, όλα αυτά τα στοιχεία συνθέτουν ένα ενιαίο πλαίσιο κατανόησης της συμπεριφοράς των καταναλωτών, στο οποίο η ιδιωτικότητα, η ασφάλεια και η οργανωτική υπευθυνότητα λειτουργούν ως αλληλένδετες διαστάσεις.

3.4 Εμπειρικές μελέτες για τη σχέση GDPR – εμπιστοσύνης καταναλωτή

3.4.1 Έρευνες για την εμπιστοσύνη, την ευαισθητοποίηση και την εμπειρία των καταναλωτών

Εμπειρικές έρευνες που δημοσιεύτηκαν μετά την έναρξη ισχύος του GDPR δείχνει ότι η σχέση μεταξύ ρύθμισης και εμπιστοσύνης των καταναλωτών δεν είναι ούτε αυτόματη ούτε ομοιόμορφη. Αντίθετα, η εμπιστοσύνη εξαρτάται από την ευαισθητοποίηση, την εμπειρία ζωής και τον βαθμό στον οποίο οι νομικές εγγυήσεις μεταφράζονται σε ορατές οργανωτικές πρακτικές. Οι Presthus και Sørum (2018) παρέχουν μια πρώιμη εμπειρική εικόνα μέσω μιας διαδικτυακής έρευνας που δείχνει ότι οι καταναλωτές γενικά έβλεπαν ευνοϊκά τον GDPR, εκτίμησαν τον προσανατολισμό του που βασίζεται στα δικαιώματα και ήθελαν επιρροή στον τρόπο συλλογής, χρήσης και αποθήκευσης των προσωπικών δεδομένων. Ταυτόχρονα, πολλοί ερωτηθέντες παρέμειναν αβέβαιοι για την πραγματική εφαρμογή του και για το εάν οι εταιρείες συμμορφώνονταν πραγματικά με τον Κανονισμό. Αυτός ο πρώιμος συνδυασμός αισιοδοξίας και σκεπτικισμού παρέμεινε ένα επαναλαμβανόμενο θέμα σε μεταγενέστερες μελέτες.

Μια πιο πρακτική προοπτική προσφέρεται από τους Sørum και Presthus (2020), οι οποίοι διερεύνησαν τον τρόπο με τον οποίο οι εταιρείες ανταποκρίθηκαν στα αιτήματα των καταναλωτών βάσει των Άρθρων 15 και 20. Τα ευρήματά τους αναδεικνύουν σημαντικές διαφοροποιήσεις ως προς τον χρόνο απόκρισης, την ποιότητα και τη μορφή των απαντήσεων, ενώ οι εταιρείες φαίνεται ότι ανταποκρίνονταν γενικά αποτελεσματικότερα στα αιτήματα διαβίβασης των δεδομένων σε αναγνώσιμη μορφή, δηλαδή στο δικαίωμα φορητότητας, παρά στα αιτήματα απλής πρόσβασης στα προσωπικά δεδομένα. Η σημασία αυτής της μελέτης έγκειται στην απόδειξή της ότι η εμπιστοσύνη των καταναλωτών διαμορφώνεται από τα νόμιμα δικαιώματα και από συγκεκριμένες αλληλεπιδράσεις με τους οργανισμούς. Δικαιώματα που υπάρχουν τυπικά αλλά εφαρμόζονται με ασυνέπεια μπορεί να προκαλέσουν απογοήτευση παρά ενδυνάμωση.

Συγκριτικά στοιχεία υποστηρίζουν επίσης τον ρόλο του κανονιστικού πλαισίου στη διαμόρφωση της εμπιστοσύνης. Οι Strzelecki και Rizun (2020), συγκρίνοντας τις

πρακτικές ηλεκτρονικών αγορών στην Πολωνία και την Ουκρανία, δείχνουν ότι το περιβάλλον GDPR συνδέεται με ισχυρότερη ανάπτυξη πολιτικής απορρήτου και πιο ισχυρά χαρακτηριστικά που σχετίζονται με την εμπιστοσύνη στο ηλεκτρονικό εμπόριο. Τα ευρήματά τους υποδηλώνουν ότι οι ασφαλείς μέθοδοι πληρωμής, οι διαφανείς πολιτικές και οι πρακτικές ιστοσελίδων που βασίζονται σε κανόνες συμβάλλουν στην ασφάλεια και την εμπιστοσύνη των καταναλωτών, ακόμη και όταν η ευρύτερη ασφάλεια των διακομιστών φαίνεται παρόμοια σε όλα τα περιβάλλοντα. Σε πανευρωπαϊκό επίπεδο, οι Rughiniș et al. (2021) καταδεικνύουν ότι η επίγνωση του GDPR ποικίλλει σημαντικά σε είκοσι οκτώ χώρες και συνδέεται στενά με την ψηφιακή εμπειρία, την εκπαίδευση, την ηλικία και το επάγγελμα. Η κατηγοριοποίηση που προτείνουν για τις διαφορετικές μορφές ψηφιακής συμμετοχής είναι ιδιαίτερα διαφωτιστική, καθώς αναδεικνύει ότι οι ψηφιακά ενεργοί χρήστες δεν διαθέτουν όλοι το ίδιο επίπεδο γνώσης γύρω από την προστασία των προσωπικών δεδομένων. Ειδικότερα, ορισμένοι εμφανίζουν έντονη παρουσία και συχνή δραστηριότητα στο ψηφιακό περιβάλλον, χωρίς όμως να έχουν αντίστοιχη ενημέρωση για τα δικαιώματα που κατοχυρώνει ο GDPR, στοιχείο που περιορίζει την ικανότητα του Κανονισμού να ενισχύσει ουσιαστικά την εμπιστοσύνη των πολιτών.

Αυτό το ζήτημα της ενδυνάμωσης διερευνάται περαιτέρω από τους Prince et al. (2024), οι οποίοι δείχνουν ότι η διαδικτυακή παιδεία για την προστασία της ιδιωτικής ζωής, και ιδίως η γνώση περί των διαδικασιών, συνδέεται θετικά με την ενδυνάμωση της προστασίας της ιδιωτικής ζωής των χρηστών. Είναι ενδιαφέρον ότι η επίγνωση του GDPR ως τέτοια δεν είναι πάντα αρκετή για να δημιουργήσει ενδυνάμωση, υποδεικνύοντας ότι η γνώση πρέπει να είναι εφαρμόσιμη για να επηρεάσει την εμπιστοσύνη. Οι Zhang et al. (2024) συμπληρώνουν αυτό το σημείο δείχνοντας ότι, μετά τον GDPR, οι χρήστες εξακολουθούν να ανησυχούν για τα προσωπικά δεδομένα, αλλά συχνά βιώνουν περιορισμένο έλεγχο στην πράξη. Η ευκολία, η αντιληπτή αξία, οι επιπτώσεις του δικτύου και ο κυνισμός για την προστασία της ιδιωτικής ζωής συνεχίζουν να διαμορφώνουν τη συμπεριφορά, δημιουργώντας μια απόκλιση μεταξύ των προθέσεων για την προστασία της ιδιωτικής ζωής και της πραγματικής συμπεριφοράς. Συνολικά, αυτές οι μελέτες υποδηλώνουν ότι η εμπιστοσύνη των καταναλωτών μετά τον GDPR εξαρτάται από κάτι περισσότερο από την απλή νομική επίγνωση, καθώς επηρεάζεται από την παιδεία, τη χρηστικότητα, τις ψηφιακές ρουτίνες και την αντιληπτή πρακτικότητα της άσκησης των δικαιωμάτων.

3.4.2 Διαφάνεια και αντιληπτή συμμόρφωση

Μια δεύτερη ομάδα μελετών επικεντρώνεται στη διαφάνεια, την κατανόηση και την αντιληπτή συμμόρφωση. Οι Betzing et al. (2020) εξετάζουν τη λήψη αποφάσεων που σχετίζονται με την προστασία της ιδιωτικής ζωής σε περιβάλλοντα κινητής τηλεφωνίας και διαπιστώνουν ότι η αυξημένη διαφάνεια βελτιώνει την κατανόηση των πρακτικών επεξεργασίας δεδομένων από τους χρήστες, παρόλο που δεν μειώνει απαραίτητα την αποδοχή των αδειών. Αυτό είναι ένα σημαντικό αποτέλεσμα επειδή υποδηλώνει ότι η διαφάνεια συμβάλλει στη λήψη τεκμηριωμένων αποφάσεων ακόμη και όταν η συμπεριφορά παραμένει αμετάβλητη. Οι Zhang et al. (2020) καταλήγουν σε ένα σχετικό συμπέρασμα σε μια πειραματική μελέτη που δείχνει ότι η εθελοντική υιοθέτηση του GDPR αυξάνει την εμπιστοσύνη και την πρόθεση αποκάλυψης των δεδομένων των πελατών, ιδιαίτερα όταν οι δηλώσεις απορρήτου είναι πιο ευανάγνωστες. Η αναγνωσιμότητα, επομένως, γίνεται μια σημαντική μεταβλητή μεταξύ της επίσημης συμμόρφωσης και της αντίληψης των καταναλωτών.

Οι Dexe et al. (2022) επεκτείνουν το ζήτημα της διαφάνειας στην αυτοματοποιημένη λήψη αποφάσεων. Η μελέτη τους για τις απαντήσεις των ασφαλιστικών εταιρειών σε αιτήματα για ουσιαστικές πληροφορίες δείχνει ότι οι οργανισμοί συχνά δυσκολεύονται να παρέχουν σαφείς, προσανατολισμένες στον καταναλωτή εξηγήσεις. Η μελέτη αποκαλύπτει ότι το δικαίωμα σε εξηγήσεις φιλτράρεται μέσω της γλώσσας, της ερμηνείας και της οργανωτικής ικανότητας. Αυτό έχει σημασία για την εμπιστοσύνη, επειδή οι αδιαφανείς ή ελλιπείς απαντήσεις μπορεί να αποδυναμώσουν την εμπιστοσύνη ακόμη και όταν επιχειρείται κάποιος βαθμός συμμόρφωσης. Περαιτέρω στοιχεία προέρχονται από τους Dorfleitner et al. (2023), οι οποίοι αναλύουν τις δηλώσεις απορρήτου εταιριών της FinTech πριν και μετά την εφαρμογή του GDPR. Διαπιστώνουν ότι οι δηλώσεις έγιναν μεγαλύτερες, πιο τυποποιημένες και λιγότερο ευανάγνωστες, υπονομεύοντας έτσι την κατανόηση των χρηστών. Το συμπέρασμά τους είναι ιδιαίτερα σημαντικό για κάθε αξιολόγηση της εμπιστοσύνης. Ένας κανονισμός μπορεί να αυξήσει την αποκάλυψη, ενώ ταυτόχρονα να μειώσει την κατανοησιμότητα, εάν οι οργανισμοί ανταποκριθούν μέσω φορμαλιστικής επέκτασης της τεκμηρίωσης.

Οι Brunotte et al. (2023) εμπλουτίζουν τη σχετική συζήτηση, αναδεικνύοντας ότι οι επεξηγήσεις για τον τρόπο διαχείρισης της ιδιωτικότητας μπορούν να

λειτουργήσουν ενισχυτικά τόσο για την εμπιστοσύνη των τελικών χρηστών όσο και για το επίπεδο ενημέρωσής τους σε ζητήματα προστασίας προσωπικών δεδομένων. Τα ευρήματά τους δείχνουν ότι οι χρήστες ενδιαφέρονται ιδιαίτερα για εξηγήσεις που διευκρινίζουν γιατί χρειάζονται τα δεδομένα, για ποιους σκοπούς υποβάλλονται σε επεξεργασία και ποιος μπορεί να έχει πρόσβαση σε αυτά. Στην πράξη, οι μελέτες αυτές δείχνουν ότι η εμπιστοσύνη ενισχύεται όταν η παροχή πληροφοριών συνοδεύεται από επεξηγήσεις σαφείς, εύληπτες και κατάλληλα διαμορφωμένες για το συγκεκριμένο περιβάλλον χρήσης, με επίκεντρο τις πραγματικές ανάγκες κατανόησης των χρηστών και όχι την τυπική νομική θωράκιση της επιχείρησης.

3.4.3 Δείκτες εμπιστοσύνης και κανονιστική συμμόρφωση

Μια τρίτη ομάδα μελετών εξετάζει αυστηρότερους δείκτες συμμόρφωσης. Οι Aridor et al. (2023) αναλύουν τον αντίκτυπο της ρύθμισης της ιδιωτικής ζωής στον κλάδο των δεδομένων και παρέχουν εμπειρικά στοιχεία που αποδεικνύουν ότι ο GDPR άλλαξε τα οικονομικά της χρήσης των προσωπικών δεδομένων. Τα ευρήματά τους δείχνουν μετρήσιμες αλλαγές στη συμπεριφορά του κλάδου δεδομένων, υποδεικνύοντας ότι ο Κανονισμός επηρέασε τις πρακτικές της αγοράς. Αυτό είναι σημαντικό επειδή η εμπιστοσύνη των καταναλωτών είναι πιθανό να εξαρτάται από την αντιληπτή συμμόρφωση, αλλά και από το εάν οι εταιρείες μειώνουν πραγματικά τις εκμεταλλευτικές ή αδιαφανείς μορφές εξαγωγής δεδομένων.

Οι Miller et al. (2025) παρέχουν ιδιαίτερα ισχυρή εμπειρική τεκμηρίωση για το ζήτημα αυτό, εξετάζοντας πώς ο GDPR επηρέασε τη χρήση τεχνολογιών παρακολούθησης της διαδικτυακής συμπεριφοράς των χρηστών. Η ανάλυσή τους δείχνει ότι οι εκδότες που υπάγονται στο πεδίο εφαρμογής του Κανονισμού καταγράφουν χαμηλότερη χρήση τέτοιων τεχνολογιών που σχετίζονται με πιο παρεμβατικές μορφές συλλογής και διαβίβασης προσωπικών δεδομένων, σε σύγκριση με συγκρίσιμους εκδότες εκτός του αντίστοιχου κανονιστικού πλαισίου. Η μελέτη αποκτά ιδιαίτερη βαρύτητα, καθώς αποτυπώνει πραγματικές μεταβολές σε παρατηρήσιμες πρακτικές επεξεργασίας και δεν περιορίζεται σε αυτοαναφορές ή αντιλήψεις των χρηστών. Ως εκ τούτου, ενισχύει το επιχείρημα ότι ο GDPR μπορεί να επιφέρει ουσιαστικό περιορισμό επεμβατικών πρακτικών δεδομένων και, μέσω αυτού, να στηρίξει πιο έμπρακτα την εμπιστοσύνη των καταναλωτών.

Συνολικά, η εμπειρική βιβλιογραφία που παρουσιάστηκε στην ενότητα αυτή δείχνει ότι ο GDPR έχει βελτιώσει την ευαισθητοποίηση, έχει ενισχύσει τον διάλογο για τα δικαιώματα και έχει αυξήσει την πίεση για οργανωτική διαφάνεια. Ωστόσο, οι επιπτώσεις του στην εμπιστοσύνη είναι άνισες, επειδή οι νομικές εγγυήσεις πρέπει να μετατραπούν σε αναγνώσιμες ειδοποιήσεις, εφαρμόσιμα δικαιώματα, κατανοητές εξηγήσεις και παρατηρήσιμες αλλαγές στις πρακτικές δεδομένων. Η ενίσχυση της εμπιστοσύνης καθίσταται πιο ουσιαστική όταν η συμμόρφωση αφενός επικοινωνείται με σαφή και κατανοητό τρόπο προς τους χρήστες, αφετέρου αποδεικνύεται έμπρακτα μέσα από πραγματικές αλλαγές στις οργανωτικές και τεχνολογικές πρακτικές. Η ισχυρότερη απόδειξη ενίσχυσης της εμπιστοσύνης εμφανίζεται όταν η συμμόρφωση είναι τόσο κοινοποιήσιμη όσο και συμπεριφορικά πραγματική. Κατά συνέπεια, η σχέση μεταξύ του GDPR και της εμπιστοσύνης των καταναλωτών γίνεται καλύτερα κατανοητή ως εξής. Ο Κανονισμός δημιουργεί την δομή για την δημιουργία εμπιστοσύνης, αλλά οι οργανισμοί, οι διεπαφές και οι πρακτικές επιβολής καθορίζουν εάν αυτή αποκτά νόημα στην καθημερινή ψηφιακή ζωή. Από την ανάλυση προκύπτει επίσης ότι οι μελλοντικές αξιολογήσεις θα πρέπει να ενσωματώνουν δείκτες εμπιστοσύνης με ελέγχους συμμόρφωσης, μελέτες διεπαφών και δεδομένα συμπεριφοράς σε επίπεδο αγοράς. Μόνο μια τέτοια συνδυασμένη προσέγγιση μπορεί να δείξει με σαφήνεια κατά πόσο ο GDPR περιορίζεται στην απλή ενημέρωση των καταναλωτών για τα δικαιώματά τους ή αν επιφέρει ουσιαστικό μετασχηματισμό του περιβάλλοντος διαχείρισης δεδομένων, δημιουργώντας συνθήκες μέσα στις οποίες η εμπιστοσύνη προς τις επιχειρήσεις θεμελιώνεται πιο πειστικά, διατηρείται στον χρόνο και αποκτά πραγματικό περιεχόμενο για τους καταναλωτές. Αυτή παραμένει η εμπειρική πρόκληση για την έρευνα εμπιστοσύνης των καταναλωτών μετά τον GDPR στην Ευρώπη.

Η μέτρηση της εμπιστοσύνης αποκτά μεγαλύτερη αναλυτική αξία όταν συνδυάζει αντιλήψεις χρηστών, πραγματική άσκηση δικαιωμάτων και λειτουργικές επιδόσεις της επιχείρησης. Ένα ολοκληρωμένο σύστημα παρακολούθησης μπορεί να περιλαμβάνει δείκτες σε επίπεδο δικαιωμάτων, παραπόνων, συγκατάθεσης, παραβιάσεων και διατήρησης πελατών. Η περιοδική παρουσίαση των αποτελεσμάτων ανά κανάλι εξυπηρέτησης, κατηγορία αιτήματος και ομάδα χρηστών υποστηρίζει την έγκαιρη αναγνώριση αποκλίσεων και τη διαφανή αξιολόγηση της κανονιστικής συμμόρφωσης.

Πίνακας 8: Προτεινόμενες μετρικές προστασίας και εμπιστοσύνης καταναλωτών

Δείκτης	Τρόπος υπολογισμού	Ερμηνευτική χρήση
Άσκηση δικαιωμάτων	Ολοκληρωμένα αιτήματα πρόσβασης, διόρθωσης, διαγραφής και φορητότητας ως ποσοστό των ενεργών χρηστών	Βαθμός πρακτικής αξιοποίησης των κατοχυρωμένων δικαιωμάτων
Μέσος και διάμεσος χρόνος απόκρισης	Ημερολογιακές ημέρες από την παραλαβή έως την ολοκλήρωση του αιτήματος	Ταχύτητα και σταθερότητα της οργανωτικής απόκρισης
Εμπρόθεσμη ολοκλήρωση	Αιτήματα που ολοκληρώθηκαν μέσα στη νόμιμη προθεσμία ως ποσοστό όλων των ολοκληρωμένων αιτημάτων	Συνέπεια προς τις κανονιστικές απαιτήσεις
Καταγγελίες ανά 10.000 πελάτες	Συνολικές καταγγελίες προς την επιχείρηση και τις αρχές προς ενεργούς πελάτες, με αναγωγή σε 10.000	Συγκρίσιμη ένταση προβλημάτων μεταξύ περιόδων και μονάδων
Επιτυχής επίλυση παραπόνων	Επιλυμένα παράπονα ως ποσοστό των υποθέσεων που έκλεισαν	Αποτελεσματικότητα μηχανισμού αποκατάστασης
Χρόνος ενημέρωσης μετά από περιστατικό	Ώρες από την επιβεβαίωση της παραβίασης έως την πρώτη ενημέρωση των επηρεαζόμενων προσώπων	Ετοιμότητα, διαφάνεια και υπευθυνότητα επικοινωνίας
Ανάκληση συγκατάθεσης	Ανακλήσεις ως ποσοστό των ενεργών συγκαταθέσεων ανά υπηρεσία	Αποδοχή πρακτικών επεξεργασίας και ποιότητα ενημέρωσης
Κατανόηση πολιτικής απορρήτου	Ποσοστό ορθών απαντήσεων σε σύντομο έλεγχο κατανόησης χρηστών	Σαφήνεια και χρηστικότητα της πληροφόρησης
Μεταβολή εμπιστοσύνης	Διαφορά μέσης βαθμολογίας εμπιστοσύνης πριν και μετά από περιστατικό ή διορθωτική παρέμβαση	Έκταση υποβάθμισης και βαθμός αποκατάστασης
Διατήρηση πελατών μετά από παραβίαση	Επηρεαζόμενοι πελάτες που παραμένουν ενεργοί μετά από τρεις ή έξι μήνες ως ποσοστό του συνόλου	Συμπεριφορική συνέπεια του περιστατικού και της απόκρισης

4. Επιχειρηματική ανάπτυξη και διαχείριση προσωπικών δεδομένων

4.1 Η προστασία δεδομένων ως στρατηγικό πλεονέκτημα

4.1.1 Από τη συμμόρφωση στην αξία εμπιστοσύνης

Η προστασία δεδομένων αποτελεί για τις επιχειρήσεις σήμερα έναν στρατηγικό πόρο που διαμορφώνει τον τρόπο με τον οποίο αυτές χτίζουν σχέσεις με τους καταναλωτές, οργανώνουν τη δημιουργία αξίας και τοποθετούνται σε ανταγωνιστικές αγορές. Η σύγχρονη έρευνα δείχνει ότι οι πρακτικές απορρήτου επηρεάζουν την εμπιστοσύνη των καταναλωτών, την αντιληπτή νομιμότητα και την προθυμία τους να συνεργαστούν με οργανισμούς σε ψηφιακά περιβάλλοντα. Οι Fox, Lynn και Rosati (2022) καταδεικνύουν ότι οι οπτικοποιημένες ετικέτες GDPR βελτιώνουν τις αντιλήψεις για την ιδιωτικότητα, τον έλεγχο και την αξιοπιστία, ενώ παράλληλα ενισχύουν την προθυμία αλληλεπίδρασης και αποκάλυψης δεδομένων. Αυτό το εύρημα δείχνει ότι η συμμόρφωση αποκτά στρατηγική σημασία όταν γίνεται ορατή, κατανοητή και ουσιαστική για τον χρήστη. Παράλληλα, οι εταιρικές πρακτικές απορρήτου λειτουργούν ως σήμα ποιότητας που επηρεάζει τις αξιολογήσεις της αγοράς και τις κρίσεις σε επίπεδο επωνυμίας.

Η στρατηγική φύση της προστασίας δεδομένων φαίνεται ακόμη πιο καθαρά όταν η ιδιωτικότητα ερμηνεύεται υπό το πρίσμα της μακροπρόθεσμης απόδοσης της εταιρείας. Οι Chisam et al. (2026) εξηγούν ότι η ρύθμιση της ιδιωτικότητας δημιουργεί μια αρχική ένταση κόστους-οφέλους, ωστόσο αυτή η ένταση σταδιακά εξελίσσεται σε κέρδη που βασίζονται στην εμπιστοσύνη και υποστηρίζουν ισχυρότερη απόδοση με την πάροδο του χρόνου. Η ανάλυσή τους στις διεθνείς αγορές τοποθετεί την ιδιωτικότητα ως μια δυναμική στρατηγική μεταβλητή πέρα από το στατικό κόστος συμμόρφωσης. Οι Vallejo Blanxart et al. (2026) καταλήγουν σε ένα σχετικό συμπέρασμα μέσω της μελέτης τους για τους διευθυντές μάρκετινγκ, δείχνοντας ότι οι εταιρείες εξακολουθούν συχνά να θεωρούν την ιδιωτικότητα ως νομική υποχρέωση, ενώ οι ισχυρότερες ευκαιρίες προκύπτουν όταν αυτή διαχειρίζεται ως στρατηγικό περιουσιακό στοιχείο ικανό να ενισχύσει την καινοτομία και τις σχέσεις με τους πελάτες. Υπό αυτή την έννοια, η ιδιωτικότητα υποστηρίζει την ανάπτυξη των

επιχειρήσεων ενισχύοντας την αξιοπιστία στα διεθνή ανταγωνιστικά επιχειρηματικά περιβάλλοντα.

Περαιτέρω στοιχεία προσφέρουν οι Avramidis et al. (2026), οι οποίοι και αυτοί αντιλαμβάνονται την ιδιωτικότητα και την ασφάλεια των δεδομένων των πελατών ως μια σαφή στρατηγική της εταιρείας. Τα ευρήματά τους δείχνουν ότι οι εταιρείες ανταποκρίνονται στον ισχυρότερο ανταγωνισμό στην αγορά προϊόντων επενδύοντας στην ιδιωτικότητα και την ασφάλεια ως ανταγωνιστικό διαφοροποιητικό παράγοντα. Αν και αυτή η στρατηγική περιλαμβάνει συμβιβασμούς σε έσοδα και ρευστότητα, μειώνει επίσης τον κίνδυνο δικαστικών διαφορών και ενισχύει την ανθεκτικότητα των εταιριών. Οι Carl et al. (2024) προσθέτουν μια οπτική γωνία από την πλευρά των καταναλωτών, δείχνοντας ότι οι δραστηριότητες ιδιωτικότητας και ασφάλειας δημιουργούν ευρύτερες θετικές αντιλήψεις για την εταιρική ψηφιακή ευθύνη. Ως αποτέλεσμα, η προστασία δεδομένων συμβάλλει σε μια ευρύτερη εικόνα της ηθικής ψηφιακής συμπεριφοράς που μπορεί να αυξήσει τη συνολική αξία φήμης της εταιρείας. Μαζί, αυτές οι μελέτες αποδεικνύουν ότι η μετάβαση από τη συμμόρφωση στην εμπιστοσύνη αναδιαμορφώνει την ιδιωτικότητα από μια αμυντική υποχρέωση σε μια παραγωγική πηγή νομιμότητας και διαφοροποίησης στην αγορά.

4.1.2 Προστασία δεδομένων από τον σχεδιασμό

Η μετάβαση από τη νομική συμμόρφωση στο στρατηγικό πλεονέκτημα εξαρτάται από τον τρόπο με τον οποίο η ιδιωτικότητα ενσωματώνεται στα οργανωτικά συστήματα, τα προϊόντα και τις διεπαφές από τα πρώτα στάδια σχεδιασμού. Η Ιδιωτικότητα από τον Σχεδιασμό και η Ιδιωτικότητα από Προεπιλογή (Privacy by Design και Privacy by Default) παρέχουν το πιο άμεσο πλαίσιο για αυτήν την ενσωμάτωση, επειδή μεταφράζουν τις κανονιστικές αρχές σε λειτουργικές δομές. Οι Grafenstein et al. (2024) δείχνουν ότι η αποτελεσματική προστασία δεδομένων από τον σχεδιασμό απαιτεί τη συντονισμένη αλληλεπίδραση του νόμου, του οπτικού σχεδιασμού και της έρευνας για την εμπειρία των χρηστών. Η εργασία τους σχετικά με τα εικονίδια ιδιωτικότητας καταδεικνύει ότι η διαφάνεια και ο έλεγχος γίνονται πιο αποτελεσματικά όταν οι πληροφορίες δομούνται μέσω προσβάσιμων οπτικών και διαδικαστικών συστημάτων. Υπό αυτή την έννοια, ο ίδιος ο σχεδιασμός γίνεται ένας μηχανισμός διακυβέρνησης μέσω του οποίου οι χρήστες μπορούν να κατανοήσουν τις επιλογές ιδιωτικότητας και να ασκήσουν ουσιαστική δράση.

Οι Dehling και Sunyaev (2023) εμβαθύνουν περαιτέρω, υποστηρίζοντας ότι ο τρόπος με τον οποίο παρέχεται η διαφάνεια πρέπει να προσαρμόζεται στις πληροφοριακές ανάγκες των χρηστών. Η θεωρία τους για τη διαφάνεια των πρακτικών ιδιωτικότητας πληροφοριών τονίζει ότι η χρήσιμη διαφάνεια προκύπτει όταν οι πληροφορίες ιδιωτικότητας ανταποκρίνονται στις κοινωνικοτεχνικές συνθήκες της λήψης αποφάσεων των χρηστών. Αυτή η αντίληψη ευθυγραμμίζεται με την Ιδιωτικότητα από Προεπιλογή, επειδή οι προεπιλεγμένες ρυθμίσεις και οι δομές πληροφοριών μπορούν να καθοδηγήσουν τα άτομα προς ασφαλείς και ενημερωμένες αλληλεπιδράσεις. Όταν οι οργανισμοί αναπτύσσουν ειδοποιήσεις απορρήτου, πίνακες ελέγχου, διαδικασίες συγκατάθεσης και συστήματα ελέγχου με αυτόν τον τρόπο, δημιουργούν μια πρακτική βάση για εμπιστοσύνη, λογοδοσία και διαρκή συμμετοχή.

Η σημασία αυτής της προσέγγισης ενισχύεται από τους Vallejo Blanxart et al. (2026), οι οποίοι εντοπίζουν σημαντικά κενά στην εφαρμογή της προστασίας της ιδιωτικής ζωής ήδη από τον σχεδιασμό σε όλες τις εταιρείες. Τα αποτελέσματά τους υποδηλώνουν ότι οι οργανισμοί αποκτούν μεγαλύτερη στρατηγική αξία για τις εταιρείες όταν οι διαδικασίες προστασίας της ιδιωτικής ζωής και οι υποστηρικτικές τεχνολογίες ενσωματώνονται πλήρως στις πρακτικές μάρκετινγκ και δεδομένων. Τέλος, οι Magrizos et al. (2026) παρέχουν συμπληρωματικά στοιχεία δείχνοντας ότι οι οπτικοποιημένες πολιτικές απορρήτου αυξάνουν την εμπιστοσύνη στην επωνυμία Τα ευρήματά τους αποκαλύπτουν ότι οι διαφανείς επιλογές σχεδιασμού μπορούν να βελτιώσουν την ερμηνεία των πρακτικών συλλογής δεδομένων και μπορούν να δικαιολογήσουν τη χρήση δεδομένων με τρόπους που οι καταναλωτές αντιλαμβάνονται ως δίκαιους.

Η πρακτική εφαρμογή της προστασίας δεδομένων από τον σχεδιασμό μπορεί να οργανωθεί ως επαναλαμβανόμενος έλεγχος σε κάθε νέο προϊόν, υπηρεσία ή ουσιώδη μεταβολή συστήματος. Το άρθρο 25 του GDPR συνδέει τα κατάλληλα τεχνικά και οργανωτικά μέτρα με την τεχνολογική στάθμη, το κόστος εφαρμογής, τη φύση, το πεδίο, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και με την πιθανότητα και τη σοβαρότητα των κινδύνων. Το ακόλουθο checklist μετατρέπει τις αρχές αυτές σε ελέγξιμα επιχειρησιακά βήματα (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016, άρθρο 25· Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, χ.χ.).

Πίνακας 9: Checklist προστασίας δεδομένων από τον σχεδιασμό και εξ ορισμού

Πεδίο ελέγχου	Ερώτημα εφαρμογής	Ενδεικτικό τεκμήριο	Κατάσταση
Σκοπός και νόμιμη βάση	Έχουν προσδιοριστεί ο σκοπός, η νόμιμη βάση και η αναγκαιότητα κάθε πράξης επεξεργασίας;	Χάρτης σκοπών, νομική αξιολόγηση, μητρώο δραστηριοτήτων	☐ Ολοκληρώθηκε ☐ Σε εξέλιξη ☐ Ενέργεια
Ελαχιστοποίηση δεδομένων	Συλλέγονται μόνο τα δεδομένα που εξυπηρετούν άμεσα τον δηλωμένο σκοπό;	Κατάλογος πεδίων, αιτιολόγηση αναγκαιότητας, δοκιμή περιορισμού	☐ Ολοκληρώθηκε ☐ Σε εξέλιξη ☐ Ενέργεια
Ρυθμίσεις εξ ορισμού	Οι αρχικές ρυθμίσεις περιορίζουν την πρόσβαση, τη διατήρηση, την κοινοποίηση και την ορατότητα;	Ρυθμίσεις συστήματος, στιγμιότυπα διεπαφής, τεχνικές προδιαγραφές	☐ Ολοκληρώθηκε ☐ Σε εξέλιξη ☐ Ενέργεια
Διαφάνεια και εμπειρία χρήστη	Παρέχονται σαφείς πληροφορίες στα κατάλληλα σημεία της διαδρομής του χρήστη;	Πολιτική απορρήτου, πολυεπίπερη ενημέρωση, εικονίδια, δοκιμές κατανόησης	☐ Ολοκληρώθηκε ☐ Σε εξέλιξη ☐ Ενέργεια
Έλεγχος πρόσβασης	Έχουν αποδοθεί δικαιώματα πρόσβασης σύμφωνα με τον ρόλο και την επιχειρησιακή ανάγκη;	Πίνακας ρόλων, αρχεία πρόσβασης, περιοδική επανεξέταση δικαιωμάτων	☐ Ολοκληρώθηκε ☐ Σε εξέλιξη ☐ Ενέργεια
Χρόνος διατήρησης και διαγραφή	Υπάρχουν σαφή όρια διατήρησης και αυτοματοποιημένες ή ελεγχόμενες διαδικασίες διαγραφής;	Πολιτική διατήρησης, κανόνες διαγραφής, αρχεία εκτέλεσης	☐ Ολοκληρώθηκε ☐ Σε εξέλιξη ☐ Ενέργεια
Ασφάλεια και ψευδωνυμοποίηση	Εφαρμόζονται μέτρα ανάλογα με τον κίνδυνο, όπως κρυπτογράφηση, ψευδωνυμοποίηση και καταγραφή συμβάντων;	Αρχιτεκτονική ασφάλειας, δοκιμές, σχέδιο αντιμετώπισης περιστατικών	☐ Ολοκληρώθηκε ☐ Σε εξέλιξη ☐ Ενέργεια
Δικαιώματα υποκειμένων	Το σύστημα υποστηρίζει πρόσβαση, διόρθωση, διαγραφή, περιορισμό, εναντίωση και φορητότητα;	Ροές αιτημάτων, πρότυπα απάντησης, μετρικές χρόνου απόκρισης	☐ Ολοκληρώθηκε ☐ Σε εξέλιξη ☐ Ενέργεια

Πεδίο ελέγχου	Ερώτημα εφαρμογής	Ενδεικτικό τεκμήριο	Κατάσταση
Προμηθευτές και τρίτα μέρη	Έχουν ελεγχθεί οι ρόλοι, οι συμβάσεις, οι διαβιβάσεις και τα μέτρα των συνεργατών;	Συμβάσεις επεξεργασίας, αξιολόγηση προμηθευτών, μητρώο διαβιβάσεων	☐ Ολοκληρώθηκε ☐ Σε εξέλιξη ☐ Ενέργεια
Δοκιμή και λογοδοσία	Έχουν καταγραφεί οι αποφάσεις, οι δοκιμές, οι εγκρίσεις και η περιοδική επανεξέταση;	Πρακτικά έγκρισης, αναφορές ελέγχου, σχέδιο επανεξέτασης	☐ Ολοκληρώθηκε ☐ Σε εξέλιξη ☐ Ενέργεια

Το checklist συμπληρώνεται κατά την έναρξη του έργου, πριν από την έγκριση παραγωγικής λειτουργίας και έπειτα από κάθε ουσιώδη μεταβολή. Η κοινή υπογραφή του υπευθύνου έργου, του DPO, της νομικής υπηρεσίας και της ασφάλειας πληροφοριών δημιουργεί τεκμήριο λογοδοσίας και επιτρέπει έγκαιρη προσαρμογή των σχεδιαστικών επιλογών.

4.1.3 Ο ρόλος της διαφάνειας στη φήμη και ανταγωνιστικότητα

Η διαφάνεια παίζει κεντρικό ρόλο στη μετατροπή των πρακτικών απορρήτου σε αποτελέσματα που βελτιώνουν τη φήμη και τον ανταγωνισμό. Πρόσφατη έρευνα δείχνει ότι η διαφάνεια έχει στρατηγική αξία όταν υπερβαίνει την απλή διαθεσιμότητα πληροφοριών και συνδέεται με τη σαφήνεια, την προνοητικότητα και την κατανοησιμότητα. Οι Sansome, Wilkie και Conduit (2024) δείχνουν ότι η αντιληπτή διαθεσιμότητα πληροφοριών χρησιμεύει ως απαραίτητο προηγούμενο της διαφάνειας της επωνυμίας, ενώ τα καθοριστικά αποτελέσματα προκύπτουν μέσω της ποιότητας της διαφανούς επικοινωνίας. Η άποψή τους συνδέει τη διαφάνεια με τις αντιλήψεις για την ηθική της επωνυμίας και εξηγεί γιατί οι εταιρείες επωφελούνται όταν η επικοινωνία για την προστασία της ιδιωτικής ζωής είναι προληπτική, σαφής και αντικειμενική. Επομένως, η διαφάνεια λειτουργεί ως ερμηνευτικό σήμα που διαμορφώνει τον τρόπο με τον οποίο τα ενδιαφερόμενα μέρη αξιολογούν τον ηθικό χαρακτήρα μιας επωνυμίας.

Οι Montecchi et al. (2024) επίσης αντιλαμβάνονται την αντιληπτή διαφάνεια της επωνυμίας ως μια έννοια που αποτελείται από παρατηρησιμότητα, κατανοησιμότητα και πρόθεση γνωστοποίησης κρίσιμων πληροφοριών εκ μέρους των

εταιριών. Αυτό το πλαίσιο είναι ιδιαίτερα σημαντικό για τη στρατηγική που σχετίζεται με την προστασία της ιδιωτικής ζωής, επειδή υποδεικνύει ότι οι καταναλωτές ανταμείβουν τις εταιρείες όταν η διαφάνεια φαίνεται σκόπιμη και κατανοητή. Καθώς η διαφάνεια συνδέεται και με την ακεραιότητα και την αυθεντικότητα, ενισχύει την εμπιστοσύνη της επωνυμίας και υποστηρίζει την ανταγωνιστική τοποθέτηση. Οι Magrizos et al. (2026) επιβεβαιώνουν αυτή τη λογική στο συγκεκριμένο πλαίσιο των πολιτικών απορρήτου, δείχνοντας ότι τα επεξηγηματικά infographics αυξάνουν την εμπιστοσύνη. Οι Fox et al. (2022) καταδεικνύουν επίσης ότι η οπτική επικοινωνία απορρήτου αυξάνει την προθυμία για συναλλαγές και αποκάλυψη δεδομένων. Αυτά τα ευρήματα υποδηλώνουν ότι η διαφάνεια βελτιώνει τόσο τα αποτελέσματα στις σχέσεις με τους πελάτες όσο και τις συμπεριφορικές προθέσεις.

Σε ευρύτερο στρατηγικό επίπεδο, η προστασία δεδομένων ενισχύει την ανταγωνιστικότητα όταν οι εταιρείες χρησιμοποιούν τη διαφάνεια για να επικοινωνήσουν την ευθύνη και να μειώσουν την αβεβαιότητα στις ψηφιακές ανταλλαγές. Οι Carl et al. (2024) δείχνουν ότι οι καταναλωτές εκτιμούν τις εταιρείες που εκφράζουν ψηφιακή ευθύνη μέσω δραστηριοτήτων απορρήτου και ασφάλειας, ενώ οι Avramidis et al. (2026) δείχνουν ότι η ιδιωτικότητα και η ασφάλεια μπορούν να λειτουργήσουν ως στρατηγικές απαντήσεις στον ανταγωνισμό της αγοράς. Οι Chisam et al. (2026) επεκτείνουν αυτό το επιχείρημα σε όλες τις διεθνείς αγορές εξηγώντας ότι τα κέρδη που βασίζονται στην εμπιστοσύνη προκύπτουν με την πάροδο του χρόνου όταν η προστασία της ιδιωτικότητας δημιουργεί αξιόπιστη συμμόρφωση στα μάτια των ενδιαφερόμενων μερών. Επομένως, η διαφάνεια εμπλουτίζει τη φήμη, υποστηρίζει τη δημιουργία εμπιστοσύνης και δημιουργεί συνθήκες για μακροπρόθεσμη ανταγωνιστική διαφοροποίηση.

4.2 Οικονομικές επιπτώσεις της συμμόρφωσης

4.2.1 Κόστη εφαρμογής GDPR για ΜΜΕ και μεγάλες επιχειρήσεις

Οι οικονομικές επιπτώσεις της συμμόρφωσης με τον GDPR ποικίλλουν μεταξύ των επιχειρήσεων, επειδή οι κανονιστικές υποχρεώσεις αλληλεπιδρούν με το μέγεθος της επιχείρησης, την τεχνική ικανότητα και την εξάρτηση από τα προσωπικά δεδομένα. Για τις μικρές και μεσαίες επιχειρήσεις, η συμμόρφωση συχνά απαιτεί προσαρμογές στη διακυβέρνηση, την τεκμηρίωση, τη χαρτογράφηση δεδομένων, τους εσωτερικούς

ελέγχους και τις διαδικασίες λογοδοσίας. Ο Brodin (2019) δείχνει ότι οι ΜΜΕ σπάνια επιτυγχάνουν συμμόρφωση μέσω μεμονωμένων νομικών διορθώσεων. Αντίθετα, χρειάζονται ένα δομημένο πλαίσιο που συντονίζει τις πολιτικές, τις ευθύνες, την αξιολόγηση κινδύνου και τις λειτουργικές διαδικασίες. Σε πολλές μικρότερες επιχειρήσεις, η πρόκληση έγκειται λιγότερο στην κατανόηση των νομικών αρχών και περισσότερο στη μετάφρασή τους σε επαναλήψιμες διαδικασίες με δεδομένους τους περιορισμούς στον αριθμό του προσωπικού και στην δυνατότητα για επίσημη εξειδίκευση.

Οι Jakobi et al. (2020) διευρύνουν αυτήν την άποψη δείχνοντας ότι η εφαρμογή του GDPR αντικατοπτρίζει μια σύγκρουση μεταξύ των νομικών προσδοκιών, των επιχειρηματικών συμφερόντων και των στόχων προστασίας των καταναλωτών. Η ανάλυσή τους υπογραμμίζει ότι τα συστήματα πληροφοριών διαδραματίζουν κεντρικό ρόλο στη συμφιλίωση αυτών των εντάσεων, επειδή οι επιχειρήσεις πρέπει να δημιουργήσουν χρησιμοποιήσιμες μορφές ελέγχου πρόσβασης, διαχείρισης συναινέσεων, ελαχιστοποίησης δεδομένων και διαφάνειας. Τέτοιες προσαρμογές επιβάλλουν σταθερό κόστος συμμόρφωσης που οι μεγαλύτερες επιχειρήσεις μπορούν να απορροφήσουν πιο εύκολα λόγω ισχυρότερων διοικητικών υποδομών και πιο ανεπτυγμένων λειτουργιών συστημάτων πληροφοριών. Αντιθέτως, οι μικρότερες επιχειρήσεις αντιμετωπίζουν αναλογικά μεγαλύτερες δυσκολίες, επειδή τα ίδια νομικά πρότυπα απαιτούν επενδύσεις σε συστήματα, τεκμηρίωση και εμπειρογνωμοσύνη που επιβαρύνουν τους στενότερους προϋπολογισμούς. Έτσι, το οικονομικό βάρος της συμμόρφωσης κατανέμεται άνισα ακόμη και όταν οι νομικές απαιτήσεις είναι τυπικά ομοιόμορφες.

Παρόμοια συμπεράσματα προκύπτουν μέσα από ευρύτερα εμπειρικά στοιχεία σχετικά με την απόδοση των επιχειρήσεων. Οι Frey και Presidente (2024) διαπιστώνουν ότι ο GDPR μείωσε την κερδοφορία για τις επιχειρήσεις που είναι περισσότερο εκτεθειμένες στις ευρωπαϊκές αγορές, ιδίως μέσω της αύξησης του κόστους. Οι εταιρείες τεχνολογίας αντιμετώπισαν υψηλότερα έξοδα, πιέσεις στο μισθολογικό κόστος και ισχυρότερα κίνητρα για επενδύσεις σε καινοτομίες που σχετίζονται με τον GDPR. Είναι σημαντικό ότι τα μεγαλύτερα βάρη έπεσαν στις μικρότερες εταιρείες.

Οι Smirnova και Travieso Morales (2025) στην ανάλυσή τους για τις νεοσύστατες επιχειρήσεις δείχνουν ότι οι προκλήσεις συμμόρφωσης προκύπτουν από τις διασυνδεδεμένες επιπτώσεις της κανονιστικής πολυπλοκότητας, της τεχνικής πολυπλοκότητας και της οργανωτικής ικανότητας. Η μελέτη τους προσδιορίζει την εκπαίδευση του προσωπικού ως παράγοντα μεσολάβησης μεταξύ αυτών των πολυπλοκοτήτων και του συνολικού κόστους συμμόρφωσης, υποδηλώνοντας ότι οι περιορισμοί πόρων ενισχύουν την οικονομική πίεση της ρύθμισης για τις επιχειρήσεις αυτές. Ο Farhad (2024) συνδέει την ανάλυση κόστους και τη στρατηγική προσαρμογής, αποδεικνύοντας ότι οι νόμοι περί προστασίας δεδομένων επηρεάζουν τα επιχειρηματικά μοντέλα. Η συμμόρφωση αλλάζει τις ροές εργασίας, τις πρακτικές συλλογής δεδομένων, την επικοινωνία με τους πελάτες και τις στρατηγικές των ψηφιακών πλατφορμών, πράγμα που σημαίνει ότι το κόστος προκύπτει τόσο σε άμεσες όσο και σε έμμεσες μορφές. Το άμεσο κόστος περιλαμβάνει νομικές συμβουλές, τεχνικές αναβαθμίσεις, ελέγχους δεδομένων και επανασχεδιασμό πολιτικής. Το έμμεσο κόστος περιλαμβάνει πιο αργό πειραματισμό, αλλαγές στη λογική της δημιουργίας εσόδων και την ανάγκη επανασχεδιασμού των καινοτομιών γύρω από τις απαιτήσεις απορρήτου. Ταυτόχρονα ωστόσο, αυτή η αναδιάρθρωση μπορεί να τονώσει νέες μορφές δημιουργίας αξίας.

Η συγκριτική οικονομική αποτίμηση αποδίδει με ποιοτικούς όρους τη σχετική ένταση του κόστους και το εύρος του αναμενόμενου οφέλους. Η χρήση σχετικών κατηγοριών ανταποκρίνεται στη διαφοροποίηση του πραγματικού κόστους ανά κλάδο, ένταση επεξεργασίας δεδομένων, τεχνολογική ωριμότητα και υφιστάμενο σύστημα διακυβέρνησης. Ο επόμενος πίνακας συνθέτει τα ευρήματα των Brodin (2019), Jakobi et al. (2020), Frey και Presidente (2024), Smirnova και Travieso Morales (2025), Martin et al. (2017) και Gimpel et al. (2018).

Πίνακας 10: Συγκριτική αποτίμηση κόστους και οφέλους συμμόρφωσης με τον GDPR

Διάσταση	ΜΜΕ	Μεγάλες επιχειρήσεις	Χρονικός ορίζοντας	Επιχειρηματική επίδραση
Κόστος νομικής και συμβουλευτικής υποστήριξης	Υψηλή σχετική επιβάρυνση	Μέτρια σχετική επιβάρυνση και υψηλή απόλυτη δαπάνη	Βραχυπρόθεσμος	Τεκμηρίωση, συμβάσεις, πολιτικές και εξειδικευμένη καθοδήγηση

Διάσταση	ΜΜΕ	Μεγάλες επιχειρήσεις	Χρονικός ορίζοντας	Επιχειρηματική επίδραση
Κόστος DPO και εξειδικευμένου προσωπικού	Υψηλή σχετική επιβάρυνση, συχνά μέσω εξωτερικής υπηρεσίας	Υψηλή απόλυτη δαπάνη με εσωτερικές ομάδες και κατανομή ρόλων	Συνεχής	Ενισχύει τη λογοδοσία και τον συντονισμό
Χαρτογράφηση δεδομένων και αρχεία επεξεργασίας	Μέτρια έως υψηλή σχετική επιβάρυνση	Υψηλή απόλυτη δαπάνη λόγω όγκου και πολυπλοκότητας	Βραχυπρόθεσμος και συνεχής	Βελτιώνει την ορατότητα των ροών και την ποιότητα δεδομένων
Τεχνικές αναβαθμίσεις και ασφάλεια	Υψηλή σχετική επιβάρυνση	Υψηλή απόλυτη δαπάνη και δυνατότητα οικονομιών κλίμακας	Μεσοπρόθεσμος	Μειώνει την πιθανότητα περιστατικών και το κόστος αποκατάστασης
Εκπαίδευση προσωπικού	Μέτρια έως υψηλή σχετική επιβάρυνση	Υψηλή απόλυτη δαπάνη με ευρύτερη οργανωτική κάλυψη	Συνεχής	Περιορίζει ανθρώπινα σφάλματα και ενισχύει την κουλτούρα συμμόρφωσης
Επανασχεδιασμός διαδικασιών και προϊόντων	Υψηλή σχετική επιβάρυνση σε περιορισμένους πόρους	Μέτρια έως υψηλή σχετική επιβάρυνση σε σύνθετα οικοσυστήματα	Βραχυπρόθεσμος και μεσοπρόθεσμος	Δημιουργεί καθαρότερες διαδικασίες και ασφαλέστερη καινοτομία
Μείωση κανονιστικής και δικαστικής έκθεσης	Υψηλό αναμενόμενο όφελος	Υψηλό αναμενόμενο όφελος και μεγάλη απόλυτη αξία	Μεσοπρόθεσμος και μακροπρόθεσμος	Περιορίζει πρόστιμα, διαφορές και δαπάνες διαχείρισης κρίσεων
Εμπιστοσύνη και πιστότητα πελατών	Υψηλό όφελος για διαφοροποίηση και διατήρηση πελατών	Υψηλό όφελος σε κλίμακα και προστασία εταιρικής φήμης	Μεσοπρόθεσμος και μακροπρόθεσμος	Ενισχύει επαναλαμβανόμενες συναλλαγές και ποιότητα σχέσης

Διάσταση	ΜΜΕ	Μεγάλες επιχειρήσεις	Χρονικός ορίζοντας	Επιχειρηματική επίδραση
Ποιότητα δεδομένων και αποτελεσματικότητα αποφάσεων	Μέτριο έως υψηλό όφελος	Υψηλό όφελος λόγω όγκου και διασύνδεσης συστημάτων	Μεσοπρόθεσμος	Περιορίζει περιττά δεδομένα και βελτιώνει τη διοικητική πληροφόρηση
Πρόσβαση σε συνεργασίες και αγορές	Υψηλό όφελος για αλυσίδες προμηθευτών και συμβάσεις	Υψηλό όφελος για διεθνή οικοσυστήματα και δημόσιες συμβάσεις	Μεσοπρόθεσμος	Η τεκμηριωμένη συμμόρφωση λειτουργεί ως κριτήριο αξιοπιστίας
Καινοτομία με ενσωματωμένη ιδιωτικότητα	Μέτριο έως υψηλό όφελος με στοχευμένες επενδύσεις	Υψηλό όφελος μέσω κλιμάκωσης και τεχνολογικής διαφοροποίησης	Μακροπρόθεσμος	Υποστηρίζει νέα προϊόντα, ασφαλή αξιοποίηση δεδομένων και ανταγωνιστικό πλεονέκτημα
Συνολικό ισοζύγιο	Αρχικά υψηλή αναλογική επιβάρυνση και σταδιακή δημιουργία αξίας	Υψηλή απόλυτη επένδυση και ισχυρή δυνατότητα απόδοσης σε κλίμακα	Από βραχυπρόθεσμο σε μακροπρόθεσμο	Η στρατηγική ενσωμάτωση μετατρέπει τη συμμόρφωση σε οργανωτική ικανότητα

Για τις ΜΜΕ, η οικονομική αποτελεσματικότητα ενισχύεται μέσω σταδιακής προτεραιοποίησης των υψηλότερων κινδύνων, αξιοποίησης κοινών προτύπων, εξωτερικής υποστήριξης DPO και επιλογής τεχνολογικών λύσεων ανάλογων με την κλίμακα. Για τις μεγάλες επιχειρήσεις, η μεγαλύτερη απόδοση συνδέεται με κεντρική διακυβέρνηση, αυτοματοποίηση ελέγχων, κοινές μετρικές και ενιαία διαχείριση προμηθευτών. Και στις δύο κατηγορίες, το καθαρό όφελος γίνεται περισσότερο ορατό σε μεσοπρόθεσμο και μακροπρόθεσμο ορίζοντα.

4.2.2 Οφέλη από την ενίσχυση της φήμης και της πιστότητας πελατών

Παρόλο που η συμμόρφωση εισάγει μετρήσιμο κόστος, η βιβλιογραφία δείχνει επίσης ότι οι εταιρείες μπορούν να μετατρέψουν τις υπεύθυνες πρακτικές δεδομένων σε οφέλη φήμης και σχέσεων. Οι Martin et al. (2017) παρέχουν στοιχεία σύμφωνα με

τα οποία η διαφάνεια και ο έλεγχος στη διαχείριση δεδομένων μειώνουν την ευπάθεια των πελατών και καταστέλλουν τις επιβλαβείς επιπτώσεις που σχετίζονται με τις αντιλήψεις για παραβίαση της ιδιωτικής ζωής. Η μελέτη τους καταδεικνύει ότι όταν οι πελάτες αισθάνονται ότι οι εταιρείες διατηρούν τα δεδομένα τους χωρίς σαφείς διασφαλίσεις, η εμπιστοσύνη μειώνεται, όπως και η απόδοση της εταιρείας. Αντίθετα, οι διαφανείς και ελεγχόμενες πρακτικές δεδομένων δημιουργούν πιο ευνοϊκές αντιδράσεις των πελατών και προστατεύουν τις εταιρείες από τη μείωση της αξίας της. Η διαχείριση της ιδιωτικής ζωής διαμορφώνει επομένως την εμπιστοσύνη και την απόδοση των μεταγενέστερων σταδίων.

Οι Gimpel et al. (2018) εμβαθύνουν περαιτέρω, εξετάζοντας τη θετική πλευρά των μέτρων προστασίας της ιδιωτικής ζωής από την οπτική γωνία του πελάτη. Τα ευρήματά τους δείχνουν ότι πολλές πρακτικές προστασίας της ιδιωτικής ζωής θεωρούνται βασικές προσδοκίες ποιότητας, ενώ ορισμένα μέτρα προστασίας της ιδιωτικής ζωής έχουν ελκυστική ποιότητα και μπορούν να ικανοποιήσουν ενεργά τους πελάτες. Αυτή η διάκριση έχει σημασία για την οικονομική ανάλυση επειδή υποδηλώνει ότι η προστασία της ιδιωτικής ζωής δημιουργεί αξία σε περισσότερα από ένα επίπεδα. Πρώτον, οι εταιρείες χρειάζονται ισχυρά μέτρα για να ανταποκριθούν στις βασικές προσδοκίες και να εξασφαλίσουν νομιμότητα. Δεύτερον, η ανώτερη εφαρμογή της προστασίας της ιδιωτικής ζωής μπορεί να διαφοροποιήσει μια επωνυμία και να αυξήσει την ικανοποίηση των πελατών πάνω από τα τυπικά επίπεδα της αγοράς. Συνεπώς, η ιδιωτικότητα λειτουργεί τόσο ως προϋπόθεση για την εμπιστοσύνη όσο και ως παράγοντας ενίσχυσης της αφοσίωσης και της εμπειρίας των πελατών.

Στοιχεία από πιο συγκεκριμένα περιβάλλοντα υποστηρίζουν το ίδιο συμπέρασμα. Οι Chen et al. (2023) δείχνουν ότι η αντιληπτή διαφάνεια των πρακτικών απορρήτου μιας επιχείρησης έχει θετική επίδραση στη δέσμευση των πελατών. Η μελέτη τους διαπιστώνει επίσης ότι οι πρακτικές απορρήτου επηρεάζουν τις συμπεριφορικές αντιδράσεις μέσω της παραποίησης πληροφοριών, πράγμα που σημαίνει ότι τα αδύναμα περιβάλλοντα απορρήτου μπορούν να μειώσουν την ποιότητα των δεδομένων καθώς και τη δύναμη της σχέσης. Όταν οι πελάτες αισθάνονται ασφαλείς, είναι πιο πιθανό να παρέχουν ακριβείς πληροφορίες και να διατηρούν τη δέσμευση με την εταιρεία. Οι Swani et al. (2023) καταδεικνύουν ομοίως ότι η ικανοποίηση των προσδοκιών των αγοραστών για την ιδιωτικότητα ενισχύει την

εμπιστοσύνη στην ιδιωτικότητα, την ικανοποίηση από την ιδιωτικότητα, τη δέσμευση και τις προθέσεις για συνέχιση της επιχειρηματικής δραστηριότητας. Η συμβολή τους είναι ιδιαίτερα χρήσιμη επειδή επεκτείνει τη λογική της αξίας της ιδιωτικότητας από τις καταναλωτικές αγορές στις σχέσεις μεταξύ επιχειρήσεων.

Οι Kang et al. (2025) προσθέτουν ότι η εταιρική ευθύνη για την ιδιωτικότητα γίνεται ακόμη πιο αποτελεσματική όταν συνοδεύεται από εκπαίδευση των πελατών. Στη μελέτη τους, η ευθύνη για την ιδιωτικότητα σε συνδυασμό με τις εκπαιδευτικές προσπάθειες ενισχύει την εμπιστοσύνη των πελατών, τις στάσεις της επωνυμίας και τις προθέσεις επίσκεψης. Αυτό το αποτέλεσμα είναι σημαντικό, επειδή δείχνει ότι οι εταιρείες δημιουργούν ισχυρότερες αποδόσεις από τις επενδύσεις στην ιδιωτικότητα όταν γνωστοποιούν τον σκοπό και την αξία αυτών των επενδύσεων στους χρήστες. Η φήμη και η αφοσίωση έτσι, προκύπτουν όταν η ιδιωτικότητα μεταφράζεται σε κατανοητές αποδείξεις φροντίδας, ικανότητας και ευθύνης.

4.2.3 Παραδείγματα επιχειρηματικής επιτυχίας μέσω υπεύθυνης διαχείρισης δεδομένων

Η υπεύθυνη διαχείριση δεδομένων συμβάλλει στην επιχειρηματική επιτυχία όταν οι εταιρείες ενσωματώνουν την ιδιωτικότητα σε ευρύτερες στρατηγικές και επιχειρησιακές επιλογές. Ο Farhad (2024) δείχνει ότι οι εταιρείες τεχνολογίας ανταποκρίνονται όλο και περισσότερο στις απαιτήσεις ιδιωτικότητας αναθεωρώντας τα επιχειρηματικά μοντέλα με τρόπους που υποστηρίζουν την καινοτομία παράλληλα με τη συμμόρφωση. Οι Martin et al. (2017) ενισχύουν αυτήν την προοπτική συνδέοντας τις διαφανείς πρακτικές δεδομένων με την ισχυρότερη εμπιστοσύνη των πελατών και τα καλύτερα αποτελέσματα της εταιρείας, ενώ οι Gimpel et al. (2018) δείχνουν ότι ορισμένα μέτρα προστασίας της ιδιωτικής ζωής δημιουργούν ανταγωνιστικό πλεονέκτημα ικανοποιώντας τους πελάτες. Οι Chen et al. (2023), Swani et al. (2023) και Kang et al. (2025) καταδεικνύουν περαιτέρω ότι η εμπιστοσύνη, η ικανοποίηση, η δέσμευση και οι συμπεριφορικές προθέσεις βελτιώνονται όταν οι πρακτικές απορρήτου είναι ορατές, αξιόπιστες και υποστηρίζονται εκπαιδευτικά.

Συνολικά, η βιβλιογραφία παρουσιάζει ένα συμπέρασμα, σύμφωνα με το οποίο η συμμόρφωση με τον GDPR δημιουργεί σημαντικό κόστος, ειδικά για τις ΜΜΕ, τις νεοσύστατες επιχειρήσεις και τις επιχειρήσεις με περιορισμένη οργανωτική ικανότητα,

όπως δείχνουν οι Brodin (2019), Jakobi et al. (2020), Frey και Presidente (2024) και Smirnova και Travieso Morales (2025). Ωστόσο, το ίδιο σύνολο ερευνών δείχνει επίσης ότι οι επενδύσεις στην ιδιωτικότητα μπορούν να αποφέρουν κέρδη στη φήμη, ισχυρότερη αφοσίωση των πελατών, καλύτερη ποιότητα πληροφοριών και πιο ανθεκτικά επιχειρηματικά μοντέλα. Οι οικονομικές επιπτώσεις της συμμόρφωσης είναι επομένως διττής φύσης. Το κόστος κυριαρχεί βραχυπρόθεσμα όταν οι εταιρείες αντιμετωπίζουν τον GDPR ως μια υποχρέωση, ενώ τα οφέλη γίνονται πιο ορατά μεσοπρόθεσμα και μακροπρόθεσμα όταν οι εταιρείες ενσωματώνουν την ιδιωτικότητα στην οικοδόμηση εμπιστοσύνης, την εκπαίδευση των πελατών και τη στρατηγική διαφοροποίηση. Υπό αυτή την έννοια, η υπεύθυνη διαχείριση δεδομένων λειτουργεί ως μηχανισμός μέσω του οποίου η νομική προσαρμογή μπορεί να εξελιχθεί σε ανταγωνιστικό πλεονέκτημα με την πάροδο του χρόνου.

4.3 Ψηφιακός μετασχηματισμός και ασφάλεια πληροφοριών

Τα προηγούμενα υποκεφάλαια έδειξαν ότι η προστασία δεδομένων δημιουργεί εμπιστοσύνη, επηρεάζει την απόδοση της εταιρείας και μπορεί να υποστηρίξει την ανταγωνιστική διαφοροποίηση όταν ενσωματώνεται στην υπεύθυνη οργανωτική πρακτική. Το παρόν υποκεφάλαιο εξετάζει τις τεχνολογικές και λειτουργικές συνθήκες που επιτρέπουν στις δεσμεύσεις περί απορρήτου να λειτουργούν στην πράξη. Ο ψηφιακός μετασχηματισμός διευρύνει την κλίμακα, την ταχύτητα και τη στρατηγική σημασία της χρήσης δεδομένων, ωστόσο διευρύνει επίσης την έκθεση σε κυβερνοαπειλές, τεχνικές ευπάθειες και κινδύνους φήμης. Για αυτόν τον λόγο, η ασφάλεια των πληροφοριών καθίσταται κεντρικός πυλώνας της βιώσιμης διακυβέρνησης δεδομένων, συνδέοντας τη διαχείριση κινδύνων, τις τεχνολογίες ενίσχυσης του απορρήτου και την αποκατάσταση της εμπιστοσύνης μετά από παραβίαση σε ένα ενιαίο πεδίο επιχειρηματικής στρατηγικής.

4.3.1 Ανάλυση κινδύνων και πρακτικών κυβερνοασφάλειας

Ο ψηφιακός μετασχηματισμός έχει εντείνει την εξάρτηση των εταιρειών από διασυνδεδεμένες υποδομές, εξωτερικούς προμηθευτές, υπηρεσίες cloud, εργαλεία τεχνητής νοημοσύνης και αναλύσεις σε πραγματικό χρόνο. Αυτό το νέο περιβάλλον δημιουργεί σημαντικές ευκαιρίες για καινοτομία στις υπηρεσίες, αλλά ταυτόχρονα διευρύνει το πεδίο των κυβερνοκινδύνων που καλούνται να διαχειριστούν οι

οργανισμοί. Οι Wang, Asif, Shahzad και Ashfaq (2024) στην έρευνά τους στον τραπεζικό τομέα δείχνουν ότι η ενσωμάτωση παλαιού συστήματος, ο κίνδυνος προμηθευτών, οι εξελισσόμενες απαιτήσεις συμμόρφωσης και η εμπιστοσύνη των πελατών διαμορφώνουν την ατζέντα κυβερνοασφάλειας των εταιρειών που βρίσκονται σε ψηφιακή μετάβαση. Τα ευρήματά τους υποδηλώνουν ότι οι οργανισμοί βλέπουν όλο και περισσότερο την ιδιωτικότητα και την κυβερνοασφάλεια ως αλληλεξαρτώμενους και όχι ως ξεχωριστούς τομείς. Οι ισχυροί έλεγχοι πρόσβασης, η συνεχής παρακολούθηση απειλών, η εκπαίδευση των εργαζομένων, τα πλαίσια διακυβέρνησης και η κρυπτογράφηση δεδομένων αναδεικνύονται ως βασικές πρακτικές επειδή μειώνουν την έκθεση στον ψηφιακό κίνδυνο, ενώ παράλληλα υποστηρίζουν την εμπιστοσύνη και την κανονιστική ευθυγράμμιση.

Η οικονομική σημασία αυτής της ενσωμάτωσης ενισχύεται περαιτέρω από τον Türegün (2025), ο οποίος διαπιστώνει ότι η ισχυρότερη ενσωμάτωση μέτρων αντιμετώπισης του κυβερνοκινδύνου σχετίζεται με καλύτερη οικονομική απόδοση στις τράπεζες. Η εν λόγω μελέτη δείχνει ότι οι δαπάνες από μόνες τους δεν εγγυώνται καλύτερα αποτελέσματα. Μεγαλύτερη αξία προκύπτει όταν τα μέτρα κυβερνοασφάλειας ευθυγραμμίζονται με ευρύτερους στρατηγικούς στόχους διαχείρισης κινδύνου και ενσωματώνονται σε σχέδια ψηφιακού μετασχηματισμού. Τα σοβαρά περιστατικά παραβίασης της ασφάλειας αυξάνουν το κόστος και αποδυναμώνουν την κερδοφορία, ενώ η στρατηγικά ενσωματωμένη κυβερνοασφάλεια βελτιώνει την ανθεκτικότητα. Αυτό το συμπέρασμα είναι σημαντικό επειδή τοποθετεί την κυβερνοασφάλεια στη διαδικασία λήψης διοικητικών αποφάσεων αντί να την αντιμετωπίζει ως μια καθαρά τεχνική λειτουργία υποστήριξης.

Οι Abrardi, Comino και Grassini (2025) διευρύνουν τη συζήτηση εξετάζοντας τα οικονομικά του κυβερνοκινδύνου σε εταιρείες, χρήστες, χάκερ και ρυθμιστικές αρχές. Η ανασκόπησή τους καταδεικνύει ότι ο κυβερνοκίνδυνος δεν περιορίζεται στις άμεσες απώλειες από παραβιάσεις, αλλά επηρεάζει επίσης τα κίνητρα, τη λογική ασφάλισης, τη συμπεριφορά των καταναλωτών, τον κανονιστικό σχεδιασμό και τα επενδυτικά πρότυπα. Σε αυτό το ευρύτερο πλαίσιο, οι οργανισμοί χρειάζεται να αντιμετωπίζουν την κυβερνοασφάλεια ως οργανικό στοιχείο της οικονομικής οργάνωσης της ψηφιακής επιχείρησης. Οι Slapničar, Axelsen και Eulerich (2025) τονίζουν ότι, παρότι πολλοί οργανισμοί παρουσιάζουν τη διαχείριση του

κυβερνοκινδύνου ως αυστηρά βασισμένη σε μετρήσιμα δεδομένα, στην πραγματικότητα αυτή διαμορφώνεται μέσα από τη σύζευξη ποιοτικών εκτιμήσεων και ποσοτικών ενδείξεων. Η προσέγγιση αυτή είναι ιδιαίτερα χρήσιμη, επειδή δείχνει ότι η αποτελεσματική διακυβέρνηση του ψηφιακού κινδύνου στηρίζεται στη σύνθεση τεχνικής μέτρησης, διοικητικής ερμηνείας και οργανωσιακής μάθησης. Έτσι, η ανάλυση κινδύνου καθίσταται πιο ουσιαστική όταν συνδυάζει εμπειρικά δεδομένα με πρακτική κρίση και διαρκή στρατηγική αναθεώρηση.

4.3.2 Τεχνολογίες προστασίας δεδομένων

Εάν η διαχείριση του κυβερνοκινδύνου ορίζει την οργανωτική λογική της προστασίας, οι τεχνολογίες ενίσχυσης της ιδιωτικότητας παρέχουν τα τεχνικά μέσα μέσω των οποίων τα δεδομένα μπορούν να χρησιμοποιηθούν με μεγαλύτερη ασφάλεια σε σύνθετα ψηφιακά οικοσυστήματα. Οι Auñón et al. (2024) εξετάζουν τις τεχνολογίες ενίσχυσης της ιδιωτικότητας από την οπτική γωνία των ευρωπαϊκών χώρων δεδομένων και δείχνουν ότι αυτά τα εργαλεία έχουν γίνει απαραίτητα για την ασφαλή κοινή χρήση δεδομένων σε περιβάλλοντα ευαίσθητα στην ιδιωτικότητα. Η ανάλυσή τους υπογραμμίζει την αυξανόμενη σημασία της μάθησης και των σχετικών λύσεων διατήρησης της ιδιωτικότητας, επειδή οι εταιρείες χρειάζεται να ανταλλάσσουν δεδομένα χωρίς να παραδίδουν τον έλεγχο των ευαίσθητων πληροφοριών. Η μελέτη είναι ιδιαίτερα σημαντική για επιχειρηματικά περιβάλλοντα όπου η εμπιστοσύνη και η διαλειτουργικότητα πρέπει να αναπτύσσονται ταυτόχρονα.

Τα συστήματα που βασίζονται στο blockchain καταδεικνύουν την ίδια ανάγκη για ασφαλείς και ευαίσθητες ως προς την ιδιωτικότητα υποδομές δεδομένων. Οι Zhou et al. (2024) εξηγούν ότι το blockchain προσφέρει αμετάβλητες διαδικασίες, ιχνηλασιμότητα και ισχυρότερη διαχείριση ταυτότητας, ωστόσο η διαφανής δομή του μπορεί επίσης να δημιουργήσει ανησυχίες για την ιδιωτικότητα. Η έρευνά τους δείχνει ότι οι αποδείξεις μηδενικής γνώσης (zero knowledge proofs) παρέχουν μια πολλά υποσχόμενη μέθοδο για την εξισορρόπηση αυτών των εντάσεων, επιτρέποντας την επαλήθευση ταυτότητας και τη δημιουργία αποδείξεων χωρίς περιττή αποκάλυψη δεδομένων. Αυτή η γνώση είναι εξαιρετικά σημαντική για τις ψηφιακές επιχειρήσεις, επειδή καταδεικνύει ότι η καινοτομία στην ασφαλή κοινή χρήση ταυτότητας εξαρτάται από τον συνδυασμό της ασφάλειας, της λογοδοσίας και της ιδιωτικότητας στον ίδιο σχεδιασμό. Μια παρόμοια λογική εξισορρόπησης εμφανίζεται στην αντιμετώπιση της

ανωνυμοποίησης. Οι Holzenberger και Maxwell (2025) εξετάζουν τις δοκιμές του GDPR για την ανωνυμοποίηση και για κατάλληλα τεχνικά και οργανωτικά μέτρα μέσω ενός ποσοτικού πλαισίου. Η συμβολή τους είναι σημαντική επειδή μετατρέπει τα ασαφή νομικά πρότυπα σε ένα σαφέστερο αξιολογικό μοντέλο που λαμβάνει υπόψη τον κίνδυνο ταυτοποίησης, την προσπάθεια επίθεσης και το κόστος χρησιμότητας της προστασίας. Με αυτόν τον τρόπο, η ανωνυμοποίηση παρουσιάζεται ως στρατηγική επιλογή που απαιτεί κρίση.

Οι Madhusudhanan και Jose (2025) επεκτείνουν την τεχνολογική προοπτική σε ολόκληρο τον κύκλο ζωής των δεδομένων. Η έρευνά τους εξετάζει τη διατήρηση της ιδιωτικότητας κατά τη συλλογή, την αποθήκευση, την επεξεργασία, την κοινή χρήση, τη μετάδοση, τη διατήρηση, τη διαγραφή και τον έλεγχο πρόσβασης. Αυτή η προσέγγιση του κύκλου ζωής είναι ιδιαίτερα χρήσιμη για τον ψηφιακό μετασχηματισμό, επειδή οι εταιρείες δεν επεξεργάζονται πλέον δεδομένα σε μεμονωμένα στάδια, αλλά διαχειρίζονται συνεχείς ροές προσωπικών και ευαίσθητων πληροφοριών που διακινούνται σε συστήματα, συνεργάτες και περιβάλλοντα αποφάσεων. Επομένως, τεχνολογίες όπως η κρυπτογράφηση, οι μέθοδοι ανωνυμοποίησης, οι έλεγχοι πρόσβασης και οι δομές και διαδικασίες διατήρησης της ιδιωτικότητας γίνονται πιο αποτελεσματικές όταν συντονίζονται σε ολόκληρο τον κύκλο ζωής των δεδομένων αντί να εισάγονται ως κατακερματισμένοι έλεγχοι.

4.3.3 Διαχείριση περιστατικών παραβίασης και αποκατάστασης εμπιστοσύνης

Ακόμη και ισχυρά προληπτικά συστήματα λειτουργούν σε περιβάλλοντα όπου οι παραβιάσεις παραμένουν πιθανές, γεγονός που καθιστά την αντιμετώπιση τέτοιων περιστατικών βασική διάσταση της στρατηγικής ασφάλειας πληροφοριών. Οι Masuch, Greve και Trang (2021) εξετάζουν την απολογία και την αποζημίωση ως στρατηγικές αποκατάστασης μετά από μια παραβίαση δεδομένων σε ψηφιακές υπηρεσίες που σχετίζονται με την υγεία και δείχνουν ότι και οι δύο ενέργειες μπορούν να βελτιώσουν την ικανοποίηση από τη διαδικασία αποκατάστασης και να υποστηρίξουν τη θετική συμπεριφορά πελατών. Τα ευρήματά τους δείχνουν ότι η διαχείριση μετά την παραβίαση εξαρτάται από την κατανόηση των προσδοκιών των πελατών και την ευθυγράμμιση των ενεργειών αποκατάστασης με τη σοβαρότητα και το πλαίσιο του περιστατικού. Η αποκατάσταση της εμπιστοσύνης στηρίζεται επομένως, τόσο στην

τεχνική αντιμετώπιση του περιστατικού όσο και στη συμβολική και επικοινωνιακή επανόρθωση απέναντι στους ενδιαφερόμενους.

Οι Wang, Yan, Munyon et al. (2025) εξετάζουν το πώς οι πληροφορίες απόδοσης διαμορφώνουν τις αντιδράσεις των μετόχων μετά από παραβιάσεις δεδομένων. Τα αποτελέσματά τους δείχνουν ότι οι παραβιάσεις που θεωρούνται εσωτερικά προκαλούμενες παράγουν ισχυρότερες αρνητικές αντιδράσεις της αγοράς. Ταυτόχρονα, οι συμβολικές ενέργειες διαχείρισης της κρίσης και το ευνοϊκό κλίμα στα μέσα ενημέρωσης μπορούν να μετριάσουν αυτή την επίδραση. Αυτό το εύρημα είναι εξαιρετικά σημαντικό για την εταιρική φήμη, επειδή δείχνει ότι οι εταιρείες κρίνονται όχι μόνο από την ύπαρξη μιας παραβίασης αλλά και από το ερμηνευτικό πλαίσιο που την περιβάλλει. Η διαχείριση παραβιάσεων γίνεται έτσι μέρος της επικοινωνίας σε κρίσεις, της σηματοδότησης διακυβέρνησης και της διαχείρισης των σχέσεων με τα ενδιαφερόμενα μέρη.

Συνολικά, ο ψηφιακός μετασχηματισμός ενισχύει την ανάγκη για ολοκληρωμένη ασφάλεια πληροφοριών, επειδή η ιδιωτικότητα, η κυβερνοασφάλεια, ο τεχνολογικός σχεδιασμός και η αποκατάσταση της εμπιστοσύνης λειτουργούν πλέον ως αμοιβαία ενισχυόμενες διαστάσεις της βιώσιμης επιχειρηματικής ανάπτυξης. Οι πρακτικές κυβερνοασφάλειας προστατεύουν τη συνέχεια και μειώνουν την οικονομική έκθεση, οι τεχνολογίες ενίσχυσης της ιδιωτικότητας επιτρέπουν την υπεύθυνη χρήση δεδομένων και οι αποτελεσματικές αντιδράσεις σε παραβιάσεις διατηρούν τη νομιμότητα μετά από ανατρεπτικά γεγονότα. Μαζί, αυτά τα στοιχεία καθορίζουν εάν ο ψηφιακός μετασχηματισμός δημιουργεί εμπιστοσύνη ή ευπάθεια στα μάτια των πελατών, των ρυθμιστικών αρχών, των συνεργατών και των επενδυτών.

4.3.4 Πρακτικά υποδείγματα Εκτίμησης Αντικτύπου σχετικά με την Προστασία Δεδομένων

Η Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων (Data Protection Impact Assessment, DPIA) αποτελεί εργαλείο λογοδοσίας και διαχείρισης κινδύνου πριν από την έναρξη επεξεργασίας που ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων. Το άρθρο 35 του GDPR προβλέπει συστηματική περιγραφή της επεξεργασίας, αξιολόγηση αναγκαιότητας και αναλογικότητας, εκτίμηση κινδύνων και καταγραφή των μέτρων αντιμετώπισης. Η

ελληνική ΑΠΔΠΧ συνδέει την DPIA με την τεκμηρίωση της λογοδοσίας και τη μείωση του κινδύνου σε αποδεκτό επίπεδο (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016, άρθρο 35· Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, χ.χ.).

Πίνακας 11: Προκαταρκτικός έλεγχος υψηλού κινδύνου

Κριτήριο	Ερώτημα ελέγχου	Ναι	Παρατηρήσεις
Συστηματική και εκτεταμένη αξιολόγηση ή κατάρτιση προφίλ	Αξιολογούνται συμπεριφορά, οικονομική κατάσταση, υγεία, προτιμήσεις, αξιοπιστία ή απόδοση;	☐	
Αυτοματοποιημένες αποφάσεις με σημαντική επίδραση	Η επεξεργασία επηρεάζει πρόσβαση σε υπηρεσία, τιμολόγηση, πίστωση, εργασία ή άλλο ουσιώδες συμφέρον;	☐	
Ειδικές κατηγορίες ή δεδομένα ποινικών καταδικών	Πραγματοποιείται επεξεργασία ευαίσθητων δεδομένων σε μεγάλη κλίμακα ή με συστηματικό χαρακτήρα;	☐	
Συστηματική παρακολούθηση	Παρακολουθούνται δημόσιοι χώροι, διαδικτυακή συμπεριφορά, θέση ή επικοινωνιακές συνήθειες;	☐	
Ευάλωτα υποκείμενα	Αφορούν τα δεδομένα παιδιά, εργαζομένους, ασθενείς, ηλικιωμένους ή πρόσωπα με περιορισμένη διαπραγματευτική ισχύ;	☐	
Νέα ή συνδυασμένη τεχνολογία	Χρησιμοποιούνται τεχνητή νοημοσύνη, βιομετρικά συστήματα, IoT, blockchain ή νέες τεχνικές ανάλυσης;	☐	
Συνδυασμός συνόλων δεδομένων	Συνδέονται δεδομένα από διαφορετικές πηγές με σκοπό εξαγωγή νέων συμπερασμάτων;	☐	
Μεγάλη κλίμακα ή μακρά διάρκεια	Η επεξεργασία καλύπτει μεγάλο αριθμό προσώπων, εκτεταμένο γεωγραφικό πεδίο ή μακροχρόνια παρακολούθηση;	☐	
Περιορισμός δικαιώματος ή πρόσβασης	Η επεξεργασία επηρεάζει ουσιαστικά τη δυνατότητα άσκησης δικαιωμάτων ή χρήσης υπηρεσίας;	☐	
Σοβαρές πιθανές συνέπειες	Προκύπτει κίνδυνος διάκρισης, οικονομικής απώλειας, αποκάλυψης, κλοπής ταυτότητας ή βλάβης φήμης;	☐	

Η συγκέντρωση δύο ή περισσότερων κριτηρίων αποτελεί ισχυρή ένδειξη ανάγκης DPIA, ενώ η ένταση ενός μόνο κριτηρίου μπορεί επίσης να τεκμηριώσει υψηλό

κίνδυνο. Η τελική απόφαση καταγράφεται μαζί με την αιτιολόγηση και τη γνώμη του DPO.

Πίνακας 12: Πρότυπο καταγραφής Εκτίμησης Αντικτύπου

Πεδίο DPIA	Περιεχόμενο προς συμπλήρωση
Στοιχεία έργου	Τίτλος έργου, υπεύθυνος επεξεργασίας, επιχειρησιακός υπεύθυνος, DPO, ημερομηνία, έκδοση και ημερομηνία επανεξέτασης.
Περιγραφή επεξεργασίας	Πράξεις συλλογής, καταχώρισης, ανάλυσης, κοινοποίησης, αποθήκευσης και διαγραφής, μαζί με τα χρησιμοποιούμενα συστήματα.
Σκοποί και νόμιμες βάσεις	Σαφής σκοπός ανά πράξη επεξεργασίας, νόμιμη βάση, επιχειρησιακή ανάγκη και σχέση με το προϊόν ή την υπηρεσία.
Υποκείμενα και κατηγορίες δεδομένων	Ομάδες προσώπων, είδη προσωπικών δεδομένων, ειδικές κατηγορίες, δεδομένα παιδιών και στοιχεία αυξημένης ευαισθησίας.
Ροές, αποδέκτες και διαβιβάσεις	Πηγές δεδομένων, εσωτερικοί χρήστες, εκτελούντες την επεξεργασία, τρίτοι αποδέκτες, τόποι αποθήκευσης και διεθνείς διαβιβάσεις.
Αναγκαιότητα και αναλογικότητα	Σύνδεση κάθε δεδομένου με τον σκοπό, εναλλακτικές λύσεις, ελαχιστοποίηση, ακρίβεια, χρονικά όρια διατήρησης και ρυθμίσεις εξ ορισμού.
Διαφάνεια και δικαιώματα	Τρόπος ενημέρωσης, διαχείριση συγκατάθεσης όπου εφαρμόζεται, διαδικασίες πρόσβασης, διόρθωσης, διαγραφής, εναντίωσης και ανθρώπινης παρέμβασης.
Προσδιορισμός κινδύνων	Σενάρια μη εξουσιοδοτημένης πρόσβασης, απώλειας, υπερβολικής συλλογής, αδιαφανούς κατάρτισης προφίλ, ανακριβών συμπερασμάτων και άνισης μεταχείρισης.
Αρχική αξιολόγηση κινδύνου	Βαθμολογία πιθανότητας και σοβαρότητας, αιτιολόγηση και συνολική κατάταξη κάθε κινδύνου.
Μέτρα αντιμετώπισης	Κρυπτογράφηση, ψευδωνυμοποίηση, έλεγχοι πρόσβασης, περιορισμός σκοπού, δοκιμές ασφάλειας, έλεγχοι μεροληψίας, εκπαίδευση και συμβατικές εγγυήσεις.
Υπολειπόμενος κίνδυνος	Νέα βαθμολογία μετά την εφαρμογή μέτρων, αποδοχή κινδύνου, πρόσθετες ενέργειες και υπεύθυνος ολοκλήρωσης.
Διαβούλευση	Γνώμη DPO, απόψεις επιχειρησιακών ομάδων, εκπροσώπων υποκειμένων ή ειδικών και τεκμηρίωση των παρατηρήσεων.
Απόφαση και παρακολούθηση	Έγκριση, όροι έναρξης, δείκτες παρακολούθησης, ημερομηνία επανεξέτασης και γεγονότα που ενεργοποιούν νέα αξιολόγηση.

Πίνακας 13: Συνοπτικό παράδειγμα DPIA ηλεκτρονικού καταστήματος

Πεδίο	Ενδεικτική συμπλήρωση
Περιγραφή	Σύστημα που αναλύει ιστορικό αγορών, αλληλεπίδραση με προϊόντα και προτιμήσεις χρήστη με σκοπό εξατομικευμένες προτάσεις και προσφορές.
Σκοπός και νόμιμη βάση	Βελτίωση εμπειρίας και σχετικότητας προσφορών. Η νόμιμη βάση προσδιορίζεται ανά πράξη επεξεργασίας, με συγκατάθεση για μη αναγκαίους ιχνηλάτες και τεκμηριωμένη αξιολόγηση όπου εξετάζεται έννομο συμφέρον.
Βασικοί κίνδυνοι	Αδιαφανής κατάρτιση προφίλ, υπερβολική συλλογή, ανακριβή συμπεράσματα, άνιση διαφοροποίηση προσφορών, μη εξουσιοδοτημένη πρόσβαση και εκτεταμένη διατήρηση.
Αρχική αξιολόγηση	Πιθανότητα μέτρια έως υψηλή και σοβαρότητα μέτρια έως υψηλή, λόγω συστηματικής παρακολούθησης και δημιουργίας προφίλ.
Μέτρα μείωσης	Ελαχιστοποίηση πεδίων, ψευδωνυμοποίηση αναγνωριστικών, σαφής ενημέρωση, εύκολη εναντίωση, περιορισμένη διατήρηση, κρυπτογράφηση, έλεγχος πρόσβασης, δοκιμές ακρίβειας και ανθρώπινη εποπτεία.
Υπολειπόμενος κίνδυνος	Μέτριος μετά την εφαρμογή των μέτρων, με μηνιαία παρακολούθηση αιτημάτων και παραπόνων και εξαμηνιαία επανεξέταση του μοντέλου.
Απόφαση	Έγκριση πιλοτικής λειτουργίας με περιορισμένο σύνολο δεδομένων, τεκμηρίωση συγκατάθεσης, επανέλεγχο πριν από κλιμάκωση και συμμετοχή του DPO στην αξιολόγηση αλλαγών.

Όταν η αξιολόγηση καταλήγει σε υψηλό υπολειπόμενο κίνδυνο, η διαδικασία συνεχίζεται με προηγούμενη διαβούλευση με την αρμόδια εποπτική αρχή σύμφωνα με το άρθρο 36 του GDPR. Η DPIA παραμένει ζωντανό έγγραφο και επανεξετάζεται κατά την αλλαγή σκοπού, τεχνολογίας, κατηγοριών δεδομένων, κλίμακας ή προφίλ κινδύνου

4.4 Η πρόκληση της καινοτομίας σε ρυθμισμένο περιβάλλον

4.4.1 Σύγκρουση ανάμεσα σε καινοτομία και κανονιστική συμμόρφωση

Η ανάπτυξη των επιχειρήσεων εξαρτάται ολοένα και περισσότερο από την ικανότητα των εταιρειών να συλλέγουν, να συνδέουν και να αναλύουν δεδομένα σε

όλα τα προϊόντα, τις πλατφόρμες και τα οικοσυστήματα. Ταυτόχρονα, αυτή η λογική έντασης δεδομένων αναπτύσσεται μέσα σε ένα πυκνό κανονιστικό περιβάλλον που διαμορφώνεται από τη νομοθεσία περί απορρήτου, τη διακυβέρνηση πλατφορμών και τις αυξανόμενες προσδοκίες λογοδοσίας. Για αυτόν τον λόγο, η καινοτομία και η συμμόρφωση αναπτύσσονται πλέον σε μια σχέση συνεχούς προσαρμογής και συντονισμού. Οι Holmström και Magnusson (2025) αναλύουν αυτή τη σχέση μέσω του Πλαισίου Αξιολόγησης Κυριαρχίας Δεδομένων (Data Sovereignty Assessment Framework), το οποίο δείχνει ότι οι οργανισμοί πρέπει να εξισορροπούν τη νομική συμμόρφωση, την ιδιοκτησία και τον έλεγχο, την τοπική προσαρμογή, τα δικαιώματα και την ηθική και την ευθυγράμμιση του οικοσυστήματος, ενώ παράλληλα επιδιώκουν καινοτομία που βασίζεται σε δεδομένα. Η ανάλυσή τους είναι σημαντική επειδή αναδιατυπώνει την κυριαρχία από μια περιοριστική νομική απαίτηση σε μια στρατηγική δυνατότητα που μπορεί να επιτρέψει την καινοτομία όταν αυτή ενσωματώνεται στον σχεδιασμό διακυβέρνησης.

Αυτός ο διττός χαρακτήρας της ρύθμισης εμφανίζεται επίσης σε εταιρείες που βασίζονται σε προϊόντα και επιδιώκουν να επεκτείνουν τις ψηφιακές υπηρεσίες μέσω συνδεδεμένων συσκευών και επιχειρηματικών μοντέλων που στηρίζονται σε δεδομένα. Οι Schäfer et al. (2023) προσδιορίζουν ένα ευρύ σύνολο προκλήσεων για την προστασία της ιδιωτικής ζωής των δεδομένων που εκτείνονται από τις προσδοκίες των πελατών έως τους περιορισμούς σε επίπεδο οικοσυστήματος και τα εσωτερικά οργανωτικά εμπόδια. Η συμβολή τους είναι ιδιαίτερα χρήσιμη επειδή παρουσιάζει την ιδιωτικότητα και τις επιχειρήσεις που βασίζονται στα δεδομένα ως συμβατές όταν οι εταιρείες υιοθετούν αρχές όπως η πελατοκεντρική προστασία της ιδιωτικής ζωής, η ευθυγραμμισμένη διαχείριση κινδύνων και οι τεχνολογικά υποστηριζόμενες νομικές διαδικασίες. Από αυτή την άποψη, η συμμόρφωση δομεί την καινοτομία και υποστηρίζει τη νομιμότητα της ανάπτυξης ψηφιακών υπηρεσιών. Η πρόκληση για τη διοίκηση έγκειται στο σχεδιασμό διαδικασιών που επιτρέπουν τη συνετή ανάληψη κινδύνων, διατηρώντας παράλληλα τα δικαιώματα και τις προσδοκίες των υποκειμένων των δεδομένων.

Επιπλέον, ο Krämer (2024) δείχνει ότι οι γνωστοποιήσεις απορρήτου εφαρμογών διαμορφώνονται τόσο από τον GDPR όσο και από τους κανόνες ιδιωτικής διακυβέρνησης των καταστημάτων εφαρμογών. Οι ετικέτες απορρήτου στο Apple App

Store και το Google Play Store στοχεύουν στην απλοποίηση της διαφάνειας, ωστόσο ο σχεδιασμός τους μπορεί να μην αντανακλά επαρκώς την πλήρη συμμόρφωση με τα ευρωπαϊκά πρότυπα προστασίας δεδομένων. Αυτό σημαίνει ότι η καινοτομία στα εργαλεία γνωστοποίησης μπορεί να βελτιώσει τη χρηστικότητα, δημιουργώντας παράλληλα νέες ασάφειες συμμόρφωσης. Οι Raibulet και Wang (2025) ενισχύουν αυτήν την ανησυχία μέσω της μελέτης τους για τους Χάρτες Google, η οποία δείχνει ότι οι πολιτικές απορρήτου παραμένουν δύσκολες στην ανάγνωση και την κατανόηση για τους περισσότερους χρήστες. Το ζήτημα αφορά επομένως το χάσμα μεταξύ της νομικής μορφής, του σχεδιασμού της πλατφόρμας και της κατανόησης από τους χρήστες.

4.4.2 Η έννοια του "data ethics" στις ψηφιακές επιχειρήσεις

Καθώς οι επιχειρήσεις που βασίζονται σε δεδομένα επεκτείνουν την τεχνολογική τους ικανότητα, ο ηθικός αναστοχασμός καθίσταται απαραίτητο συστατικό του υπεύθυνου ψηφιακού μετασχηματισμού. Οι Eke και Stahl (2024) δείχνουν ότι οι τρέχουσες ευρωπαϊκές πολιτικές δεδομένων μπορούν να ερμηνευθούν ως πλαίσια που διαμορφώνονται από τα ανθρώπινα δικαιώματα, τις καθιερωμένες αρχές και την ανησυχία για τις κοινωνικές συνέπειες των ψηφιακών τεχνολογιών. Η ανάλυσή τους δείχνει ότι το κανονιστικό περιβάλλον περιέχει ήδη ισχυρό ηθικό περιεχόμενο, ακόμη και όταν η εφαρμογή παραμένει άνιση. Αυτή η διαπίστωση είναι εξαιρετικά σημαντική για τις επιχειρήσεις, επειδή σημαίνει ότι η συμμόρφωση με τους κανόνες διακυβέρνησης δεδομένων φέρει μια έμμεση ηθική διάσταση που περιλαμβάνει αξιοπρέπεια, δικαιοσύνη, αυτονομία και κοινωνική ευθύνη.

Οι Fülöp, Ionescu και Topor (2025) εμβαθύνουν περαιτέρω, εξετάζοντας τα ηθικά διλήμματα που συνοδεύουν την ψηφιακή μετάβαση στις επιχειρήσεις. Η συστηματική τους ανασκόπηση δείχνει ότι η ψηφιοποίηση απαιτεί από τις εταιρείες να επανεξετάσουν τα επιχειρηματικά μοντέλα, τις εσωτερικές διαδικασίες, τις σχέσεις με τα ενδιαφερόμενα μέρη και τις προτάσεις αξίας με τρόπους που παραμένουν ευθυγραμμισμένοι με τις ηθικές προσδοκίες. Η ηθική των δεδομένων, επομένως, εκτείνεται πέρα από την τυπική νομιμότητα και εισέρχεται στα πεδία της οργανωτικής κρίσης, της τεχνολογικής ευθύνης και του στρατηγικού προσανατολισμού. Στην πράξη, οι ηθικές ψηφιακές επιχειρήσεις περιλαμβάνουν ενεργό στοχασμό σχετικά με το πώς

οι τεχνολογίες διαμορφώνουν τα συμφέροντα των πελατών, των εργαζομένων, των συνεργατών και της κοινωνίας.

Ένα πιο εφαρμοσμένο μοντέλο προσφέρεται από τους Tiron Tudor και Deliu (2026), οι οποίοι αναπτύσσουν ένα πλαίσιο λήψης αποφάσεων για την Εταιρική Ψηφιακή Ευθύνη για οργανισμούς παροχής υπηρεσιών. Το πλαίσιο τους δίνει έμφαση στη διαφάνεια, την λογοδοσία, τη δικαιοσύνη και τη βιωσιμότητα ως πυλώνες που μπορούν να ενσωματωθούν προοδευτικά σε όλα τα τμήματα και τις λειτουργίες των επιχειρήσεων. Αυτή η έρευνα είναι ιδιαίτερα σημαντική, επειδή δείχνει πώς η ψηφιακή ευθύνη γίνεται μέρος της διαχειριστικής επιλογής, της κατανομής πόρων και της θεσμικής κουλτούρας. Υπό αυτή την έννοια, η ηθική των δεδομένων υποστηρίζει την καινοτομία ενισχύοντας την ανθεκτικότητα, την εμπιστοσύνη των ενδιαφερόμενων μερών και τη μακροπρόθεσμη νομιμότητα.

Η περίπτωση της Meta καταδεικνύει γιατί αυτή η ηθική διάσταση έχει σημασία. Η Daza Ramírez (2025) υποστηρίζει ότι οι πρακτικές απορρήτου της Meta στο Facebook αποκαλύπτουν τη διαρκή ένταση μεταξύ της συμμόρφωσης και της εκμετάλλευσης των δεδομένων χρηστών με βάση τη διαφήμιση. Η μελέτη υποδηλώνει ότι η ηθική αριστεία απαιτεί έναν βαθύτερο αναπροσανατολισμό πέρα από τη νομιμότητα και τη διαχείριση της φήμης. Με αυτήν την έννοια, ένας ισχυρότερος προσανατολισμός προς την ανθρώπινη ευημερία και την ουσιαστική κοινωνική αλληλεπίδραση μπορεί να ευθυγραμμίσει τους επιχειρηματικούς στόχους της πλατφόρμας με τον σεβασμό στην ιδιωτικότητα.

4.4.3 Βέλτιστες πρακτικές

Οι βέλτιστες πρακτικές προκύπτουν όταν οι οργανισμοί συνδυάζουν τη συμμόρφωση με την προστασία της ιδιωτικής ζωής, τον ηθικό προσανατολισμό και την προσαρμογή σε συγκεκριμένες πλατφόρμες. Η Google προσφέρει μια χαρακτηριστική περίπτωση επειδή οι υπηρεσίες της βασίζονται σε μεγάλο βαθμό στη συνεχή συλλογή δεδομένων σε όλα τα περιβάλλοντα χρηστών. Οι Krämer (2024) και Raibulet και Wang (2025) δείχνουν ότι τα οικοσυστήματα που σχετίζονται με την Google αποκαλύπτουν τόσο την αξία όσο και τους περιορισμούς των γνωστοποιήσεων απορρήτου. Η αποτελεσματική πρακτική απαιτεί μεγαλύτερη σαφήνεια, επαλήθευση και

αναγνωσιμότητα, έτσι ώστε η διαφάνεια να υποστηρίζει την ενημερωμένη χρήση παρά τη συμβολική συμμόρφωση.

Η Apple παρέχει ένα διαφορετικό μοντέλο μέσω της Διαφάνειας Παρακολούθησης Εφαρμογών (App Tracking Transparency). Ο Krämer (2026) δείχνει ότι το πλαίσιο της Apple μείωσε ορισμένους κινδύνους που σχετίζονται με την παρακολούθηση και μετέτρεψε τις πρακτικές συναίνεσης σε ολόκληρη την αγορά των κινητών. Ταυτόχρονα, επέκτεινε την εξουσία της Apple να ορίζει πρότυπα προστασίας της ιδιωτικής ζωής εντός ενός αυστηρά ελεγχόμενου οικοσυστήματος. Αυτή η περίπτωση καταδεικνύει ότι η ιδιωτική διακυβέρνηση μπορεί να επιταχύνει την προστασία της ιδιωτικής ζωής, ενώ παράλληλα αναδιαμορφώνει τον ανταγωνισμό και τις σχέσεις εξάρτησης. Η βέλτιστη πρακτική περιλαμβάνει, επομένως, την επίγνωση του πώς η ηγεσία στην προστασία της ιδιωτικής ζωής επηρεάζει την ευρύτερη δομή της αγοράς.

Οι ελληνικές εταιρείες παρέχουν μια πρόσθετη εφαρμοσμένη προοπτική. Οι Kareklas, Michalopoulou και Giannakopoulou (2024) δείχνουν ότι η εφαρμογή του GDPR στις ελληνικές επιχειρήσεις περιλάμβανε τεχνολογικές, νομικές και οργανωτικές αλλαγές, σημαντικό κόστος και έντονη ανάγκη για καθοδήγηση από τις αρμόδιες αρχές. Τα ευρήματά τους υπογραμμίζουν τον στρατηγικό ρόλο του Υπεύθυνου Προστασίας Δεδομένων και τη σημασία της ενσωμάτωσης της συμμόρφωσης στις οργανωτικές διαδικασίες.

Οι Holmström και Magnusson (2025) δείχνουν ότι η καινοτομία αποδίδει περισσότερο όταν οι οργανισμοί αξιολογούν συστηματικά την κυριαρχία των δεδομένων και συντονίζουν νομικές, τεχνολογικές και επιχειρησιακές λειτουργίες. Με παρόμοιο τρόπο, οι Schäfer et al. (2023) υπογραμμίζουν ότι οι πρακτικές προστασίας δεδομένων γίνονται αποτελεσματικότερες όταν οι νομικές υπηρεσίες, οι τεχνολογικές ομάδες και οι υπεύθυνοι ανάπτυξης προϊόντων εργάζονται μέσα από κοινές διαδικασίες. Έτσι, η επιτυχημένη καινοτομία σε ρυθμιζόμενο περιβάλλον στηρίζεται στην έγκαιρη ενσωμάτωση της ιδιωτικότητας, στη σύνδεση του ηθικού προβληματισμού με τον σχεδιασμό και στη λειτουργία της συμμόρφωσης ως μοχλού υπεύθυνης ανάπτυξης, εμπιστοσύνης των πελατών και διαρκούς ανταγωνιστικότητας και ισχυρότερης θεσμικής και οργανωσιακής αξιοπιστίας.

5. Σύγχρονες προκλήσεις και προοπτικές

Το Κεφάλαιο 5 μετακινεί τη συζήτηση από τις στρατηγικές και επιχειρησιακές επιπτώσεις της προστασίας δεδομένων στις αναδυόμενες προκλήσεις που καθορίζουν το μέλλον των ψηφιακών επιχειρήσεων. Ενώ το προηγούμενο κεφάλαιο έδειξε ότι η ιδιωτικότητα μπορεί να υποστηρίξει την εμπιστοσύνη, την ανταγωνιστικότητα και την οργανωτική ανθεκτικότητα, το παρόν κεφάλαιο εξετάζει πώς αυτή η σχέση αναδιαμορφώνεται από την τεχνητή νοημοσύνη, την ανάλυση μεγάλων δεδομένων, τις υποδομές cloud, τις διασυνοριακές ροές δεδομένων, τις εξελισσόμενες ηθικές ανησυχίες και τις νέες προσδοκίες διακυβέρνησης. Εξετάζει επίσης τις θεσμικές και διαχειριστικές συνθήκες που υποστηρίζουν τη βιώσιμη επιχειρηματική ανάπτυξη σε ένα περιβάλλον δεδομένων με αυστηρή ρύθμιση. Με αυτόν τον τρόπο, το Κεφάλαιο 5 επεκτείνει την ανάλυση από την προσαρμογή σε επίπεδο επιχείρησης στους ευρύτερους νομικούς, τεχνολογικούς και κοινωνικούς μετασχηματισμούς που επηρεάζουν τη σύγχρονη προστασία των καταναλωτών και την επιχειρηματική ανάπτυξη.

5.1 Νέες τάσεις και ρυθμιστικές εξελίξεις

5.1.1 Τεχνητή νοημοσύνη και αυτόματη λήψη αποφάσεων

Η τεχνητή νοημοσύνη έχει γίνει ένας από τους σημαντικότερους μοχλούς του ψηφιακού μετασχηματισμού των επιχειρήσεων, ωστόσο η επέκτασή της εντείνει επίσης την κανονιστική ανησυχία σχετικά με την αυτοματοποιημένη λήψη αποφάσεων, την αδιαφάνεια και την έλλειψη δικαιοσύνης. Η αλληλεπίδραση μεταξύ του GDPR και του Νόμου της ΕΕ για την Τεχνητή Νοημοσύνη καταδεικνύει αυτή τη νέα φάση ρύθμισης, στην οποία η συμμόρφωση εκτείνεται πέρα από τις παραδοσιακές υποχρεώσεις απορρήτου και ενσωματώνει όλο και περισσότερο τη διακυβέρνηση του συστημικού κινδύνου. Οι Hohmann και Kollár (2025) εξηγούν ότι ο Κανονισμός (ΕΕ) 2024/1689 για την Τεχνητή Νοημοσύνη εισάγει ένα συμπληρωματικό αλλά αυστηρότερο επίπεδο για την επεξεργασία που βασίζεται στην Τεχνητή Νοημοσύνη, ειδικά για συστήματα υψηλού κινδύνου. Η ανάλυσή τους δείχνει ότι ο Νόμος ενισχύει τις απαιτήσεις που σχετίζονται με την αξιολόγηση κινδύνου, την ανθρώπινη εποπτεία, την τεκμηρίωση και τη διακυβέρνηση δεδομένων, ευθυγραμμίζοντας έτσι την

καινοτομία με την ευρύτερη προστασία της διαφάνειας, της δικαιοσύνης και της λογοδοσίας. Στην πράξη, το νομικό περιβάλλον για την Τεχνητή Νοημοσύνη δεν αφορά πλέον μόνο την επεξεργασία δεδομένων, αλλά και την αρχιτεκτονική των συστημάτων αποφάσεων και τις θεσμικές συνθήκες υπό τις οποίες λειτουργούν.

Αυτή η ευρύτερη προοπτική που βασίζεται στα δικαιώματα αναπτύσσεται περαιτέρω από τους Thomaidou και Limniotis (2025), οι οποίοι εξετάζουν την αλληλεπίδραση μεταξύ του νόμου περί προστασίας δεδομένων και της Εκτίμησης Επιπτώσεων στα Θεμελιώδη Δικαιώματα (Fundamental Rights Impact Assessment). Η εν λόγω έρευνα είναι ιδιαίτερα σημαντική επειδή προτείνει ένα ολοκληρωμένο μοντέλο που συνδυάζει την Εκτίμηση Επιπτώσεων στην Προστασία Δεδομένων με μια ευρύτερη αξιολόγηση των συστημάτων Τεχνητής Νοημοσύνης με επίκεντρο τα δικαιώματα. Μια τέτοια προσέγγιση αναγνωρίζει ότι οι κίνδυνοι της αυτοματοποιημένης λήψης αποφάσεων εκτείνονται πέρα από την ιδιωτικότητα, σε τομείς όπως οι διακρίσεις, η αυτονομία, οι διαδικαστικές εγγυήσεις και η κοινωνική συμμετοχή.

Οι Wulf και Seizov (2024) προσθέτουν μια σημαντική εμπειρική διάσταση, δείχνοντας ότι οι τρέχουσες γνωστοποιήσεις Τεχνητής Νοημοσύνης που επιβάλλονται από τον GDPR παραμένουν ασαφείς, ασυνεπείς και ανεπαρκείς για τις προσδοκίες των υποκειμένων των δεδομένων. Η μελέτη τους καταδεικνύει ότι το δικαίωμα ενημέρωσης σχετικά με την αυτοματοποιημένη επεξεργασία παραμένει περιορισμένο στην πράξη, επειδή οι γνωστοποιήσεις συχνά στερούνται σαφήνειας και ουσιαστικής εξήγησης. Συνολικά, αυτές οι μελέτες δείχνουν ότι η ρύθμιση της Τεχνητής Νοημοσύνης κινείται προς ένα πιο ολοκληρωμένο μοντέλο λογοδοσίας, στο οποίο ο τεχνικός σχεδιασμός, η νομική γνωστοποίηση και η αξιολόγηση των ανθρωπίνων δικαιωμάτων πρέπει να λειτουργούν από κοινού. Αυτή η πορεία υποδηλώνει ότι η μελλοντική διακυβέρνηση της Τεχνητής Νοημοσύνης θα ανταμείβει ολοένα και περισσότερο τις εταιρείες που συνδυάζουν τον νόμιμο αυτοματισμό με την εξηγησιμότητα, τη διαδικαστική πειθαρχία και τον αποδεδειγμένο σεβασμό των ατομικών δικαιωμάτων σε όλο τον κύκλο λήψης αποφάσεων.

Η εστίαση του AI Act στην αυτοματοποιημένη λήψη αποφάσεων στηρίζεται σε προσέγγιση βάσει κινδύνου. Ο Κανονισμός διακρίνει απαγορευμένες πρακτικές, συστήματα υψηλού κινδύνου, συστήματα που υπάγονται σε ειδικές υποχρεώσεις

διαφάνειας και εφαρμογές ελάχιστου κινδύνου. Η ταξινόμηση εξαρτάται κυρίως από τον σκοπό και το πλαίσιο χρήσης και από τη δυνατότητα του συστήματος να επηρεάζει την υγεία, την ασφάλεια ή τα θεμελιώδη δικαιώματα. Για την προστασία του καταναλωτή ιδιαίτερη σημασία έχουν οι εφαρμογές που καθορίζουν πρόσβαση σε πιστώσεις, ασφάλιση υγείας ή ζωής και άλλες ουσιώδεις υπηρεσίες, καθώς και τα συστήματα που διαμορφώνουν επιλογές μέσω εξατομικευμένων συστάσεων ή αλληλεπίδρασης με ψηφιακούς βοηθούς (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2024).

Η σχέση του AI Act με το άρθρο 22 του GDPR είναι συμπληρωματική. Ο GDPR κατοχυρώνει εγγυήσεις για το φυσικό πρόσωπο όταν μια απόφαση βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία και παράγει έννομα ή αντίστοιχα σημαντικά αποτελέσματα. Οι εγγυήσεις περιλαμβάνουν ενημέρωση για τη λογική και τις συνέπειες της επεξεργασίας, δυνατότητα ανθρώπινης παρέμβασης, έκφραση άποψης και αμφισβήτηση του αποτελέσματος. Το AI Act οργανώνει παράλληλα τη διακυβέρνηση του ίδιου του συστήματος μέσω διαχείρισης κινδύνων, ποιοτικής διακυβέρνησης δεδομένων, τεχνικής τεκμηρίωσης, καταγραφής συμβάντων, ακρίβειας, κυβερνοασφάλειας και αποτελεσματικής ανθρώπινης εποπτείας. Η κοινή εφαρμογή των δύο Κανονισμών μεταφέρει τη λογοδοσία από το τελικό αποτέλεσμα σε ολόκληρο τον κύκλο ζωής του συστήματος (European Data Protection Board, 2018· Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2024).

Η ανθρώπινη εποπτεία αποκτά ουσιαστικό χαρακτήρα όταν ο αρμόδιος διαθέτει επαρκή κατάρτιση, θεσμική εξουσία και τεχνική δυνατότητα να ερμηνεύσει, να παρακάμψει, να αντιστρέψει ή να διακόψει το αποτέλεσμα του συστήματος. Η οργανωτική διαδικασία χρειάζεται να περιορίζει τη μεροληψία αυτοματοποίησης, δηλαδή την τάση άκριτης αποδοχής της αλγοριθμικής πρότασης. Για τον σκοπό αυτό, η επιχείρηση ορίζει σαφή κριτήρια κλιμάκωσης σε άνθρωπο, τεκμηριώνει την αιτιολογία της τελικής απόφασης και παρακολουθεί τη συχνότητα με την οποία οι ανθρώπινοι αξιολογητές επιβεβαιώνουν ή μεταβάλλουν τις συστάσεις του συστήματος.

Για συστήματα υψηλού κινδύνου του Παραρτήματος ΙΙΙ, η ενημέρωση του φυσικού προσώπου ότι η απόφαση λαμβάνεται ή υποστηρίζεται από Τεχνητή Νοημοσύνη αποτελεί κρίσιμο στοιχείο διαφάνειας. Σε συγκεκριμένες περιπτώσεις, όπως η αξιολόγηση πιστοληπτικής ικανότητας και η τιμολόγηση ασφάλισης υγείας ή

ζωής, ο φορέας εφαρμογής πραγματοποιεί Εκτίμηση Επιπτώσεων στα Θεμελιώδη Δικαιώματα. Όπου η επεξεργασία προσωπικών δεδομένων δημιουργεί υψηλό κίνδυνο, η εκτίμηση αυτή συμπληρώνει την DPIA του άρθρου 35 του GDPR. Η συνδυασμένη αξιολόγηση καλύπτει ιδιωτικότητα, ισότητα, αποτελεσματική προσφυγή, οικονομικό αποκλεισμό, ανθρώπινη αυτονομία και επιπτώσεις σε ευάλωτες ομάδες.

Η πρώτη ετήσια επανεξέταση της Ευρωπαϊκής Επιτροπής το 2026 διατήρησε ως βασικό σημείο αναφοράς τις υφιστάμενες κατηγορίες υψηλού κινδύνου και ανέδειξε πεδία για συνεχή παρακολούθηση, όπως η είσπραξη οφειλών, η πρόσβαση σε ουσιώδεις ιδιωτικές υπηρεσίες και ορισμένες μορφές ψηφιακής αλληλεπίδρασης με ευάλωτους καταναλωτές. Η εξέλιξη αυτή υπογραμμίζει τη σημασία ενός δυναμικού μητρώου χρήσεων Τεχνητής Νοημοσύνης και περιοδικής επανεκτίμησης της ταξινόμησης κάθε συστήματος (European Commission, 2026).

Εξάλλου, τα ακόλουθα σενάρια αποτυπώνουν τον τρόπο με τον οποίο η ίδια τεχνολογία μπορεί να δημιουργεί διαφορετική κανονιστική και επιχειρησιακή έκθεση ανάλογα με τον σκοπό, τα δεδομένα, την ομάδα που επηρεάζεται και τη βαρύτητα της απόφασης. Η ανάλυση κάθε χρήσης προηγείται της προμήθειας ή ανάπτυξης του συστήματος και επικαιροποιείται σε κάθε ουσιώδη μεταβολή.

Πίνακας 14: Σενάρια εφαρμογής Τεχνητής Νοημοσύνης και απαιτούμενες εγγυήσεις

Σενάριο	Κανονιστική κατάταξη	Κύριοι κίνδυνοι	Προτεινόμενες εγγυήσεις
Αυτοματοποιημένη αξιολόγηση αίτησης καταναλωτικού δανείου	Υψηλού κινδύνου κατά το Παράρτημα ΙΙΙ για πιστοληπτική ικανότητα. Παράλληλη εφαρμογή του άρθρου 22 GDPR όταν η απόφαση είναι αποκλειστικά αυτοματοποιημένη και σημαντική.	Οικονομικός αποκλεισμός, έμμεσες διακρίσεις, αδιαφανής απόρριψη και ανακριβή δεδομένα.	DPIA και FRIA, ανθρώπινη επανεξέταση, κατανοητή αιτιολόγηση, διαδικασία ένστασης, έλεγχοι ισότητας και ποιότητας δεδομένων.
Κατάταξη βιογραφικών και επιλογή υποψηφίων	Υψηλού κινδύνου κατά το Παράρτημα ΙΙΙ για πρόσληψη και επιλογή προσωπικού.	Αναπαραγωγή ιστορικών ανισοτήτων, αποκλεισμός ομάδων και υπερβολική	Αντιπροσωπευτικά δεδομένα, δοκιμές μεροληψίας, ουσιαστική ανθρώπινη αξιολόγηση,

Σενάριο	Κανονιστική κατάταξη	Κύριοι κίνδυνοι	Προτεινόμενες εγγυήσεις
		εξάρτηση από τη βαθμολογία.	ενημέρωση υποψηφίων, τεκμηρίωση κριτηρίων και προσφυγή.
Αξιολόγηση κινδύνου και τιμολόγηση ασφάλισης υγείας ή ζωής	Υψηλού κινδύνου κατά το Παράρτημα ΙΙΙ. Αυξημένη προστασία όταν χρησιμοποιούνται δεδομένα υγείας ή συναφή συμπεράσματα.	Διακρίσεις, δυσανάλογη τιμολόγηση, αποκάλυψη ευαίσθητων χαρακτηριστικών και περιορισμός πρόσβασης.	FRIA, DPIA, ελαχιστοποίηση δεδομένων, έλεγχος αναλογικότητας, περιοδική επαλήθευση ακρίβειας, ανθρώπινη αναθεώρηση και σαφής αιτιολογία.
Chatbot εξυπηρέτησης και σύστημα προτάσεων προϊόντων	Υποχρεώσεις διαφάνειας κατά το άρθρο 50. Η ταξινόμηση αυστηροποιείται όταν το σύστημα επηρεάζει ουσιωδώς αποφάσεις ή αξιοποιεί χειριστικές τεχνικές.	Σύγχυση ως προς την ανθρώπινη ή μηχανική ταυτότητα, ακατάλληλες συμβουλές, υπερβολική εξατομίκευση και έκθεση ευάλωτων χρηστών.	Σαφής γνωστοποίηση αλληλεπίδρασης με AI, δυνατότητα μετάβασης σε άνθρωπο, όρια στις συμβουλές, έλεγχος περιεχομένου, προστασία ανηλίκων και καταγραφή παραπόνων.
Δυναμική εξατομίκευση προσφορών και τιμών	Η κανονιστική αξιολόγηση εξαρτάται από το αποτέλεσμα και τον τρόπο επιρροής. Οι χειριστικές ή εκμεταλλευτικές πρακτικές που προκαλούν σημαντική βλάβη εμπίπτουν στις απαγορεύσεις του άρθρου 5.	Αθέμιτη διαφοροποίηση, αξιοποίηση κοινωνικής ή οικονομικής ευαλωτότητας, περιορισμός ενημερωμένης επιλογής και απώλεια εμπιστοσύνης.	Κανόνες δίκαιης τιμολόγησης, απαγόρευση χρήσης ευαίσθητων χαρακτηριστικών, έλεγχος ευάλωτων ομάδων, διαφάνεια παραμέτρων και ανεξάρτητος έλεγχος επιπτώσεων.

5.1.2 Big Data analytics και προφίλ καταναλωτών

Η ραγδαία ανάπτυξη της ανάλυσης μεγάλων δεδομένων έχει μεταμορφώσει τη μελέτη και τη διαχείριση της καταναλωτικής συμπεριφοράς. Τεράστιοι όγκοι δομημένων και μη δομημένων δεδομένων επιτρέπουν πλέον στις εταιρείες να μοντελοποιούν τις προτιμήσεις, να προβλέπουν αποφάσεις, να εξατομικεύουν την

επικοινωνία και να βελτιστοποιούν τις στρατηγικές τιμολόγησης και προώθησης με πρωτοφανή ακρίβεια. Οι Liu et al. (2026) δείχνουν μέσω μιας συστηματικής ανασκόπησης ότι τα μεγάλα δεδομένα χρησιμοποιούνται ευρέως για την ανάλυση καταναλωτικών προτύπων, συναισθημάτων και μηχανισμών λήψης αποφάσεων, συνδυάζοντας προηγμένες αναλυτικές μεθόδους με ερωτήματα έρευνας συμπεριφοράς. Τα ευρήματά τους δείχνουν επίσης ότι η ποιότητα των δεδομένων, η αλγοριθμική ερμηνευσιμότητα και η προστασία της ιδιωτικής ζωής παραμένουν κεντρικές ανησυχίες. Αυτό το σημείο είναι κρίσιμο επειδή δείχνει ότι η αξία των μεγάλων δεδομένων είναι άρρηκτα συνδεδεμένη με τις συνθήκες υπό τις οποίες συλλέγονται, ερμηνεύονται και εφαρμόζονται στην εμπορική πρακτική.

Οι κανονιστικές επιπτώσεις γίνονται πιο ορατές στο πλαίσιο της ηλεκτρονικής παρακολούθησης. Οι Miller, Lukic και Skiera (2026) διαπιστώνουν ότι ο GDPR οδήγησε σε μείωση των τεχνολογιών παρακολούθησης που χρησιμοποιούν οι ιστοσελίδες και οι ψηφιακές πλατφόρμες στην Ευρωπαϊκή Ένωση, περιορίζοντας ιδιαίτερα τις πιο παρεμβατικές πρακτικές ως προς την ιδιωτικότητα. Αυτό το αποτέλεσμα υποδηλώνει ότι η ρύθμιση μπορεί να αναδιαμορφώσει την τεχνική υποδομή μέσω της οποίας πραγματοποιείται η δημιουργία προφίλ καταναλωτών, ακόμη και αν δεν εξαλείψει εντελώς την παρακολούθηση. Οι επιπτώσεις είναι ιδιαίτερα σημαντικές για τις εταιρείες που βασίζονται στην εξατομικευμένη διαφήμιση, επειδή η δημιουργία προφίλ λειτουργεί πλέον σε ένα πιο περιορισμένο περιβάλλον συναίνεσης, διαφάνειας και λογοδοσίας.

Οι Leijten και van der Hof (2025) επεκτείνουν αυτήν τη συζήτηση εστιάζοντας στην εμπορική δημιουργία προφίλ ανηλίκων. Η ανάλυσή τους δείχνει ότι η δημιουργία προφίλ ανηλίκων για εμπορικούς σκοπούς εγείρει σοβαρές ανησυχίες που βασίζονται στα δικαιώματα και απαιτεί μια προληπτική κανονιστική προσέγγιση. Η μελέτη είναι ιδιαίτερα σημαντική επειδή εισάγει μια ουσιαστική ταξινόμηση των πρακτικών δημιουργίας προφίλ, ενώ παράλληλα τονίζει ότι ο GDPR, ο Νόμος περί Ψηφιακών Υπηρεσιών και ο Νόμος περί Τεχνητής Νοημοσύνης πρέπει να ερμηνεύονται από κοινού όταν πρόκειται για ευάλωτες ομάδες.

5.1.3 Cloud computing και διεθνείς μεταφορές δεδομένων

Το cloud computing αντιπροσωπεύει μια ακόμη καθοριστική τάση στον ψηφιακό μετασχηματισμό, επειδή επιτρέπει την επεκτασιμότητα, την οικονομική αποδοτικότητα, την απομακρυσμένη πρόσβαση και την εντατική επεξεργασία δεδομένων πέρα από τα οργανωτικά και γεωγραφικά όρια των επιχειρήσεων. Ωστόσο, δημιουργεί επίσης νέες κανονιστικές προκλήσεις που σχετίζονται με την ασφάλεια, την εξάρτηση, τη συγκέντρωση και τις διασυνοριακές μεταφορές δεδομένων. Ο Christakis (2024) αποτυπώνει αυτό το εξελισσόμενο τοπίο μέσω της έννοιας της ελεύθερης ροής δεδομένων με εμπιστοσύνη, τονίζοντας ότι η παγκόσμια κινητικότητα δεδομένων εξαρτάται πλέον από την κανονιστική αξιοπιστία και τις θεσμικές διασφαλίσεις. Οι διασυνοριακές μεταφορές έχουν γίνει στρατηγικό ζήτημα, επειδή οι εταιρείες λειτουργούν σε ένα κατακερματισμένο διεθνές περιβάλλον στο οποίο διαφορετικές δικαιοδοσίες εφαρμόζουν διαφορετικά πρότυπα για την πρόσβαση, την αποθήκευση και τη νόμιμη επεξεργασία των δεδομένων.

Ένα πιο συγκεκριμένο παράδειγμα εμφανίζεται στους Chan και Toh (2025), οι οποίοι αναλύουν τις ρήτρες διεθνούς μεταφοράς δεδομένων στις πολιτικές απορρήτου των smartwatch. Η μελέτη τους δείχνει ότι οι όροι που διέπουν τη μεταφορά, την αποθήκευση και τη χρήση φορητών δεδομένων συχνά παραμένουν ασαφείς ή ασυνεπείς, περιορίζοντας την κατανόηση των χρηστών και αποδυναμώνοντας την λογοδοσία. Αυτό το εύρημα είναι σημαντικό επειδή αποκαλύπτει ότι ο κίνδυνος διεθνούς μεταφοράς δεν είναι μόνο θέμα υποδομής, αλλά και επικοινωνίας και συμβατικού σχεδιασμού.

Ο Kun (2024) εξετάζει παρόμοιες περιπτώσεις στον χρηματοπιστωτικό τομέα, όπου η αυξανόμενη χρήση υπηρεσιών cloud έχει μετατοπίσει τη ρύθμιση από τον λειτουργικό κίνδυνο στον συστημικό κίνδυνο. Σύμφωνα με τον Νόμο για την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα (Digital Operational Resilience Act), η εποπτεία ασχολείται ολοένα και περισσότερο με τη συγκέντρωση, την ανθεκτικότητα και τον συντονισμό πολλαπλών ρυθμιστικών αρχών. Οι Xu και Zuo (2026) παρέχουν ένα ευρύτερο πλαίσιο σε επίπεδο εταιρείας, προσδιορίζοντας τρεις κύριες διαστάσεις του διασυνοριακού κινδύνου δεδομένων, δηλαδή την κανονιστική πολυπλοκότητα, την ασφάλεια και το απόρρητο των δεδομένων και τη συνέχεια της επιχείρησης. Η εργασία τους δείχνει ότι οι εταιρείες χρειάζονται πρακτικά εργαλεία για να ανταποκριθούν στις

απαιτήσεις των σύγχρονων κατακερματισμένων περιβαλλόντων δεδομένων. Συνολικά, το cloud computing και οι διεθνείς μεταφορές δεδομένων καταδεικνύουν πώς η ψηφιακή ανάπτυξη εξαρτάται πλέον από την ικανότητα διαχείρισης του νομικού κατακερματισμού, της τεχνικής ευπάθειας και της θεσμικής εμπιστοσύνης εντός ενός ενιαίου στρατηγικού πλαισίου.

5.2 Ηθικά διλήμματα και κοινωνικές επιπτώσεις

5.2.1 Όρια στην επεξεργασία ευαίσθητων δεδομένων

Η επέκταση των επιχειρήσεων που βασίζονται σε δεδομένα έχει εντείνει τη χρήση δεδομένων υγείας και άλλων ευαίσθητων δεδομένων, δημιουργώντας ευκαιρίες για καινοτομία, ενώ παράλληλα εγείρει ηθικές και κοινωνικές ανησυχίες. Τα δεδομένα υγείας είναι ιδιαίτερα σημαντικά επειδή μπορούν να υποστηρίξουν την έρευνα, την ιατρική ακριβείας και καλύτερες δημόσιες υπηρεσίες, ωστόσο εκθέτουν επίσης τα άτομα σε κινδύνους διακρίσεων, επιτήρησης, αποκλεισμού και απώλειας αξιοπρέπειας. Οι Quinn, Ellyne και Yao (2024) δείχνουν ότι ο Ευρωπαϊκός Χώρος Δεδομένων Υγείας (European Health Data Space) στοχεύει στη διευκόλυνση της δευτερογενούς χρήσης δεδομένων υγείας μέσω Φορέων Πρόσβασης σε Δεδομένα Υγείας, αλλά αυτή η φιλοδοξία παραμένει περιορισμένη από τον GDPR, ειδικά όταν εμπλέκονται χρήσεις με εμπορικό προσανατολισμό. Η ανάλυσή τους υπογραμμίζει ότι η νόμιμη πρόσβαση εξαρτάται από έγκυρες νομικές βάσεις, ελαχιστοποίηση δεδομένων, περιορισμό αποθήκευσης και προσεκτική αξιολόγηση συμβατότητας. Αυτό σημαίνει ότι η καινοτομία στην κοινή χρήση δεδομένων υγείας είναι ηθικά αποδεκτή μόνο όταν υπάρχουν λογικές δημόσιου συμφέροντος και ισχυρές νομικές εγγυήσεις.

Οι Rodríguez Mejías et al. (2024) ενισχύουν αυτή τη θέση εξετάζοντας την ασφαλή υποδομή δεδομένων IMPaCT για ηλεκτρονικά αρχεία υγείας στην έρευνα για την ιατρική ακριβείας. Η μελέτη τους δείχνει ότι η βιωσιμότητα των χώρων δεδομένων υγείας εξαρτάται από ασφαλή περιβάλλοντα επεξεργασίας, ισχυρούς οργανωτικούς ρόλους και τεχνικές διασφαλίσεις που διατηρούν το εμπιστευτικό καθήκον φροντίδας των δημόσιων αρχών. Συνεπώς, η επεξεργασία ευαίσθητων δεδομένων απαιτεί μια λογική διακυβέρνησης που συνδέει το δημόσιο όφελος με τη διαλειτουργικότητα, τη λογοδοσία και την ασφάλεια. Το ζήτημα αφορά μεν τη συμμόρφωση, αλλά και τη

νομιμότητα της χρήσης δευτερογενών δεδομένων σε τομείς όπου οι πληροφορίες είναι προσωπικές.

Περαιτέρω ενδείξεις αυτών των ορίων εμφανίζονται στην επαγγελματική πρακτική. Οι İyigün και Ergene (2026) δείχνουν ότι πολλοί καρδιολόγοι δεν έχουν επίσημη εκπαίδευση στην προστασία δεδομένων, χρησιμοποιούν μη ασφαλείς πλατφόρμες για τη μετάδοση δεδομένων και έχουν περιορισμένη επίγνωση της ανωνυμοποίησης και των νομικών απαιτήσεων. Τα ευρήματά τους καταδεικνύουν ένα σοβαρό χάσμα μεταξύ των νομικών κανόνων και της καθημερινής διαχείρισης των προσωπικών δεδομένων υγείας. Αυτό το χάσμα δημιουργεί κίνδυνο για την ιδιωτικότητα για τους ασθενείς, ενώ παράλληλα αποδυναμώνει την εμπιστοσύνη στα ψηφιακά συστήματα υγείας. Συνολικά, οι μελέτες αυτές αναδεικνύουν ότι η επεξεργασία ευαίσθητων δεδομένων χρειάζεται να οργανώνεται μέσα σε σαφές κανονιστικό πλαίσιο, με ασφαλείς υποδομές, ισχυρή θεσμική επάρκεια και σταθερή μέριμνα για την προστασία των ευάλωτων ατόμων.

5.2.2 Η ισορροπία μεταξύ προστασίας της ιδιωτικότητας και επιχειρηματικής αξιοποίησης των δεδομένων

Ένα δεύτερο ηθικό δίλημμα αφορά τη σχέση μεταξύ της ιδιωτικότητας και της δημιουργίας εμπορικής αξίας. Οι εταιρείες βασίζονται ολοένα και περισσότερο σε ψηφιακά αποτυπώματα, δεδομένα συμπεριφοράς και προγνωστικά αναλυτικά στοιχεία για τη βελτιστοποίηση των προϊόντων, την εξατομίκευση της επικοινωνίας και την επέκταση των επιχειρηματικών ευκαιριών. Ωστόσο, αυτή η επιχειρηματική λογική διατηρεί την κοινωνική της νομιμοποίηση μόνο όταν συνοδεύεται από ουσιαστική προστασία των ατόμων, διαφάνεια και σεβασμό των δικαιωμάτων τους. Οι Ayaz, Hosseini Tabaghdehi, Rosli και Tambay (2025) εξετάζουν αυτήν την πρόκληση από την οπτική γωνία των μικρών και μεσαίων επιχειρήσεων και υποστηρίζουν ότι η διαχείριση του ψηφιακού αποτυπώματος θα πρέπει να προσεγγίζεται ως μια διπλή διαδικασία δημιουργίας επιχειρηματικής αξίας και προστασίας της κοινωνικής αξίας. Το πλαίσιό τους δίνει έμφαση στη διαφάνεια, την προστασία δεδομένων, το απόρρητο δεδομένων και τον μετασχηματισμό δεδομένων, υποστηριζόμενο από τη συμμετοχή των ενδιαφερόμενων μερών. Αυτή η οπτική είναι σημαντική επειδή ορίζει την ιδιωτικότητα ως προϋπόθεση για την ηθική επιχειρηματικότητα και όχι ως εμπόδιο στην ανάπτυξη.

Οι Ervits και Maintz (2025) προσθέτουν μια σημαντική οπτική από την πλευρά των καταναλωτών, δείχνοντας ότι οι χρήστες συστημάτων ευφυών οχημάτων είναι συχνά πρόθυμοι να ανταλλάξουν προσωπικά δεδομένα για λόγους ευκολίας. Τα αποτελέσματά τους αποκαλύπτουν ότι η αντιληπτή ευκολία αυξάνει το άνοιγμα στην κοινή χρήση δεδομένων ακόμη και όταν οι συμμετέχοντες προειδοποιούνται για τους κινδύνους περί απορρήτου. Αυτό αναδεικνύει την ένταση της σχέσης ανταλλαγής ανάμεσα στην ευχρηστία και στην προστασία της ιδιωτικότητας σε ψηφιακά διαμεσολαβούμενα περιβάλλοντα. Ταυτόχρονα, υπογραμμίζει την ηθική ευθύνη των εταιρειών και των ρυθμιστικών αρχών να ορίζουν όρια που οι καταναλωτές ενδέχεται να υποτιμούν τη στιγμή της επιλογής.

Οι Schumann et al. (2025) επεκτείνουν τη συζήτηση σε περιβάλλοντα μεταξύ επιχειρήσεων, όπου οι εταιρείες προμηθευτών αναζητούν πρόσβαση σε ιδιόκτητα δεδομένα εταιρειών πελατών προκειμένου να προσφέρουν υπηρεσίες που βασίζονται σε δεδομένα. Το πολυεπίπεδο πλαίσιό τους δείχνει ότι η λήψη αποφάσεων που σχετίζονται με την προστασία της ιδιωτικής ζωής σε περιβάλλοντα B2B περιλαμβάνει διάφορους παράγοντες, αντιλήψεις κινδύνου και οργανωτικές παραμέτρους. Η ισορροπία μεταξύ προστασίας και επιχειρηματικής χρήσης δεν είναι επομένως ένα απλό ζήτημα ατομικής προτίμησης, αλλά μια δομημένη διαπραγμάτευση πάνω στην εμπιστοσύνη, την εξάρτηση και τον έλεγχο. Η ηθική πρόκληση για τις σύγχρονες επιχειρήσεις έγκειται στη δημιουργία εμπορικής αξίας χωρίς να μειώνεται η ιδιωτικότητα.

5.2.3 Το «δικαίωμα στη λήθη» και οι ψηφιακές ταυτότητες

Το δικαίωμα στη λήθη προσθέτει μια περαιτέρω κοινωνική διάσταση συνδέοντας την προστασία δεδομένων με τη μνήμη, την προσωπική ανάπτυξη και τη συνεχή ορατότητα των ατόμων σε ψηφιακά περιβάλλοντα. Οι Zhang et al. (2025) εξηγούν ότι αυτό το δικαίωμα γίνεται πιο περίπλοκο στην εποχή των μεγάλων γλωσσικών μοντέλων, επειδή τέτοια συστήματα αποθηκεύουν και επεξεργάζονται πληροφορίες διαφορετικά από τις μηχανές αναζήτησης. Η συζήτησή τους δείχνει ότι τεχνικές λύσεις όπως η διαφορική ιδιωτικότητα, η μηχανική από-μάθηση, η επεξεργασία μοντέλων και τα προστατευτικά όρια μπορούν να βοηθήσουν τους οργανισμούς να ανταποκριθούν σε αιτήματα διαγραφής, ωστόσο η πρόκληση παραμένει εννοιολογικά και λειτουργικά απαιτητική. Αυτό καθιστά το δικαίωμα στη

λήθη κεντρικό παράδειγμα του πώς τα νομικά δικαιώματα πρέπει να εξελίσσονται παράλληλα με τις τεχνολογικές υποδομές.

Η Kohl (2023) παρέχει μια ευρύτερη νομική και πολιτισμική ερμηνεία δείχνοντας ότι το δικαίωμα στη λήθη αντικατοπτρίζει ένα ευρωπαϊκό άνοιγμα στην ιδιωτικότητα στο κοινό. Η ανάλυσή της υποδηλώνει ότι η νομοθεσία περί προστασίας δεδομένων προστατεύει όχι μόνο το απόρρητο αλλά και την ικανότητα των ατόμων να διαχειρίζονται τη δημόσια διατήρηση των προσωπικών τους πληροφοριών. Αυτό είναι σημαντικό για τις σύγχρονες ψηφιακές ταυτότητες, οι οποίες διαμορφώνονται όλο και περισσότερο μέσω αναζητήσιμων αρχείων, αλληλεπιδράσεων πλατφορμών και αλγοριθμικών συμπερασμάτων. Το δικαίωμα στη λήθη υποστηρίζει επομένως μια μορφή χρονικής δικαιοσύνης, επιτρέποντας στους ανθρώπους να αναδιαμορφώσουν τον τρόπο με τον οποίο οι προηγούμενες πληροφορίες επηρεάζουν τις παρούσες και μελλοντικές ευκαιρίες ζωής.

Τα εθνικά συστήματα ψηφιακής ταυτότητας καθιστούν τη συζήτηση αυτή ακόμη πιο σύνθετη, καθώς συνδέουν την ευχέρεια πρόσβασης, την ασφαλή ταυτοποίηση και τη χρήση δημόσιων υπηρεσιών με εκτεταμένες υποδομές επεξεργασίας προσωπικών δεδομένων. Οι Naghmouchi et al. (2025) δείχνουν ότι η επιτυχής λειτουργία των συστημάτων αυτών εξαρτάται από την τεχνολογική τους συγκρότηση, το κατάλληλο νομικό πλαίσιο και την ύπαρξη ισχυρών εγγυήσεων προστασίας δεδομένων. Παράλληλα, αναδεικνύουν κρίσιμα ζητήματα που αφορούν την κρατική κυριαρχία, καθώς και την κατανομή ρόλων και ευθυνών μεταξύ δημόσιων και ιδιωτικών φορέων. Οι Abomhara et al. (2024) συμπληρώνουν αυτήν την ανάλυση δείχνοντας ότι η προστασία της ιδιωτικής ζωής εκ σχεδιασμού (Privacy by Design) στα εθνικά συστήματα ταυτοποίησης εξαρτάται σε μεγάλο βαθμό από τις στάσεις των ενδιαφερόμενων μερών, την εκπαίδευση, τις σαφείς οδηγίες και την ευαισθητοποίηση. Αυτά τα ευρήματα δείχνουν ότι τα συστήματα ψηφιακής ταυτότητας μπορούν να υποστηρίξουν την ένταξη, την αποτελεσματικότητα και την αξιόπιστη πρόσβαση όταν η ιδιωτικότητα ενσωματώνεται στο σχεδιασμό και τη διακυβέρνησή τους.

5.3 Πολιτικές και στρατηγικές για βιώσιμη επιχειρηματική ανάπτυξη

Η παρούσα ενότητα στρέφεται από τους αναδυόμενους κινδύνους και τα ηθικά διλήμματα προς τις οργανωτικές απαντήσεις που μπορούν να υποστηρίξουν τη βιώσιμη επιχειρηματική ανάπτυξη σε περιβάλλοντα έντασης δεδομένων. Η κεντρική της προϋπόθεση είναι ότι η μακροπρόθεσμη ανταγωνιστικότητα δεν εξαρτάται μόνο από τη συμμόρφωση με τη νομοθεσία ή την τεχνική προστασία, αλλά και από τις δομές διακυβέρνησης, τους θεσμικούς ρόλους και τις δυνατότητες του εργατικού δυναμικού που καθιστούν δυνατή την υπεύθυνη χρήση δεδομένων στην καθημερινή πρακτική. Για τον λόγο αυτό, η ενότητα εξετάζει τη διακυβέρνηση και τη διαφάνεια των δεδομένων, τον στρατηγικό ρόλο του DPO και τη σημασία της εκπαίδευσης του προσωπικού και της γνώσης για τα δεδομένα ως αμοιβαία ενισχυτικούς πυλώνες της ανθεκτικής ψηφιακής ανάπτυξης.

5.3.1 Διακυβέρνηση δεδομένων (data governance) και εταιρική διαφάνεια

Η βιώσιμη επιχειρηματική ανάπτυξη από την ικανότητα των εταιρειών να διαχειρίζονται τα δεδομένα ως περιουσιακό στοιχείο. Στα σύγχρονα ψηφιακά περιβάλλοντα, η διακυβέρνηση δεδομένων υποστηρίζει την ποιότητα των αποφάσεων, την ευθυγράμμιση των κανονισμών, τη λειτουργική συνέπεια και την εμπιστοσύνη των ενδιαφερομένων μερών. Οι Bernardo et al. (2024) δείχνουν ότι η διακυβέρνηση δεδομένων έχει ωριμάσει σε ένα ευρύ διεπιστημονικό πεδίο που συνδέει βασικές έννοιες, πλαίσια, μοντέλα ωριμότητας, διασφάλιση δεδομένων και ψηφιακή νομιμότητα. Η έρευνά τους είναι σημαντική επειδή παρουσιάζει τη διακυβέρνηση ως έναν θεμελιώδη μηχανισμό μέσω του οποίου οι εταιρείες μπορούν να μεγιστοποιήσουν την αξία των δεδομένων διατηρώντας παράλληλα τον έλεγχο, την ποιότητα και την λογοδοσία. Από αυτή την οπτική γωνία, η διαφάνεια είναι μια εσωτερική προϋπόθεση για καλά οργανωμένες διαδικασίες δεδομένων. Υποστηρίζει επίσης την καλύτερη επικοινωνία με τις ρυθμιστικές αρχές, τους συνεργάτες και τους πελάτες, καθιστώντας τις ευθύνες για τα δεδομένα ορατές, κατανοητές και εφαρμόσιμες σε όλες τις επιχειρηματικές μονάδες με συνέπεια.

Οι Acev et al. (2025) ενισχύουν αυτό το επιχείρημα αποδεικνύοντας ότι τα αποτελεσματικά πλαίσια διακυβέρνησης δεδομένων είναι απαραίτητα για την ασφαλή και αξιόπιστη ανταλλαγή δεδομένων μεταξύ νομικών οντοτήτων. Η συστηματική τους

ανάλυση, υπογραμμίζει την ανάγκη ευθυγράμμισης των στοιχείων διακυβέρνησης με τα προβλεπόμενα περιουσιακά στοιχεία, όπως η αξιοπιστία, η φερεγγυότητα και η ελεγχόμενη διαλειτουργικότητα. Αυτή η συμβολή είναι ιδιαίτερα χρήσιμη για επιχειρήσεις που λειτουργούν σε συνεργατικά οικοσυστήματα όπου η ανταλλαγή δεδομένων λαμβάνει χώρα πέρα από τα στενά οργανωτικά όρια. Η διαφάνεια σε αυτά τα πλαίσια αποκτά στρατηγική αξία επειδή μειώνει την αβεβαιότητα σχετικά με την ποιότητα των δεδομένων και την ακεραιότητα των συναλλαγών. Οι Kim, Park και Park (2026) παρέχουν εμπειρική υποστήριξη για αυτή τη λογική μέσω της μελέτης τους για το μοντέλο εμπιστοσύνης δεδομένων, δείχνοντας ότι τόσο η αντιληπτή διαφάνεια των δεδομένων όσο και η αντιληπτή διαφάνεια των συναλλαγών διαμορφώνουν την αποδοχή των χρηστών, ειδικά υπό συνθήκες ασυμμετρίας πληροφοριών. Τα ευρήματά τους δείχνουν ότι η διαφάνεια λειτουργεί ως ένας υπό όρους παράγοντας συμμετοχής και συνδέεται στενά με τη φήμη, την ασφάλεια και την θεσμική αξιοπιστία.

Οι Volz et al. (2025) επεκτείνουν τη συζήτηση εξετάζοντας τη διακυβέρνηση σε πολυπαραγοντικά ψηφιακά οικοσυστήματα. Τα στοιχεία τους δείχνουν ότι οι αρχές διακυβέρνησης αναδύονται μέσω της συνεχούς προσαρμογής και όχι μέσω του στατικού σχεδιασμού. Αυτή η γνώση είναι κρίσιμη για τη βιώσιμη ανάπτυξη, επειδή οι εταιρείες δημιουργούν όλο και περισσότερο αξία μέσω δικτύων πλατφορμών, συνεργατών και πηγών δεδομένων που δεν μπορούν να διαχειριστούν μόνο μέσω άκαμπτων κανόνων. Η εταιρική διαφάνεια λειτουργεί επομένως ως μια δυναμική οργανωτική ικανότητα που υποστηρίζει τον συντονισμό, την εμπιστοσύνη και τη νομιμότητα, επιτρέποντας παράλληλα στις ρυθμίσεις διακυβέρνησης να εξελίσσονται ως απάντηση σε εσωτερικές και εξωτερικές πιέσεις.

5.3.2 Ο ρόλος του DPO και της εταιρικής κουλτούρας συμμόρφωσης

Μέσα σε αυτήν την δομή διακυβέρνησης, ο Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer, DPO) κατέχει έναν ιδιαίτερα στρατηγικό ρόλο, επειδή η αποτελεσματική συμμόρφωση εξαρτάται από την ερμηνεία, τον συντονισμό και την πολιτισμική επιρροή. Οι Alashoor et al. (2025) υποστηρίζουν ότι οι ΥΠΔ μπορούν να οικοδομήσουν ισχυρότερες εταιρικές κουλτούρες απορρήτου όταν προχωρούν πέρα από την επιβολή κανόνων από πάνω προς τα κάτω και αξιολογούν την οργανωσιακή πρακτική μέσω βασικών μηχανισμών, μηχανισμών αναφοράς και συνδυαστικών μηχανισμών. Το πλαίσιό τους είναι πολύτιμο επειδή αντιλαμβάνεται την κουλτούρα

απορρήτου ως κάτι που μπορεί να μετρηθεί, να ενισχυθεί και να ενσωματωθεί σε ολόκληρο τον οργανισμό.

Οι Young και Visser (2026) εμβαθύνουν περαιτέρω, εξετάζοντας τον ΥΠΔ ως παράγοντα που λειτουργεί μεταξύ ανταγωνιστικών θεσμικών λογικών. Η μελέτη τους δείχνει ότι οι ΥΠΔ διαχειρίζονται τις εντάσεις μεταξύ κανονιστικών απαιτήσεων και οργανωτικών προτεραιοτήτων και μπορούν να ασκήσουν εξουσία εντοπίζοντας χώρους όπου απαιτούνται ηθική κρίση και συγκεκριμένες τακτικές. Έτσι, η κουλτούρα συμμόρφωσης αναπτύσσεται όταν η ηγεσία στην προστασία της ιδιωτικής ζωής συνδέει τις επίσημες υποχρεώσεις με τις πρακτικές που καθορίζονται μέσω της θεσμικής λήψης αποφάσεων. Οι Wiefling, Tolsdorf και Lo Iacono (2022) προσθέτουν μια εφαρμοσμένη προοπτική από τα ψηφιακά οικοσυστήματα. Η μελέτη τους, βασισμένη σε συνεντεύξεις με ΥΠΔ, δείχνει ότι οι προκλήσεις σχετικά με την προστασία της ιδιωτικής ζωής σε σύνθετα οικοσυστήματα σχετίζονται με νομικές υποχρεώσεις, δικαιώματα υποκειμένων δεδομένων και την εφαρμογή μέτρων προστασίας. Αυτά τα ευρήματα επιβεβαιώνουν ότι η κουλτούρα συμμόρφωσης εξαρτάται από τον συνεχή διαλειτουργικό συντονισμό και από την ικανότητα των ΥΠΔ να μεταφράζουν αφηρημένες νομικές απαιτήσεις σε εφαρμόσιμες διαδικασίες. Ένας βιώσιμος οργανισμός χρειάζεται επομένως μια κουλτούρα συμμόρφωσης στην οποία η ιδιωτικότητα αναγνωρίζεται ως κοινή διαχειριστική ευθύνη και όχι ως περιφερειακό νομικό ζήτημα.

5.3.3 Εκπαίδευση προσωπικού και ενίσχυση του γραμματισμού δεδομένων

Η μακροπρόθεσμη επιτυχία των δομών διακυβέρνησης και συμμόρφωσης εξαρτάται από τις ικανότητες των εργαζομένων που συλλέγουν, ερμηνεύουν, ασφαλίζουν και χρησιμοποιούν δεδομένα στην καθημερινή εργασία. Ο Fattah (2024) δείχνει ότι η γνώση δεδομένων μεσολαβεί στη σχέση μεταξύ της διακυβέρνησης δεδομένων και της κουλτούρας που βασίζεται σε δεδομένα. Αυτό το εύρημα είναι κεντρικό για την παρούσα ενότητα, επειδή υποδεικνύει ότι οι ρυθμίσεις διακυβέρνησης δημιουργούν οργανωσιακή αξία όταν οι εργαζόμενοι διαθέτουν την ικανότητα να κατανοούν τα δεδομένα, να αξιολογούν τη συνάφειά τους και να τα χρησιμοποιούν στην υπεύθυνη λήψη αποφάσεων. Επομένως, η γνώση δεδομένων μετατρέπει την επίσημη διακυβέρνηση σε βιωμένη οργανωσιακή πρακτική.

Η εκπαίδευση είναι εξίσου σημαντική στον τομέα της ευαισθητοποίησης για την ασφάλεια. Οι Alyami, Sammon, Neville και Mahony (2022) προσδιορίζουν κρίσιμους παράγοντες επιτυχίας για αποτελεσματικά προγράμματα Εκπαίδευσης, Κατάρτισης και Ευαισθητοποίησης για την Ασφάλεια και τα οργανώνουν σε έναν κύκλο ζωής σχεδιασμού, ανάπτυξης, εφαρμογής και αξιολόγησης. Η εργασία τους υποδηλώνει ότι η εκπαίδευση επιτυγχάνει όταν είναι συστηματική, ευαίσθητη στο πλαίσιο και διατηρείται με την πάροδο του χρόνου. Αυτό είναι ιδιαίτερα σημαντικό για τη διακυβέρνηση της ιδιωτικότητας, επειδή η ασφαλής και νόμιμη διαχείριση δεδομένων εξαρτάται από τη συμπεριφορά και όχι μόνο από κείμενα πολιτικής ή τεχνικά συστήματα. Με αυτήν την έννοια, οι εργαζόμενοι γίνονται κεντρικοί παράγοντες στην προστασία των οργανωσιακών και προσωπικών δεδομένων.

Οι Nikou, De Reuver και Mahboob Kanafi (2022) συμπληρώνουν αυτήν την προσέγγιση δείχνοντας ότι η πληροφοριακή και η ψηφιακή παιδεία επηρεάζουν τις αντιλήψεις των εργαζομένων για την ευκολία χρήσης και την πρόθεσή τους να υιοθετήσουν ψηφιακές τεχνολογίες στον χώρο εργασίας. Τα ευρήματά τους δείχνουν ότι η παιδεία διαμορφώνει την πρακτική αποδοχή των ψηφιακών εργαλείων και ως εκ τούτου επηρεάζει την επιτυχία του ψηφιακού μετασχηματισμού ευρύτερα. Συνολικά, η βιβλιογραφία δείχνει ότι η βιώσιμη επιχειρηματική ανάπτυξη απαιτεί μια ολοκληρωμένη στρατηγική στην οποία η διακυβέρνηση δεδομένων δημιουργεί τη δομική βάση, οι ΥΠΔ καλλιεργούν μια οργανωτική κουλτούρα που σέβεται την ιδιωτικότητα και η συνεχής εκπαίδευση ενισχύει την παιδεία και την ευαισθητοποίηση που απαιτούνται για την υπεύθυνη χρήση δεδομένων. Μια τέτοια στρατηγική επιτρέπει στις εταιρείες να ευθυγραμμίσουν τη διαφάνεια, την λογοδοσία, την καινοτομία και τη μακροπρόθεσμη ανθεκτικότητα μέσα σε ένα συνεκτικό μοντέλο αξιόπιστης ανάπτυξης.

5.3.4 Προτεινόμενες πολιτικές για υπεύθυνη αυτοματοποιημένη λήψη αποφάσεων

Η αποτελεσματική αντιμετώπιση των κινδύνων της Τεχνητής Νοημοσύνης απαιτεί ενιαίο πλαίσιο πολιτικής που συνδέει τη νομική συμμόρφωση, την τεχνική διασφάλιση και την επιχειρησιακή λογοδοσία. Η πολιτική εφαρμόζεται σε συστήματα που αναπτύσσονται εσωτερικά και σε λύσεις τρίτων παρόχων, καλύπτοντας από την αρχική ιδέα και την προμήθεια έως την παραγωγική λειτουργία, την παρακολούθηση και την απόσυρση.

Πίνακας 15: Πλαίσιο πολιτικών αντιμετώπισης κινδύνων αυτοματοποιημένων αποφάσεων

#	Πολιτική	Περιεχόμενο εφαρμογής	Ενδεικτική μετρική
1	Μητρώο συστημάτων AI	Καταγραφή σκοπού, ιδιοκτήτη, παρόχου, δεδομένων, ομάδων που επηρεάζονται και επιπέδου κινδύνου.	Ποσοστό συστημάτων με ολοκληρωμένη καταχώριση και ετήσια επανεξέταση.
2	Ταξινόμηση και έγκριση πριν από τη χρήση	Έλεγχος υπαγωγής σε απαγορευμένες πρακτικές, υψηλό κίνδυνο ή υποχρεώσεις διαφάνειας πριν από προμήθεια ή ανάπτυξη.	Ποσοστό έργων που λαμβάνουν έγκριση νομικής υπηρεσίας, DPO και υπευθύνου κινδύνου.
3	Συνδυασμένη DPIA και FRIA	Ενιαία αξιολόγηση ιδιωτικότητας, ισότητας, αυτονομίας, προσφυγής και επιπτώσεων σε ευάλωτες ομάδες.	Αριθμός ανοικτών μέτρων μείωσης και ποσοστό ολοκλήρωσης πριν από παραγωγική λειτουργία.
4	Διακυβέρνηση δεδομένων και έλεγχος μεροληψίας	Πρότυπα ποιότητας, αντιπροσωπευτικότητας, ιχνηλασιμότητας, ελαχιστοποίησης και περιοδικής δοκιμής ανά ομάδα.	Διαφορά σφάλματος ή δυσμενούς αποτελέσματος μεταξύ συναφών ομάδων και ποσοστό διορθωτικών ενεργειών.
5	Ουσιαστική ανθρώπινη εποπτεία	Καθορισμός αρμοδιοτήτων, ορίων αυτονομίας, κριτηρίων παράκαμψης και δυνατότητας ασφαλούς διακοπής.	Ποσοστό αποφάσεων που επανεξετάζονται και ποσοστό περιπτώσεων όπου η ανθρώπινη κρίση μεταβάλλει το αποτέλεσμα.
6	Διαφάνεια και δικαίωμα αμφισβήτησης	Ενημέρωση για χρήση AI, βασικούς παράγοντες απόφασης, συνέπειες, δυνατότητα ανθρώπινης παρέμβασης και διαδικασία ένστασης.	Χρόνος απόκρισης σε αιτήματα εξήγησης, αριθμός ενστάσεων και ποσοστό αναθεωρημένων αποφάσεων.
7	Έλεγχος προμηθευτών	Συμβατικές απαιτήσεις για τεχνική τεκμηρίωση, logs, ασφάλεια, δοκιμές, υποστήριξη ελέγχων και γνωστοποίηση αλλαγών.	Ποσοστό κρίσιμων προμηθευτών με ολοκληρωμένη αξιολόγηση και ρήτρες συμμόρφωσης.
8	Παρακολούθηση και διαχείριση περιστατικών	Συνεχής μέτρηση απόδοσης, drift, παραπόνων, σφαλμάτων και σημαντικών συμβάντων με σαφή διαδικασία κλιμάκωσης.	Χρόνος εντοπισμού, χρόνος διορθωτικής ενέργειας και αριθμός επαναλαμβανόμενων περιστατικών.
9	AI literacy και εκπαίδευση ρόλων	Στοχευμένη κατάρτιση διοίκησης, DPO, νομικής υπηρεσίας, τεχνικών ομάδων και ανθρώπινων επόπτων.	Ποσοστό ολοκλήρωσης κατάρτισης και αποτελέσματα αξιολόγησης επάρκειας.

#	Πολιτική	Περιεχόμενο εφαρμογής	Ενδεικτική μετρική
10	Επιτροπή διακυβέρνησης AI	Διατμηματικό όργανο με αρμοδιότητα έγκρισης, επανεξέτασης κινδύνων, παρακολούθησης δεικτών και αναστολής χρήσης.	Συχνότητα συνεδριάσεων, αριθμός αποφάσεων και ποσοστό μέτρων που ολοκληρώνονται εντός προθεσμίας.

Η εφαρμογή του πλαισίου μπορεί να οργανωθεί σε τρία επίπεδα. Στο πρώτο επίπεδο πραγματοποιούνται απογραφή και ταξινόμηση των συστημάτων. Στο δεύτερο επίπεδο εφαρμόζονται εκτιμήσεις επιπτώσεων, τεχνικές δοκιμές, συμβατικές εγγυήσεις και διαδικασίες ανθρώπινης εποπτείας. Στο τρίτο επίπεδο λειτουργούν μετρικές, εσωτερικός έλεγχος, αναφορές περιστατικών και περιοδική επανέγκριση. Η δομή αυτή διευκολύνει την αναλογική εφαρμογή στις ΜΜΕ και στις μεγάλες επιχειρήσεις, επειδή επιτρέπει κοινό πυρήνα ελέγχων με διαφορετικό βαθμό οργανωτικής εξειδίκευσης.

Στην Ελλάδα, κατά τον χρόνο ολοκλήρωσης της εργασίας, το σχέδιο νόμου για το εθνικό εφαρμοστικό πλαίσιο του AI Act είχε εισαχθεί στη Βουλή. Το προτεινόμενο σχήμα όριζε την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ως κεντρική αρχή εποπτείας της αγοράς και εθνικό σημείο επαφής και προέβλεπε τη δημιουργία Κέντρου Συντονισμού και Τεχνογνωσίας Τεχνητής Νοημοσύνης. Η εξέλιξη αυτή ενισχύει την ανάγκη των επιχειρήσεων να οργανώσουν από τώρα μητρώα AI, διαδικασίες ταξινόμησης και τεκμηριωμένη συνεργασία με τις αρμόδιες αρχές (Υπουργείο Ψηφιακής Διακυβέρνησης και Τεχνητής Νοημοσύνης, 2026).

5.4 Συνολική αποτίμηση των επιπτώσεων του GDPR στην ανάπτυξη

Η Ενότητα 5.4 συγκεντρώνει τις προηγούμενες αναλύσεις του Κεφαλαίου 5 και αξιολογεί την ευρύτερη αναπτυξιακή σημασία του GDPR. Αφού εξέτασε τις νέες τεχνολογικές τάσεις, τα ηθικά διλήμματα και τις απαντήσεις στη διακυβέρνηση, το κεφάλαιο στρέφεται τώρα στη συνολική ισορροπία μεταξύ του κανονιστικού βάρους και των επιχειρηματικών ευκαιριών. Επίσης, εξετάζει την ευρύτερη γεωπολιτική σημασία του Κανονισμού, διερευνώντας πώς η Ευρωπαϊκή Ένωση έχει αναδειχθεί ως σημείο αναφοράς για τη διεθνή διακυβέρνηση της ιδιωτικής ζωής. Με αυτόν τον τρόπο, η ενότητα προσφέρει τόσο μια επιχειρηματική όσο και μια κανονιστική αξιολόγηση,

συνδέοντας τις συνέπειες σε επίπεδο επιχείρησης με την παγκόσμια διάδοση των ευρωπαϊκών προτύπων προστασίας δεδομένων.

5.4.1 Ανάλυση ισορροπίας ανάμεσα στην ρυθμιστική επιβάρυνση και τα επιχειρηματικά οφέλη

Οποιαδήποτε συνολική αξιολόγηση του GDPR πρέπει να προχωρήσει πέρα από τους αρχικούς ισχυρισμούς που παρουσιάζουν τον Κανονισμό είτε ως ένα δαπανηρό νομικό βάρος είτε ως μια αδιαμφισβήτητη επιτυχία. Η εμπειρική βιβλιογραφία, αντίθετα, υποδεικνύει μια διαφοροποιημένη εικόνα στην οποία ο GDPR παράγει τόσο περιορισμούς όσο και ευκαιρίες ανάλογα με το μέγεθος της επιχείρησης, τον τομέα, τη δομή της αγοράς και το μοντέλο εσόδων των επιχειρήσεων. Οι Li, Li, Li, Zhang και Li (2025) παρέχουν ένα χρήσιμο σημείο εκκίνησης της σχετικής συζήτησης μέσω της συστηματικής τους ανασκόπησης της εμπειρικής βιβλιογραφίας. Η σύνθεσή τους οργανώνει τα στοιχεία του GDPR σε επίγνωση και εμπιστοσύνη, λειτουργική απόδοση, επιπτώσεις και κανονιστική σαφήνεια. Αυτή η δομή είναι σημαντική επειδή δείχνει ότι ο Κανονισμός δεν μπορεί να κριθεί αποκλειστικά μέσω του κόστους συμμόρφωσης, καθώς τα αποτελέσματά του επεκτείνονται στην εμπιστοσύνη των καταναλωτών, στις οργανωτικές διαδικασίες, στην τεχνολογική αλλαγή και στις ευρύτερες θεσμικές συνέπειες.

Τα στοιχεία για το κανονιστικό βάρος παραμένουν ωστόσο, σημαντικά. Οι Peukert, Bechtold, Batikas και Kretschmer (2022) δείχνουν ότι ο GDPR μείωσε τις αλληλεπιδράσεις των ιστότοπων με τρίτους παρόχους τεχνολογίας και συνέβαλε σε μεγαλύτερη συγκέντρωση της αγοράς στις υπηρεσίες τεχνολογίας. Το αποτέλεσμα ήταν ιδιαίτερα ορατό σε λιγότερο δημοφιλείς ιστότοπους και σε δραστηριότητες που σχετίζονται με τη συλλογή προσωπικών δεδομένων. Οι Johnson, Shriver και Goldberg (2023) επιβεβαιώνουν ένα παρόμοιο μοτίβο, διαπιστώνοντας ότι η χρήση από προμηθευτές μειώθηκε μετά την εφαρμογή, ενώ η συγκέντρωση αυξήθηκε μεταξύ των μεγάλων προμηθευτών τεχνολογίας, ειδικά σε κατηγορίες με μεγάλη ένταση δεδομένων, όπως τα cookies, η διαφήμιση και τα αναλυτικά στοιχεία. Αυτές οι μελέτες είναι ιδιαίτερα σημαντικές επειδή δείχνουν ότι η ρύθμιση της ιδιωτικότητας μπορεί να προστατεύει τους χρήστες, ενώ ταυτόχρονα ενισχύει τους κυρίαρχους παράγοντες που διαθέτουν τους οργανωτικούς και τεχνικούς πόρους που απαιτούνται για να προσαρμοστούν γρήγορα. Το βάρος της ρύθμισης είναι επομένως άνισο και οι

μικρότερες επιχειρήσεις μπορούν να αντιμετωπίσουν αναλογικά υψηλότερο κόστος προσαρμογής.

Το ίδιο συμπέρασμα προκύπτει από μελέτες για την απόδοση των ιστότοπων και την εμπλοκή των χρηστών. Οι Congiu, Sabatino και Sapi (2022) διαπιστώνουν ότι ο GDPR μείωσε τις επισκέψεις στους ιστότοπους και την εμπλοκή των χρηστών μακροπρόθεσμα, μειώνοντας τόσο τα πληρωμένα όσο και τα μη πληρωμένα κανάλια επισκεψιμότητας. Τα αποτελέσματά τους υποδηλώνουν ότι η ρύθμιση της ιδιωτικότητας μπορεί να μειώσει την αποτελεσματικότητα της διαφήμισης και να μεταβάλει την ορατότητα στο διαδίκτυο. Ταυτόχρονα, δεν επιβεβαιώνονται από τα στοιχεία όλοι οι φόβοι σχετικά με την οικονομική ζημία. Οι Lefrere, Warberg, Cheyre, Marotta και Acquisti (2025) δείχνουν ότι παρόλο που οι ευρωπαϊκοί ιστότοποι ειδήσεων και μέσων ενημέρωσης άλλαξαν τις πρακτικές συλλογής δεδομένων τους, δεν υπέστησαν αρνητικές επιπτώσεις στην παροχή περιεχομένου, στους δείκτες ποιότητας ή στα ποσοστά επιβίωσης σε σχέση με τους ιστότοπους των Ηνωμένων Πολιτειών. Αυτό είναι ένα σημαντικό εύρημα, επειδή καταδεικνύει ότι οι εταιρείες μπορούν να προσαρμοστούν σε αυστηρότερα πρότυπα απορρήτου χωρίς απαραίτητα να χάσουν την ικανότητά τους να παράγουν, να δημιουργούν έσοδα και να διανέμουν αξία.

Τα επιχειρηματικά οφέλη του GDPR γίνονται σαφέστερα όταν εξετάζεται η εμπιστοσύνη των καταναλωτών και η ποιότητα των δεδομένων ως παράγοντες που επηρεάζουν την απόδοση της αγοράς. Οι Li, Lee, Raghu και Shi (2024) διαπιστώνουν ότι ο GDPR αύξησε την απόδοση των ξένων εφαρμογών για κινητά στις αγορές της Ευρωπαϊκής Ένωσης, υποστηρίζοντας το επιχείρημα ότι η ρύθμιση του απορρήτου μπορεί να τονώσει το ψηφιακό εμπόριο μειώνοντας τις ανησυχίες των καταναλωτών και αυξάνοντας την προθυμία υιοθέτησης άγνωστων υπηρεσιών. Ο Κανονισμός, επομένως, λειτουργεί όχι μόνο ως εμπόδιο αλλά και ως μηχανισμός διαβεβαίωσης από την πλευρά της ζήτησης. Ένα σχετικό σημείο εμφανίζεται στους Cao και Kretschmer (2026), οι οποίοι δείχνουν ότι η μεγαλύτερη έκθεση στον GDPR οδήγησε μεγάλες χρηματοπιστωτικές εταιρείες των Ηνωμένων Πολιτειών να βελτιώσουν τα λειτουργικά έσοδα, την τυποποίηση δεδομένων και την καινοτομία που σχετίζεται με τη μηχανική μάθηση με την πάροδο του χρόνου. Η μελέτη αυτή είναι ιδιαίτερα σημαντική επειδή υποδηλώνει ότι οι επενδύσεις στη συμμόρφωση μπορούν να πυροδοτήσουν έναν

βαθύτερο οργανωτικό μετασχηματισμό, βελτιώνοντας την ποιότητα των συστημάτων δεδομένων μακροπρόθεσμα.

Μια συμπληρωματική θεωρητική προοπτική προσφέρεται από τους Choe, Matsushima και Shekhar (2025), οι οποίοι δείχνουν ότι ο GDPR μπορεί να βελτιώσει την ευημερία όταν το μοντέλο εσόδων της εταιρείας εξαρτάται περισσότερο από τη χρήση υπηρεσιών παρά από την εντατική δημιουργία εσόδων από προσωπικά δεδομένα. Υπό αυτές τις συνθήκες, η αυστηρότερη διαχείριση της ιδιωτικότητας μπορεί να αυξήσει τη ζήτηση μεταξύ των καταναλωτών με υψηλότερες ανησυχίες για την ιδιωτικότητα, επιτρέποντας παράλληλα στις εταιρείες να επωφεληθούν από καλύτερα ευθυγραμμισμένες τιμές και συνθήκες εμπιστοσύνης. Αυτό το επιχείρημα διευκρινίζει ότι η τελική ισορροπία εξαρτάται από το υποκείμενο επιχειρηματικό μοντέλο. Το γενικό δίδαγμα από τη βιβλιογραφία είναι ότι ο GDPR δημιουργεί βραχυπρόθεσμες πιέσεις, αλλά μπορεί επίσης να δημιουργήσει μεσοπρόθεσμα και μακροπρόθεσμα κέρδη στην εμπιστοσύνη, την ποιότητα των δεδομένων, την εσωτερική πειθαρχία και τη νομιμότητα της αγοράς. Η επίδρασή του στην ανάπτυξη είναι επομένως μάλλον υπό όρους παρά ομοιόμορφη.

5.4.2 Το παράδειγμα της ΕΕ ως πρότυπο διεθνούς κανονιστικής πολιτικής

Η συνολική σημασία του GDPR εκτείνεται πέρα από τις εσωτερικές ευρωπαϊκές επιπτώσεις του, επειδή έχει γίνει παγκόσμιο σημείο αναφοράς για τη ρύθμιση της ιδιωτικής ζωής. Οι Ryngaert και Taylor (2020) εξηγούν ότι ο GDPR λειτουργεί ως μια μορφή παγκόσμιας ρύθμισης της προστασίας δεδομένων μέσω της εμβέλειας του και του πλαισίου επάρκειας που διέπει τις διεθνείς μεταφορές δεδομένων. Η ανάλυσή τους δείχνει ότι το ευρωπαϊκό δίκαιο επηρεάζει φορείς εκτός της Ένωσης, ακόμη και όταν ο επίσημος στόχος είναι η προστασία μόνο των ευρωπαϊκών υποκειμένων δεδομένων. Αυτή η ικανότητα προβολής προτύπων πέρα από τα εδαφικά σύνορα καθιστά τον GDPR ένα σημαντικό παράδειγμα του πώς η τοπική ρύθμιση αποκτά παγκόσμια σημασία στην ψηφιακή διακυβέρνηση.

Οι Birnhack και Mundlak (2025) δείχνουν ότι η επιρροή της Ευρωπαϊκής Ένωσης φαίνεται και στο ότι έχει δημιουργηθεί διεθνώς ένας ολόκληρος επαγγελματικός χώρος γύρω από την προστασία δεδομένων και της ιδιωτικότητας. Δηλαδή, όλο και περισσότεροι οργανισμοί, ακόμη και εκτός ΕΕ, υιοθετούν πρακτικές

και πρότυπα του GDPR. Η μελέτη τους δείχνει ότι οι οργανισμοί εκτός της Ευρωπαϊκής Ένωσης μπορούν να υιοθετήσουν πρότυπα GDPR ακόμη και χωρίς άμεση εγχώρια υποχρέωση, είτε επειδή η διασυνοριακή επιχειρηματική ολοκλήρωση καθιστά την υιοθέτηση αυτή πρακτικά απαραίτητη είτε επειδή ο Κανονισμός έχει γίνει ένα αναγνωρισμένο σημείο αναφοράς ορθής πρακτικής. Αυτό το εύρημα είναι εξαιρετικά σημαντικό, επειδή δείχνει ότι η επιρροή της Ευρωπαϊκής Ένωσης λειτουργεί μέσω επαγγελματικών κανόνων, οργανωτικών διαδικασιών και προσδοκιών φήμης. Ως αποτέλεσμα, ο GDPR έχει γίνει τόσο ένα κανονιστικό πλαίσιο όσο και ένα παγκόσμιο μοντέλο διακυβέρνησης, διαμορφώνοντας τον τρόπο με τον οποίο οι εταιρείες, οι επαγγελματίες και οι οργανισμοί ορίζουν την υπεύθυνη διαχείριση δεδομένων στην ευρύτερη ψηφιακή οικονομία.

Συνολικά, αυτές οι μελέτες υποστηρίζουν ότι ο GDPR εισήγαγε πραγματικές τριβές, ειδικά για τις μικρότερες εταιρείες, τους μεσάζοντες που απαιτούν μεγάλη ποσότητα δεδομένων και τους φορείς που εξαρτώνται από αδιαφανή συστήματα παρακολούθησης. Ωστόσο, ενθάρρυνε επίσης υψηλότερα πρότυπα διακυβέρνησης, ισχυρότερη εμπιστοσύνη των χρηστών και ένα διακρατικό πλαίσιο λογοδοσίας. Υπό αυτή την έννοια, η Ευρωπαϊκή Ένωση λειτουργεί ως καθοριστικός ρυθμιστικός πόλος για την ιδιωτικότητα εντός της επικράτειάς της και, ταυτόχρονα, διαμορφώνει ολοένα περισσότερο τα κριτήρια με τα οποία αξιολογείται η ψηφιακή ανάπτυξη σε διαφορετικές δικαιοδοσίες και τομείς παγκοσμίως.

6. Συμπεράσματα και προτάσεις πολιτικής

6.1 Συνοπτικά συμπεράσματα βιβλιογραφικής ανάλυσης

Η βιβλιογραφική ανασκόπηση ανέδειξε ότι η προστασία των προσωπικών δεδομένων έχει εξελιχθεί σε ένα θεμελιώδες πεδίο, το οποίο συνδέει το δίκαιο, την τεχνολογία, την αγορά και τις δημοκρατικές αξίες στο ευρωπαϊκό περιβάλλον. Η ανάλυση του δεύτερου κεφαλαίου κατέδειξε ότι τα προσωπικά δεδομένα λειτουργούν πλέον ως πληροφοριακά αγαθά με υψηλή κανονιστική, κοινωνική και οικονομική σημασία, τα οποία διαμορφώνονται από την τεχνητή νοημοσύνη, τα Big Data, τις διασυνδεδεμένες συσκευές, την προγνωστική ανάλυση και τα οικοσυστήματα πλατφορμών. Η εννοιολογική αυτή διεύρυνση εξηγεί γιατί το σύγχρονο δίκαιο προστασίας δεδομένων υπερβαίνει την παραδοσιακή ιδέα της μυστικότητας και ενσωματώνεται πλέον στα πεδία της διακυβέρνησης, της λογοδοσίας, της εποπτείας και της προστασίας δικαιωμάτων. Παράλληλα, η ιστορική μετάβαση από την Οδηγία του 1995 στον Γενικό Κανονισμό για την Προστασία Δεδομένων, σε συνδυασμό με την ελληνική προσαρμογή μέσω του Ν. 4624/2019 και τον εποπτικό ρόλο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ανέδειξε ένα συνεκτικό πλαίσιο νόμιμης επεξεργασίας, θεσμικής επιτήρησης και κανονιστικής εφαρμογής.

Η ίδια η βιβλιογραφική έρευνα έδειξε επίσης ότι η προστασία δεδομένων εντάσσεται πλέον σε ένα ευρύτερο οικοσύστημα ψηφιακής διακυβέρνησης. Δίπλα στον GDPR, το πλαίσιο ePrivacy, ο Κανονισμός για τις Ψηφιακές Υπηρεσίες, ο Κανονισμός για τις Ψηφιακές Αγορές, ο Κανονισμός για τη Διακυβέρνηση Δεδομένων και ο Κανονισμός για την Τεχνητή Νοημοσύνη συγκροτούν μια πολυεπίπεδη ρυθμιστική δομή, η οποία συνδέει την ιδιωτικότητα με δίκαιες αγορές, αξιόπιστες πλατφόρμες, ασφαλείς επικοινωνίες και υπεύθυνη καινοτομία. Μέσα σε αυτό το πλαίσιο, η προστασία των προσωπικών δεδομένων αναδεικνύεται σε κεντρικό άξονα της ευρωπαϊκής ψηφιακής συνταγματικότητας.

Το τρίτο κεφάλαιο μετέφερε την ανάλυση από τη νομική συγκρότηση στο πεδίο του καταναλωτή και της ψηφιακής εμπιστοσύνης. Η ανασκόπηση κατέδειξε ότι ο Ευρωπαίος καταναλωτής διαθέτει ένα πλέγμα δικαιωμάτων που περιλαμβάνει πλέον την ιδιωτικότητα, την ασφάλεια δεδομένων και την προστασία από χειριστικές εμπορικές πρακτικές. Ταυτόχρονα, η εμπιστοσύνη αναδείχθηκε ως κοινωνική και

στρατηγική συνθήκη, η οποία διαμορφώνεται από τη διαφάνεια, την κατανοητότητα, τις αξιόπιστες εγγυήσεις και την υπεύθυνη εταιρική συμπεριφορά. Οι εμπειρικές μελέτες που εξετάστηκαν στο κεφάλαιο αυτό έδειξαν ότι οι επιδράσεις του GDPR στην εμπιστοσύνη εξαρτώνται σε μεγάλο βαθμό από την πρακτική χρηστικότητα των σχετικών ρυθμίσεων. Ευανάγνωστες ενημερώσεις, ουσιαστική άσκηση δικαιωμάτων, ορατές εγγυήσεις ασφάλειας και πειστική επικοινωνία μετατρέπουν τη θεσμική ρύθμιση σε βιωμένη εμπιστοσύνη του καταναλωτή.

Το τέταρτο κεφάλαιο ανέδειξε ότι η προστασία δεδομένων μπορεί να νοηθεί πλέον και ως επιχειρηματική ικανότητα, πέρα από τη νομική της διάσταση. Η ιδιωτικότητα, όταν ενσωματώνεται στον σχεδιασμό, στη διακυβέρνηση και στην επικοινωνία, ενισχύει τη φήμη, την αφοσίωση των πελατών και την οργανωσιακή ανθεκτικότητα. Παράλληλα, η ανάλυση έδωσε έμφαση στο οικονομικό βάρος της συμμόρφωσης, ιδίως για τις μικρότερες επιχειρήσεις, ενώ κατέδειξε ότι η υπεύθυνη διαχείριση δεδομένων μπορεί να βελτιώσει την εμπιστοσύνη, την ποιότητα της πληροφορίας και τη στρατηγική διαφοροποίηση.

Τέλος, το πέμπτο κεφάλαιο συνέδεσε τη διακυβέρνηση της ιδιωτικότητας με τις αναδυόμενες τεχνολογίες, τα ηθικά ζητήματα και την οργανωσιακή επάρκεια. Η τεχνητή νοημοσύνη, το cloud computing, οι ψηφιακές ταυτότητες, οι διασυνοριακές ροές δεδομένων και το data literacy αναδείχθηκαν ως κρίσιμα ζητήματα για το μέλλον της προστασίας του καταναλωτή και της επιχειρηματικής ανάπτυξης. Συνολικά, η βιβλιογραφία στηρίζει το συμπέρασμα ότι η προστασία δεδομένων λειτουργεί ταυτόχρονα ως νομική εγγύηση, ως μηχανισμός εμπιστοσύνης, ως αρχή διακυβέρνησης και ως παράγοντας ψηφιακής ανάπτυξης.

6.2 Κεντρικά ευρήματα για τη σχέση προστασίας δεδομένων – επιχειρηματικής ανάπτυξης

Κεντρικό εύρημα της παρούσας εργασίας αποτελεί το ότι η προστασία των προσωπικών δεδομένων και η επιχειρηματική ανάπτυξη συνδέονται πλέον με τρόπο άμεσο, δομικό και αμφίδρομο. Η βιβλιογραφική ανάλυση έδειξε ότι η ισχυρή διακυβέρνηση της ιδιωτικότητας ενισχύει τη θεσμική νομιμοποίηση των επιχειρήσεων, καλλιεργεί την εμπιστοσύνη των πελατών, αυξάνει την οργανωσιακή ανθεκτικότητα και βελτιώνει την ικανότητα προσαρμογής σε ένα ψηφιακό περιβάλλον που

μεταβάλλεται διαρκώς. Η σχέση αυτή γίνεται ακόμη πιο ευδιάκριτη σε αγορές όπου οι επιχειρήσεις στηρίζονται στη συλλογή, στην ανάλυση και στην αξιοποίηση δεδομένων για σκοπούς εξατομίκευσης, εμπορικής στόχευσης και αυτοματοποιημένης λήψης αποφάσεων. Στα περιβάλλοντα αυτά, η επιχειρηματική ανάπτυξη αποκτά πιο στέρεα θεμέλια όταν υποστηρίζεται από νόμιμη επεξεργασία, διαφανή επικοινωνία, επαρκή ασφάλεια και ουσιαστικό σεβασμό των δικαιωμάτων του καταναλωτή.

Ένα πρώτο κρίσιμο εύρημα αφορά την εμπιστοσύνη. Οι μελέτες που εξετάστηκαν ανέδειξαν ότι οι καταναλωτές αξιολογούν όλο και περισσότερο τις επιχειρήσεις μέσα από τις πρακτικές διαχείρισης των δεδομένων τους. Η εμπιστοσύνη ενισχύεται όταν οι οργανισμοί αποσαφηνίζουν με ακρίβεια τους σκοπούς της επεξεργασίας, παρέχουν πραγματικό βαθμό ελέγχου, προστατεύουν αποτελεσματικά τις πληροφορίες και επικοινωνούν με σταθερότητα και συνέπεια. Η ψηφιακή εμπιστοσύνη λειτουργεί ως ουσιαστικός πόρος για την επιχείρηση, επειδή στηρίζει την πρόθεση γνωστοποίησης πληροφοριών, τη συνέχιση της σχέσης των καταναλωτών με την επιχείρηση και τη διαρκή συμμετοχή του χρήστη στις ψηφιακές υπηρεσίες της. Υπό αυτή την έννοια, η προστασία δεδομένων συμβάλλει άμεσα στην αφοσίωση των πελατών και στη σταθερότητα των σχέσεων που αναπτύσσουν με την επιχείρηση.

Ένα δεύτερο εύρημα αφορά τη στρατηγική διάσταση της ιδιωτικότητας. Η εργασία έδειξε ότι οι επιχειρήσεις αποκτούν ανταγωνιστική αξία όταν η ιδιωτικότητα παύει να αντιμετωπίζεται ως στενή υποχρέωση συμμόρφωσης και ενσωματώνεται στη συνολική διοικητική και επιχειρηματική τους λογική. Η προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, οι ευανάγνωστες γνωστοποιήσεις, οι αποτελεσματικές πρακτικές ασφάλειας και η ώριμη διαχείριση περιστατικών παραβίασης ενισχύουν τη φήμη, την αξιοπιστία και τη συνολική επίδοση της επιχείρησης. Μέσα από αυτή την προοπτική, η προστασία δεδομένων αναδεικνύεται σε μοχλό βελτίωσης της ποιότητας διακυβέρνησης και σε παράγοντα που καθιστά την καινοτομία πιο αξιόπιστη και πιο αποδεκτή από τους ενδιαφερόμενους.

Ένα τρίτο εύρημα συνδέεται με τα κόστη και τις ανταλλαγές που συνεπάγεται η συμμόρφωση. Η βιβλιογραφία κατέδειξε ότι η συμμόρφωση επιφέρει ουσιαστικές επιβαρύνσεις, ιδίως για μικρότερες επιχειρήσεις, νεοφυείς εταιρείες και φορείς που δραστηριοποιούνται σε τομείς ιδιαίτερα εξαρτώμενους από τα δεδομένα. Η εφαρμογή του κανονιστικού πλαισίου απαιτεί νομική εξειδίκευση, τεχνολογικές επενδύσεις,

εκπαίδευση προσωπικού, τεκμηρίωση διαδικασιών, μηχανισμούς εσωτερικού ελέγχου και επανασχεδιασμό οργανωσιακών πρακτικών. Ωστόσο, η ίδια βιβλιογραφία ανέδειξε ότι αυτές οι επενδύσεις μπορούν να βελτιώσουν την ποιότητα των δεδομένων, να ενισχύσουν τις οργανωσιακές ρουτίνες, να καλλιεργήσουν ουσιαστικότερη λογοδοσία και να υποστηρίξουν πιο πειθαρχημένες μορφές καινοτομίας. Η σχέση ανάμεσα στην προστασία δεδομένων και στην ανάπτυξη οργανώνεται, επομένως, γύρω από μια δυναμική όπου οι βραχυπρόθεσμες πιέσεις συνυπάρχουν με μακροπρόθεσμα οφέλη.

Ένα τέταρτο εύρημα αφορά τον ρόλο της τεχνολογικής μεταβολής. Η τεχνητή νοημοσύνη, τα Big Data, οι υποδομές cloud και οι διασυνοριακές ροές δεδομένων έχουν μετασχηματίσει την πρακτική σημασία των προσωπικών δεδομένων και έχουν ενισχύσει την ανάγκη για σύνθετους μηχανισμούς διακυβέρνησης. Σε αυτό το περιβάλλον, η προστασία δεδομένων στηρίζει την επιχειρηματική ανάπτυξη όταν οι επιχειρήσεις συνδυάζουν ασφάλεια, διαφάνεια, ηθικό προβληματισμό και θεσμική επάρκεια. Η διακυβέρνηση δεδομένων, ο ενεργός ρόλος του DPO και η επένδυση στο data literacy αναδείχθηκαν ως κρίσιμοι παράγοντες μακροπρόθεσμης επίδοσης. Συνολικά, η εργασία κατέληξε ότι ο GDPR έχει επιφέρει μια σύνθετη αλλά ισορροπημένη επίδραση. Η ρυθμιστική πίεση, η ενίσχυση της εμπιστοσύνης και η βελτίωση της διακυβέρνησης συνυπάρχουν στο ίδιο πεδίο. Για τον λόγο αυτό, η προστασία δεδομένων εμφανίζεται ως θεμέλιο της ψηφιακής επιχειρηματικότητας στην Ευρώπη, αλλά και ευρύτερα.

6.3 Προτάσεις πολιτικής για επιχειρήσεις και ρυθμιστικούς φορείς

Η βιβλιογραφική ανάλυση στηρίζει μια προσέγγιση πολιτικής στην οποία η προστασία των προσωπικών δεδομένων αντιμετωπίζεται ως κοινή αναπτυξιακή ευθύνη επιχειρήσεων και ρυθμιστικών φορέων. Για τις επιχειρήσεις, η αποτελεσματικότερη κατεύθυνση αφορά την ένταξη της ιδιωτικότητας στον πυρήνα της στρατηγικής τους λειτουργίας. Η προστασία δεδομένων αποκτά μεγαλύτερη αξία όταν συνδέεται με τον στρατηγικό σχεδιασμό, τον σχεδιασμό προϊόντων και υπηρεσιών, την εμπορική επικοινωνία, την οργανωσιακή ασφάλεια και τη διαχείριση περιστατικών. Σαφείς ενημερώσεις προς τους χρήστες, φιλικές προς την ιδιωτικότητα προεπιλογές, ισχυροί μηχανισμοί ελέγχου πρόσβασης, τεχνολογίες ενίσχυσης της ιδιωτικότητας και συστηματική εκπαίδευση προσωπικού ενδυναμώνουν τη συμμόρφωση και ενισχύουν την αξιοπιστία της επιχείρησης στην αγορά.

Ιδιαίτερη σημασία έχει και η καλλιέργεια μιας εσωτερικής κουλτούρας προστασίας δεδομένων. Η συνεργασία ανάμεσα στις νομικές υπηρεσίες, στις τεχνολογικές ομάδες, στη διοίκηση και στα τμήματα μάρκετινγκ δημιουργεί συνθήκες ουσιαστικότερης εφαρμογής των αρχών του GDPR. Παράλληλα, η ενεργή ενημέρωση των καταναλωτών γύρω από τα δικαιώματα και τις διαθέσιμες επιλογές τους ενισχύει την εμπιστοσύνη και βελτιώνει τη σχέση επιχείρησης και πελάτη. Έτσι, η προστασία δεδομένων εξελίσσεται από διοικητική υποχρέωση σε στοιχείο ανταγωνιστικού πλεονεκτήματος.

Από την πλευρά των ρυθμιστικών αρχών, χρήσιμη κατεύθυνση αποτελεί η παροχή πρακτικότερης καθοδήγησης και η ανάπτυξη κλαδικών προτύπων εφαρμογής. Οδηγοί συμμόρφωσης, υποδείγματα για εκτιμήσεις αντικτύπου, ερμηνευτικά κείμενα για επεξεργασίες υψηλού κινδύνου, για αυτοματοποιημένα συστήματα λήψης αποφάσεων και για διασυνοριακές διαβιβάσεις δεδομένων μπορούν να προσφέρουν μεγαλύτερη ασφάλεια και να διευκολύνουν ιδίως τις μικρότερες επιχειρήσεις. Η ενίσχυση της συνεργασίας ανάμεσα στις εθνικές και ευρωπαϊκές εποπτικές αρχές συμβάλλει επίσης στη συνεκτικότητα της εποπτείας, στη σταθερότητα του κανονιστικού περιβάλλοντος και στην εμπιστοσύνη προς τους θεσμούς. Ένα πλαίσιο που συνδυάζει καθοδήγηση, πρόληψη και αποτελεσματική εποπτεία υπηρετεί ταυτόχρονα την προστασία δικαιωμάτων και τη βιώσιμη ψηφιακή καινοτομία.

Για τη μετατροπή των προτάσεων πολιτικής σε εφαρμόσιμη διοικητική ατζέντα, προτείνεται το ακόλουθο σχέδιο δράσης. Κάθε βήμα συνδέει έναν σαφή φορέα ευθύνης, μια συγκεκριμένη ενέργεια και έναν δείκτη παρακολούθησης, ώστε η προστασία δεδομένων να ενσωματώνεται μετρήσιμα στη λειτουργία των επιχειρήσεων και των ρυθμιστικών φορέων.

Πίνακας 16: Πρακτικό σχέδιο εφαρμογής προτάσεων πολιτικής

#	Πρακτικό βήμα	Κύρια ενέργεια	Υπεύθυνοι φορείς	Ενδεικτικός δείκτης
1	**Ενίσχυση του DPO**	Άμεση αναφορά στη διοίκηση, εγκεκριμένο ετήσιο σχέδιο εργασίας, πρόσβαση σε επαρκείς πόρους και συμμετοχή στις	Διοίκηση, DPO	Ποσοστό έργων στα οποία ο DPO συμμετέχει από το στάδιο του σχεδιασμού

#	Πρακτικό βήμα	Κύρια ενέργεια	Υπεύθυνοι φορείς	Ενδεικτικός δείκτης
		αποφάσεις για νέα προϊόντα, συστήματα και συνεργασίες.		
2	**Επένδυση στο data literacy**	Ετήσιο πρόγραμμα εκπαίδευσης ανά ρόλο για διοίκηση, μάρκετινγκ, πληροφορική, ανθρώπινο δυναμικό και εξυπηρέτηση πελατών, με σύντομη αξιολόγηση γνώσεων.	DPO, HR, IT	Ποσοστό ολοκλήρωσης εκπαίδευσης και επίδοση στην αξιολόγηση
3	**Ανάπτυξη κλαδικών προτύπων**	Δημιουργία προτύπων DPIA, χαρτογράφησης δεδομένων, ενημέρωσης χρηστών και διαχείρισης περιστατικών για υγεία, τουρισμό, χρηματοπιστωτικές υπηρεσίες και λιανεμπόριο.	Εποπτικές αρχές, επαγγελματικοί φορείς	Αριθμός κλαδικών εργαλείων και ποσοστό υιοθέτησης από επιχειρήσεις
4	**Ενσωμάτωση Privacy by Design**	Θέσπιση υποχρεωτικού ελέγχου ιδιωτικότητας πριν από την έγκριση κάθε νέου προϊόντος, υπηρεσίας, εφαρμογής ή αυτοματοποιημένης διαδικασίας.	Ομάδες προϊόντος, IT, DPO	Ποσοστό νέων έργων που περνούν από τεκμηριωμένο έλεγχο
5	**Πίνακας δεικτών συμμόρφωσης και εμπιστοσύνης**	Μηνιαία ή τριμηνιαία παρακολούθηση αιτημάτων δικαιωμάτων, χρόνου απόκρισης, περιστατικών, παραπόνων, ανακλήσεων συγκατάθεσης και δεικτών εμπιστοσύνης πελατών.	DPO, Compliance, Διοίκηση	Χρόνος απόκρισης, ποσοστό εμπρόθεσμης διεκπεραίωσης και τάση παραπόνων
6	**Στοχευμένη υποστήριξη ΜΜΕ**	Παροχή απλουστευμένων υποδειγμάτων, συμβουλευτικών κόμβων, κοινών υπηρεσιών DPO και χρηματοδοτικών κινήτρων	Κράτος, επιμελητήρια, εποπτικές αρχές	Αριθμός ΜΜΕ που αξιοποιούν εργαλεία και ποσοστό ολοκλήρωσης

#	Πρακτικό βήμα	Κύρια ενέργεια	Υπεύθυνοι φορείς	Ενδεικτικός δείκτης
		για βασικές τεχνικές και οργανωτικές επενδύσεις.		σχεδίων συμμόρφωσης
7	**Διακυβέρνηση συστημάτων τεχνητής νοημοσύνης**	Καταγραφή όλων των συστημάτων AI, ταξινόμηση κινδύνου, ανθρώπινη εποπτεία, τεκμηρίωση δεδομένων εκπαίδευσης και συνδυασμένη αξιολόγηση DPIA και επιπτώσεων θεμελιωδών δικαιωμάτων.	AI governance team, DPO, Νομική υπηρεσία	Ποσοστό συστημάτων AI με ολοκληρωμένο φάκελο αξιολόγησης
8	**Δοκιμές ετοιμότητας και θεσμική συνεργασία**	Ετήσιες ασκήσεις αντιμετώπισης παραβίασης, σαφές πρωτόκολλο ενημέρωσης καταναλωτών και σταθερός δίαυλος συνεργασίας με εποπτικές αρχές και κλαδικούς φορείς.	Διοίκηση, IT Security, DPO	Χρόνος εντοπισμού, χρόνος απόκρισης και ποσοστό ολοκλήρωσης διορθωτικών ενεργειών

6.4 Περιορισμοί της έρευνας

Η παρούσα εργασία στηρίζεται σε βιβλιογραφική και ερμηνευτική προσέγγιση, γεγονός που καθορίζει την εμβέλεια των συμπερασμάτων της. Η σύνθεση επιστημονικών άρθρων, νομικών κειμένων, θεσμικών εκθέσεων και εμπειρικών μελετών προσφέρει ευρεία θεώρηση της σχέσης ανάμεσα στην προστασία δεδομένων, στην εμπιστοσύνη των καταναλωτών και στην επιχειρηματική ανάπτυξη. Παράλληλα, η απουσία πρωτογενών δεδομένων από καταναλωτές, στελέχη επιχειρήσεων, DPO και εποπτικούς φορείς περιορίζει τη δυνατότητα άμεσης επαλήθευσης των συμπερασμάτων στην ελληνική επιχειρηματική πραγματικότητα. Η εργασία αποδίδει συνεπώς τις κυρίαρχες τάσεις και τους βασικούς μηχανισμούς που αναδεικνύει η διαθέσιμη γνώση, ενώ η μέτρηση της πραγματικής έντασης των επιδράσεων απαιτεί ειδικά σχεδιασμένη εμπειρική έρευνα.

Ένας δεύτερος περιορισμός προκύπτει από την ετερογένεια του υλικού που εξετάστηκε. Οι μελέτες διαφοροποιούνται ως προς τη χώρα, τον κλάδο, το μέγεθος των επιχειρήσεων, τη χρονική περίοδο, το ερευνητικό σχέδιο και τους δείκτες που χρησιμοποιούν. Η εμπιστοσύνη αποτιμάται άλλοτε μέσω πρόθεσης χρήσης, άλλοτε μέσω αντιλαμβανόμενης ασφάλειας ή αφοσίωσης, ενώ το κόστος συμμόρφωσης προσεγγίζεται μέσα από νομικές, τεχνολογικές και οργανωτικές δαπάνες διαφορετικής έκτασης. Αυτή η ποικιλία ενισχύει την πολυδιάστατη κατανόηση του θέματος, ενώ περιορίζει την πλήρη συγκρισιμότητα των ευρημάτων και τη διαμόρφωση ενιαίων ποσοτικών εκτιμήσεων.

Η γεωγραφική και κλαδική κατανομή της διαθέσιμης βιβλιογραφίας αποτελεί επίσης σημαντική παράμετρο. Μεγάλο μέρος της εμπειρικής τεκμηρίωσης προέρχεται από διεθνείς αγορές, μεγάλες ψηφιακές πλατφόρμες και κλάδους υψηλής έντασης δεδομένων. Η ελληνική αγορά, οι μικρές και μεσαίες επιχειρήσεις, ο τουρισμός, το λιανεμπόριο και οι μικρότεροι πάροχοι ψηφιακών υπηρεσιών εκπροσωπούνται σε μικρότερη έκταση. Οι οργανωτικές δυνατότητες, οι διαθέσιμοι πόροι και η ωριμότητα των μηχανισμών συμμόρφωσης διαφοροποιούνται ουσιαστικά ανάμεσα σε μικρές και μεγάλες επιχειρήσεις. Η μεταφορά των διεθνών συμπερασμάτων στο ελληνικό περιβάλλον χρειάζεται επομένως κλαδική και οργανωτική προσαρμογή.

Πρόσθετος περιορισμός συνδέεται με την ταχύτητα των κανονιστικών και τεχνολογικών εξελίξεων. Η σταδιακή εφαρμογή του AI Act, η ανάπτυξη νέων κατευθυντήριων γραμμών, η διάδοση παραγωγικών συστημάτων τεχνητής νοημοσύνης και η επέκταση των υποδομών cloud μεταβάλλουν διαρκώς το περιβάλλον αυτοματοποιημένης λήψης αποφάσεων. Οι υποχρεώσεις των επιχειρήσεων και οι μορφές κινδύνου εξελίσσονται παράλληλα με τις τεχνολογικές δυνατότητες. Τα συμπεράσματα της εργασίας αποτυπώνουν το ισχύον στάδιο της σχετικής συζήτησης και αποκτούν μεγαλύτερη αξία μέσα από περιοδική επικαιροποίηση με βάση τη νέα νομολογία, την εποπτική πρακτική και τις τεχνικές εφαρμογές.

Τέλος, η οικονομική αποτίμηση των επιπτώσεων βασίστηκε κυρίως σε ποιοτικές και συγκριτικές ενδείξεις. Η διαθέσιμη βιβλιογραφία τεκμηριώνει κατηγορίες κόστους και οφέλους, ενώ παρουσιάζει περιορισμένη ομοιογένεια ως προς συγκεκριμένα χρηματικά μεγέθη, χρονικούς ορίζοντες και δείκτες απόδοσης. Η εκτίμηση της καθαρής οικονομικής επίδρασης της συμμόρφωσης απαιτεί στοιχεία για

επενδύσεις σε ανθρώπινο δυναμικό και τεχνολογία, κόστος διαχείρισης περιστατικών, απώλεια πελατών, μεταβολή φήμης και μακροπρόθεσμη απόδοση. Η απουσία κοινής βάσης μέτρησης περιορίζει την εξαγωγή γενικευμένων οικονομικών συμπερασμάτων για όλους τους τύπους επιχειρήσεων.

6.5 Προτάσεις για μελλοντική έρευνα και θεσμική εμβάθυνση

Η μελλοντική έρευνα μπορεί αρχικά να επικεντρωθεί στην ποσοτική αποτίμηση του κόστους και των επιχειρηματικών οφελών της συμμόρφωσης στην Ελλάδα. Μια κλαδικά διαστρωματωμένη έρευνα σε μικρές, μεσαίες και μεγάλες επιχειρήσεις θα μπορούσε να καταγράψει τις δαπάνες για DPO, νομική υποστήριξη, τεχνολογικές αναβαθμίσεις, εκπαίδευση, DPIA και διαχείριση περιστατικών. Η ίδια έρευνα μπορεί να εξετάσει μεταβολές στην εμπιστοσύνη, στην πιστότητα πελατών, στην ποιότητα δεδομένων και στη λειτουργική ανθεκτικότητα. Η συγκριτική ανάλυση μεταξύ τουρισμού, λιανεμπορίου, υγείας, χρηματοπιστωτικών υπηρεσιών και ηλεκτρονικού εμπορίου θα προσφέρει σαφέστερη εικόνα των κλαδικών διαφορών.

Ιδιαίτερα χρήσιμη κατεύθυνση αποτελεί η εμπειρική μελέτη του ρόλου και της ανεξαρτησίας του DPO. Συνεντεύξεις με DPO, διοικητικά στελέχη, νομικές υπηρεσίες και ομάδες πληροφορικής μπορούν να εξετάσουν την πρόσβαση του DPO στη διοίκηση, τη συμμετοχή του στον σχεδιασμό προϊόντων, την επάρκεια των πόρων και την πραγματική επιρροή του στις αποφάσεις. Παράλληλα, πιλοτικά προγράμματα data literacy μπορούν να αξιολογηθούν πριν και μετά την εφαρμογή τους ως προς τη γνώση των εργαζομένων, τη συχνότητα λαθών, τον χρόνο απόκρισης σε περιστατικά και την ποιότητα τεκμηρίωσης. Με αυτόν τον τρόπο θα αποτιμηθεί η συμβολή της οργανωσιακής μάθησης στην ουσιαστική συμμόρφωση.

Η συνδυασμένη εφαρμογή του GDPR και του AI Act συγκροτεί ένα ακόμη πεδίο υψηλής ερευνητικής προτεραιότητας. Μελέτες περίπτωσης σε πιστοληπτική αξιολόγηση, ασφάλιση, δυναμική τιμολόγηση, επιλογή προσωπικού και εξατομικευμένο ηλεκτρονικό εμπόριο μπορούν να εξετάσουν την ποιότητα της ανθρώπινης εποπτείας, την εξηγησιμότητα, τη δυνατότητα αμφισβήτησης και τη λειτουργία των εκτιμήσεων αντικτύπου. Πειραματικές έρευνες με καταναλωτές μπορούν να συγκρίνουν διαφορετικές μορφές ενημέρωσης και εξήγησης μιας

αυτοματοποιημένης απόφασης, με βασικές μεταβλητές την αντιλαμβανόμενη δικαιοσύνη, την κατανόηση, την εμπιστοσύνη και την πρόθεση άσκησης δικαιωμάτων.

Περαιτέρω έρευνα χρειάζεται και για τις συνέπειες των παραβιάσεων δεδομένων στην αγορά. Διαχρονικές μελέτες και αναλύσεις γεγονότων μπορούν να εξετάσουν τη μεταβολή της φήμης, της αξίας της επιχείρησης, της διατήρησης πελατών και του όγκου παραπόνων πριν και μετά από ένα περιστατικό. Η σύγκριση διαφορετικών στρατηγικών απόκρισης, όπως η άμεση ενημέρωση, η ανάληψη ευθύνης, η αποζημίωση και η παροχή πρακτικής υποστήριξης, θα επιτρέψει την αναγνώριση των αποτελεσματικότερων μηχανισμών αποκατάστασης της εμπιστοσύνης.

Μια ακόμη συγκεκριμένη κατεύθυνση αφορά την ανάπτυξη ενός σύνθετου δείκτη ψηφιακής εμπιστοσύνης και κανονιστικής ωριμότητας. Ο δείκτης μπορεί να συνδυάζει τη σαφήνεια των ενημερώσεων, τον αντιλαμβανόμενο έλεγχο, την ασφάλεια, τον χρόνο απόκρισης στα αιτήματα δικαιωμάτων, τη διαχείριση παραπόνων και την πρόθεση συνέχισης της χρήσης μιας υπηρεσίας. Η ψυχομετρική επικύρωσή του σε διαφορετικούς κλάδους θα δημιουργήσει κοινό εργαλείο αξιολόγησης και θα ενισχύσει τη συγκρισιμότητα των ερευνών.

Σε θεσμικό επίπεδο, ιδιαίτερη αξία παρουσιάζει η πιλοτική εφαρμογή κλαδικών προτύπων για DPIA, Privacy by Design, αυτοματοποιημένες αποφάσεις και διαχείριση περιστατικών. Η αξιολόγησή τους μπορεί να εξετάσει τον βαθμό υιοθέτησης, τη μείωση του διοικητικού κόστους, την ποιότητα της τεκμηρίωσης και την αποτελεσματικότητα των μέτρων προστασίας. Συγκριτικές μελέτες μεταξύ της Ελλάδας και άλλων κρατών μελών μπορούν επίσης να αναλύσουν τον χρόνο επίλυσης καταγγελιών, τη μορφή της εποπτικής καθοδήγησης και την υποστήριξη που παρέχεται στις ΜΜΕ. Αυτές οι ερευνητικές κατευθύνσεις θα συνδέσουν στενότερα τη θεωρητική γνώση με την εφαρμογή και θα προσφέρουν τεκμηριωμένες βάσεις για αποτελεσματικότερες δημόσιες και επιχειρηματικές πολιτικές.

Βιβλιογραφία

Abomhara, M., Nweke, L. O., Yayilgan, S. Y., et al. (2024). Enhancing privacy protections in national identification systems: An examination of stakeholders' knowledge, attitudes, and practices of Privacy by Design. *International Journal of Information Security, 23*, 3665–3689.

Abrardi, L., Comino, S., & Grassini, S. (2025). The economics of cyber risk: A survey of the literature. *Journal of Industrial and Business Economics*.

Acev, D., Biyani, S., Rieder, F., et al. (2025). Systematic analysis of data governance frameworks and their relevance to data trusts. *Management Review Quarterly*.

Alashoor, T., Boodraj, M., Quintanilha, A., Palme, S., & Aldawood, H. (2025). Insights on how data privacy officers can build a corporate privacy culture. *MIS Quarterly Executive, 24*(1).

Alhumud, A. A., Leonidou, L. C., Alarfaj, W., & Ioannidis, A. (2025). The impact of digital CSR disclosure on customer trust and engagement: The moderating role of consumer deontology and law obedience. *Journal of Business Research, 186*, 115035.

Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2022). The critical success factors for Security Education, Training and Awareness program effectiveness: A lifecycle model. *Information Technology & People, 36*(8), 94–125.

Alzaidi, M. S., & Agag, G. (2022). The role of trust and privacy concerns in using social media for e retail services: The moderating role of COVID 19. *Journal of Retailing and Consumer Services, 68*, 103042.

Aridor, G., Che, Y.-K., & Salz, T. (2023). The effect of privacy regulation on the data industry: Empirical evidence from GDPR. *The RAND Journal of Economics, 54*, 695–730.

Auñón, J. M., Hurtado-Ramírez, D., Porras-Díaz, L., Irigoyen-Peña, B., Rahmian, S., Al-Khazraji, Y., Soler-Garrido, J., & Kotsev, A. (2024). Evaluation and utilisation of privacy enhancing technologies: A data spaces perspective. *Data in Brief, 55*, 110560.

Avramidis, P., Panagopoulos, N. G., Serfes, K., & Vlachos, P. A. (2026). Customer data privacy and security as a firm strategy: Financial implications, risks, and the role of product market competition. *Journal of Business Research, 208*.

Ayaz, O., Hosseini Tabaghdehi, S. A., Rosli, A., & Tambay, P. (2025). Ethical implications of employee and customer digital footprint: SMEs perspective. *Journal of Business Research, 188*, 115088.

Bernardo, B. M. V., São Mamede, H., Barroso, J. M. P., & Duarte dos Santos, V. M. P. (2024). Data governance and quality management: Innovation and breakthroughs across different fields. *Journal of Innovation & Knowledge, 9*(4), 100598.

Betzing, J. H., Tietz, M., vom Brocke, J., & others. (2020). The impact of transparency on mobile privacy decision making. *Electronic Markets, 30*, 607–625.

Birnhack, M. D., & Mundlak, G. (2025). The Brussels effects and the rise of a privacy profession. *International Data Privacy Law, 15*(2), 138–155.

Brito Bastos, F., & Pałka, P. (2023). Is centralised General Data Protection Regulation enforcement a constitutional necessity? *European Constitutional Law Review, 19*(3), 487–517

Brkan, M. (2017). AI supported decision making under the general data protection regulation. In *Proceedings of the 16th Edition of the International Conference on Artificial Intelligence and Law* (pp. 3–8). ACM.

Brodin, M. (2019). A framework for GDPR compliance for small and medium sized enterprises. *European Journal for Security Research, 4*, 243–264.

Brunotte, W., Specht, A., Chazette, L., & Schneider, K. (2023). Privacy explanations: A means to end-user trust. *Journal of Systems and Software, 195*, 111545.

Canhoto, A. I., Keegan, B. J., & Ryzhikh, M. (2024). Snakes and ladders: Unpacking the personalisation privacy paradox in the context of AI enabled personalisation in the physical retail environment. *Information Systems Frontiers, 26*, 1005–1024.

Cao, R., & Kretschmer, T. (2026). Regulation as opportunity: Proactive GDPR compliance in the US financial services industry. *Industrial and Corporate Change, 35*(1), 150–170.

Cardoso, A., Gabriel, M., Figueiredo, J., Oliveira, I., Rêgo, R., Silva, R., Oliveira, M., & Meirinhos, G. (2022). Trust and loyalty in building the brand relationship with the customer: Empirical analysis in a retail chain in Northern Brazil. *Journal of Open Innovation: Technology, Market, and Complexity, 8*(3), 109.

Carl, K. V., Mihale Wilson, C., Zibuschka, J., et al. (2024). A consumer perspective on corporate digital responsibility: An empirical evaluation of consumer preferences. *Journal of Business Economics, 94*, 979–1024.

Chan, H. Y., & Toh, H. J. (2025). A document analysis of international data transfer terms in smartwatch privacy policies: Inadequacies and recommendations for improvements. *International Review of Law, Computers & Technology*, 1–22.

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly, 35*(3), 445–459.

Chen, S. J., Tran, K. T., Xia, Z. R., Waseem, D., Zhang, J. A., & Potdar, B. (2023). The double edged effects of data privacy practices on customer responses. *International Journal of Information Management, 69*, 102600.

Chisam, N., Moffett, J. W., Germann, F., et al. (2026). Privacy trade offs in international markets. *Journal of International Business Studies*.

Choe, C., Matsushima, N., & Shekhar, S. (2025). The bright side of the GDPR: Welfare improving privacy management. *Management Science, 71*(8).

Christakis, T. (2024). Data free flow with trust: Current landscape, challenges and opportunities. *Journal of Cyber Policy, 9*(1), 95–120.

Congiu, R., Sabatino, L., & Sapi, G. (2022). The impact of privacy regulation on web traffic: Evidence from the GDPR. *Information Economics and Policy, 61*, 101003.

Daigle, B., & Khan, M. (2020). The EU General Data Protection Regulation: An analysis of enforcement trends by EU data protection authorities. *Journal of International Commerce and Economics*.

Daza Ramírez, M. T. (2025). Meta's privacy practices on Facebook: Compliance, integrity, and a framework for excellence. *Discover Artificial Intelligence, 5*, Article 139.

Dehling, T., & Sunyaev, A. (2023). A design theory for transparency of information privacy practices. *Information Systems Research, 35*(3), 956–977.

Dexe, J., Franke, U., Söderlund, K., & others. (2022). Explaining automated decision-making: A multinational study of the GDPR right to meaningful information. *The Geneva Papers on Risk and Insurance Issues and Practice, 47*, 669–697.

Dorfleitner, G., Hornuf, L., & Kreppmeier, J. (2023). Promise not fulfilled: FinTech, data privacy, and the GDPR. *Electronic Markets, 33*, 33.

Eke, D., & Stahl, B. (2024). Ethics in the governance of data and digital technology: An analysis of European data regulations and policies. *Digital Society, 3*, Article 11.

Ervits, I., & Maintz, J. (2025). The trade off between convenience and privacy: Sharing personal data with intelligent vehicles in exchange for convenient driving. *Entertainment Computing, 54*, 100950.

Evans, R., Hajli, N., & Nisar, T. M. (2023). Privacy enhancing factors and consumer concerns: The moderating effects of the General Data Protection Regulation. *British Journal of Management, 34*, 2075–2092.

Farhad, M. A. (2024). Consumer data protection laws and their impact on business models in the tech industry. *Telecommunications Policy, 48*(9), 102836.

Fattah, I. A. (2024). The mediating effect of data literacy competence in the relationship between data governance and data driven culture. *Industrial Management & Data Systems, 124*(5), 1823–1845.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management & Data Systems, 106*(5), 601–620.

Ford, A., Al-Nemrat, A., Ghorashi, S. A., & Davidson, J. (2023). The impact of GDPR infringement fines on the market value of firms. *Information and Computer Security, 31*(1), 51–64.

Fox, G., Lynn, T., & Rosati, P. (2022). Enhancing consumer perceptions of privacy and trust: A GDPR label perspective. *Information Technology & People, 35*(8), 181–204.

Frey, C. B., & Presidente, G. (2024). Privacy regulation and firm performance: Estimating the GDPR effect globally. *Economic Inquiry, 62*(3), 1074–1089.

Fülöp, M. T., Ionescu, C. A., & Topor, D. I. (2025). Digital business world and ethical dilemmas: A systematic literature review. *Digital Finance, 7*, 23–41.

Gentile, G., & Lynskey, O. (2022). Deficient by design? The transnational enforcement of the GDPR. *International and Comparative Law Quarterly, 71*(4), 799–830.

Georgiadis, G., & Poels, G. (2022). Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review. *Computer Law & Security Review, 44*, 105640.

Gimpel, H., Kleindienst, D., Nüske, N., et al. (2018). The upside of data privacy: Delighting customers by implementing data privacy measures. *Electronic Markets, 28*, 437–452.

Grafenstein, M. von, Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: Effective data protection by design based on Art. 25 GDPR. *Computer Law & Security Review, 52*, 105924.

Gupta, A., & Dhami, A. (2015). Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites. *Journal of Direct, Data and Digital Marketing Practice, 17*, 43–53.

Haddara, M., Salazar, A., & Langseth, M. (2023). Exploring the impact of GDPR on big data analytics operations in the e commerce industry. *Procedia Computer Science, 219*, 767–777.

Hohmann, B., & Kollár, G. (2025). Reflections on the data protection compliance of AI systems under the EU AI Act. *Cogent Social Sciences, 11*(1).

Holmström, J., & Magnusson, J. (2025). Balancing innovation and regulation: The Data Sovereignty Assessment Framework. *Business Horizons*. Advance online publication.

Holzenberger, N., & Maxwell, W. (2025). A quantitative approach to the GDPR's anonymisation and appropriate technical and organisational measures tests. *Computer Law & Security Review, 59*, 106173.

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law, 28*(1), 65–98.

İyigün, U., & Ergene, D. (2026). Legal and ethical breaches in personal health data handling among cardiologists: A multicenter survey on compliance gaps and forensic risk. *Forensic Science International: Reports, 13*, 100444.

Jakobi, T., von Grafenstein, M., Legner, C., et al. (2020). The role of IS in the conflicting interests regarding GDPR. *Business & Information Systems Engineering, 62*, 261–272.

Johnson, G. A., Shriver, S. K., & Goldberg, S. G. (2023). Privacy and market concentration: Intended and unintended consequences of the GDPR. *Management Science, 69*(10).

Kang, L., Yhee, Y., Li, L., Lee, S. Y., & Koo, J. (2025). The effectiveness of corporate privacy responsibility and customer education on consumer responses in the digital era. *International Journal of Contemporary Hospitality Management, 37*(11), 3836–3854.

Kareklas, N., Michalopoulou, Z., & Giannakopoulou, F. (2024). Implementing GDPR in Greek companies: The necessary steps for integration. *Journal of Integrated Information Management, 5*(1), 7–12.

Kareklas, N., Michalopoulou, Z., & Giannakopoulou, F. (2024). Implementing GDPR in Greek companies: The necessary steps for integration. *Journal of Integrated Information Management, 5*(1), 7–12.

Kim, Y. J., Park, Y. S., & Park, S.-P. (2026). Enhancing data governance through transparency: An empirical study of the data trust model. *Technological Forecasting and Social Change, 225*, 124551.

Kohl, U. (2023). The right to be forgotten in data protection law and two Western cultures of privacy. *International & Comparative Law Quarterly, 72*(3), 737–769.

Krämer, J. (2024). The death of privacy policies: How app stores shape GDPR compliance of apps. *Internet Policy Review, 13*(2).

Krämer, J. (2026). Balancing privacy and platform power in the mobile ecosystem: The case of Apple's App Tracking Transparency. *Computer Law & Security Review, 60*, 106255.

Kun, E. (2024). Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks, and examining challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act. *Computer Law & Security Review, 52*, 105931.

Lefrere, V., Warberg, L., Cheyre, C., Marotta, V., & Acquisti, A. (2025). Does privacy regulation harm content providers? A longitudinal analysis of the impact of the GDPR. *Management Science, 72*(3).

Leijten, E. L., & van der Hof, S. (2025). Dissecting the commercial profiling of children: A proposed taxonomy and assessment of the GDPR, UCPD, DSA and AI Act in light of the precautionary principle. *Computer Law & Security Review, 57*, 106143.

Li, S. (2023). Compensation for non material damage under Article 82 GDPR: A review of Case C-300/21. *Maastricht Journal of European and Comparative Law, 30*(3), 335–345.

Li, W., Li, Z., Li, W., Zhang, Y., & Li, A. (2025). Mapping the empirical literature of the GDPR's in effectiveness and effectiveness: A systematic review. *Computer Law & Security Review, 57*, 106129.

Li, Z., Lee, G., Raghu, T. S., & Shi, Z. (2024). Impact of the General Data Protection Regulation on the global mobile app market: Digital trade implications of data protection and privacy regulations. *Information Systems Research, 36*(2).

Liu, Q., Wang, R., Pareti, M., et al. (2026). Big data in consumer behavior research: A systematic review of data sources, analytical methods, and research questions. *Journal of Marketing Analytics*.

Madhusudhanan, S., & Jose, A. C. (2025). Privacy preservation techniques through data lifecycle: A comprehensive literature survey. *Computers & Security, 155*, 104473.

Magrizos, S., Campora, M., Lamprinakos, G., Giovanis, A., & Christofi, M. (2026). Transparency by design: The effect of privacy policies visualisation on brand trust and perceived intrusion. *Behaviour & Information Technology, 45*(3), 450–462.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58.

Masuch, K., Greve, M., & Trang, S. (2021). What to do after a data breach? Examining apology and compensation as response strategies for health service providers. *Electronic Markets, 31*, 829–848.

Miller, K. M., Lukic, K., & Skiera, B. (2026). The impact of the General Data Protection Regulation on online tracking. *International Journal of Research in Marketing, 43*(1), 48–70.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read or do not read online privacy notices. *Journal of Interactive Marketing, 18*(3), 15–29.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs, 35*, 27–44.

Mohr, H., & Walter, Z. (2019). Formation of consumers' perceived information security: Examining the transfer of trust in online retailers. *Information Systems Frontiers, 21*, 1231–1250.

Montecchi, M., Plangger, K., West, D., & de Ruyter, K. (2024). Perceived brand transparency: A conceptualization and measurement scale. *Psychology & Marketing, 41*(10), 2274–2297.

Mühlhoff, R. (2023). Predictive privacy: Collective data protection in the context of artificial intelligence and big data. *Big Data & Society, 10*(1).

Naghmouchi, M., Laurent, M., Levallois-Barth, C., & Kaaniche, N. (2025). Perspectives on national digital identity systems. *Blockchain: Research and Applications*, Article 100429.

Nikkhah, H. R. (2025). A field experiment on response strategy in non alternative environments: A moderated mediation model. *Information & Management, 62*(4), 104134.

Nikou, S., De Reuver, M., & Mahboob Kanafi, M. (2022). Workplace literacy skills: How information and digital literacy affect adoption of digital technology. *Journal of Documentation, 78*(7), 371–391.

Orlando, A. (2025). A semantic approach to understanding GDPR fines: From text to compliance insights. *Computer Law and Security Review, 59*, 106187.

Peukert, C., Bechtold, S., Batikas, M., & Kretschmer, T. (2022). Regulatory spillovers and data governance: Evidence from the GDPR. *Marketing Science, 41*(4).

Pichlak, M., & Gaczoł, K. (2023). Simple and advanced reflexivity in GDPR enforcement: Empirical evidence from DPA activity. *International Data Privacy Law, 13*(4), 267–283.

Pollach, I. (2011). Online privacy as a corporate social responsibility: An empirical study. *Business Ethics: A European Review, 20*(1), 88–102.

Presthus, W., & Sørum, H. (2018). Are consumers concerned about privacy? An online survey emphasizing the General Data Protection Regulation. *Procedia Computer Science, 138*, 603–611.

Prince, C., Omrani, N., & Schiavone, F. (2024). Online privacy literacy and users' information privacy empowerment: The case of GDPR in Europe. *Information Technology & People, 37*(8), 1–24.

Quinn, P., & Malgieri, G. (2021). The difficulty of defining sensitive data: The concept of sensitive data in the EU data protection framework. *German Law Journal, 22*(8), 1583–1612.

Quinn, P., Ellyne, E., & Yao, C. (2024). Will the GDPR restrain Health Data Access Bodies under the European Health Data Space. *Computer Law & Security Review, 54*, 105993.

Raibulet, C., & Wang, K. (2025). Awareness of privacy and data collection: Exploring privacy policy effectiveness in Google Maps. *Frontiers in Computer Science, 7*, Article 1568179.

Rhahla, M., Allegue, S., & Abdellatif, T. (2021). Guidelines for GDPR compliance in Big Data systems. *Journal of Information Security and Applications, 61*, 102896.

Rodríguez Mejías, S., Degli-Esposti, S., González-García, S., & Parra-Calderón, C. L. (2024). Toward the European Health Data Space: The IMPaCT Data secure infrastructure for EHR based precision medicine research. *Journal of Biomedical Informatics, 156*, 104670.

Rughiniș, R., Rughiniș, C., Vulpe, S. N., & Rosner, D. (2021). From social netizens to data citizens: Variations of GDPR awareness in 28 European countries. *Computer Law & Security Review, 42*, 105585.

Ruohonen, J., & Hjerppe, K. (2022). The GDPR enforcement fines at glance. *Information Systems, 106*, 101876.

Ryngaert, C., & Taylor, M. (2020). The GDPR as global data protection regulation? *AJIL Unbound, 114*, 5–9.

Sansome, K., Wilkie, D., & Conduit, J. (2024). Beyond information availability: Specifying the dimensions of consumer perceived brand transparency. *Journal of Business Research, 170*, 114358.

Saxena, C., & Thakur, P. (2024). Mediating role of trust and privacy concerns between web assurance mechanism and purchase intention of online products. *Telematics and Informatics Reports, 16*, 100177.

Schäfer, F., Gebauer, H., Gröger, C., Gassmann, O., & Wortmann, F. (2023). Data driven business and data privacy: Challenges and measures for product based companies. *Business Horizons, 66*(4), 493–504.

Schumann, J. H., Zimmermann, J., Steinhoff, L., Totzek, D., van der Borgh, M., & Martin, K. D. (2025). Toward a multilayered framework of privacy related decision making in B2B. *Journal of Business Research, 190*, 115243.

Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security based approach to understand the pattern of adoption. *Interacting with Computers, 22*(5), 428–438.

Slapničar, S., Axelsen, M., & Eulerich, M. (2025). Cyber risk management: An illusion of a risk based approach. *Journal of Management Control*.

Smirnova, Y., & Travieso Morales, V. (2025). Tech startups and general data protection regulation: An empirical exploration of compliance challenges. *Journal of Small Business and Enterprise Development, 32*(8), 54–82.

Sørum, H., & Presthus, W. (2020). Dude, where's my data? The GDPR in practice, from a consumer's point of view. *Information Technology & People, 34*(3), 912–929.

Steele, V. (2022). Corporate social responsibility, data protection and the digital economy. *LMJU Student Law Journal, 2*.

Strzelecki, A., & Rizun, M. (2020). Consumers' security and trust for online shopping after GDPR: Examples from Poland and Ukraine. *Digital Policy, Regulation and Governance, 22*(4), 289–305.

Swani, K., Labrecque, L., & Markos, E. (2024). Are B2B data breaches concerning? Consequences of buyer's or firm's data loss on buyer and supplier related outcomes. *Industrial Marketing Management, 119*, 43–61.

Swani, K., Milne, G. R., & Brown, B. P. (2023). The benefits of meeting buyer privacy expectations across information, time, and space dimensions. *Industrial Marketing Management, 112*, 14–26.

Thomaidou, A., & Limniotis, K. (2025). Navigating through human rights in AI: Exploring the interplay between GDPR and Fundamental Rights Impact Assessment. *Journal of Cybersecurity and Privacy, 5*(1), Article 7.

Thomas, L., Gondal, I., Oseni, T., & Firmin, S. (2022). A framework for data privacy and security accountability in data breach communications. *Computers & Security, 116*, 102657.

Tiron Tudor, A., & Deliu, D. (2026). Charting the course: Embedding corporate digital responsibility into service organizations' decision making. *Journal of Service Management, 37*(2), 197–226.

Türegün, N. (2025). Digital transformation and cybersecurity risks. *International Journal of Accounting Information Systems, 56*, 100749.

Vallejo Blanxart, A., Peláez, A., Ibáñez, D. G., et al. (2026). Privacy centric marketing: Managerial insights for compliance and competitive differentiation. *Review of Managerial Science*.

van der Merwe, J., & Al Achkar, Z. (2022). Data responsibility, corporate social responsibility, and corporate digital responsibility. *Data & Policy, 4*, e12.

van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of Consumer Policy, 42*, 91–107.

Volz, F., Münch, C., Lohmüller, M., & Küffner, C. (2025). From data jungle to data governance in digital ecosystems: Empirical evidence from a multiple holistic case study. *Journal of Business Research, 201*, 115747.

Wachter, S. (2018). The GDPR and the Internet of Things: A three step transparency model. *Law, Innovation and Technology, 10*(2), 266–294.

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security, 147*, 104051.

Wang, X., Yan, J., Munyon, T. P., et al. (2025). Breached but not broken: How attributional information shapes shareholder reactions to firms following data breaches. *Corporate Reputation Review, 28*, 71–92.

Wiefling, S., Tolsdorf, J., & Lo Iacono, L. (2022). Data protection officers' perspectives on privacy challenges in digital ecosystems. In *Proceedings of SPOSE 2022*.

Wolff, J., & Atallah, N. (2021). Early GDPR penalties: Analysis of implementation and fines through May 2020. *Journal of Information Policy, 11*, 63–103.

Wong, B. (2019). Delimiting the concept of personal data after the GDPR. *Legal Studies, 39*(3), 517–532.

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28*(3), 889–897.

Wulf, A. J., & Seizov, O. (2024). Please understand we cannot provide further information: Evaluating content and transparency of GDPR mandated AI disclosures. *AI & Society, 39*, 235–256.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798–824.

Xu, W., & Zuo, X. (2026). Confronting cross border data risks. *Journal of Global Information Management, 34*(1).

Young, S., & Visser, F. (2026). Agency between logics: Data privacy tactics, ethics, and the power of the Data Protection Officer. *Journal of Technical Writing and Communication, 56*(1), 79–92.

Zhang, D., Finckenberg-Broman, P., Hoang, T., et al. (2025). Right to be forgotten in the era of large language models: Implications, challenges, and solutions. *AI Ethics, 5*, 2445–2454.

Zhang, J. H., Koivumäki, T., & Chalmers, D. (2024). Privacy vs convenience: Understanding intention behavior divergence post-GDPR. *Computers in Human Behavior, 160*, 108382.

Zhang, Y., Wang, T., & Hsu, C. (2020). The effects of voluntary GDPR adoption and the readability of privacy statements on customers' information disclosure intention and trust. *Journal of Intellectual Capital, 21*(2), 145–163.

Zhou, L., Diro, A., Saini, A., Kaisar, S., & Hiep, P. C. (2024). Leveraging zero knowledge proofs for blockchain based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications, 80*, 103678.

Επίσημοι φορείς

EUR Lex. Γενικός κανονισμός για την προστασία δεδομένων.

EUR Lex. Προστασία δεδομένων προσωπικού χαρακτήρα.

EUR-Lex. *Data protection in the electronic communications sector*.

EUR-Lex. *Digital Services Act*.

EUR-Lex. *European data governance*.

EUR-Lex. *Protection of privacy in the electronic communications sector*.

EUR-Lex. *Rules for trustworthy artificial intelligence in the EU*.

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2019). *Νόμος 4624/2019 σε μετάφραση της ΑΠΔΠΧ.*

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2019). *Περίληψη της απόφασης 26/2019 της Ελληνικής ΑΠΔΠΧ.*

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2024α). *Ετήσια έκθεση 2024*.

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2024β). *Απόφαση 42/2024*.

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. *(χ.χ.α). Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.*

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. *(χ.χ.β). Νομικό πλαίσιο προσωπικών δεδομένων.*

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. *(χ.χ.γ). Καταγγελία στην ΑΠΔΠΧ.*

Επίσημοι διαδικτυακοί τόποι

European Commission. (2025). Commission publishes the guidelines on prohibited artificial intelligence practices, as defined by the AI Act. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

European Commission. (2025). Key consumer data. https://commission.europa.eu/strategy-and-policy/policies/consumers/consumer-protection-policy/key-consumer-data_en

European Commission. (2026). Report on the need to review the list of prohibited AI practices and of high-risk AI systems listed in Annex III of the AI Act (COM(2026) 234 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026DC0234

European Data Protection Board. (2018). Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01). https://www.edpb.europa.eu/documents/guideline/automated-decision-making-and-profiling_en

European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts. Official Journal of the European Union, L 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

European Parliament. (2021). Consumer protection: How the EU boosts consumer rights. https://www.europarl.europa.eu/topics/en/article/20210506STO03603/consumer-protection-how-the-eu-boosts-consumer-rights

Eurostat. (2026). More than a third of online shoppers face issues. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260311-1

Federal Trade Commission. (2019). FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

Information Commissioner's Office. (2020α). British Airways penalty notice. https://ico.org.uk/media2/migrated/2618421/ba-penalty-20201016.pdf

Information Commissioner's Office. (2020β). Marriott International Inc. penalty notice. https://ico.org.uk/media2/migrated/2618524/marriott-international-inc-mpn-20201030.pdf

Lawspot. (2021). Προστασία των καταναλωτών: Πώς ενισχύεται το νομικό πλαίσιο της ΕΕ [Infographic]. https://www.lawspot.gr/nomika-nea/prostasia-ton-katanaloton-pos-enishyetai-nomiko-plaisio-tis-ee-infographic/

Newmoney. (2026). Πρόστιμο 150.000 ευρώ σε ηλεκτρονικό κατάστημα για παραπλάνηση καταναλωτών. https://www.newmoney.gr/roh/palmos-oikonomias/epixeiriseis/prostimo-e150-000-se-ilektroniko-katastima-gia-paraplanisi-katanaloton/

Ευρωπαϊκή Ένωση. *(2012).* Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.

Ευρωπαϊκή Επιτροπή. (2017). *Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και για την κατάργηση της Οδηγίας 2002/58/ΕΚ*.

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης. *(1995). Οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.*

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης. (2002). *Οδηγία 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών*.

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης. (2016). *Κανονισμός (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ*.

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης. (2022α). *Κανονισμός (ΕΕ) 2022/2065 για μια ενιαία αγορά ψηφιακών υπηρεσιών και για την τροποποίηση της Οδηγίας 2000/31/ΕΚ.*

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης. (2022β). *Κανονισμός (ΕΕ) 2022/1925 για αμφισβητήσιμες και δίκαιες αγορές στον ψηφιακό τομέα.*

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης. (2022γ). *Κανονισμός (ΕΕ) 2022/868 για την ευρωπαϊκή διακυβέρνηση δεδομένων.*

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης. (2024). *Κανονισμός (ΕΕ) 2024/1689 για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη.*

Ευρωπαϊκό Κοινοβούλιο, & Συμβούλιο της Ευρωπαϊκής Ένωσης. (2005). Οδηγία 2005/29/ΕΚ για τις αθέμιτες εμπορικές πρακτικές των επιχειρήσεων προς τους καταναλωτές στην εσωτερική αγορά.

Ευρωπαϊκό Κοινοβούλιο, & Συμβούλιο της Ευρωπαϊκής Ένωσης. (2011). Οδηγία 2011/83/ΕΕ για τα δικαιώματα των καταναλωτών.

Συνήγορος του Καταναλωτή. (2026). Ετήσια έκθεση 2024. https://www.synigoroskatanaloti.gr/sites/default/files/annual_exhibitions/attached_files/2026-05/StK-Annual-Report-2024.pdf

Τσότσου, Α. (2020). Η προστασία του καταναλωτή στο ηλεκτρονικό εμπόριο. Lawyer. https://lawyermagazine.gr/i-prostasia-tou-katanalwth-sto-hlektroniko-emporio/

Υπηρεσία Προστασίας Καταναλωτή Κύπρου. (2025). Αποτελέσματα ελέγχου καταστημάτων πώλησης σχολικών ειδών.

https://consumer.gov.cy/gr/ενημέρωση/ανακοινώσεις/αποτελέσματα-ελέγχου-καταστημάτων-πώλησης-σχολικών-ειδών

Υπουργείο Ανάπτυξης. (2024). Πρόστιμα συνολικού ύψους 1.480.000 ευρώ σε 11 επιχειρήσεις. https://www.mindev.gov.gr/πρόστιμα-συνολικού-ύψους-1-480-000-ευρώ-σε-11-επ/

Υπουργείο Ψηφιακής Διακυβέρνησης και Τεχνητής Νοημοσύνης. (2026). Στη Βουλή το σχέδιο νόμου για το Εθνικό Εφαρμοστικό Πλαίσιο του Κανονισμού για την Τεχνητή Νοημοσύνη (AI Act). https://www.mindigital.gr/archives/8936