



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Πρόγραμμα Μεταπτυχιακών Σπουδών
«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»
Ακαδημαϊκό έτος 2024-2025

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της Φαφαλιού Άννας (Α.Μ.: ΜΔΙ2355)

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ: ΣΧΕΣΗ
ΑΛΛΗΛΟΣΥΜΠΛΗΡΩΣΗΣ Η/ΚΑΙ ΑΝΤΙΘΕΣΗΣ;
CYBERSECURITY AND DATA PROTECTION: A COMPLEMENTARY
AND/OR OPPOSING RELATIONSHIP?

Επιβλέπουσα:

Λίλιαν Μήτρου

Πειραιάς, Ιούνιος 2025

© 2025

Της Φαφαλιού Άννας

ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

Τμήμα Ψηφιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Το Πόνημα αυτό αφιερώνω στους γονείς μου,

Σοφία και Νίκο,

τους δύο «φάρους» της ζωής μου...

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα μεταπτυχιακή διπλωματική εργασία εκπονήθηκε στο πλαίσιο του Μεταπτυχιακού Προγράμματος Σπουδών “Δίκαιο και Τεχνολογίες Πληροφορικής και Επικοινωνιών - *Law & ICT*” του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς. Αποτελεί τον καρπό της πιο πνευματικά γόνιμης περιόδου της ζωής μου έως τώρα και έρχεται να επιστεγάσει τα δύο αξέχαστα τελευταία έτη.

Θα ήθελα πρωτίστως να εκφράσω τις θερμές μου ευχαριστίες στην επιβλέπουσα καθηγήτριά μου, Λίλιαν Μήτρου, για την εμπνευσμένη καθοδήγηση, την επιστημονική εποπτεία και τα διαρκή ερεθίσματα καθ’ όλη τη διάρκεια των μεταπτυχιακών μου σπουδών. Η συμβολή της στον επιστημονικό χώρο διαχρονικά υπήρξε για εμένα έμπνευση να ακολουθήσω το δύσβατο μονοπάτι της μελέτης των ποικίλων πτυχών της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων.

Ιδιαίτερη θέση στην ευχαριστήρια αυτή ενότητα, αλλά και στην ωρίμανσή μου επιστημονικά, έχει ο Διευθυντής του ΠΜΣ, Καθηγητής Στέφανος Γκρίτζαλης. Η οξύνοια και η ακεραιότητά του μου αποδεικνύουν πως τα πιο στέρεα νομικά συμπεράσματα μπορούν να επιτευχθούν πάντα κατόπιν ενδελεχούς στάθμισης κάθε ατομικού δικαιώματος, χωρίς κανένα εξ αυτών να διυλίζεται, ακόμα και στους πιο χαλεπούς καιρούς.

Ευχαριστώ, επίσης, όλους τους καθηγητές και τις καθηγήτριες του Προγράμματος για το υψηλό επίπεδο διδασκαλίας, τη μεταδοτικότητα, τη διαθεσιμότητα και την ευρύτητα σκέψης που μοιράστηκαν απλόχερα. Η ακαδημαϊκή εμπειρία των δύο αυτών ετών υπήρξε για εμένα εφελκυστήριο για περαιτέρω επιστημονικές αναζητήσεις, πάντα με κριτήριο την διεπιστημονικότητα και τη σφαιρική γνώση.

Ιδιαίτερη μνεία οφείλω στην υποστήριξη που έλαβα μέσω της **υποτροφίας αριστείας**, με την οποία με τίμησε το Πανεπιστήμιο Πειραιώς, για το εαρινό εξάμηνο του ακαδημαϊκού έτους 2023-2024.

Θερμές ευχαριστίες, τέλος, εκφράζω προς όλους τους οικείους μου για την αμέριστη στήριξη, την υπομονή και την αδιάλειπτη πίστη στις δυνατότητές μου.

ΠΕΡΙΛΗΨΗ	10
Abstract	12
ΕΙΣΑΓΩΓΗ	14
ΚΕΦΑΛΑΙΟ 1 - ΕΙΣΑΓΩΓΙΚΟ ΘΕΩΡΗΤΙΚΟ ΠΛΑΙΣΙΟ – ΟΡΙΟΘΕΤΗΣΗ ΤΗΣ ΑΝΑΛΥΣΗΣ	16
1.1 Ορισμοί και Εννοιολογικές Διακρίσεις	16
1.1.1 Κυβερνοασφάλεια: Αντικείμενο, Πεδίο και Θεμελιώδεις Αρχές	16
1.1.2 Προστασία Προσωπικών Δεδομένων: Νομικές και Θεσμικές Διαστάσεις ..	17
1.1.3 Σχέση και Διασύνδεση μεταξύ Κυβερνοασφάλειας και Προστασίας Δεδομένων	17
1.2 ΘΕΩΡΗΤΙΚΕΣ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΚΕΣ ΠΡΟΣΕΓΓΙΣΕΙΣ	18
1.2.1 Ρυθμιστική Θεωρία και Risk-Based Regulation	18
1.2.2 Νομικός Θετικισμός και Θεωρίες Δικαιωμάτων	19
1.2.3 Τεχνο-ρυθμιστική Προσέγγιση: Privacy by Design και Accountability	19
1.2.4 Κριτικές Θεωρίες Ιδιωτικότητας: Η Θεωρία της Πλαισιακής Ακεραιότητας (Contextual Integrity)	20
1.3. Μεθοδολογία της Διπλωματικής Εργασίας	21
Ειδική βιβλιογραφία κεφαλαίου 1	22
ΚΕΦΑΛΑΙΟ 2 - ΘΕΣΜΙΚΟ ΚΑΙ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ	23
2.1 Ευρωπαϊκό Ρυθμιστικό Πλαίσιο για την Προστασία Δεδομένων	23
2.1.1 Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR): Βασικές Αρχές και Υποχρεώσεις	23
2.1.2 Ο ρόλος του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (EDPB) και των Εθνικών Αρχών	25
2.1.3 Η εφαρμογή του GDPR σε διακρατικά περιβάλλοντα και η νομολογία Schrems I & II	27

2.2 Αρχές και διακυβέρνηση της κυβερνοασφάλειας στην ΕΕ	28
2.2.1 Οδηγία NIS 2: Επέκταση της Ευθύνης για την Κυβερνοασφάλεια	32
2.2.2 Ο Κανονισμός για την Κυβερνοασφάλεια (EU Cybersecurity Act)	34
2.2.3 ΑΝΑΓΚΗ ΓΙΑ ΕΝΙΑΙΟ ΡΥΘΜΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΣΤΗΝ ΕΕ	35
2.2.4 Ψηφιακή Κυριαρχία και εντοπιότητα Δεδομένων στην ΕΕ.....	36
2.3 Διεθνείς Συνθήκες και Πρωτοβουλίες στον Τομέα της Κυβερνοασφάλειας και της Προστασίας Δεδομένων	38
2.3.1 Η Σύμβαση της Βουδαπέστης για το Κυβερνοέγκλημα	38
2.3.2 Πρωτοβουλίες του ΟΟΣΑ για την Διακυβέρνηση Δεδομένων	39
2.4 Το Εθνικό Πλαίσιο στην Ελλάδα: Διακυβέρνηση, Αρμοδιότητες και Νομοθεσία	41
2.4.1 Αρμόδιες Αρχές και Νομοθετικό Πλέγμα.....	41
2.4.2 Η Εθνική Στρατηγική Κυβερνοασφάλειας (2020–2025)	42
Ειδική βιβλιογραφία κεφαλαίου 2.....	43
ΚΕΦΑΛΑΙΟ 3 - Η ΑΡΡΗΚΤΗ ΣΧΕΣΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ: ΣΥΓΚΡΟΥΣΗ Ή ΣΥΓΚΛΙΣΗ;	47
3.1. Η θεμελιώδης σημασία της κυβερνοασφάλειας για την προστασία προσωπικών δεδομένων	48
3.1.1 Το δικαίωμα στην ιδιωτικότητα ως κριτήριο οριοθέτησης των μέτρων κυβερνοασφάλειας.....	48
3.1.2 ΑΝΤΙΦΑΣΕΙΣ ΚΑΙ ΠΡΟΚΛΗΣΕΙΣ: ΠΡΟΣ ΜΙΑ ΛΕΙΤΟΥΡΓΙΚΗ ΣΥΝΘΕΣΗ	49
3.1.3 ΤΟ ΠΛΑΙΣΙΟ ΤΗΣ «ΨΗΦΙΑΚΗΣ ΕΜΠΙΣΤΟΣΥΝΗΣ»	50
3.2 Ο «διάλογος» μεταξύ της κυβερνοασφάλειας και της ελεύθερης ροής δεδομένων εντός ΕΕ.....	51
3.2.1 NIS2 και Cyber Resilience Act	51
3.2.2 Το όραμα της ΕΕ για ελεύθερη ροή δεδομένων σε έναν ασφαλή κυβερνοχώρο	52
3.2.3 Data Act και Data Governance Act	53

3.2.4 Κανονισμός DORA: Προς ένα Ψηφιακά Ανθεκτικό Χρηματοπιστωτικό σύστημα στην ΕΕ	55
Ειδική Βιβλιογραφία κεφαλαίου 3	57
ΚΕΦΑΛΑΙΟ 4 - ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ, BIG DATA ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ: ΕΝΑ ΠΛΑΙΣΙΟ ΤΕΧΝΟΛΟΓΙΚΩΝ ΠΡΟΚΛΗΣΕΩΝ ΚΑΙ ΝΟΜΙΚΗΣ ΠΡΟΣΑΡΜΟΓΗΣ.....	59
4.1 Η Τεχνητή Νοημοσύνη ως παράγων μεταβολής της έννοιας της ιδιωτικότητας.....	59
4.2 Big Data και κοινωνική τυποποίηση μέσω προφίλ	62
4.3 Τεχνολογικές εφαρμογές μετρίασης του κινδύνου περιστατικού παραβίασης προσωπικών δεδομένων	63
4.3.1 Κρυπτογράφηση, ανωνυμοποίηση, ψευδωνυμοποίηση	63
4.3.2 Το αντίκρισμα στην ευρωπαϊκή νομολογία	64
4.3.3 Καινοτομίες προσεγγίσεις στην ασφάλεια δεδομένων	65
4.4 Η ενσωμάτωση της "Privacy by design " στην ΤΝ	67
Ειδική βιβλιογραφία κεφαλαίου 4.....	68
ΚΕΦΑΛΑΙΟ 5 - ΜΕΛΕΤΕΣ ΠΕΡΙΠΤΩΣΗΣ ΚΑΙ ΕΦΑΡΜΟΓΕΣ	73
5.1 Ορισμός και Διαχείριση Περιστατικών Παραβίασης Προσωπικών Δεδομένων.....	73
5.2 Περιπτωσιολογία περιστατικών παραβίασης	75
5.2.1 Διεθνή περιστατικά παραβίασης	75
5.2.2 Περιστατικά παραβίασης στην Ελλάδα.....	79
5.3 Καλές Πρακτικές Προστασίας Δεδομένων σε Εταιρείες Τεχνολογίας.....	81
5.4 Από την Κανονιστική Αρχή στην Πρακτική Εφαρμογή: Η Ασφάλεια Εξ Αρχής και το Παράδειγμα της Ελλάδας.....	83
Ειδική βιβλιογραφία κεφαλαίου 5.....	85
ΚΕΦΑΛΑΙΟ 6 – ΣΥΜΠΕΡΑΣΜΑΤΙΚΕΣ ΣΚΕΨΕΙΣ - ΔΕΟΝΤΟΛΟΓΙΑ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ: ΠΡΟΣ ΕΝΑ ΔΗΜΟΚΡΑΤΙΚΟ ΨΗΦΙΑΚΟ ΜΕΛΛΟΝ	89
6.1 Η προσέγγιση από πλευράς Δικαίου	89

6.2 Μία φιλοσοφική θεώρηση	92
Ειδική βιβλιογραφία κεφαλαίου 6	94
ΠΑΡΑΡΤΗΜΑ 1: ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ	98
ΠΑΡΑΡΤΗΜΑ 2: ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ ΚΑΙ ΕΙΚΟΝΩΝ	100
ΠΙΝΑΚΑΣ ΒΙΒΛΙΟΓΡΑΦΙΚΩΝ ΑΝΑΦΟΡΩΝ	101
Ξενόγλωσση Βιβλιογραφία	101
<i>Ευρωπαϊκή Νομολογία</i>	<i>113</i>
Ελληνόγλωσση Βιβλιογραφία	115
<i>Ελληνική Νομοθεσία</i>	<i>115</i>

ΠΕΡΙΛΗΨΗ

Η παρούσα μεταπτυχιακή διπλωματική εργασία εστιάζει στη σχέση μεταξύ της **προστασίας προσωπικών δεδομένων** και της **κυβερνοασφάλειας**, δύο τομέων οι οποίοι αναδεικνύονται ως δομικοί πυλώνες του σύγχρονου ψηφιακού κράτους δικαίου. Η εξέλιξη της τεχνολογίας, οι θεσμικές πρωτοβουλίες της Ευρωπαϊκής Ένωσης και οι γεωπολιτικές απειλές επαναπροσδιορίζουν συνεχώς τα όρια, τις συγκλίσεις και τις εντάσεις μεταξύ των δύο αυτών πλαισίων. Η μελέτη επιχειρεί να αναδείξει τη **συστημική και συμπληρωματική διάσταση** των δύο πεδίων, χωρίς να αγνοεί τις στιγμές **κανονιστικής ή επιχειρησιακής τριβής**.

Αρχικά, παρουσιάζεται η **ευρωπαϊκή και διεθνής κανονιστική θεμελίωση**, με έμφαση στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR), την Οδηγία NIS 2 για την ασφάλεια των δικτύων και πληροφοριών, τον Κανονισμό DORA, καθώς και την εξελισσόμενη ευρωπαϊκή στρατηγική ψηφιακής κυριαρχίας.

Σε δεύτερο επίπεδο, εξετάζονται οι **θεωρητικές προσεγγίσεις** που φωτίζουν τη σχέση των δύο πλαισίων, ιδίως μέσα από τη μεθοδολογία risk-based λογοδοσίας (accountability), τις αρχές της ασφάλειας και της προστασίας by design, καθώς και την έννοια της ψηφιακής κυριαρχίας. Ακολουθεί **ανάλυση της νομολογίας**, με έμφαση στις υποθέσεις Schrems I και II, και την απόφαση Volkszählungsurteil του Γερμανικού Συνταγματικού Δικαστηρίου, που κατοχύρωσε τη συνταγματική αρχή του πληροφοριακού αυτοκαθορισμού.

Ιδιαίτερη έμφαση δίνεται σε **πραγματικά περιστατικά παραβίασης δεδομένων**, τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα, στην Ελλάδα και διεθνώς. Οι περιπτώσεις αυτές εξετάζονται υπό το πρίσμα της θεσμικής απόκρισης, της διαχειριστικής επάρκειας και των συνεπειών για τη συμμόρφωση με το ισχύον κανονιστικό πλαίσιο. Αναλύονται επίσης οι **τεχνολογικές εξελίξεις**, όπως η Τεχνητή Νοημοσύνη, το Blockchain και η αρχιτεκτονική Zero Trust, ως παράγοντες που επαναδιαμορφώνουν το νομικό τοπίο και θέτουν νέα διλήμματα ως προς την ιδιωτικότητα και την ασφάλεια.

Η εργασία καταλήγει σε μία **διεπιστημονική προσέγγιση**, ενσωματώνοντας στοιχεία από τη νομική θεωρία, την πολιτική φιλοσοφία και την τεχνολογική ηθική. Αναδεικνύεται η ανάγκη για **ολιστικές πολιτικές ψηφιακής διακυβέρνησης**, που θα διασφαλίζουν τη διαλειτουργικότητα μεταξύ πλαισίων, τη λογοδοσία φορέων και τον σεβασμό των θεμελιωδών δικαιωμάτων. Ειδικό βάρος δίδεται στη θεμελίωση της **ψηφιακής κυριαρχίας** της ΕΕ έναντι τρίτων κρατών και πολυεθνικών, καθώς και στη συμβολή της εθνικής στρατηγικής κυβερνοασφάλειας στην ενίσχυση της εθνικής ανθεκτικότητας. Τέλος, προτείνεται ένα θεσμικό και ηθικό πλαίσιο που θεμελιώνεται σε αξίες της δημοκρατίας, της δικαιοσύνης του John Rawls, της διαβουλευτικής δημοκρατίας του Jurgen Habermas και της πολυφωνίας στον δημόσιο διάλογο της Hana Arendt, ενόψει των τεχνολογικών προκλήσεων του μέλλοντος.

Abstract

This master's thesis explores the relationship between **data protection** and **cybersecurity**, two interdependent fields that shape the architecture of the modern digital rule of law. As technological developments, geopolitical shifts, and regulatory transformations progress, the convergence—and at times tension—between privacy and security frameworks has emerged as a crucial challenge for both public governance and private sector accountability.

The study first analyzes the **legal and regulatory foundations** of both domains, focusing on key European legislative instruments such as the General Data Protection Regulation (GDPR), the NIS 2 Directive on network and information systems security, and the Digital Operational Resilience Act (DORA).

The thesis then develops a **theoretical foundation** for understanding the symbiotic relationship between cybersecurity and data protection, through concepts such as risk-based accountability, privacy and security by design/default, and digital sovereignty. Landmark **case law**, including Schrems I & II and the German Federal Constitutional Court's Volkszählungsurteil, are analyzed as legal touchstones that define the boundaries of informational self-determination in democratic societies.

A comprehensive review of **data breach incidents** is presented, both in Greece and internationally, highlighting the scope, impact, and response mechanisms to cyberattacks across different sectors. These case studies illustrate the operational challenges of compliance, the effectiveness of institutional coordination, and the necessity for resilience mechanisms in both critical infrastructure and public administration. The study also examines emerging **technological paradigms**—including Artificial Intelligence, Blockchain, and Zero Trust architecture—as transformative forces that challenge traditional data governance and raise novel legal and ethical questions.

Finally, the thesis concludes with a **normative and philosophical reflection** on the future of digital governance. It argues for holistic and adaptive policy approaches that bridge regulatory silos, enhance institutional transparency, and uphold fundamental rights in the digital age.

Building on principles drawn from political philosophy – such as Rawlsian justice, Habermasian deliberative democracy, and Arentian plurality – the thesis advocates for a **democratic ethos of technology** that foregrounds human dignity, institutional trust, and strategic autonomy for the European Union in a fragmented digital world.

ΕΙΣΑΓΩΓΗ

Η εποχή της ψηφιακής διακυβέρνησης και της μαζικής επεξεργασίας δεδομένων χαρακτηρίζεται από πρωτόγνωρες δυνατότητες και αδιαμφισβήτητα οφέλη για τη δημόσια διοίκηση, την επιχειρηματικότητα και την κοινωνική ζωή. Η ταχύτατη πρόοδος των τεχνολογιών πληροφορικής και επικοινωνιών (εφεξής οι «ΤΠΕ») συνοδεύεται ωστόσο από σοβαρούς κινδύνους και εντάσεις: η εκτεταμένη χρήση προσωπικών δεδομένων εγείρει θεμελιώδη ερωτήματα για την ιδιωτικότητα, ενώ η αυξανόμενη εξάρτηση από ψηφιακές υποδομές καθιστά τους θεσμούς ευάλωτους σε επιθέσεις, παραβιάσεις και κακόβουλες παρεμβάσεις. Η ανάγκη για ισχυρή και αξιόπιστη προστασία των προσωπικών δεδομένων, καθώς και για συνεκτικές στρατηγικές κυβερνοασφάλειας, αποτελεί πλέον κομβικό άξονα πολιτικής, νομικής και τεχνικής διαχείρισης.

Στο πλαίσιο αυτό, η εργασία επιχειρεί να χαρτογραφήσει τη σύνθετη και συχνά διαλεκτική σχέση ανάμεσα στην προστασία των προσωπικών δεδομένων και την κυβερνοασφάλεια, δύο πεδία που εξελίχθηκαν αρχικά με διακριτές στοχεύσεις και εργαλεία, αλλά πλέον συγκλίνουν σε κοινές θεσμικές και πρακτικές προσεγγίσεις. Το βασικό ερώτημα που τίθεται είναι εάν και σε ποιο βαθμό οι δύο αυτοί τομείς λειτουργούν αλληλοσυμπληρωματικά ή βρίσκονται σε σχέση έντασης, και πώς μπορεί να επιτευχθεί η ισορροπία μεταξύ ασφάλειας και προστασίας του διακινδυνευομένου αγαθού, της ιδιωτικότητας.

Αφετηρία της ανάλυσης αποτελεί το ρυθμιστικό πλαίσιο της Ευρωπαϊκής Ένωσης (εφεξής η «ΕΕ» ή η «Ένωση»), με κεντρικούς άξονες τον Γενικό Κανονισμό για την Προστασία Δεδομένων GDPR (εφεξής ο «GDPR» ή ο «Κανονισμός»), την Οδηγία NIS και τη μετεξέλιξή της, NIS 2 (εφεξής η NIS2» ή η «Οδηγία»), καθώς και τους πιο πρόσφατους κανονισμούς για τη διακυβέρνηση των δεδομένων (Data Governance Act, Data Act) και την τεχνητή νοημοσύνη (Artificial Intelligence Act, εφεξής η «AI Act»). Η ευρωπαϊκή προσέγγιση βασίζεται σε ένα πολυεπίπεδο σύστημα προστασίας, το οποίο συνδυάζει νομική δεσμευτικότητα, τεχνολογική καινοτομία και θεσμική λογοδοσία. Παράλληλα, εξετάζονται σημαντικές

διεθνείς πρωτοβουλίες, όπως η Σύμβαση της Βουδαπέστης για το κυβερνοέγκλημα, οι οδηγίες του ΟΟΣΑ για το data stewardship και οι διεθνείς πρακτικές προστασίας δεδομένων.

Η μελέτη επεκτείνεται και στο ελληνικό θεσμικό πλαίσιο, καταγράφοντας την ενσωμάτωση των ευρωπαϊκών οδηγιών και κανονισμών στην εθνική έννομη τάξη, με έμφαση στον νόμο 4624/2019 για την εφαρμογή του GDPR και τον πρόσφατο νόμο 5002/2022 που τροποποιεί την οδηγία NIS στην Ελλάδα. Παράλληλα, αναλύεται η εθνική στρατηγική κυβερνοασφάλειας (2020–2025), ενώ παρουσιάζονται καλές πρακτικές φορέων όπως η ΑΑΔΕ στην υιοθέτηση προτύπων ISO για την ασφάλεια πληροφοριών. Η μελέτη περιλαμβάνει επίσης περιστατικά παραβίασης στον δημόσιο και ιδιωτικό τομέα, λειτουργώντας ως εμπειρική βάση για τη συζήτηση περί επάρκειας ή ελλείψεων του εφαρμοζόμενου πλαισίου.

Ιδιαίτερη έμφαση δίδεται στις θεωρητικές και τεχνολογικές εξελίξεις που διαμορφώνουν το παρόν και το μέλλον της προστασίας δεδομένων και της ασφάλειας. Αναλύονται κριτικά σύγχρονες τεχνολογίες όπως η τεχνητή νοημοσύνη, το blockchain και η αρχιτεκτονική zero trust, τόσο ως παράγοντες ενίσχυσης της ασφάλειας, όσο και ως προκλήσεις για την προστασία της ιδιωτικότητας και των θεμελιωδών δικαιωμάτων. Επιπλέον, διερευνώνται εναλλακτικές προσεγγίσεις προστασίας της ιδιωτικότητας, όπως η θεωρία της συγκειμενικής ακεραιότητας (contextual integrity), που επαναπροσδιορίζει το ζήτημα της ιδιωτικότητας όχι ως απόλυτο δικαίωμα αλλά ως λειτουργία κοινωνικών κανόνων ροής πληροφορίας.

Η μεθοδολογική προσέγγιση της εργασίας είναι διεπιστημονική και συνδυάζει νομική ανάλυση, πολιτική θεωρία και τεχνική τεκμηρίωση. Επιχειρείται όχι μόνο η αποτύπωση των υφιστάμενων εργαλείων και των νέων τεχνολογικών δυνατοτήτων, αλλά και η εννοιολογική ερμηνεία των εντάσεων που προκύπτουν όταν συγκρούονται στόχοι ασφάλειας, καινοτομίας και θεμελιωδών δικαιωμάτων. Ιδιαίτερη σημασία έχει ο εντοπισμός σημείων ασυμβατότητας ή αλληλοεπικάλυψης μεταξύ νομοθετημάτων, η πρακτική εφαρμογή τους και η ανάγκη για μεγαλύτερη κανονιστική συνοχή και τεχνική διαλειτουργικότητα.

Τελικός στόχος της εργασίας είναι η διατύπωση συγκεκριμένων προτάσεων πολιτικής, θεσμικών βελτιώσεων και τεχνικών μέτρων, με σκοπό τη θωράκιση του ψηφιακού

περιβάλλοντος και την ενίσχυση της εμπιστοσύνης των πολιτών. Σε μια εποχή όπου η πληροφορία είναι δύναμη, η προστασία της γίνεται πράξη δημοκρατίας: συνεπώς, ο τρόπος με τον οποίο διαχειριζόμαστε τα δεδομένα καθορίζει και τη μορφή της κοινωνίας που οικοδομούμε.

ΚΕΦΑΛΑΙΟ 1 - ΕΙΣΑΓΩΓΙΚΟ ΘΕΩΡΗΤΙΚΟ ΠΛΑΙΣΙΟ – ΟΡΙΟΘΕΤΗΣΗ ΤΗΣ ΑΝΑΛΥΣΗΣ

1.1 Ορισμοί και Εννοιολογικές Διακρίσεις

Η εννοιολογική αποσαφήνιση των όρων "κυβερνοασφάλεια" και "προστασία προσωπικών δεδομένων" αποτελεί κρίσιμη αφετηρία για τη θεωρητική εδραίωση της ανάλυσης. Σύμφωνα με τον Ευρωπαϊκό Οργανισμό για την Κυβερνοασφάλεια (εφεξής ο «ENISA»), η κυβερνοασφάλεια νοείται ως το σύνολο των στρατηγικών, πολιτικών, τεχνικών και οργανωτικών μέτρων που διασφαλίζουν την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριακών συστημάτων και των δεδομένων. Αντίστοιχα, η προστασία προσωπικών δεδομένων, όπως ορίζεται στον GDPR, αφορά το δικαίωμα των φυσικών προσώπων στον έλεγχο των δεδομένων που τα αφορούν, ανεξαρτήτως μορφής ή μεθόδου επεξεργασίας τους.

Παρότι οι δύο αυτοί όροι συχνά συγχέονται στη δημόσια συζήτηση, συνιστούν διακριτά αλλά διασυνδεδεμένα πεδία. Η κυβερνοασφάλεια έχει ως πρωταρχικό στόχο την προστασία των συστημάτων, ενώ η προστασία δεδομένων εστιάζει στα υποκείμενα των δεδομένων και στα δικαιώματά τους. Όπως παρατηρεί πρόσφατη μελέτη,¹ η σύγκλιση αυτών των δύο τομέων οφείλεται εν μέρει στην ψηφιοποίηση της διοίκησης και της αγοράς, η οποία αυξάνει την έκθεση των προσωπικών δεδομένων σε κυβερνοαπειλές.

1.1.1 Κυβερνοασφάλεια: Αντικείμενο, Πεδίο και Θεμελιώδεις Αρχές

Η κυβερνοασφάλεια αφορά την πρόληψη, ανίχνευση και απόκριση σε συμβάντα ασφάλειας στον κυβερνοχώρο. Αφορά τόσο υλικές υποδομές (π.χ. δίκτυα, διακομιστές, τερματικές συσκευές) όσο και άυλες διαδικασίες (π.χ. διαχείριση ταυτότητας, έλεγχος πρόσβασης,

¹ Kuner et al. (2021).

διαχείριση περιστατικών). Σύμφωνα με την NIS2, η κυβερνοασφάλεια είναι καίρια για την προστασία κρίσιμων υποδομών, την αδιάλειπτη παροχή υπηρεσιών και τη συνολική εμπιστοσύνη των πολιτών στο ψηφιακό περιβάλλον.

Οι θεμελιώδεις αρχές της κυβερνοασφάλειας περιλαμβάνουν την αρχή της προληπτικής προστασίας (proactive security), την αρχή της διαχείρισης κινδύνου (risk-based approach), καθώς και την αρχή της λογοδοσίας και διαρκούς επιτήρησης (accountability & monitoring). Η εφαρμογή αυτών των αρχών οφείλει να είναι τεχνολογικά ουδέτερη και να λαμβάνει υπόψη το συνεχώς μεταβαλλόμενο τοπίο απειλών.

1.1.2 Προστασία Προσωπικών Δεδομένων: Νομικές και Θεσμικές

Διαστάσεις

Η προστασία δεδομένων έχει αναγνωρισθεί ως θεμελιώδες ατομικό δικαίωμα στην Ευρωπαϊκή Ένωση (Άρθρο 8 Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ (εφεξής ο «ΧΘΔΕΕ»). Ο GDPR αποτελεί τον κεντρικό πυλώνα του ενωσιακού πλαισίου και εφαρμόζεται οριζόντια σε δημόσιο και ιδιωτικό τομέα. Οι αρχές της νομιμότητας, διαφάνειας και δίκαιης επεξεργασίας, της ελαχιστοποίησης των δεδομένων, της ακρίβειας και περιορισμένης αποθήκευσης αποτελούν βασικές αρχές στις οποίες «στέκεται» ο Κανονισμός, καθώς και στην υποχρέωση ασφάλειας και λογοδοσίας (άρθρα 5-6 GDPR).

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής η «Αρχή» ή η «ΑΠΔΠΧ») στην Ελλάδα αποτελεί την αρμόδια Αρχή, ενώ σε ευρωπαϊκό επίπεδο λειτουργεί το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (εφεξής το «ΕΣΠΔ» ή το «EDPB»), το οποίο εκδίδει οδηγίες, συστάσεις και γνωμοδοτήσεις για την ερμηνεία του Κανονισμού.

1.1.3 Σχέση και Διασύνδεση μεταξύ Κυβερνοασφάλειας και Προστασίας

Δεδομένων

Η σχέση μεταξύ κυβερνοασφάλειας και προστασίας δεδομένων είναι πολυεπίπεδη. Από τη μία πλευρά, τα τεχνικά και οργανωτικά μέτρα ασφαλείας συνιστούν προϋπόθεση για τη διασφάλιση της ιδιωτικότητας. Από την άλλη, οι αρχές προστασίας δεδομένων επιβάλλουν

όρια και εγγυήσεις στις πρακτικές κυβερνοασφάλειας, ιδίως όταν εμπλέκονται ευαίσθητα δεδομένα ή συστήματα επιτήρησης. Χαρακτηριστικό παράδειγμα αυτής της διασύνδεσης είναι η εφαρμογή του άρθρου 32 του GDPR, που απαιτεί από τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία να εφαρμόζουν κατάλληλα μέτρα ασφαλείας λαμβάνοντας υπόψη τον κίνδυνο. Επίσης, η οδηγία NIS 2 προβλέπει υποχρεώσεις για τις οντότητες κρίσιμης σημασίας οι οποίες επεξεργάζονται προσωπικά δεδομένα. Η συμμόρφωση με τα πρότυπα ISO/IEC 27001 και 27701 ενισχύει τον δεσμό μεταξύ ασφαλείας και ιδιωτικότητας.

1.2 ΘΕΩΡΗΤΙΚΕΣ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΚΕΣ ΠΡΟΣΕΓΓΙΣΕΙΣ

Η σύνθετη αλληλεπίδραση μεταξύ τεχνολογίας, δικαίου και κοινωνίας απαιτεί μια πολύπλευρη μεθοδολογική προσέγγιση για την κατανόηση της προστασίας προσωπικών δεδομένων και της κυβερνοασφάλειας. Η υποενότητα αυτή διερευνά τις κύριες θεωρητικές προσεγγίσεις που στηρίζουν τη σύγχρονη ρυθμιστική αρχιτεκτονική και προσφέρει πλαίσιο αναφοράς για την ερμηνεία κανονιστικών και τεχνολογικών εργαλείων, τα οποία θα αποτελέσουν αντικείμενο της παρούσης Διπλωματικής Εργασίας.

1.2.1 Ρυθμιστική Θεωρία και Risk-Based Regulation

Η έννοια της ρυθμιστικής λογικής με βάση τον κίνδυνο (risk-based regulation) καθιερώθηκε ως θεμέλιο στο δίκαιο της προστασίας δεδομένων με την υιοθέτηση του GDPR. Το άρθρο 32 αυτού εισάγει ρητά την αξιολόγηση κινδύνων ως παράγοντα που διαμορφώνει την επιλογή των τεχνικών και οργανωτικών μέτρων. Η προσέγγιση αυτή βασίζεται στην αρχή της αναλογικότητας και προϋποθέτει τη διενέργεια Εκτίμησης Αντικτύπου (Data Protection Impact Assessment – DPIA) για επεξεργασίες υψηλού κινδύνου.

Η προσέγγιση βάσει κινδύνου (risk-based approach) αποτελεί θεμελιώδη αρχή τόσο στα ευρωπαϊκά όσο και στα διεθνή πρότυπα κυβερνοασφάλειας, όπως καταδεικνύουν οι

κατευθυντήριες γραμμές του ENISA,² αλλά και το ISO/IEC 27001, έκδοση του 2022.³ Αυτή η προσέγγιση επιτρέπει ευελιξία στην εφαρμογή μέτρων, προσαρμόζοντάς τα δυναμικά στον μεταβαλλόμενο κίνδυνο, έναντι μιας αυστηρής και στατικής τυπολατρίας· παράλληλα, η αρχή της λογοδοσίας (accountability) αναδεικνύεται ως κεντρικός μηχανισμός διασφάλισης της αποτελεσματικότητας και διαφάνειας του συστήματος ασφάλειας.

1.2.2 Νομικός Θετικισμός και Θεωρίες Δικαιωμάτων

Η θεμελίωση της προστασίας της ιδιωτικότητας εδράζεται στο άρθρο 8 του ΧΘΔΕΕ, το άρθρο 8 της Ευρωπαϊκής Συνθήκης για τα Δικαιώματα του Ανθρώπου (εφεξής η «ΕΣΔΑ») και το άρθρο 9Α του ελληνικού Συντάγματος. Η προσέγγιση αυτή προτάσσει την κατοχύρωση της προστασίας της ιδιωτικής ζωής ως υποκειμενικού δικαιώματος, αυτόνομου από την ελευθερία της επικοινωνίας ή της προσωπικότητας. Στο πλαίσιο αυτό, το κράτος υποχρεούται να διασφαλίζει τη θετική και αρνητική διάσταση της προστασίας των δεδομένων – προστασία από επεμβάσεις αλλά και ενεργή ρύθμιση των όρων επεξεργασίας, με απώτερο σκοπό τον όσο το δυνατόν ευρύτερο περιορισμό αυτής. Η σχετική νομολογία, όπως οι αποφάσεις *Volkzählungsurteil II* του Ανωτάτου Ομοσπονδιακού Συνταγματικού Δικαστηρίου της Γερμανίας, *Bundersverfassungsgericht* (εφεξής το «BVerfG») και *La Quadrature du Net* του Δικαστηρίου της Ευρωπαϊκής Ένωσης (εφεξής το «ΔΕΕ»), οι οποίες θα αναλυθούν σε επόμενα κεφάλαια, ενισχύουν το θεσμικό βάθος αυτής της προσέγγισης.

1.2.3 Τεχνο-ρυθμιστική Προσέγγιση: *Privacy by Design* και *Accountability*

Η αρχή της ενσωματωμένης προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και καθ' όλη τη διάρκεια ζωής του υποκειμένου ή «ζωής» των δεδομένων του (*privacy by design* και

² ENISA, (2023).

³ Η τρέχουσα έκδοση του ISO/IEC 27001:2022 τονίζει ρητά τις απαιτήσεις για συστήματα διαχείρισης ασφάλειας που βασίζονται σε risk assessment (άρθρο 6.1.2) και διασφαλίζουν την ανάθεση υπευθυνοτήτων σε risk owners, ενισχύοντας τη λογοδοσία. [advisera.com](https://www.advisera.com), (2022).

by default) αποτελεί εφαρμοσμένο μεθοδολογικό εργαλείο που γεφυρώνει την τεχνολογία και το δίκαιο. Όπως ορίζεται στο άρθρο 25 του GDPR, τα συστήματα επεξεργασίας δεδομένων πρέπει να ενσωματώνουν ήδη από τον σχεδιασμό τους μηχανισμούς περιορισμού του κινδύνου και σεβασμού των δικαιωμάτων των υποκειμένων. Η προσέγγιση αυτή ενδυναμώνει την πρακτική της προληπτικής ρυθμιστικής ενσωμάτωσης (preventive regulatory embedding), όπως έχει αναπτυχθεί σε πρόσφατες μελέτες.⁴

Η έννοια της λογοδοσίας (accountability) προσδίδει στο δίκαιο δυναμισμό, μετατρέποντας τη συμμόρφωση από τυπική σε αποδεικτέα και τεκμηριωμένη διαδικασία, καθώς ενισχύεται μέσα από εργαλεία όπως οι εσωτερικές πολιτικές ασφάλειας και η διενέργεια DPIA.

1.2.4 Κριτικές Θεωρίες Ιδιωτικότητας: Η Θεωρία της Πλαισιακής Ακεραιότητας (Contextual Integrity)

Η θεωρία της Contextual Integrity της **Helen Nissenbaum**⁵ προτείνει μια κοινωνιολογικά εμπλουτισμένη ερμηνεία της ιδιωτικότητας, σύμφωνα με την οποία η παραβίαση της ιδιωτικότητας δεν έγκειται μόνο στη διαρροή ή υπερεπεξεργασία, αλλά κυρίως στην αλλοίωση των **κανόνων πληροφοριακής ροής** που ισχύουν σε κάθε κοινωνικό πλαίσιο. Για παράδειγμα, η μετάδοση ευαίσθητων υγειονομικών δεδομένων από γιατρό προς ασφαλιστική εταιρεία χωρίς συγκατάθεση συνιστά παραβίαση, όχι επειδή είναι απλώς "επεξεργασία", αλλά επειδή παραβιάζει την πλαισιακή κανονικότητα που έχει εγκαθιδρύσει ο GDPR. Η εν λόγω θεωρία εμπλουτίζει τη νομολογιακή ερμηνεία του «έννομου συμφέροντος» και εντάσσεται στο ευρύτερο πλαίσιο ηθικής τεχνολογίας, έχοντας συμβάλει στη διαμόρφωση κριτηρίων όπως η επεξηγησιμότητα και η αναλογικότητα στο πλαίσιο και άλλων πρόσφατων νομοθετικών πρωτοβουλιών της ΕΕ, όπως η AI Act.

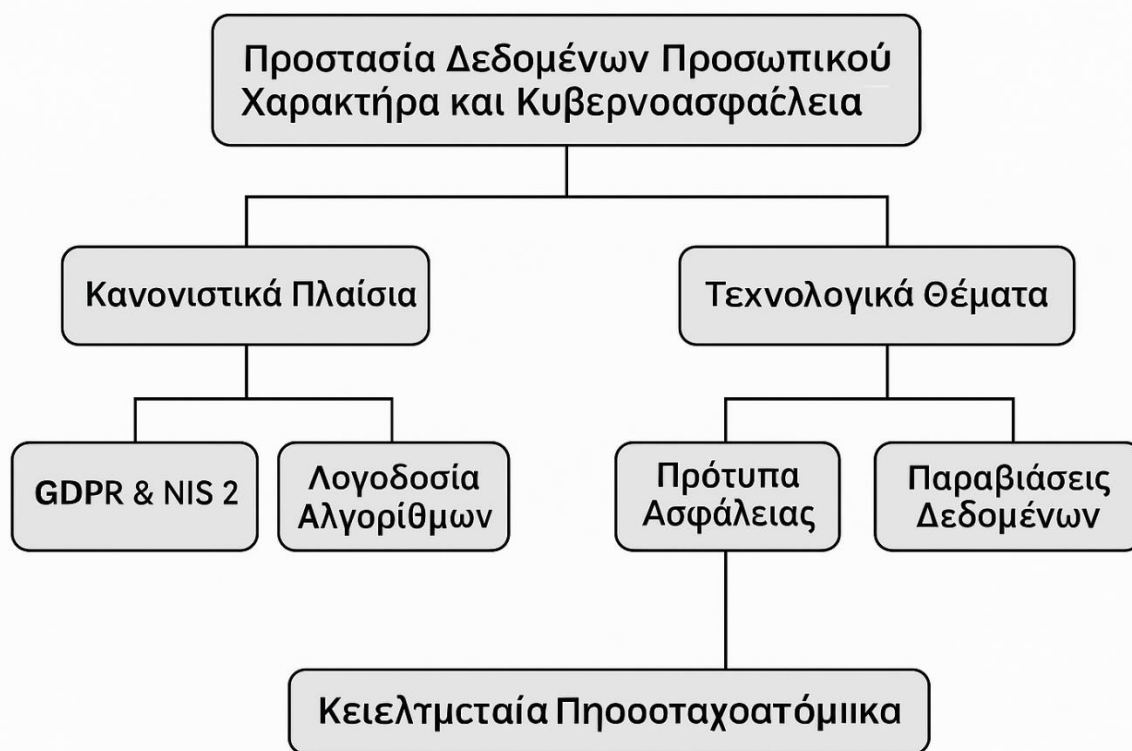
⁴ Veale & Borgesius, (2021).

⁵ Nissenbaum, H. (2009).

1.3. Μεθοδολογία της Διπλωματικής Εργασίας

Η παρούσα εργασία δομείται πάνω στην υπόθεση ότι η προστασία προσωπικών δεδομένων και η κυβερνοασφάλεια δεν είναι ανεξάρτητοι αλλά αλληλοσυμπληρούμενοι τομείς. Η ερευνητική προσέγγιση βασίζεται σε νομικοθεωρητική ανάλυση, επισκόπηση του ενωσιακού και διεθνούς κανονιστικού πλαισίου, και μελέτη περιπτώσεων. Η εικόνα που ακολουθεί παρουσιάζει ένα διαγραμματικό μοντέλο που αποτυπώνει τη σχέση μεταξύ κυβερνοασφάλειας και προστασίας προσωπικών δεδομένων. Στο πάνω μέρος τοποθετείται η έννοια της προστασίας προσωπικών δεδομένων, η οποία θεμελιώνεται (στην ΕΕ) στον GDPR και περιλαμβάνει τις νομικές υποχρεώσεις για την ασφάλεια των δεδομένων. Αντίστοιχα, στο κάτω μέρος εμφανίζεται η κυβερνοασφάλεια, η οποία σχετίζεται με τεχνολογικά και διαχειριστικά μέτρα, όπως αυτά προβλέπονται από πρότυπα και οδηγίες όπως το ISO/IEC 27001 και η NIS2.

Μεταξύ αυτών των δύο πεδίων εκτείνεται μία «ζώνη σύγκλισης», η οποία περιλαμβάνει τα τεχνικά και οργανωτικά μέτρα προστασίας, τη διαχείριση κινδύνου και την εφαρμογή προτύπων όπως το ISO/IEC 27701 για την προστασία της ιδιωτικότητας. Το διάγραμμα απεικονίζει τη λειτουργική διασύνδεση αυτών των περιοχών και αναδεικνύει το πώς η συμμόρφωση με νομικά πρότυπα συνδέεται με τεχνικές και θεσμικές πρακτικές ασφάλειας. Πρόκειται για μία απεικόνιση συνοψίζουσα την λυδία λίθο της εργασίας: ότι η προστασία δεδομένων και η κυβερνοασφάλεια είναι συμπληρωματικές και αλληλεξαρτώμενες.



Εικόνα 1: Εννοιολογική Δομή της Σχέσης Προστασίας Προσωπικών Δεδομένων και Κυβερνοασφάλειας

Ειδική βιβλιογραφία κεφαλαίου 1

- advisera.com, (2022). ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide. Διαθέσιμο εδώ: <https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/?com>
- ENISA, (2023). Interoperable EU Risk Management Framework. Διαθέσιμο εδώ: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report-Interoperable%20EU%20Risk%20Management%20Framework%20Updated.pdf>
- Kuner, C., Bygrave, L.A. & Docksey, C. (eds.) (2021) *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford: Oxford University Press. Διαθέσιμη εδώ:

https://web.archive.org/web/20210509231556id_/https://fdslive.oup.com/www.oup.com/academic/pdf/law/GDPRCommentary_ArticleUpdates.pdf

- Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press. Διαθέσιμο εδώ: https://web.archive.org/web/20220629220601id_/https://watermark.silverchair.com/jinfo_poli_1_2011
- **Veale, M. & Zuiderveen Borgesius, F.** (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4). Διαθέσιμο εδώ: <https://www.degruyterbrill.com/document/doi/10.9785/cri-2021-220402/html>

ΚΕΦΑΛΑΙΟ 2 - ΘΕΣΜΙΚΟ ΚΑΙ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

2.1 Ευρωπαϊκό Ρυθμιστικό Πλαίσιο για την Προστασία Δεδομένων

2.1.1 Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR):

Βασικές Αρχές και Υποχρεώσεις

Ο GDPR συνιστά τον θεμέλιο λίθο του ενωσιακού πλαισίου για την προστασία των προσωπικών δεδομένων. Εφαρμόζεται άμεσα σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης από τις 25 Μαΐου 2018, θέτοντας ένα ενιαίο και ομοιογενές νομικό πλαίσιο για τη συλλογή, χρήση και διατήρηση των προσωπικών δεδομένων των φυσικών προσώπων.

Στον πυρήνα του Κανονισμού εντοπίζονται οι θεμελιώδεις αρχές της επεξεργασίας: η νομιμότητα, η διαφάνεια, η ακρίβεια, η ελαχιστοποίηση των δεδομένων, ο περιορισμός του σκοπού, η χρονικά περιορισμένη αποθήκευση, καθώς και η διασφάλιση της ακεραιότητας

και της εμπιστευτικότητας των δεδομένων, όπως ορίζονται στο άρθρο 5 του Κανονισμού. Οι αρχές αυτές συγκροτούν τον κώδικα δεοντολογίας που οφείλει να διέπει κάθε πράξη επεξεργασίας προσωπικών δεδομένων εντός της Ένωσης.

Κεντρικής σημασίας στο νέο κανονιστικό καθεστώς είναι η αρχή της λογοδοσίας (accountability), η οποία εισάγει την υποχρέωση τεκμηρίωσης της συμμόρφωσης από τους υπεύθυνους επεξεργασίας. Αυτό σημαίνει ότι οι οργανισμοί δεν αρκεί απλώς να συμμορφώνονται, αλλά οφείλουν να είναι σε θέση να αποδείξουν εμπράκτως τη συμμόρφωσή τους, μέσω μέτρων όπως η κατάρτιση εσωτερικών πολιτικών προστασίας δεδομένων, η εφαρμογή τεχνικών μηχανισμών όπως η ψευδωνυμοποίηση και η κρυπτογράφηση, η εκπόνηση Μελέτης Εκτίμησης Αντικτύπου (εφεξής η «DPIA»), καθώς και η διαρκής επιτήρηση των διαδικασιών επεξεργασίας.

Παράλληλα, ο GDPR κατοχυρώνει και ενισχύει τα δικαιώματα των υποκειμένων των δεδομένων, όπως το δικαίωμα πρόσβασης, το δικαίωμα διόρθωσης ή διαγραφής, το δικαίωμα εναντίωσης, και το δικαίωμα στη φορητότητα των δεδομένων. Ιδιαίτερα κρίσιμο είναι και το άρθρο 22, το οποίο ρυθμίζει την αυτοματοποιημένη λήψη αποφάσεων, απαγορεύοντας τη λήψη αποφάσεων που παράγουν έννομα αποτελέσματα για το υποκείμενο αποκλειστικά μέσω αλγοριθμικής επεξεργασίας, εκτός αν συντρέχουν αυστηρές προϋποθέσεις.

Η εφαρμογή του GDPR σε διακρατικό επίπεδο έχει αναδείξει επίσης σοβαρά ζητήματα νομοθετικής σύγκρουσης με τρίτες χώρες, όπως διατρανώθηκε στην εμβληματική υπόθεση Schrems II (CJEU, C-311/18), στην οποία το ΔΕΕ ακύρωσε το πλαίσιο Privacy Shield μεταξύ ΕΕ και ΗΠΑ, κρίνοντας ότι το αμερικανικό δίκαιο δεν προσέφερε επαρκές επίπεδο προστασίας για τα δικαιώματα των Ευρωπαίων πολιτών. Η απόφαση αυτή ενίσχυσε τη σημασία της διενέργειας Μελετών Εκτίμησης Αντικτύπου Διαβιβάσεων (Transfer Impact Assessments - εφεξής οι «TIAs») και προώθησε τη χρήση Τυποποιημένων Συμβατικών Ρητρών (Standard Contractual Clauses – εφεξής οι «SCCs») ως μέσου διασυνοριακής προστασίας.

Αν και ο Κανονισμός εφαρμόζεται αυτοδικαίως στα κράτη μέλη, η Ελλάδα προχώρησε στην υιοθέτηση ειδικού εθνικού εφαρμοστικού νόμου. Ο Νόμος 4624/2019 (ΦΕΚ 137/Α/29-8-2019),

που τέθηκε σε ισχύ τον Αύγουστο του 2019, ρυθμίζει την εγχώρια εφαρμογή του GDPR, καθορίζοντας τον ρόλο και τις αρμοδιότητες της ΑΠΔΠΧ ως της εποπτικής αρχής της χώρας. Ο νόμος εισάγει εξειδικεύσεις για την επεξεργασία δεδομένων από δημόσιες αρχές, θεσπίζει εξαιρέσεις και διευκρινίσεις για τη δικαστική χρήση δεδομένων, και ενισχύει τη νομική βάση για την επιβολή κυρώσεων, την ελεγκτική εξουσία της ΑΠΔΠΧ και τη ρύθμιση ριψοκίνδυνων επεξεργασιών. Επιπλέον, προβλέπει ειδικούς κανόνες για την επεξεργασία δεδομένων από φορείς επιβολής του νόμου, ενσωματώνοντας ταυτόχρονα και την Οδηγία (ΕΕ) 2016/680.

Η υλοποίηση του GDPR στην ελληνική διοικητική και επιχειρηματική πραγματικότητα συνοδεύτηκε από πολλαπλές προκλήσεις, όπως η χαμηλή αρχική ετοιμότητα πολλών δημόσιων οργανισμών, η ανάγκη διαρκούς κατάρτισης των Υπευθύνων Προστασίας Δεδομένων (Data Protection Officers – DPOs), καθώς και η οριζόντια απαίτηση για συμμόρφωση σε μικρομεσαίες επιχειρήσεις, χωρίς πάντα την ύπαρξη επαρκών πόρων. Παρά τις προκλήσεις αυτές, η προοδευτική αύξηση των ελέγχων της ΑΠΔΠΧ, οι κατευθυντήριες οδηγίες που εκδίδει, καθώς και η συμμετοχή της σε ευρωπαϊκά δίκτυα, ενισχύουν τον ρυθμιστικό ρόλο της στο σύστημα προστασίας δεδομένων της χώρας.

2.1.2 Ο ρόλος του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (EDPB) και των Εθνικών Αρχών

Το EDPB αποτελεί ανεξάρτητο ευρωπαϊκό όργανο, το οποίο θεσπίστηκε από τον GDPR και αντικατέστησε την Ομάδα Εργασίας του Άρθρου 29. Ο βασικός σκοπός του είναι να διασφαλίζει τη συνεκτική εφαρμογή του GDPR και της Οδηγίας (ΕΕ) 2016/680 στα κράτη μέλη, προάγοντας την εναρμόνιση των πρακτικών ερμηνείας και επιβολής. Απαρτίζεται από εκπροσώπους όλων των εθνικών εποπτικών αρχών, της Ευρωπαϊκής Επιτροπής και του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων (εφεξής ο «EDPS»). Έχει την αρμοδιότητα να εκδίδει δεσμευτικές αποφάσεις στο πλαίσιο του μηχανισμού συνεκτικότητας (consistency mechanism), ιδίως σε περιπτώσεις διασυνοριακής επεξεργασίας δεδομένων, που ενδέχεται να προκαλέσουν συγκρούσεις μεταξύ των εποπτικών αρχών. Επιπλέον, εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές για την εφαρμογή των

διατάξεων του Κανονισμού, που λειτουργούν ως βασικό εργαλείο για τον ενιαίο νομικό προσανατολισμό.

Σημαντικός είναι ο ρόλος του στην ερμηνεία κρίσιμων εννοιών, όπως το έννομο συμφέρον, η συγκατάθεση, η επεξεργασία υψηλού κινδύνου, και η έννοια του υπεύθυνου επεξεργασίας ή του κοινού ελέγχου. Με τις Κατευθυντήριες Γραμμές του στη διάρκεια των ετών 2022–2024, το Συμβούλιο ανέπτυξε ενότητες που σχετίζονται με την τεχνητή νοημοσύνη, τα cookies, τα social media, τις διασυνοριακές μεταφορές και τα συστήματα αξιολόγησης κινδύνου σε περιβάλλοντα big data και cloud computing.

Σε εθνικό επίπεδο, κάθε κράτος μέλος διαθέτει εποπτική αρχή με ευρείες ελεγκτικές και κανονιστικές αρμοδιότητες. Στην Ελλάδα, η ΑΠΔΠΧ, η οποία ιδρύθηκε με το προϊσχύσαν νομικό πλαίσιο για τα δεδομένα προσωπικού χαρακτήρα, ήτοι με τον Ν. 2472/1997, και ενισχύθηκε νομικά με τον Ν. 4624/2019, είναι αρμόδια για την εποπτεία της εφαρμογής του GDPR και της Οδηγίας (ΕΕ) 2016/680. Η Αρχή λειτουργεί ως συνδεδετικός κρίκος μεταξύ της ευρωπαϊκής εποπτείας και των εγχώριων εφαρμοστικών μηχανισμών.

Η ΑΠΔΠΧ έχει τη δυνατότητα να διεξάγει ελέγχους, να επιβάλλει διοικητικά πρόστιμα, να εκδίδει γνωμοδοτήσεις και οδηγίες, καθώς και να εξετάζει καταγγελίες πολιτών. Παράλληλα, συμμετέχει ενεργά στις συνεδριάσεις του EDPB και συνδράμει στον ευρωπαϊκό διάλογο χάραξης πολιτικής προστασίας δεδομένων. Το έργο της αποτυπώνεται ετησίως στην Έκθεση Πεπραγμένων της, ενώ διαρκώς εμπλουτίζει το ψηφιακό της αποθετήριο με επικαιροποιημένες οδηγίες και αποφάσεις.⁶

Η αλληλεπίδραση μεταξύ του EDPB και των εθνικών αρχών όπως η ΑΠΔΠΧ συνιστά κρίσιμο θεσμό πολυεπίπεδης διακυβέρνησης στην ΕΕ, διασφαλίζοντας όχι μόνο τη συνοχή της εφαρμογής του GDPR, αλλά και την ενίσχυση της λογοδοσίας από κάθε φορέα που συλλέγει και εν γένει επεξεργάζεται δεδομένα φυσικών προσώπων.

⁶ Dpa.gr.

2.1.3 Η εφαρμογή του GDPR σε διακρατικά περιβάλλοντα και η νομολογία *Schrems I & II*

Η εφαρμογή του GDPR σε διακρατικά περιβάλλοντα εγείρει θεμελιώδη ζητήματα νομικής κυριαρχίας, ισοδυναμίας ρυθμιστικών εγγυήσεων και διεθνούς μεταφοράς δεδομένων. Ενώ το άρθρο 44 του GDPR επιτρέπει μεταφορές δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, αυτό τελεί υπό την προϋπόθεση ότι εξασφαλίζεται «επαρκές επίπεδο προστασίας», ισοδύναμο με αυτό που εγγυάται το δίκαιο της ΕΕ.

Η προβληματική σχέση μεταξύ του ρυθμιστικού πλαισίου της ΕΕ και των Ηνωμένων Πολιτειών αναδείχθηκε μέσα από τις εμβληματικές υποθέσεις **Schrems I** (CJEU, C-362/14) και **Schrems II** (CJEU, C-311/18), οι οποίες διαμόρφωσαν το θεσμικό τοπίο των διεθνών διαβιβάσεων δεδομένων.

Στην υπόθεση *Schrems I*, το Δικαστήριο της Ευρωπαϊκής Ένωσης (εφεξής το «ΔΕΕ» ή το «Δικαστήριο») ακύρωσε την Απόφαση Επάρκειας Safe Harbor, κρίνοντας ότι το δίκαιο των ΗΠΑ δεν παρείχε επαρκές επίπεδο προστασίας, λόγω ανεπαρκών περιορισμών στην πρόσβαση των αμερικανικών αρχών ασφαλείας στα ευρωπαϊκά δεδομένα. Η ακύρωση του Safe Harbor οδήγησε στη δημιουργία του μηχανισμού Privacy Shield το 2016.

Ωστόσο, το 2020, με την **απόφαση Schrems II**,⁸ το Δικαστήριο ακύρωσε και το Privacy Shield, υπογραμμίζοντας ότι οι πρακτικές επιτήρησης των ΗΠΑ δεν ήταν συμβατές με τα θεμελιώδη δικαιώματα που κατοχυρώνει ο ΧΘΔΕΕ, ιδίως ως προς την αναλογικότητα, τη δικαστική προστασία και τη διαδικασία προσφυγής. Επιπλέον, το ΔΕΕ έθεσε αυξημένες απαιτήσεις για την εφαρμογή **SCCs**, υποχρεώνοντας τους υπευθύνους επεξεργασίας να διενεργούν **TIAs** πριν τη διαβίβαση, εξετάζοντας το κατά πόσον η νομοθεσία της τρίτης χώρας καθιστά τις SCCs αποτελεσματικές στην πράξη.

Οι εξελίξεις αυτές επηρέασαν ιδιαίτερα πολυεθνικές επιχειρήσεις που διαχειρίζονται προσωπικά δεδομένα Ευρωπαίων πολιτών. Ο GDPR, μέσω των άρθρων 45 έως 49, διαμορφώνει ένα σύνθετο καθεστώς, το οποίο περιλαμβάνει όχι μόνο Τυποποιημένες Ρήτρες

⁷ CJEU, (2015).

⁸ CJEU, (2020).

αλλά και δεσμευτικούς εταιρικούς κανόνες (Binding Corporate Rules – BCRs), μηχανισμούς πιστοποίησης και εξαιρέσεις σε ειδικές περιπτώσεις. Το 2023, η Ευρωπαϊκή Επιτροπή παρουσίασε ένα νέο πλαίσιο επάρκειας, το **EU-US Data Privacy Framework**,⁹ το οποίο, ωστόσο, τελεί υπό αυστηρή επιτήρηση, καθώς αναμένεται νέα νομική πρόκληση (πιθανή *Schrems III*).

Σε πρακτικό επίπεδο, οι οργανισμοί καλούνται να υιοθετούν πολυεπίπεδα μέτρα προστασίας, που περιλαμβάνουν νομικά, τεχνικά και οργανωτικά στοιχεία, προκειμένου να διασφαλίζεται η ουσιαστική προστασία των δεδομένων ανεξαρτήτως γεωγραφικού τόπου. Η χρήση κρυπτογράφησης, ψευδωνυμοποίησης και η τοπική αποθήκευση (data localization) αποτελούν βασικές τεχνικές συμμόρφωσης.

Η νομολογία **Schrems I και II** έχει λειτουργήσει ως επιταχυντής για την αναθεώρηση της παγκόσμιας διακυβέρνησης δεδομένων, σηματοδοτώντας τη μετάβαση από απλή κανονιστική επάρκεια σε ένα πρότυπο **ουσιαστικής εγγύησης δικαιωμάτων**, με αυξημένη λογοδοσία από όλους τους εμπλεκόμενους φορείς.

2.2 Αρχές και διακυβέρνηση της κυβερνοασφάλειας στην ΕΕ

Η ενίσχυση της κυβερνοασφάλειας αποτελεί στρατηγική προτεραιότητα για την Ευρωπαϊκή Ένωση, η οποία έχει προωθήσει ένα σύστημα πολυεπίπεδης διακυβέρνησης με βασικούς θεσμικούς φορείς: τον European Union Agency for Cybersecurity (εφεξής ο «ENISA»), το CERT-EU¹⁰ και την Ευρωπαϊκή Ομάδα Συνεργασίας NIS,¹¹ η οποία εκδίδει δεσμευτικές κατευθυντήριες γραμμές, τεχνικού κυρίως χαρακτήρα. Ο ENISA λειτουργεί ως κεντρικός κόμβος τεχνικής τεχνογνωσίας, παρέχοντας κατευθυντήριες οδηγίες και αξιολογήσεις

⁹ **EU-US Data Privacy Framework, (2024).**

¹⁰ CERT-EU. Είναι η Υπηρεσία Κυβερνοασφάλειας για τα Θεσμικά και Λοιπά Όργανα και Οργανισμούς της ΕΕ.

¹¹ EU NIS Cooperation Group.

κινδύνου, ενώ η NIS Cooperation Group ενισχύει τη διακρατική συνεργασία και εναρμόνιση πολιτικών.¹²

Σε μία σύντομη επισκόπηση του διεθνούς τοπίου, αντιπαραβολή μπορεί να γίνει με τις Ηνωμένες Πολιτείες, όπου η CISA (Cybersecurity and Infrastructure Security Agency)¹³ ασκεί κεντρικό συντονιστικό ρόλο, επικουρούμενη από τεχνικά πρότυπα του NIST (National Institute of Standards and Technology)¹⁴, με ιδιαίτερη έμφαση στο "Cybersecurity Framework".¹⁵ Αντίθετα, η προσέγγιση της Κίνας παραμένει περισσότερο κρατικά ελεγχόμενη, με αυστηρή

¹² ENISA, (2022).

¹³ Η CISA είναι η Ομοσπονδιακή Υπηρεσία Κυβερνοασφάλειας και Ασφάλειας Υποδομών των ΗΠΑ. Υπάγεται στο Υπουργείο Εσωτερικής Ασφάλειας (DHS) και είναι υπεύθυνη για την προστασία κρίσιμων υποδομών της χώρας (όπως ενέργεια, μεταφορές, τηλεπικοινωνίες, υγεία) από ψηφιακές και φυσικές απειλές. Η CISA αναπτύσσει πολιτικές και εργαλεία για την κυβερνοασφάλεια, συνεργάζεται με τον δημόσιο και ιδιωτικό τομέα και ανταποκρίνεται σε περιστατικά που σχετίζονται με την ασφάλεια πληροφοριακών συστημάτων.

¹⁴ Ο NIST είναι ο Ομοσπονδιακός Οργανισμός Προτύπων και Τεχνολογίας των ΗΠΑ, υπαγόμενος στο Υπουργείο Εμπορίου. Αποστολή του είναι να προάγει την καινοτομία και την οικονομική ανταγωνιστικότητα μέσω της ανάπτυξης προτύπων, μεθοδολογιών και τεχνολογιών στους τομείς της μέτρησης, της επιστήμης και της ασφάλειας των πληροφοριών.

¹⁵ Το Cybersecurity Framework των ΗΠΑ, γνωστό και ως NIST Cybersecurity Framework (CSF), είναι ένα πλαίσιο που αναπτύχθηκε από τον NIST των ΗΠΑ για να βοηθήσει οργανισμούς όλων των μεγεθών και τομέων να κατανοήσουν, να αξιολογήσουν και να βελτιώσουν τη διαχείριση του κινδύνου κυβερνοασφάλειας. Η πιο πρόσφατη έκδοσή του είναι το CSF 2.0, το οποίο παρέχει καθοδήγηση και βέλτιστες πρακτικές για τη διαχείριση κινδύνων κυβερνοασφάλειας.

ιεραρχία κυβερνητικών παρεμβάσεων μέσω του Cyberspace Administration of China¹⁶ και κεντρικού σχεδιασμού για την ψηφιακή λογοκρισία.¹⁷

«Επιστρέφοντας» σε Ευρωπαϊκό έδαφος, η ανάγκη για σαφή κατανομή αρμοδιοτήτων και εγγυήσεων διαφάνειας στη λήψη αποφάσεων ασφαλείας έχει επίσης απασχολήσει τη νομολογία του ΔΕΕ. Στην υπόθεση *La Quadrature du Net* (C-511/18), το ΔΕΕ έκρινε ότι η μαζική και γενικευμένη αποθήκευση μεταδεδομένων επικοινωνίας από ιδιωτικούς παρόχους, κατ' εντολή κρατικών αρχών, παραβιάζει τις αρχές αναλογικότητας και αναγκαιότητας που απορρέουν από τα άρθρα 7 και 8 του ΧΘΔΕΕ.¹⁸

Η συμμετοχή του ιδιωτικού τομέα στη διαμόρφωση πολιτικής για την κυβερνοασφάλεια έχει ενισχυθεί μέσα από δομές *soft law* και προτύπων αυτορρύθμισης. Τα διεθνή πρότυπα

¹⁶ Η Cyberspace Administration of China (CAC) είναι η κύρια ρυθμιστική αρχή της Κίνας για το διαδίκτυο, την κυβερνοασφάλεια και το ψηφιακό περιεχόμενο. Υπάγεται άμεσα στο Κεντρικό Κόμμα και είναι υπεύθυνη για την εποπτεία της διαδικτυακής πληροφορίας, τη διαχείριση δεδομένων, την επιβολή περιορισμών λογοκρισίας, καθώς και την εφαρμογή της κινεζικής νομοθεσίας για την προστασία προσωπικών δεδομένων και την ασφάλεια δικτύων.

¹⁷ Creemers, (2016). Στη μελέτη αυτή παρουσιάζεται η Κινεζική πραγματικότητα, που διαφέρει παρασάγγας από την καθ' ημάς. Εν συνόψει:

- Αναδιοργάνωση της κυβερνητικής δομής: Στις αρχές της διακυβέρνησης του Xi Jinping (2012–2014), έγινε πλήρης αναμόρφωση της διαδικτυακής διακυβέρνησης, δημιουργώντας ενιαίο, κεντρικά ελεγχόμενο θεσμικό πλαίσιο που ενσωματώνει την προπαγάνδα, την καθοδήγηση της κοινής γνώμης και την κοινωνική διαχείριση μέσω ψηφιακών μέσων.
- Μείωση της διαδικτυακής αυτονομίας: Η «ανεξέλεγκτη» ελευθερία της έκφρασης καταργήθηκε, οι ψηφιακές πλατφόρμες πια λειτουργούν υπό αυστηρή εποπτεία του κράτους, περιορίζοντας δραστικά τυχόν «αυθόρμητες» παρεμβάσεις της κοινωνίας.
- Υιοθέτηση ψηφιακών εργαλείων ελέγχου: Το άρθρο τονίζει πώς η Κίνα ενσωματώνει τεχνολογία (data analytics, κοινωνική αξιολόγηση, social credit) στη στρατηγική της, με στόχο την συνεχή παρακολούθηση και τη διαχείριση της κοινής γνώμης.

¹⁸ CJEU, (2020).

ISO/IEC 27001 και ISO/IEC 27701¹⁹ αποτελούν βασικούς μηχανισμούς διασφάλισης της ασφάλειας των πληροφοριών και της διαχείρισης προσωπικών δεδομένων αντίστοιχα. Η ενσωμάτωσή τους στις εσωτερικές πολιτικές συμμόρφωσης πολυεθνικών οργανισμών καταδεικνύει τη στροφή προς ρυθμιστικά πρότυπα οιονεί ιδιωτικής προέλευσης.²⁰ Οι δημόσιες-ιδιωτικές συμπράξεις (Public-Private Partnerships – PPPs) αποκτούν επίσης αυξανόμενη σημασία, τόσο στον τομέα της πρόληψης όσο και στην ανταπόκριση σε περιστατικά. Οι συνεργασίες αυτές, όπως το European Cybersecurity Competence Network ή η πλατφόρμα Europol-EC3, διευκολύνουν την ανταλλαγή τεχνικής πληροφορίας και βέλτιστων πρακτικών, ενισχύοντας τη συνοχή και την αποτελεσματικότητα της ευρωπαϊκής ψηφιακής άμυνας.²¹

Η νομολογία του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου (εφεξής το «ΕΔΔΑ») έχει υπογραμμίσει τη σημασία του θεσμικού πλαισίου που διέπει τη συνεργασία δημοσίου και ιδιωτικού τομέα. Στην υπόθεση *Liberty and Others v. United Kingdom* (2008), το ΕΔΔΑ έκρινε ότι η απουσία επαρκών ρυθμιστικών εγγυήσεων για τη συνεργασία

¹⁹ Το πρότυπο **ISO/IEC 27001** καθορίζει ένα πλαίσιο για τη θέσπιση, υλοποίηση, παρακολούθηση και διαρκή βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), με στόχο τη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών σε οργανισμούς. Το πρότυπο **ISO/IEC 27701** αποτελεί επέκταση του ISO/IEC 27001 και εστιάζει στη διαχείριση πληροφοριών προσωπικού χαρακτήρα, παρέχοντας οδηγίες για την ενσωμάτωση υποχρεώσεων προστασίας δεδομένων σε ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών.

²⁰ Greenleaf, (2021). Η μελέτη του καθηγητή του University of New South Wales στην Αυστραλία περιλαμβάνει παγκόσμιους πίνακες με τις χώρες που διαθέτουν νόμους προστασίας δεδομένων (145 χώρες κατά το έτος δημοσίευσης, 2021) και αναλύει πώς τα πρότυπα ISO/IEC 27001 & 27701 χρησιμοποιούνται ως εργαλεία soft-law και αυτορρύθμισης από πολυεθνικές εταιρείες. Αυτοί οι περιοδικοί πίνακες θεωρούνται από τους πιο αξιόπιστους παγκοσμίως.

²¹ ENISA, (2021).

τηλεπικοινωνιακών παρόχων με κρατικές αρχές στο πλαίσιο μαζικών παρακολουθήσεων συνιστούσε παραβίαση του άρθρου 8 της ΕΣΔΑ.²²

2.2.1 Οδηγία NIS 2: Επέκταση της Ευθύνης για την Κυβερνοασφάλεια

Η Οδηγία (ΕΕ) 2022/2555, γνωστή ως NIS 2, αποτελεί την αναθεωρημένη εκδοχή της αρχικής Οδηγίας NIS (2016/1148), και εντάσσεται στο ευρύτερο ευρωπαϊκό πλαίσιο ενίσχυσης της κυβερνοασφάλειας. Αντικαθιστά την πρώτη NIS και στοχεύει στη δημιουργία ενός υψηλού κοινού επιπέδου ασφάλειας δικτύων και συστημάτων πληροφοριών σε όλη την Ευρωπαϊκή Ένωση. Η NIS 2 αντανακλά τη ραγδαία αύξηση των ψηφιακών απειλών και την ανάγκη συστημικής προσέγγισης στον κυβερνοχώρο, ενισχύοντας την κανονιστική πίεση προς κρίσιμους οργανισμούς, τόσο δημόσιους όσο και ιδιωτικούς.

Ένα από τα σημαντικότερα χαρακτηριστικά της NIS 2 είναι η διεύρυνση του πεδίου εφαρμογής της. Η νέα Οδηγία περιλαμβάνει πλέον περισσότερους τομείς υψηλής σημασίας, όπως οι φορείς υγειονομικής περίθαλψης, οι πάροχοι δημόσιας διοίκησης, τα ταχυδρομεία, οι υποδομές ύδρευσης, οι κατασκευαστές εξοπλισμού πληροφορικής, καθώς και κρίσιμοι πάροχοι cloud και data centers. Η νέα κατάταξη οργανισμών σε “ουσιώδεις” (essential) και “σημαντικούς” (important) φορείς έχει στόχο την προσαρμογή των υποχρεώσεων στην κρισιμότητα των υπηρεσιών που παρέχουν.

Η NIS 2 εισάγει αυστηρότερες απαιτήσεις διακυβέρνησης και λογοδοσίας, προβλέποντας την προσωπική ευθύνη των μελών της διοίκησης σε περίπτωση πλημμελούς διαχείρισης θεμάτων ασφάλειας (άρθρο 20). Δεδομένου ότι η προέλευση των κυβερνοαπειλών μπορεί να ποικίλει, δεν είναι απίθανο να προκύψει οποτεδήποτε η οποιαδήποτε βλάβη. Ως εκ τούτου, τα μέτρα διαχείρισης κυβερνοκινδύνων που λαμβάνει η οντότητα θα πρέπει να προστατεύουν όχι μόνο τα δικτυακά και πληροφοριακά συστήματά της, αλλά και το φυσικό περιβάλλον των εν λόγω συστημάτων από οποιοδήποτε γεγονός, όπως δολιοφθορά, κλοπή, πυρκαγιά, πλημμύρα, τηλεπικοινωνιακές ή ηλεκτρολογικές βλάβες ή μη εξουσιοδοτημένη φυσική πρόσβαση, θέτοντας σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την

²² ECHR, (2008).

ακεραιότητα ή την εμπιστευτικότητα των αποθηκευμένων, μεταδιδόμενων ή υπό επεξεργασία δεδομένων ή των υπηρεσιών που προσφέρονται από τα δικτυακά και πληροφοριακά συστήματα ή είναι προσβάσιμες μέσω αυτών.

Ιδιαίτερη έμφαση δίνεται στη διαλειτουργικότητα και ανταλλαγή πληροφοριών για κυβερνοαπειλές, μέσω της δημιουργίας CSIRTs (Computer Security Incident Response Teams) και της ενίσχυσης του ρόλου του European Cyber Crises Liaison Organisation Network (EU-CyCLONe), ο οποίος δρα υποστηρικτικά στις εθνικές αρχές σε περιόδους ψηφιακών κρίσεων. Πλέον, προβλέπεται αυστηρό χρονοδιάγραμμα αναφοράς περιστατικών κυβερνοασφάλειας: προκαταρκτική ειδοποίηση εντός 24 ωρών από την ανίχνευση, αναλυτική αναφορά εντός 72 ωρών και τελική έκθεση εντός 30 ημερών. Παράλληλα, εισάγεται θεσμός ICSSO (Information and Cybersecurity Senior Strategic Officer), με ρητή ευθύνη της διοίκησης των οργανισμών για την τήρηση των μέτρων ασφάλειας. Η οδηγία NIS 2 ενισχύει επίσης τους μηχανισμούς κυρώσεων: προβλέπεται η επιβολή διοικητικών προστίμων που μπορεί να φθάσουν έως και τα 10 εκατομμύρια ευρώ ή το 2% του παγκόσμιου ετήσιου κύκλου εργασιών, ανάλογα με το ποιο ποσό είναι μεγαλύτερο (άρθρο 34).

Εν συνόλω, η Οδηγία αντικατοπτρίζει την προσπάθεια της ΕΕ να περάσει από την αντιδραστική σε προληπτική προσέγγιση, ενισχύοντας την ανθεκτικότητα των ψηφιακών οικοσυστημάτων απέναντι σε εξελισσόμενες απειλές, με κανονιστικά και τεχνικά μέσα που στηρίζονται στις αρχές της τεκμηριωμένης λογοδοσίας (accountability) και της διαχειρισιμότητας κινδύνου (risk management by design).

Η ενσωμάτωση της NIS 2 μέσω του Ν. 5160/2024 (ΦΕΚ Α' 195/27.11.2024) επιβεβαιώνει τη βούληση της Ελλάδας να ευθυγραμμιστεί με τις ευρωπαϊκές αρχές ψηφιακής ανθεκτικότητας, ενισχύοντας παράλληλα τον θεσμικό έλεγχο και την τεχνική επάρκεια των εθνικών υποδομών. Ωστόσο, παραμένουν προκλήσεις, όπως η διασφάλιση των απαραίτητων πόρων, η διαλειτουργικότητα των δομών και η πρακτική εφαρμογή της αρχής της λογοδοσίας στο πεδίο της κυβερνοασφάλειας.

2.2.2 Ο Κανονισμός για την Κυβερνοασφάλεια (EU Cybersecurity Act)

Ο Κανονισμός (ΕΕ) 2019/881, γνωστός και ως Cybersecurity Act (εφεξής η “Cybersecurity Act”),²³ αποτελεί ένα από τα βασικά θεσμικά εργαλεία της Ευρωπαϊκής Ένωσης για την ενίσχυση της κυβερνοασφάλειας εντός της Ενιαίας Ψηφιακής Αγοράς. Τέθηκε σε ισχύ την 27η Ιουνίου 2019 και καθιερώνει ένα ευρωπαϊκό πλαίσιο πιστοποίησης κυβερνοασφάλειας, ενώ ταυτόχρονα ενισχύει τον ρόλο του ENISA, καθιστώντας την μόνιμο οργανισμό με διευρυμένες αρμοδιότητες.

Η βασική συμβολή της Cybersecurity Act συνίσταται στη θεσμοθέτηση ενιαίου πλαισίου πιστοποίησης για προϊόντα, υπηρεσίες και διαδικασίες τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ), σε επίπεδο ΕΕ. Το πλαίσιο αυτό παρέχει τρία επίπεδα εμπιστοσύνης – βασικό, ουσιαστικό και υψηλό – επιτρέποντας την ταξινόμηση κάθε πιστοποιητικού με βάση την αυστηρότητα των απαιτήσεων που πληροί. Η δημιουργία του πλαισίου πιστοποίησης αποσκοπεί στη μείωση του κατακερματισμού των εθνικών συστημάτων πιστοποίησης, στη διευκόλυνση της ελεύθερης κυκλοφορίας ψηφιακών προϊόντων και υπηρεσιών και στην ενίσχυση της εμπιστοσύνης των χρηστών στη χρήση νέων τεχνολογιών όπως το Internet of Things (IoT), τα δίκτυα 5G και τα υπολογιστικά νέφη (cloud computing).

Η Cybersecurity Act προσδιορίζει ότι τα συστήματα πιστοποίησης αναπτύσσονται από την ENISA σε συνεργασία με τα κράτη μέλη και τα ενδιαφερόμενα μέρη, ενώ η Ευρωπαϊκή Επιτροπή διατηρεί την αρμοδιότητα έγκρισης και έκδοσης των αντίστοιχων κανονιστικών πράξεων. Αν και οι περισσότερες πιστοποιήσεις είναι μέχρι στιγμής εθελοντικές, παρέχεται η δυνατότητα υποχρεωτικής εφαρμογής τους μέσω ειδικών κανονισμών ή τεχνικών προτύπων σε τομείς κρίσιμης σημασίας (π.χ. υγεία, ενέργεια, δημόσια διοίκηση).

Στο ευρύτερο πλαίσιο της ευρωπαϊκής ψηφιακής στρατηγικής, η Cybersecurity Act λειτουργεί συμπληρωματικά προς την Οδηγία NIS 2 και την AI Act, ενισχύοντας την οριζόντια διαλειτουργικότητα των πολιτικών ασφάλειας στον κυβερνοχώρο. Επιβεβαιώνεται έτσι ο ρόλος του ENISA ως κόμβου εμπειρογνωμοσύνης, ενισχύοντας τη

²³ EU Cybersecurity Act, (2019).

λειτουργία ευρωπαϊκών κέντρων συντονισμού και απόκρισης σε περιστατικά (CSIRTs), την παραγωγή ετήσιων αξιολογήσεων απειλών (threat landscapes), και την αλληλοϋποστήριξη μεταξύ ΕΕ και κρατών μελών στη διαχείριση κυβερνοκρίσεων. Η Cybersecurity Act θεωρείται ένα από τα πλέον κρίσιμα θεμέλια για την οικοδόμηση ψηφιακής κυριαρχίας (digital sovereignty) της ΕΕ, καθώς παρέχει τεχνική, θεσμική και στρατηγική ενίσχυση του ψηφιακού οικοσυστήματος της Ένωσης.

2.2.3 ΑΝΑΓΚΗ ΓΙΑ ΕΝΙΑΙΟ ΡΥΘΜΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΣΤΗΝ ΕΕ

Η θεσμική συνύπαρξη πολλαπλών κανονιστικών πλαισίων στην ΕΕ, όπως ο GDPR, η NIS 2 και η AI Act, δημιουργεί προκλήσεις ερμηνείας και εφαρμογής. Ειδικότερα, η NIS 2 απαιτεί από κρίσιμους φορείς να λαμβάνουν μέτρα κυβερνοασφάλειας, ενώ ο GDPR επιβάλλει υποχρεώσεις ως προς την ασφάλεια της επεξεργασίας προσωπικών δεδομένων (άρθρα 5 και 32). Η AI Act προσθέτει ένα τρίτο επίπεδο υποχρεώσεων, ιδίως όταν οι τεχνολογίες τεχνητής νοημοσύνης χρησιμοποιούνται σε ευαίσθητα περιβάλλοντα. Η απουσία εναρμονισμένης μεθοδολογίας συμμόρφωσης επιβαρύνει τους οργανισμούς με αντικρουόμενες απαιτήσεις, υπονομεύοντας την αποτελεσματικότητα του συστήματος.²⁴ Και εάν το πεδίο των προσωπικών δεδομένων φαίνεται να έχει ξεκαθαρίσει μετά την επιβολή του GDPR, στον τομέα της κυβερνοασφάλειας, παρά το μεγαλεπίβολο όραμα της NIS2 για ομοιογενή αντίδραση έναντι των κυβερνοαπειλών, τα κράτη μέλη παρουσιάζουν μεγάλες αποκλίσεις, αν αναλογιστεί κανείς το τεράστιο κόστος της συμμόρφωσης με τις νέες απαιτήσεις. Για παράδειγμα, ας σκεφτούμε πως η NIS2 θέτει στο μικροσκόπιο, εκτός από την κάθε οντότητα αυτοτελώς, και την αλυσίδα των προμηθευτών του. Αυτό είναι που διαπίστωσε, μεταξύ λοιπών, ο Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας (European CyberSecurity Organisation, εφεξής ο «ECSO», μόλις τον Ιανουάριο του 2025.²⁵ Το «White Paper - NIS2 Implementation: Challenges & Priorities» αναλύει τις προκλήσεις και τις προτεραιότητες στην εφαρμογή της Οδηγίας NIS2 στην ΕΕ. Συγκεκριμένα, επισημαίνεται η κατακερματισμένη

²⁴ Veale & Zuiderveen Borgesius, (2021).

²⁵ ECSO, (2025).

εφαρμογή μεταξύ των κρατών μελών, οι δυσκολίες που αντιμετωπίζουν οι Μικρές και Μεσαίες Επιχειρήσεις (εφεξής οι «ΜΜΕ») και οι νέοι τομείς λόγω ελλιπών πόρων και εμπειρίας, καθώς και οι διαφοροποιημένες απαιτήσεις για την αναφορά περιστατικών και τη διαχείριση κινδύνων. Τονίζονται επίσης οι ανάγκες για εναρμόνιση των διαδικασιών, την ανάπτυξη κοινών προτύπων και την ενίσχυση της διαχείρισης της ασφάλειας της εφοδιαστικής αλυσίδας σε ευρωπαϊκό επίπεδο. Το White Paper καταδεικνύει τη σημασία της εναρμόνισης της εφαρμογής της NIS2, δεδομένου ότι η πλειοψηφία των κρατών μελών της ΕΕ δεν έχει ακόμη ενσωματώσει τις απαιτήσεις της, παρά την προθεσμία της 17ης Οκτωβρίου 2024.

Τα παραπάνω ζητήματα έχουν τεθεί στο προσκήνιο και μέσω αποφάσεων εθνικών συνταγματικών δικαστηρίων. Το BVerfG, επί παραδείγματι, με την απόφαση Volkszählungsurteil II, επαναδιατύπωσε την αρχή του πληροφοριακού αυτοκαθορισμού ως συνταγματικό θεμέλιο, επισημαίνοντας την ανάγκη για θεσμικά επαρκή και συνεκτικά συστήματα προστασίας δεδομένων έναντι διασταυρούμενων νομικών πλαισίων και πολυεπίπεδων τεχνολογικών παρεμβάσεων.²⁶

2.2.4 Ψηφιακή Κυριαρχία και εντοπιότητα Δεδομένων στην ΕΕ

Η έννοια της ψηφιακής κυριαρχίας (digital sovereignty) αποκτά ολοένα και μεγαλύτερη σημασία στο πεδίο της τεχνολογικής πολιτικής, καθώς η ΕΕ, τα κράτη μέλη της, αλλά και άλλες παγκόσμιες δυνάμεις συνειδητοποιούν ότι η ψηφιακή εξάρτηση ισοδυναμεί με στρατηγική ευαλωτότητα. Ψηφιακή κυριαρχία δεν σημαίνει απαραίτητα αυτοδυναμία σε όλα τα πεδία, αλλά την ικανότητα ενός κράτους ή ενός υπερεθνικού σχηματισμού να ελέγχει και να διαμορφώνει τις προϋποθέσεις της τεχνολογικής του ανάπτυξης, διασφαλίζοντας παράλληλα την προστασία των θεμελιωδών δικαιωμάτων, της οικονομικής σταθερότητας και της ασφάλειας των πολιτών του. Αυτό συνεπάγεται την αυτονομία της ΕΕ να καθορίζει η ίδια τους όρους πρόσβασης, αποθήκευσης, επεξεργασίας και μεταφοράς των δεδομένων

²⁶ BVerfG, (2008).

εντός της, χωρίς να υπόκειται σε εξωεδαφικές πολιτικές ή εταιρικά συμφέροντα που παρακάμπτουν το ενωσιακό κεκτημένο.

Η Ευρωπαϊκή Επιτροπή έχει περιγράψει την ψηφιακή κυριαρχία ως την ικανότητα της ΕΕ «να καθορίζει τους δικούς της κανόνες και να λαμβάνει αποφάσεις βασισμένες στις δικές της αξίες, αντί να εξαρτάται από τεχνολογικές λύσεις τρίτων χωρών».²⁷ Η στόχευση αυτή αντανακλάται σε μια σειρά πολιτικών, όπως η **Ψηφιακή Στρατηγική της Ευρώπης**, το **GAIA-X**,²⁸ οι Ευρωπαϊκοί Χώροι Δεδομένων (European Data Spaces), όπως το πολυσυζητημένο EHDS,²⁹ η **European Cloud Federation**, και οι πρωτοβουλίες για **ευρωπαϊκά πρότυπα τεχνολογιών** τεχνητής νοημοσύνης και κυβερνοασφάλειας.

Κεντρικό στοιχείο της ψηφιακής κυριαρχίας αποτελεί η **κυριαρχία στα δεδομένα** (data sovereignty), η οποία σχετίζεται στενά με τη **γεωγραφική εντοπιότητα** των δεδομένων (data localization). Πρόκειται για την απαίτηση να παραμένουν τα δεδομένα εντός των φυσικών ή νομικών συνόρων ενός κράτους ή μιας οντότητας, ώστε να αποφεύγεται η υπαγωγή τους σε αλλοδαπά καθεστάτα επιτήρησης, όπως το αμερικανικό FISA ή το κινεζικό Cybersecurity Law.³⁰ Η επιδίωξη της ΕΕ να προστατεύσει τα προσωπικά δεδομένα των πολιτών της έναντι αθέμιτων διαβιβάσεων και επεξεργασίας οδήγησε στην ενίσχυση της **αρχής της διατήρησης δεδομένων εντός ΕΕ** ή υπό καθεστώς «ισοδύναμης προστασίας».

²⁷ European Commission, (2020).

²⁸ Η πρωτοβουλία GAIA-X φιλοδοξεί να προσφέρει ένα διαλειτουργικό, ανοικτό και ασφαλές cloud οικοσύστημα, ευθυγραμμισμένο με τις αρχές της ΕΕ για ιδιωτικότητα και προστασία δεδομένων. Βασίζεται σε αποκεντρωμένες υποδομές, τεχνικά APIs και μηχανισμούς ταυτοποίησης με βάση το Self-Sovereign Identity.

²⁹ Το European Health Data Space (EHDS) προωθεί την πρόσβαση σε δευτερογενή χρήση δεδομένων υγείας (π.χ. για έρευνα ή χάραξη πολιτικής), ενώ ενσωματώνει στοιχεία του GDPR (άρθρα 9 και 89) για ειδικές κατηγορίες δεδομένων. Η λειτουργία του EHDS προβλέπει τη σύσταση «Health Data Access Bodies» που θα αξιολογούν τα αιτήματα πρόσβασης και θα εγγυώνται τη συμμόρφωση με το ρυθμιστικό πλαίσιο (European Commission, 2022a).

³⁰ Bradford, (2020).

Οι νομολογιακές εξελίξεις στις υποθέσεις Schrems I και II ενίσχυσαν την στροφή προς την data localization, αποδομώντας μηχανισμούς όπως το Safe Harbor και το Privacy Shield, ενώ ταυτόχρονα οδήγησαν στην ανάγκη για διενέργεια **TIAs** ως προαπαιτούμενο εμπιστοσύνης προς κάθε δικαιοδοσία που δεν δεσμεύεται από τον GDPR.

Η στρατηγική της ΕΕ αποσκοπεί στη συγκρότηση ενός «ψηφιακού στρατηγικού αυτοπροσδιορισμού» που θα επιτρέψει την καινοτομία με εγγυημένα δικαιώματα, ασφάλεια και λογοδοσία. Το 2022, το EDPB εξέδωσε Δήλωση για την Ψηφιακή Κυριαρχία και τα Δικαιώματα των Πολιτών, υπογραμμίζοντας την ανάγκη ενίσχυσης του θεσμικού και τεχνικού ελέγχου των υποδομών cloud και AI, σε πλήρη συμμόρφωση με τον GDPR και τη στρατηγική για ανοικτό, δίκαιο και ανθεκτικό ψηφιακό οικοσύστημα στην ΕΕ.³¹ Αυτή η προσέγγιση, η οποία διασταυρώνει την προστασία δεδομένων με την γεωπολιτική σταθερότητα, αποτυπώνει τη στροφή της ΕΕ από μία καθαρά αγορακεντρική προσέγγιση προς ένα μοντέλο ρυθμιστικής κυριαρχίας που προτάσσει τη δημοκρατική λογοδοσία και τη βιώσιμη ψηφιακή ανεξαρτησία.

2.3 Διεθνείς Συνθήκες και Πρωτοβουλίες στον Τομέα της Κυβερνοασφάλειας και της Προστασίας Δεδομένων

Η παγκόσμια διάσταση των κυβερνοαπειλών και η διασυνοριακή φύση της επεξεργασίας δεδομένων επιβάλλουν τον συντονισμό μέσω διεθνών νομικών εργαλείων και πολυμερών πρωτοβουλιών. Οι διεθνείς συνθήκες και μηχανισμοί συνεργασίας λειτουργούν συμπληρωματικά προς το ενωσιακό πλαίσιο, ενισχύοντας την ασφάλεια των ψηφιακών περιβαλλόντων και την προστασία των θεμελιωδών ατομικών δικαιωμάτων.

2.3.1 Η Σύμβαση της Βουδαπέστης για το Κυβερνοέγκλημα

Η Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα (Convention on Cybercrime, ETS No. 185), γνωστή ως Σύμβαση της Βουδαπέστης,³² υπογράφηκε το 2001 και

³¹ EDPB, (2022).

³² Convention of Budapest on Cybercrime, (2001).

τέθηκε σε ισχύ το 2004. Αποτελεί την πρώτη και πιο διαδεδομένη διεθνή συνθήκη που αποσκοπεί στην εναρμόνιση των ποινικών διατάξεων κατά του κυβερνοεγκλήματος, τη διευκόλυνση της διεθνούς συνεργασίας και την ενίσχυση της διαδικαστικής δικαιοσύνης για τα εγκλήματα στο διαδίκτυο.

Η Σύμβαση έχει ευρύ πεδίο εφαρμογής, καλύπτοντας, μεταξύ άλλων, την παράνομη πρόσβαση και παρεμβολή σε υπολογιστικά συστήματα, την παραβίαση δεδομένων (data interference), τη διάδοση κακόβουλου λογισμικού (malware), τη σεξουαλική κακοποίηση παιδιών μέσω διαδικτύου, καθώς και την πειρατεία και την παραβίαση πνευματικών δικαιωμάτων.

Η Σύμβαση της Βουδαπέστης αποτελεί πρότυπο παγκόσμιας συνεργασίας στον τομέα της ψηφιακής ποινικής δικαιοσύνης, έχοντας υιοθετηθεί από περισσότερα από 65 κράτη παγκοσμίως, συμπεριλαμβανομένων και τρίτων χωρών όπως οι ΗΠΑ, ο Καναδάς, η Ιαπωνία και η Αυστραλία. Η Ελλάδα έχει επικυρώσει τη Σύμβαση και τα Πρωτόκολλά της, εντάσσοντάς την στο εσωτερικό της δίκαιο με τον Νόμο 4411/2016.³³ Το Δεύτερο Πρωτόκολλο (2022)³⁴ εστιάζει στην ενίσχυση της διασυνοριακής πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία, ανταποκρινόμενο στην αυξανόμενη ανάγκη για διαλειτουργικότητα των εθνικών ποινικών μηχανισμών.

2.3.2 Πρωτοβουλίες του ΟΟΣΑ για την Διακυβέρνηση Δεδομένων

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) έχει διαμορφώσει ένα συνεκτικό πλαίσιο αρχών για τη διακυβέρνηση των δεδομένων, με αιχμή τη Σύσταση “OECD Recommendation on Enhancing Access to and Sharing of Data” του 2021.³⁵ Η σύσταση αυτή δεν εστιάζει απλώς στη διευκόλυνση της πρόσβασης και της ανταλλαγής δεδομένων, αλλά στηρίζει την εφαρμογή προοδευτικών μοντέλων διαχείρισης, όπως η «κηδεμονία

³³ Νόμος 4411/2016 (ΦΕΚ 142/Α/3-8-2016).

³⁴ Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, (2022).

³⁵ OECD, (2021).

δεδομένων» (data stewardship), που συνδυάζει τεχνική διακυβέρνηση, θεσμική λογοδοσία και σεβασμό των θεμελιωδών δικαιωμάτων. Με τον τρόπο αυτό, ενισχύεται η ιδέα ότι οι δημόσιοι και ιδιωτικοί φορείς που επεξεργάζονται δεδομένα έχουν θεσμική υποχρέωση υπεύθυνης διαχείρισης, διαφάνειας και μη επαναπροσδιορισμού ταυτότητας.³⁶ Επιπλέον, προκρίνεται η αρχή της αναλογικής διαχείρισης κινδύνων, ιδίως σε περιβάλλοντα μεγάλης κλίμακας επεξεργασίας, όπως τα συστήματα τεχνητής νοημοσύνης ή τα πολυμερή ψηφιακά οικοσυστήματα.

Ο ΟΟΣΑ έχει λάβει ενεργό θέση παρατηρητή των μεταβαλλόμενων τεχνολογικών προτύπων και εκδίδει περιοδικές εκθέσεις για τις προκλήσεις της τεχνητής νοημοσύνης, των Big Data και της ψηφιακής ταυτότητας. Έτσι, το πλαίσιο του ΟΟΣΑ δεν λειτουργεί απλώς ως τεχνικός οδηγός, αλλά και ως καταλύτης για τη σύγκλιση διεθνών και περιφερειακών μοντέλων ρύθμισης, ενισχύοντας την προσπάθεια για καθολική και βιώσιμη προστασία των δεδομένων σε έναν διασυνδεδεμένο κόσμο. Αυτό επιτυγχάνεται μέσω της προσπάθειας για **ενσωμάτωση της ασφάλειας by design** σε όλον τον κύκλο ζωής των δεδομένων, **υποστήριξη της διατομεακής συνεργασίας** μεταξύ τεχνικών, νομικών και θεσμικών φορέων, όλα με γνώμονα τη **διασφάλιση διαλειτουργικότητας** μεταξύ των εθνικών ρυθμιστικών πλαισίων.

Καρπό της προσπάθειας αυτής αποτελεί η ανάπτυξη των «ευρωπαϊκών χώρων δεδομένων» (European Common Data Spaces), όπου επιδιώκεται διαλειτουργικότητα, διαφάνεια και ασφαλής πρόσβαση σε στρατηγικά σύνολα δεδομένων, όπως στην υγεία, στις μεταφορές και στον δημόσιο τομέα. Η σύνδεση αυτών των αρχών με την πολιτική της «ψηφιακής κυριαρχίας» της ΕΕ —δηλαδή της δυνατότητας των κρατών μελών και των πολιτών να

³⁶ Ο επαναπροσδιορισμός ταυτότητας (re-identification) αναφέρεται σε κάθε τεχνική ή μέθοδο που επιτρέπει να εντοπιστεί η ταυτότητα ενός ατόμου με βάση δεδομένα που αρχικά θεωρούνταν ανώνυμα ή ψευδωνυμοποιημένα. Συνεπώς, η αρχή του μη επαναπροσδιορισμού σημαίνει ότι όσοι διαχειρίζονται τέτοια δεδομένα (data stewards) έχουν την ηθική και νομική υποχρέωση να μην προσπαθούν, είτε άμεσα είτε έμμεσα, να ανακτήσουν την ταυτότητα του υποκειμένου των δεδομένων.

ελέγχουν την ψηφιακή τους μοίρα— υπογραμμίζει τη σημασία των δημοκρατικών εγγυήσεων στη διαχείριση των δεδομένων και στην τεχνολογική καινοτομία.

2.4 Το Εθνικό Πλαίσιο στην Ελλάδα: Διακυβέρνηση, Αρμοδιότητες και Νομοθεσία

Η Ελλάδα έχει εναρμονίσει τη νομοθεσία της με το ευρωπαϊκό θεσμικό πλαίσιο για την προστασία των προσωπικών δεδομένων και την κυβερνοασφάλεια, θεσπίζοντας ειδικούς φορείς, στρατηγικές και μηχανισμούς εφαρμογής. Το εθνικό πλαίσιο χαρακτηρίζεται από προοδευτική σύγκλιση με τα πρότυπα του GDPR και της Οδηγίας NIS 2, καθώς και από προσπάθειες ανάπτυξης διαλειτουργικών συστημάτων εποπτείας και λογοδοσίας.

2.4.1 Αρμόδιες Αρχές και Νομοθετικό Πλέγμα

Ο θεσμικός κορμός για την προστασία προσωπικών δεδομένων στην Ελλάδα συγκροτείται κυρίως από την **ΑΠΔΠΧ**, μία ανεξάρτητη αρχή συνταγματικά κατοχυρωμένη στο άρθρο 9Α του ελληνικού Συντάγματος, η οποία ιδρύθηκε με τον Ν. 2472/1997 και λειτουργεί υπό το νέο καθεστώς του Ν. 4624/2019 που ενσωματώνει τον GDPR. Η ΑΠΔΠΧ ασκεί κανονιστική, ελεγκτική και κυρωτική αρμοδιότητα, ενώ εκδίδει οδηγίες και συστάσεις για τη συμμόρφωση δημόσιων και ιδιωτικών φορέων με τον Κανονισμό. Το έργο της καλύπτει κρίσιμους τομείς όπως οι ευαίσθητες κατηγορίες δεδομένων, η βιντεοεπιτήρηση, η συγκατάθεση, καθώς και η επεξεργασία δεδομένων από δημόσιες αρχές.

Πέραν της προστασίας προσωπικών δεδομένων, η εθνική στρατηγική για τον ψηφιακό μετασχηματισμό περιλαμβάνει και την ενίσχυση της **κυβερνοασφάλειας** ως προϋπόθεση για τη διασφάλιση της εμπιστοσύνης στο ψηφιακό περιβάλλον. Στην Ελλάδα, αρμόδιος φορέας για τον σχεδιασμό, τον συντονισμό και την εποπτεία των πολιτικών κυβερνοασφάλειας είναι η **Εθνική Αρχή Κυβερνοασφάλειας (εφεξής η «ΕΑΚ»)**, η οποία υπάγεται στο **Υπουργείο Ψηφιακής Διακυβέρνησης** και λειτουργεί βάσει του **Π.Δ. 82/2021** και της **Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020–2025**.

Η ΕΑΚ έχει την ευθύνη να συντονίζει τις δράσεις για την προστασία κρίσιμων υποδομών, την πρόληψη και αντιμετώπιση κυβερνοαπειλών, καθώς και τη συμμόρφωση των δημόσιων και ιδιωτικών φορέων με την ενωσιακή και εθνική νομοθεσία, συμπεριλαμβανομένων της **NIS 2** και του **N. 5019/2023**.

Η εθνική εναρμόνιση ενισχύεται επίσης από πρωτοβουλίες για την **ψηφιοποίηση των δημόσιων υπηρεσιών**, μέσω της πλατφόρμας gov.gr, η οποία λειτουργεί υπό το πρίσμα του GDPR, παρέχοντας ενοποιημένες υπηρεσίες με κεντρικό έλεγχο των μηχανισμών ταυτοποίησης και αυθεντικοποίησης.

2.4.2 Η Εθνική Στρατηγική Κυβερνοασφάλειας (2020–2025)

Η **Εθνική Στρατηγική Κυβερνοασφάλειας για την περίοδο 2020–2025** διαμορφώθηκε από το Υπουργείο Ψηφιακής Διακυβέρνησης και βασίζεται στις αρχές πρόληψης, ανθεκτικότητας και ταχείας απόκρισης σε περιστατικά κυβερνοασφάλειας. Κύριοι στόχοι της είναι η **ενίσχυση των υποδομών κρίσιμης σημασίας**, όπως αυτοί καθορίζονται πλέον από την NIS2 και τον κυρωτικό της νόμο στην Ελλάδα,³⁷ η **καθολική εφαρμογή μέτρων τεχνικής ασφάλειας** (ISO/IEC 27001, NIS2), η **προώθηση της ευρωπαϊκής συνεργασίας**, ιδίως μέσω της συμμετοχής στον Ευρωπαϊκό Κόμβο Κυβερνοασφάλειας, και η **εκπαίδευση των πολιτών και δημοσίων υπαλλήλων** σε θέματα ασφάλειας και ιδιωτικότητας. Η Στρατηγική προκρίνει επίσης την ανάγκη υιοθέτησης του μοντέλου **"zero trust"**, δηλαδή της συνεχούς επαλήθευσης της ταυτότητας και των εξουσιοδοτήσεων των χρηστών σε όλα τα επίπεδα πρόσβασης.

Πρωτοβουλίες όπως ο **ψηφιακός μετασχηματισμός της ΑΑΔΕ** με υλοποίηση πιστοποίησης κατά ISO/IEC 27001 αποτελούν ενδεικτικά παραδείγματα εφαρμογής της Στρατηγικής σε επιμέρους δημόσιους φορείς.³⁸ Σύμφωνα με τις πιο πρόσφατες ανακοινώσεις του Υπουργείου Ψηφιακής Διακυβέρνησης (2024–2025), έχουν τεθεί σε εφαρμογή προγράμματα υποστήριξης των δημοσίων φορέων και συστήματα παρακολούθησης ωρίμανσης της

³⁷ EU Directive NIS2, (2022).

³⁸ Gov.gr, (2023).

αναπτυσσόμενης κουλτούρας κυβερνοασφάλειας, ενώ έχει δρομολογηθεί η αναθεώρηση του πλαισίου σε εναρμόνιση με την NIS 2.

Ειδική βιβλιογραφία κεφαλαίου 2

- Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press. Διαθέσιμο εδώ: <file:///C:/Users/a.fafaliou/Downloads/ssrn-2770634-1.pdf>
- *Convention of Budapest on Cybercrime*, (2001). Council of Europe ETS No. 185/2001). Διαθέσιμη εδώ: <https://rm.coe.int/1680081561>. Συγκεντρωμένα τα κείμενα της Σύμβασης και των δύο Προσθετων Πρωτοκόλλων της εδώ: <https://eur-lex.europa.eu/EL/legal-content/summary/convention-on-cybercrime.html>
- Creemers, R. (2016). *Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century*. *Journal of Contemporary China*. Διαθέσιμο εδώ: <https://www.tandfonline.com/doi/full/10.1080/10670564.2016.1206281#d1e103>
- Dpa.gr. Ο επίσημος ιστότοπος της Αρχής προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ΑΠΔΠΧ: <https://www.dpa.gr/el>
- ECSO, (2025). *White Paper - NIS2 Implementation: Challenges & Priorities*. Διαθέσιμο εδώ: <https://ecs-org.eu/ecso-uploads/2025/01/ECSO-White-Paper-NIS2-Implementation.pdf>
- EDPB (2022). *Statement on Digital Sovereignty and Citizens' Rights in the EU*. *Brussels*. Διαθέσιμο εδώ: <https://europeanmovement.eu/policy/digital-sovereignty-and-citizens-rights-2/>
- ENISA (2022). *Cybersecurity Threat Landscape Report*. European Union Agency for Cybersecurity. Διαθέσιμο εδώ: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202022.pdf>

- ENISA (2021). *Public-private partnerships for cybersecurity: evaluation and good practices*. European Union Agency for Cybersecurity. Διαθέσιμο εδώ: <https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/national-cybersecurity-strategies-0/public-private>
- EU-US Data Privacy Framework, (2024). Διαθέσιμο εδώ: [https://privacyshielddev.blob.core.windows.net/publicsiteassets/Full%20Text EU-U.S.%20DPF.pdf](https://privacyshielddev.blob.core.windows.net/publicsiteassets/Full%20Text%20EU-U.S.%20DPF.pdf)
- European Commission (2022). Proposal for a Regulation on the European Health Data Space (EHDS), COM(2022) 197 final. Διαθέσιμο εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0197>
- European Commission (2020). Shaping Europe's Digital Future. Brussels: COM(2020) 67 final. Διαθέσιμο εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0067>
- EU Directive NIS2, (2022). Οδηγία (ΕΕ) 2022/2555. Διαθέσιμη εδώ: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>
- EU NIS Cooperation Group: <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>
- EU Cybersecurity Act, (2019). *Regulation (EU) 2019/881* (Διαθέσιμος Εδώ: <https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng>)
- GDPR, (2016). (Regulation (EU) 2016/679.). Διαθέσιμος εδώ: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- Gov.gr (2023). Πιστοποίηση ISO της ΑΑΔΕ για την Ασφάλεια Πληροφοριακών Συστημάτων. Διαθέσιμο σε: https://www.aade.gr/sites/default/files/2023-11/diakirixi_anaptyxi_plaisiou_asfaleias_pliroforion.pdf
- Greenleaf, G. (2021). Global Tables of Data Privacy Laws and Bills (7th Ed, January 2021). Διαθέσιμο εδώ: <file:///C:/Users/a.fafaliou/Downloads/ssrn-3836261.pdf>

- International Standardisation Organisation ISO, ISO/IEC 27001 και ISO/IEC 27701, διαθέσιμα εδώ: <https://www.iso.org/standard/27001> και εδώ: <https://www.iso.org/standard/71670.html>
- OECD (2021). *Recommendation on Enhancing Access to and Sharing of Data*. Διαθέσιμο εδώ: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463>
- Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, (2022). Διαθέσιμο εδώ: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22023A0228\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22023A0228(01))
- US Cybersecurity Framework (CSF), σε επίσημη, εγκεκριμένη από τον NIST ελληνική μετάφραση. Διαθέσιμο εδώ: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.gre.pdf>
- Veale, M. & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4). Διαθέσιμο εδώ: <https://www.degruyterbrill.com/document/doi/10.9785/cri-2021-220402/html>
- Επίσημος ιστοχώρος της Cyberspace Administration of China (CAC): <https://www.cac.gov.cn/>
- Επίσημος ιστοχώρος της CISA (Cybersecurity and Infrastructure Security Agency): <https://www.cisa.gov/>
- Επίσημος ιστοχώρος του CERT-EU: <https://cert.europa.eu/>
- Επίσημος ιστοχώρος του EU NIS Cooperation Group: <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>
- Επίσημος ιστοχώρος του NIST (National Institute of Standards and Technology): <https://www.nist.gov/>
- Π.Δ. 82/2021 (ΦΕΚ Α' 195/30.11.2021). *Οργανισμός του Υπουργείου Ψηφιακής Διακυβέρνησης και σύσταση Εθνικού Φορέα Κυβερνοασφάλειας*. Διαθέσιμο εδώ:

<https://www.e-nomothesia.gr/kat-astynomikos-astynomia/kriseis-proagoges/proedriko-diatagma-82-2021-phek-201a-30-10-2021.html>

- Νόμος 4411/2016 (ΦΕΚ 142/Α/3-8-2016). Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών. Διαθέσιμος εδώ: <https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/nomos-4411-2016.html>
- Νόμος 4624/2019 (ΦΕΚ Α' 137/29.08.2019). Μέτρα εφαρμογής του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) και της Οδηγίας (ΕΕ) 2016/680. Διαθέσιμος εδώ: <https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-phek-137a-29-8-2019.html>
- Υπουργείο Ψηφιακής Διακυβέρνησης (2020). Εθνική Στρατηγική Κυβερνοασφάλειας 2020–2025. Αθήνα: Εθνικός Φορέας Κυβερνοασφάλειας. Διαθέσιμο σε: <https://mindigital.gr>

Νομολογία

- Bundesverfassungsgericht (εφεξής το «BVerfG») (2008). Judgment of 27 February 2008, Volkszählungsurteil II. Διαθέσιμη εδώ: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html
- CJEU, (2020). *Joined Cases C-511/18, C-512/18 and C-520/18 – La Quadrature du Net and Others*. Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0511>

- CJEU, (2020). Case C-311/18. *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Schrems II)*. Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311>
- CJEU, 2015. *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14 Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362>
- ECHR, (2008). *Liberty and Others v. United Kingdom*, App. No. 58243/00, Judgment of 1 July 2008. Διαθέσιμη εδώ: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22%3A%22001-87207%22%7D>

ΚΕΦΑΛΑΙΟ 3 - Η ΑΡΡΗΚΤΗ ΣΧΕΣΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ: ΣΥΓΚΡΟΥΣΗ Ή ΣΥΓΚΛΙΣΗ;

Η αλματώδης εξάπλωση των τεχνολογιών πληροφορικής και επικοινωνιών (εφεξής οι «ΤΠΕ» ή οι «ICTs») έχει οδηγήσει σε μια ριζική αναδιαμόρφωση των όρων υπό τους οποίους τα θεμελιώδη δικαιώματα υλοποιούνται στο ψηφιακό περιβάλλον. Στο πλαίσιο αυτό, δύο διακριτοί αλλά στενά αλληλοσυνδεδεμένοι τομείς έχουν αποκτήσει ιδιαίτερη σημασία: η προστασία των προσωπικών δεδομένων και η κυβερνοασφάλεια. Παρότι πρόκειται για πεδία που έχουν αναπτυχθεί βάσει διαφορετικών κανονιστικών λογικών και θεσμικών αναγκαιοτήτων, οι σύγχρονες απειλές και προκλήσεις στον κυβερνοχώρο καταδεικνύουν την αμοιβαία εξάρτησή τους και θέτουν επιτακτικά το ερώτημα: πρόκειται για σχέσεις συγκρουσιακές ή για στοιχεία ενός κοινού, αλληλοενισχυόμενου πλαισίου;

3.1. Η θεμελιώδης σημασία της κυβερνοασφάλειας για την προστασία προσωπικών δεδομένων

Η προστασία των προσωπικών δεδομένων, όπως κατοχυρώνεται στο άρθρο 8 του ΧΘΔΕΕ και εξειδικεύεται στον GDPR, δεν συνιστά απλώς μία αρχή τυπικού χαρακτήρα, αλλά τελεί υπό την προϋπόθεση της ύπαρξης κατάλληλων τεχνικών και οργανωτικών μέτρων ασφαλείας. Το άρθρο 32 του GDPR καθιστά σαφές ότι οι υπεύθυνοι και οι εκτελούντες την επεξεργασία φέρουν την ευθύνη διασφάλισης ενός «κατάλληλου επιπέδου ασφαλείας», ανάλογου με τη φύση, το εύρος και τη σοβαρότητα των ενδεχόμενων κινδύνων.³⁹

Συνεπώς, η κυβερνοασφάλεια δεν αποτελεί εξωτερικό ή επικουρικό παράγοντα αλλά πυρηνικό συστατικό της ουσιαστικής προστασίας των προσωπικών δεδομένων. Η ύπαρξη ευάλωτων πληροφοριακών συστημάτων συνεπάγεται αυξημένη πιθανότητα παραβίασης (data breach), με συνέπειες που εκτείνονται σε νομικό, κοινωνικό και ηθικό επίπεδο. Η αποτροπή τέτοιων παραβιάσεων εδράζεται στην εφαρμογή προηγμένων λύσεων κυβερνοασφάλειας, οι οποίες καθίστανται θεμέλιος λίθος για την πραγμάτωση του δικαιώματος στην ιδιωτικότητα.⁴⁰

3.1.1 Το δικαίωμα στην ιδιωτικότητα ως κριτήριο οριοθέτησης των μέτρων κυβερνοασφάλειας

Παρότι η κυβερνοασφάλεια διαδραματίζει κρίσιμο ρόλο στη διασφάλιση της ιδιωτικής σφαίρας, η ανάπτυξή της δεν μπορεί να εκτείνεται άνευ ορίων. Οφείλει να αναπτύσσεται εντός του πλαισίου νομιμότητας που ορίζει το δίκαιο προστασίας προσωπικών δεδομένων. Τα μέτρα ασφαλείας που λαμβάνονται, όσο απαραίτητα και αν είναι, δεν επιτρέπεται να

³⁹ GDPR, άρθρο 32.

⁴⁰ Bygrave, L. A. (2014).

παραβιάζουν την αρχή της αναλογικότητας ή να καθιστούν αδικαιολόγητα περιοριστικά τα δικαιώματα των υποκειμένων.⁴¹

Η Αρχή της Ελαχιστοποίησης των Δεδομένων (άρθρο 5 παρ. 1 γ' του GDPR) και η προσέγγιση “Privacy by Design and by Default” (άρθρο 25) αποτελούν κρίσιμα εργαλεία για την εξισορρόπηση της ανάγκης προστασίας με τον σεβασμό των θεμελιωδών δικαιωμάτων. Λύσεις όπως η καταγραφή αρχείων (logs), η παρακολούθηση δικτυακής κίνησης ή η υιοθέτηση λογισμικών ανίχνευσης απειλών πρέπει να σχεδιάζονται με τρόπο που διασφαλίζει ελαχιστοποίηση της παρεμβατικότητας και ενισχυμένη διαφάνεια.⁴²

3.1.2 ΑΝΤΙΦΑΣΕΙΣ ΚΑΙ ΠΡΟΚΛΗΣΕΙΣ: ΠΡΟΣ ΜΙΑ ΛΕΙΤΟΥΡΓΙΚΗ ΣΥΝΘΕΣΗ

Παρά την επιδιωκόμενη σύγκλιση, ενυπάρχουν δομικές εντάσεις μεταξύ των δύο τομέων. Ενδεικτικά, η χρήση αλγοριθμικών εργαλείων και τεχνητής νοημοσύνης για την πρόληψη ή αντιμετώπιση κυβερνοεπιθέσεων δημιουργεί ερωτήματα ως προς τη λογοδοσία, τη διαφάνεια και την επεξηγησιμότητα αποφάσεων που επηρεάζουν ανθρώπους. Επιπροσθέτως, πρακτικές κρατικής επιτήρησης που προβάλλονται υπό το πρόσχημα της εθνικής ασφάλειας ενδέχεται να αντιβαίνουν στα δικαιώματα των πολιτών, όπως επιβεβαιώνεται στη νομολογία του ΕΔΔΑ, όπως, επί παραδείγματι, στην υπόθεση *Big Brother Watch and Others v. United Kingdom*.⁴³ Η ουσία του προβλήματος δεν συνίσταται σε μια αναπόφευκτη αντίφαση αλλά σε θεσμικές αδυναμίες ενσωμάτωσης. Η πρόκληση αφορά τη συγκρότηση ενός ολιστικού πλαισίου κυβερνοασφάλειας, το οποίο να ενσωματώνει την προστασία των θεμελιωδών δικαιωμάτων ως οργανικό στοιχείο, και όχι ως εξωτερικό περιορισμό.

⁴¹ GDPR, Άρθρο 5 παρ. 1 περ. γ'.

⁴² GDPR, Άρθρο 25.

⁴³ ECHR, (2021).

Υπό το πρίσμα αυτό, η ΕΕ έχει διαμορφώσει ένα παράλληλο και συμπληρωματικό προς τον GDPR ρυθμιστικό οικοδόμημα. Η Cybersecurity Act ενισχύει θεσμικά τον ρόλο του ENISA ως του κατ' εξοχήν οργανισμού για την κυβερνοασφάλεια στην ΕΕ, ενώ η NIS 2 επεκτείνει τις υποχρεώσεις ασφάλειας σε κρίσιμες υποδομές και ψηφιακούς παρόχους.⁴⁴⁴⁵ Η υποχρέωση για ενσωμάτωση πολιτικών διαχείρισης κινδύνου, καθώς και η πρόβλεψη για υποχρεωτική αναφορά περιστατικών της NIS2, συγκλίνουν με τις αντίστοιχες απαιτήσεις του GDPR περί γνωστοποίησης παραβιάσεων (άρθρα 33-34). Η λειτουργική συνύπαρξη των δύο ρυθμιστικών πεδίων αποτυπώνει την αλληλεξάρτηση μεταξύ της ασφάλειας και της προστασίας της ιδιωτικότητας, διαμορφώνοντας ένα πολυεπίπεδο κανονιστικό πλέγμα. Τον Ιούνιο του 2025, ο ENISA εξέδωσε τον πιο πρόσφατο πρακτικό οδηγό του για την παροχή βοήθειας στους πληττόμενους οργανισμούς σε περιπτώσεις περιστατικού παραβίασης. Παρέχει λεπτομερή καθοδήγηση για τα τεχνικά μέτρα κυβερνοασφάλειας του άρθρου 21 της NIS2, με πρακτικά παραδείγματα συμμόρφωσης, αντιστοίχιση με το ISO 27001, NIST CSF κ.ά., προς διευκόλυνση των εθνικών ελέγχων.⁴⁶

3.1.3 ΤΟ ΠΛΑΙΣΙΟ ΤΗΣ «ΨΗΦΙΑΚΗΣ ΕΜΠΙΣΤΟΣΥΝΗΣ»

Η μετεξέλιξη των δύο τομέων σε ένα ενιαίο πρότυπο «ψηφιακής εμπιστοσύνης» (digital trust) αποτελεί τη σύγχρονη στρατηγική απάντηση στα προαναφερθέντα διλήμματα. Το υπόδειγμα αυτό υπογραμμίζει ότι η ασφάλεια και η ιδιωτικότητα δεν είναι ανταγωνιστικά αλλά συνεκτικά και αλληλοτροφοδοτούμενα μεγέθη. Ο ΟΟΣΑ και η Ευρωπαϊκή Επιτροπή έχουν ενσαρκώσει την αντίληψη αυτή σε πολιτικές και συστάσεις, επιδιώκοντας τη διαμόρφωση ενός συνεκτικού ψηφιακού οικοσυστήματος εμπιστοσύνης.⁴⁷⁴⁸ Η ενσωμάτωση της ιδιωτικότητας στην ασφάλεια αποτελεί στρατηγική αναγκαιότητα. Η ψηφιακή κυριαρχία, όπως διατυπώνεται στη Στρατηγική για την Ψηφιακή Δεκαετία της ΕΕ,

⁴⁴ European Cybersecurity Act (2019).

⁴⁵ EU Directive NIS2, (2022).

⁴⁶ ENISA, (2025).

⁴⁷ OECD. (2022).

⁴⁸ ENISA, (2023).

προϋποθέτει τη συνεκτική εφαρμογή αρχών ασφάλειας και προστασίας δεδομένων ως αλληλοενισχυόμενων στόχων⁴⁹.

3.2 Ο «διάλογος» μεταξύ της κυβερνοασφάλειας και της ελεύθερης ροής δεδομένων εντός ΕΕ

Η μετάβαση σε ένα ενιαίο και ανθεκτικό ευρωπαϊκό οικοσύστημα ψηφιακής διακυβέρνησης δεν μπορεί να επιτευχθεί χωρίς την ταυτόχρονη εμβάθυνση του διαλόγου μεταξύ της κυβερνοασφάλειας και της ελευθερίας κυκλοφορίας δεδομένων. Ας εξετάσουμε αυτόν ακριβώς τον «διάλογο» μεταξύ κανονιστικών πρωτοβουλιών όπως η οδηγία NIS 2 και ο νέος Κανονισμός για την Ψηφιακή Ανθεκτικότητα (Cyber Resilience Act), αφενός, και της ευρωπαϊκής στρατηγικής για τα δεδομένα, αφετέρου, όπως αυτή αρθρώνεται μέσα από τον Κανονισμό για τη Διακυβέρνηση των Δεδομένων (Data Governance Act) και τον Κανονισμό για τα Δεδομένα (Data Act). Η ΕΕ επιδιώκει να διαμορφώσει ένα συνεκτικό πλαίσιο, στο οποίο η ενίσχυση της τεχνολογικής ασφάλειας δεν θα λειτουργεί ανασταλτικά στη ροή δεδομένων, αλλά θα αποτελεί προϋπόθεση για τη θεμελίωση εμπιστοσύνης, διαλειτουργικότητας και ασφάλειας δικαίου στην Ψηφιακή Ενιαία Αγορά.

3.2.1 NIS2 και Cyber Resilience Act

Η πολυαναμενόμενη Cyber Resilience Act, ήτοι ο Κανονισμός ΕΕ 2847/2024 (εφεξής η «CRA»)⁵⁰ συμπληρώνει το βασικό πλαίσιο της ΕΕ για την ασφάλεια στον κυβερνοχώρο, δηλαδή την NIS2 και τον Cybersecurity Act. Η NIS2 θέτει σε εφαρμογή απαιτήσεις κυβερνοασφάλειας και υποχρεώσεις αναφοράς συμβάντων για βασικές και σημαντικές οντότητες με σκοπό την αύξηση της ανθεκτικότητάς τους. Για παράδειγμα, όλα τα προϊόντα λογισμικού και υλισμικού θα φέρουν τη σήμανση CE η οποία θα εγγυάται ότι

⁴⁹ European Commission, (2020).

⁵⁰ Στις 10/10/2024 το Συμβούλιο υιοθέτησε το τελικό κείμενο του Κανονισμού και στις 20/11/2024 αυτός δημοσιεύθηκε στην Επίσημη Εφημερίδα της ΕΕ. [Αναλυτικά για την CRA και για τα προϊόντα με ψηφιακά στοιχεία: \(European Cyber Resilience Act, \(2024\)\).](#)

συμμορφώνονται με τις απαιτήσεις του κανονισμού. Η ένδειξη «CE» εμφανίζεται σε πολλά προϊόντα που διατίθενται στο εμπόριο στη διευρυμένη ενιαία αγορά του Ευρωπαϊκού Οικονομικού Χώρου (εφεξής ο «ΕΟΧ»). Τούτο σημαίνει ότι τα προϊόντα που πωλούνται στον ΕΟΧ έχουν αξιολογηθεί και πληρούν υψηλές απαιτήσεις ως προς την ασφάλεια, την υγεία και την προστασία του περιβάλλοντος. Ο κανονισμός αυτός θα εφαρμόζεται σε όλα τα προϊόντα που συνδέονται άμεσα ή έμμεσα με άλλη συσκευή ή δίκτυο. Υπάρχουν κάποιες εξαιρέσεις για τα προϊόντα για τα οποία οι απαιτήσεις κυβερνοασφάλειας έχουν ήδη καθοριστεί σε υφιστάμενους κανόνες της ΕΕ, όπως είναι για παράδειγμα τα ιατροτεχνολογικά προϊόντα, τα προϊόντα αεροναυπηγικής και τα «αυτόνομα οχήματα». Τέλος, ο νέος κανονισμός θα επιτρέψει στους καταναλωτές να λαμβάνουν υπόψη την κυβερνοασφάλεια όταν επιλέγουν και χρησιμοποιούν προϊόντα που διασυνδέονται ψηφιακά, διότι θα τους διευκολύνει να εντοπίζουν προϊόντα υλισμικού και λογισμικού με τα κατάλληλα χαρακτηριστικά κυβερνοασφάλειας.

Η CRA αποτελεί μια προληπτική απάντηση στο εξελισσόμενο τοπίο των απειλών στον κυβερνοχώρο, προσβλέποντας στην ανάδειξη της ασφάλειας των ψηφιακών προϊόντων και υπηρεσιών ως κορωνίδα των χαρακτηριστικών που αναζητούν οι καταναλωτές. Θα τεθεί σε πλήρη ισχύ το 2027, ενώ η Ελλάδα προετοιμάζεται για τη συμμόρφωση μέσω δράσεων προσαρμογής από την ΕΑΚ και τις αρμόδιες τελωνειακές αρχές για την εποπτεία της αγοράς.

3.2.2 Το όραμα της ΕΕ για ελεύθερη ροή δεδομένων σε έναν ασφαλή κυβερνοχώρο

Εύγλωττο είναι πως όσο οι επικοινωνίες και οι συναλλαγές που πραγματοποιούνται δια του διαδικτύου αυξάνονται εκθετικά, τόσο αυξάνεται και η ανάγκη για τη διασφάλιση ασφαλών, πλην όμως απεριορίστων δυνατοτήτων διατομεακά. Προς επίτευξη αυτού, πέρα από το κανονιστικό πλαίσιο για την κυβερνοασφάλεια, η ΕΕ έχει προβεί και στη δημιουργία πλέγματος προστασίας των δεδομένων, προσωπικών και μη, σε ιδιωτικό και δημόσιο τομέα. Έτσι «γεννήθηκε» η Ευρωπαϊκή Στρατηγική για τα Δεδομένα (EU Data Strategy), προς χάριν

της ίσης πρόσβασης όλων των Ευρωπαίων πολιτών στα δεδομένα που διακινούνται στην ΕΕ και της προάσπισης των ατομικών δικαιωμάτων σε περιβάλλον διαδικτύου.

3.2.3 Data Act και Data Governance Act

Ο Κανονισμός σχετικά με τους εναρμονισμένους κανόνες για τη δίκαιη πρόσβαση στα δεδομένα και τη χρήση τους ([Data Act](#))⁵¹ τέθηκε σε ισχύ στις 11 Ιανουαρίου 2024, με πρόβλεψη να αρχίσει να εφαρμόζεται το Σεπτέμβριο του 2025. Ο Κανονισμός αποτελεί βασικό πυλώνα της [ευρωπαϊκής στρατηγικής για τα δεδομένα](#)⁵² και θα συμβάλει σημαντικά στην επίτευξη του στόχου της ψηφιακής δεκαετίας για την προώθηση του ψηφιακού μετασχηματισμού της ΕΕ.

Η Data Act συμπληρώνει τον [Κανονισμό για τη Διακυβέρνηση των Δεδομένων \(Data Governance Act \(εφεξής η «DGA»\)\)](#),⁵³ η οποία ήταν το πρώτο παραδοτέο στο πλαίσιο της [ευρωπαϊκής στρατηγικής για τα δεδομένα](#) και άρχισε να εφαρμόζεται τον Σεπτέμβριο του 2023. Ενώ η DGA ρυθμίζει τις διαδικασίες και τις δομές που διευκολύνουν την εθελοντική ανταλλαγή δεδομένων, η Data Act διευκρινίζει ποιός και υπό ποιές προϋποθέσεις δικαιούται να χρησιμοποιεί τα δεδομένα. Μαζί, οι δύο αυτές πράξεις θα διευκολύνουν την αξιόπιστη και ασφαλή πρόσβαση στα δεδομένα, προωθώντας τη χρήση τους σε βασικούς οικονομικούς τομείς και τομείς δημόσιου συμφέροντος. Θα συμβάλουν επίσης στη δημιουργία μιας ενιαίας αγοράς δεδομένων στην ΕΕ, ωφελώντας τελικά τόσο την ευρωπαϊκή οικονομία όσο και την κοινωνία στο σύνολό της. Απαιτείται θεσμική προσαρμογή για τη διαχείριση των διαφωνιών πρόσβασης σε δεδομένα μεταξύ επιχειρήσεων και καταναλωτών, καθώς και η κατοχύρωση πρόσβασης του Δημοσίου σε δεδομένα ιδιωτικού, όταν διακυβεύεται το δημόσιο συμφέρον.

⁵¹ European Data Act, (2020).

⁵² European Data Strategy, (2020). Στη φαρέτρα της βρίσκονται νομοθετήματα και κατευθυντήριες γραμμές για την ελεύθερη ροή μη προσωπικών δεδομένων μεταξύ επιχειρήσεων, για την ανοιχτή πρόσβαση και την επαναχρησιμοποίηση δεδομένων μέσω των ανοιχτών data spaces του δημοσίου τομέα, αλλά και για την Τεχνητή Νοημοσύνη.

⁵³ European Data Governance Act, (2022).

Ο Νόμος 5188/2025 για τη διακυβέρνηση δεδομένων ενσωματώνει στην ελληνική έννομη τάξη την Data Governance Act και ορίζει ως εθνική αρμόδια αρχή για την εφαρμογή της τη Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης. Αυτή η αρχή αναλαμβάνει την υποστήριξη των φορέων του δημόσιου τομέα για θέματα πρόσβασης και επαναχρησιμοποίησης δεδομένων, λειτουργώντας παράλληλα ως εθνικό και ενιαίο σημείο επαφής (one-stop shop) σύμφωνα με τις ευρωπαϊκές απαιτήσεις.

Χάρη στη Data Act, τα συνδεδεμένα προϊόντα θα πρέπει να σχεδιάζονται και να κατασκευάζονται με τρόπο που να δίνει τη δυνατότητα στους χρήστες (επιχειρήσεις ή καταναλωτές) να έχουν εύκολη και ασφαλή πρόσβαση, να χρησιμοποιούν και να μοιράζονται τα παραγόμενα δεδομένα. Πρόκειται για διατομεακή νομοθεσία, δηλαδή αρχές και κατευθυντήριες γραμμές που ισχύουν για όλους τους τομείς νομοθέτησης εντός της Ένωσης. Δεν τροποποιεί τις υφιστάμενες υποχρεώσεις πρόσβασης στα δεδομένα, ωστόσο οποιαδήποτε μελλοντική νομοθεσία θα πρέπει να ευθυγραμμίζεται με τις αρχές της.

Η DGA στοχεύει στην επαναχρησιμοποίηση δημόσιων ή προστατευόμενων δεδομένων, υπό την εποπτεία οντοτήτων που είναι γνωστές ως ενδιάμεσοι φορείς δεδομένων, και την προώθηση της κοινής χρήσης δεδομένων για αλτρουιστικούς σκοπούς. Η DGA καλύπτει τόσο προσωπικά όσο και μη προσωπικά δεδομένα, ενώ ο [GDPR](#) εφαρμόζεται κάθε φορά που εμπλέκονται προσωπικά δεδομένα. Η συμπερίληψη ενσωματωμένων εγγυήσεων, πέραν του GDPR, αποσκοπεί στην ενίσχυση της εμπιστοσύνης στην κοινή χρήση και επαναχρησιμοποίηση δεδομένων. Αυτή η οικοδόμηση εμπιστοσύνης είναι ζωτικής σημασίας για την αύξηση της διαθεσιμότητας των δεδομένων στην αγορά.

3.2.4 Κανονισμός DORA: Προς ένα Ψηφιακά Ανθεκτικό

Χρηματοπιστωτικό σύστημα στην ΕΕ

Ο Κανονισμός (ΕΕ) 2022/2554 για την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα στον Χρηματοπιστωτικό Τομέα (Digital Operational Resilience Act, εφεξής η «**DORA**»),⁵⁴ εγκρίθηκε τον Δεκέμβριο του 2022 και τέθηκε πλήρως σε εφαρμογή τον Ιανουάριο του 2025. Αποτελεί ένα από τα σημαντικότερα θεσμικά εγχειρήματα της ΕΕ για την ενίσχυση της **κυβερνοανθεκτικότητας**, με εφαρμογή σε πάνω από 20 κατηγορίες χρηματοπιστωτικών οντοτήτων, από τράπεζες και ασφαλιστικές εταιρείες έως παρόχους cloud υπηρεσιών και third-party ICT providers.

Η DORA θεμελιώνεται στην παραδοχή ότι οι **κυβερνοαπειλές** και οι **διαταραχές σε υποδομές πληροφορικής** συνιστούν συστημικούς κινδύνους, ικανούς να προκαλέσουν **διασυστημική αβεβαιότητα** και να υπονομεύσουν τη σταθερότητα του χρηματοπιστωτικού τομέα. Εισάγει, επομένως, μια **ενιαία ευρωπαϊκή προσέγγιση** για την ψηφιακή επιχειρησιακή ανθεκτικότητα (digital operational resilience), λειτουργώντας συμπληρωματικά προς την NIS2.⁵⁵

Η νομική και κανονιστική συνεισφορά της DORA εκτείνεται σε πέντε βασικούς άξονες:

1. **Διακυβέρνηση και διαχείριση κινδύνων ICT (ICT risk management):** Υποχρεώνει τους εποπτευόμενους φορείς να ενσωματώσουν πολιτικές και μηχανισμούς εντοπισμού, αξιολόγησης και αντιμετώπισης κινδύνων ΤΠΕ (άρθρα 5–12).
2. **Αναφορά περιστατικών κυβερνοασφάλειας:** Εισάγεται κοινό πλαίσιο για την **υποχρεωτική αναφορά σοβαρών περιστατικών**, εντός συγκεκριμένων χρονικών πλαισίων και με διαλειτουργικά πρότυπα (άρθρα 17–23), σε ευθυγράμμιση με τις προβλέψεις της NIS 2 και του GDPR.

⁵⁴ EU DORA Regulation, (2022).

⁵⁵ Yogosha.com, (2024).

3. **Ψηφιακές δοκιμές ανθεκτικότητας (Digital resilience testing):** Καθιερώνεται η υποχρέωση διενέργειας **προσομοιώσεων κυβερνοεπιθέσεων (TLPT)**, ιδίως για συστημικά σημαντικές επιχειρήσεις (άρθρα 24–27).
4. **Διαχείριση κινδύνων από τρίτους παρόχους τεχνολογίας (Third-party risk):** Ρυθμίζεται για πρώτη φορά σε επίπεδο ΕΕ η **συμβατική και τεχνική διακυβέρνηση σχέσεων με ICT third-party providers**, με πρόβλεψη για ειδικό ευρωπαϊκό εποπτικό πλαίσιο (άρθρα 28–44).
5. **Αρχή της αναλογικότητας και της λογοδοσίας:** Η συμμόρφωση με τις απαιτήσεις του DORA βασίζεται σε **risk-based** προσέγγιση, συνδυάζοντας την αναλογικότητα με την αυξημένη λογοδοσία του διοικητικού συμβουλίου.

Η DORA δεν λειτουργεί αποκομμένα από το ευρύτερο ρυθμιστικό οικοσύστημα. Αντίθετα, επιδιώκει διαλειτουργικότητα με τον **GDPR**, ιδίως ως προς την επεξεργασία και την ασφάλεια των προσωπικών δεδομένων σε περίπτωση κυβερνοεπιθέσεων (Άρθρα 32 και 33 GDPR), την **Οδηγία NIS 2**, διαμορφώνοντας συντονισμένες υποχρεώσεις αναφοράς και διακυβέρνησης για κρίσιμες ψηφιακές υπηρεσίες και τα πρότυπα **ISO/IEC 27001, 27005 και 22301**, ιδίως στα πεδία επιχειρησιακής συνέχειας, διαχείρισης συμβάντων και ανθεκτικότητας υποδομών. Το Άρθρο 30(3) της DORA περιλαμβάνει περαιτέρω απαιτήσεις όπου οι υπηρεσίες ΤΠΕ υποστηρίζουν μια κρίσιμη ή σημαντική λειτουργία της χρηματοοικονομικής οντότητας. Μια “κρίσιμη ή σημαντική λειτουργία” σημαίνει μια λειτουργία, η διακοπή της οποίας θα επηρεάσει σημαντικά την οικονομική απόδοση της χρηματοοικονομικής οντότητας ή τη βιωσιμότητα ή συνέχεια των υπηρεσιών και δραστηριοτήτων της.

Στο καθ’ ημάς ελληνικό πλαίσιο, η Τράπεζα της Ελλάδος και η Επιτροπή Κεφαλαιαγοράς έχουν ήδη εκδώσει **συστάσεις προσαρμογής**, ενώ σημαντικό ρόλο στην εφαρμογή του Κανονισμού διαδραματίζει η ΕΑΚ, η οποία συντονίζει ενέργειες προληπτικού ελέγχου και δοκιμών ψηφιακής ανθεκτικότητας, σε συνέργεια με τις προβλέψεις του Ν. 5019/2023.

Τέλος, η DORA εισάγει ένα **κανονιστικό μοντέλο**, στο οποίο η προστασία των πληροφοριακών συστημάτων και των δεδομένων αντιμετωπίζεται ως αναπόσπαστο μέρος της συστημικής ευστάθειας. Ενσωματώνει την **ψηφιακή ανθεκτικότητα ως δικαίωμα των χρηστών**, καθιστώντας την κυβερνοασφάλεια στοιχείο του οικονομικού και κοινωνικού συμβολαίου της ΕΕ με τους πολίτες της. Ας σημειωθεί εδώ πως ενώ η Nis2 είναι οδηγία, δίνοντας κάποιες minimum δυνατότητες στα κράτη-μέλη να αποκλίνουν από αυτήν κατά την ενσωμάτωσή της, η DORA είναι κανονισμός, ήτοι έχει άμεση ισχύ σε όλα τα κράτη-μέλη. Η ΕΕ επέλεξε να παρέμβει καθολικά και ομοιόμορφα προκειμένου να πετύχει τη μέγιστη εφαρμογή της ασφάλειας και της ανθεκτικότητας των πληροφοριακών συστημάτων στον χρηματοοικονομικό τομέα.

Ειδική Βιβλιογραφία κεφαλαίου 3

- Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press. Διαθέσιμο στο: <https://academic.oup.com/book/27114>
- GDPR, (2016). (Regulation (EU) 2016/679.). Διαθέσιμος εδώ: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- ENISA, (2023). *Cybersecurity and Data Protection by Design*. Διαθέσιμο στο: <https://www.enisa.europa.eu/publications/data-protection-engineering>
- ENISA, (2025). *NIS2 Technical Implementation Guidance*. Διαθέσιμο εδώ: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf
- ECHR, (2021). *Big Brother Watch and Others v. the United Kingdom*. Διαθέσιμη εδώ: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-210077%22%5D%7D>
- European Commission, (2020). *Europe's Digital Decade*. Διαθέσιμο στο: <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>

- EU Data Act (2020). Κανονισμός (ΕΕ) 2020/2854. Διαθέσιμος εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1749730466674>
- EU Data Governance Act, (2022). Κανονισμός (ΕΕ) 2022/868. Διαθέσιμος εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868>
- EU Directive NIS2, (2022). Οδηγία (ΕΕ) 2022/2555. Διαθέσιμη εδώ: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>
- EU DORA Regulation, (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Διαθέσιμος εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554>
- EU Cyber Resilience Act (2024). Κανονισμός (ΕΕ) 2024/2847. Διαθέσιμος εδώ: <https://www.european-cyber-resilience-act.com/>
- EU Cybersecurity Act, (2019). Κανονισμός (ΕΕ) 2019/881. Διαθέσιμο στο: <https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng>
- European Data Strategy, (2020). Διαθέσιμη εδώ: https://ec.europa.eu/commission/presscorner/api/files/attachment/862109/European_data_strategy_en.pdf
- ¹ OECD. (2022). *Enhancing Digital Security and Privacy in Policy Making*. [Online] Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf
<https://www.oecd.org/digital/enhancing-digital-security-and-privacy.pdf>
- Yogosha.com, (2024). NIS2 vs DORA: what differences and which legislation prevails? Διαθέσιμο εδώ: <https://yogosha.com/blog/nis2-vs-dora/>
- Νόμος 5188/2025 – (ΦΕΚ 49/Α/28-3-2025). Διαθέσιμος εδώ: <https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/n-5188-2025.html>

ΚΕΦΑΛΑΙΟ 4 - ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ, BIG DATA ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ: ΕΝΑ ΠΛΑΙΣΙΟ ΤΕΧΝΟΛΟΓΙΚΩΝ ΠΡΟΚΛΗΣΕΩΝ ΚΑΙ ΝΟΜΙΚΗΣ ΠΡΟΣΑΡΜΟΓΗΣ

4.1 Η Τεχνητή Νοημοσύνη ως παράγων μεταβολής της έννοιας της ιδιωτικότητας

Η ενσωμάτωση της Τεχνητής Νοημοσύνης (εφεξής TN) στο πλαίσιο επεξεργασίας προσωπικών δεδομένων προκαλεί επαναδιατύπωση θεμελιωδών νομικών και ηθικών παραδοχών περί ιδιωτικότητας. Η αυτοματοποιημένη λήψη αποφάσεων, όπως ορίζεται στο άρθρο 22 του GDPR, εισάγει ένα κανονιστικό παράδοξο: ενώ επιδιώκει την ενίσχυση της προστασίας, ενδέχεται να υπονομεύει την ουσιαστική ελευθερία των υποκειμένων μέσω τεχνολογικής αδιαφάνειας και αλγοριθμικής προκατάληψης.⁵⁶⁵⁷

Η εφαρμογή αλγορίθμων μηχανικής μάθησης απαιτεί μεγάλες ποσότητες δεδομένων, οδηγώντας συχνά σε επεξεργασία ευαίσθητων δεδομένων χωρίς την απαιτούμενη ρητή συγκατάθεση των υποκειμένων, ή επαρκείς μηχανισμούς ελέγχου.⁵⁸ Το δικαίωμα στη διαφάνεια (άρθρα 12–14 GDPR) τίθεται υπό πίεση, ιδίως όταν οι επεξηγήσεις των αλγορίθμων είναι τεχνικά δυσεφάρμοστες.

Καίρια για τη θεμελίωση του δικαιώματος στην ιδιωτικότητα, το BVerfG, το 2008, στην υπόθεση ορόσημο *Volkszählungsurteil II* αναγνώρισε το δικαίωμα στον πληροφοριακό αυτοκαθορισμό ως ακρογωνιαίο λίθο της σύγχρονης προστασίας δεδομένων. Η απόφαση επισημαίνει ότι η προσωπική αυτονομία και η δυνατότητα ελέγχου της πληροφορίας που αφορά το άτομο συνιστούν αναγκαία προϋπόθεση για τη διατήρηση της ανθρώπινης

⁵⁶ Βλ. άρθρο 22 GDPR σχετικά με την αυτοματοποιημένη λήψη αποφάσεων.

⁵⁷ Wachter, Mittelstadt and Floridi, 2017

⁵⁸ Veale, M. and Binns, R. (2017).

αξιοπρέπειας και ελευθερίας.⁵⁹⁶⁰ Η νομική αυτή θεμελίωση καθίσταται κρίσιμη στο περιβάλλον της TN, όπου η διαφάνεια στις διαδικασίες λήψης αποφάσεων συγκρούεται με την πολυπλοκότητα των αλγοριθμικών μοντέλων και την ανάγκη διασφάλισης της υπευθυνότητας των συστημάτων.

Ο Κανονισμός για την Τεχνητή Νοημοσύνη (AI Act) διαμορφώνει ένα νέο ρυθμιστικό υπόδειγμα εντός της ΕΕ, το οποίο επιχειρεί να υπερβεί τον δυϊσμό ανάμεσα σε προστασία και καινοτομία. Οι διατάξεις περί υψηλού κινδύνου, καταγραφής αλγοριθμικών λειτουργιών και ενίσχυσης ανθρώπινης εποπτείας συνιστούν εκδήλωση της αρχής της «τεχνολογικής υπευθυνότητας» (technological accountability).⁶¹

Η σχέση της AI Act με το GDPR μπορεί να ερμηνευθεί μέσω της θεωρίας της πολυεπίπεδης ρύθμισης (multi-level governance), στην οποία πολλαπλοί κανονιστικοί μηχανισμοί αλληλεπιδρούν και συνδιαμορφώνουν το ρυθμιστικό πεδίο. Η απαγόρευση χρήσεων όπως η βιομετρική επιτήρηση σε δημόσιους χώρους υποδεικνύει τη μετάβαση από μια ουδέτερη τεχνολογική στάση προς ένα μοντέλο ηθικά εμποτισμένης ρυθμιστικής παρέμβασης.

Την 27η Μαΐου 2021, η Noyb υπέβαλε καταγγελία κατά της Clearview AI στην αυστριακή Αρχή Προστασίας Δεδομένων (DSB), ζητώντας την απαγόρευση των δραστηριοτήτων επεξεργασίας δεδομένων της εταιρείας. Η Noyb υποστήριξε ότι η Clearview AI δεν μπορεί να στηριχθεί σε νόμιμη βάση για την επεξεργασία των προσωπικών δεδομένων, καθώς η επιχειρηματική της δραστηριότητα βασίζεται στη συνεχή αναζήτηση και επεξεργασία εικόνων προσώπων από το διαδίκτυο. Η DSB διαπίστωσε παραβίαση του GDPR, αλλά θεώρησε ότι η διαγραφή των προσωπικών δεδομένων ήταν επαρκές μέτρο προστασίας, και επομένως απέρριψε το αίτημα για πλήρη απαγόρευση της επεξεργασίας. Η Noyb προσέφυγε στο Ομοσπονδιακό Διοικητικό Δικαστήριο της Αυστρίας, Bundesverwaltungsgericht (εφεξής το «BVwG»), το οποίο επικρίνει την απόφαση της DSB για

⁵⁹ BVerfG, (2008).

⁶⁰ Burrell, 2016, Selbst and Barocas, 2018

⁶¹ EU AI Act, (2024).

την παράλειψη αξιολόγησης της εφαρμογής μιας απαγόρευσης. Στην υπόθεση αυτή, δεν επιβλήθηκε πρόστιμο. Το δικαστήριο επικεντρώθηκε στην ανάγκη επανεξέτασης της απόφασης της DSB για την απαγόρευση της επεξεργασίας δεδομένων, καθώς κρίνεται ότι μόνο ένα μέτρο απαγόρευσης θα μπορούσε να διασφαλίσει την πλήρη προστασία από μελλοντικές παράνομες επεξεργασίες δεδομένων.⁶²

Σε μια άλλη πολύ ενδιαφέρουσα εξέλιξη, στις 27 Φεβρουαρίου του τρέχοντος έτους το ΔΕΕ εξέδωσε απόφαση στην υπόθεση «Dun and Bradstreet Austria».⁶³ Η απόφαση αφορά την ερμηνεία του δικαιώματος πρόσβασης του υποκειμένου βάσει του Άρθρου 15(1)(η) του ΓΚΠΔ, εστιάζοντας στην υποχρέωση του υπευθύνου επεξεργασίας να παράσχει εξήγηση της αυτοματοποιημένης διαδικασίας λήψης αποφάσεων. Στην υπόθεση, μετά την άρνηση σύναψης σύμβασης λόγω αξιολόγησης πιστωτικής ικανότητας από την Dun & Bradstreet Austria, το υποκείμενο των δεδομένων ζήτησε να ενημερωθεί για τη λογική που οδήγησε στην εν λόγω απόφαση. Το Δικαστήριο κατέληξε στο ότι η παρεχόμενη εξήγηση πρέπει να είναι σαφής, συνοπτική και κατανοητή, ώστε να γίνει κατανοητό πώς ελήφθη η αυτοματοποιημένη απόφαση, ενώ ταυτόχρονα να διασφαλίζονται τα σχετικά εμπορικά απόρρητα. Συνεπώς, το δικαστήριο έκρινε ότι το Άρθρο 15(1)(η) του ΓΚΠΔ πρέπει να ερμηνεύεται ως εξής: εάν ο υπεύθυνος επεξεργασίας θεωρεί ότι οι πληροφορίες που πρέπει να παρασχεθούν στο υποκείμενο περιέχουν δεδομένα τρίτων προστατευόμενα από το ΓΚΠΔ ή εμπορικά απόρρητα, σύμφωνα με το νόημα της Οδηγίας (ΕΕ) 2016/943, τότε ο υπεύθυνος επεξεργασίας υποχρεούται να παράσχει τις εν λόγω προστατευόμενες πληροφορίες στην αρμόδια Αρχή Προστασίας Δεδομένων ή στο δικαστήριο, το οποίο πρέπει να εξισορροπήσει τα δικαιώματα και τα συμφέροντα που τίθενται υπό εξέταση, προκειμένου να προσδιοριστεί το εύρος του δικαιώματος πρόσβασης του υποκειμένου που προβλέπεται στο Άρθρο 15 του ΓΚΠΔ.

⁶² BVwG, (2025).

⁶³ CJEU, (2025).

4.2 Big Data και κοινωνική τυποποίηση μέσω προφίλ

Η επιστημονική και τεχνολογική αρχιτεκτονική των Big Data μεταβάλλει τη σχέση μεταξύ ατόμου και πληροφορίας, οδηγώντας σε νέες μορφές επιτήρησης και κοινωνικής τυποποίησης. Η διαρκής συλλογή και ανάλυση ετερογενών δεδομένων δημιουργεί δυναμικά και προβλεπτικά μοντέλα συμπεριφοράς, τα οποία συχνά εκφεύγουν των ορίων σκοπού και αναγκαιότητας της επεξεργασίας, όπως τα γνωρίζουμε από τον GDPR.⁶⁴ Αυτό λαμβάνει ακόμα μεγαλύτερες διαστάσεις εάν αναλογισθούμε πως η συλλογή και η επεξεργασία αναφέρεται σε δεδομένα μεγάλης κλίμακας, που συχνά αποτελούν αντικείμενο αγοραπωλησιών ως «πακέτα δεδομένων», με δυσθεώρητη αγοραστική αξία.⁶⁵

Η κατασκευή προφίλ (profiling), ως μεθοδολογική πρακτική στατιστικής ερμηνείας της ταυτότητας, εμπεριέχει τον κίνδυνο κανονιστικής μεροληψίας και επαναπαραγωγής κοινωνικών ανισοτήτων. Η πρακτική αυτή μπορεί να έχει δυσμενέστερες συνέπειες για το υποκείμενο, επί παραδείγματι, όταν εφαρμόζεται για σκοπούς αξιολόγησης της πιστοληπτικής ή της ασφαλιστικής ικανότητας του υποκειμένου, συχνά ευάλωτων ατόμων.⁶⁶ Η αναγνώριση αυτών των κινδύνων προϋποθέτει όχι μόνο νομική συμμόρφωση, αλλά και μια μετα-θεσμική προσέγγιση λογοδοσίας και κοινωνικού αντικτύπου, όπως θεσμοθετείται μέσω της Μελέτης Εκτίμησης Αντικτύπου, όπου αυτή απαιτείται (DPIA).⁶⁷

Η περίπτωση της Cambridge Analytica ανέδειξε τους κινδύνους που προκύπτουν από την παράνομη χρήση δεδομένων για πολιτική στόχευση και ψυχομετρική ανάλυση, επιβεβαιώνοντας την ανάγκη αυστηρότερης εποπτείας των διαδικασιών επεξεργασίας.⁶⁸ Αντίστοιχα, εφαρμογές παρακολούθησης υγείας (health tracking apps) παρακάμπτουν

⁶⁴ Άρθρο 5 GDPR για τις αρχές επεξεργασίας δεδομένων.

⁶⁵ Tene, O. and Polonetsky, J. (2012).

⁶⁶ EDPS. (2020).

⁶⁷ Άρθρο 35 GDPR σχετικά με την αξιολόγηση αντικτύπου (DPIA).

⁶⁸ Cadwalladr, C. and Graham-Harrison, E. (2018)

συχνά τις απαιτήσεις ενημερωμένης συναίνεσης, συλλέγοντας ευαίσθητα δεδομένα χωρίς ουσιαστικό έλεγχο του χρήστη.

Στην κατεύθυνση αυτή, η απόφαση GC and Others εναντίον της Γαλλικής Αρχής Προστασίας Δεδομένων, CNIL, του Δικαστηρίου της Ευρωπαϊκής Ένωσης (εφεξής το «ΔΕΕ») ανέδειξε τη σπουδαιότητα της ιδιαίτερης προστασίας που πρέπει να παρέχεται στα δεδομένα ειδικών κατηγοριών, όπως είναι τα βιομετρικά ή τα δεδομένα υγείας, όταν χρησιμοποιούνται σε διαδικασίες profiling. Το ΔΕΕ τόνισε ότι η χρήση τέτοιων δεδομένων επιβάλλει αυστηρότερη θεσμική επαγρύπνηση και περιορισμούς, προκειμένου να διασφαλιστεί η ουσιαστική προστασία των θεμελιωδών δικαιωμάτων.⁶⁹⁷⁰⁷¹

Επιπλέον, η νομολογία του ΕΔΔΑ στην υπόθεση Satakunnan Markkinapörssi Oy και Satamedia Oy κατά Φινλανδίας (2017) αναφέρεται στην επεξεργασία δημόσιων δεδομένων και το εύρος της ιδιωτικότητας που απαιτείται ακόμα και όταν τα δεδομένα αυτά προέρχονται από δημόσιες πηγές. Η απόφαση υπενθυμίζει ότι η επεξεργασία των προσωπικών δεδομένων, ακόμα και όταν αυτά είναι δημοσίως προσβάσιμα, δεν απαλλάσσει τον υπεύθυνο επεξεργασίας από την υποχρέωση σεβασμού της ιδιωτικής ζωής των υποκειμένων.⁷²⁷³

4.3 Τεχνολογικές εφαρμογές μετρίασης του κινδύνου περιστατικού παραβίασης προσωπικών δεδομένων

4.3.1 Κρυπτογράφηση, ανωνυμοποίηση, ψευδωνυμοποίηση

Οι τεχνικές ασφάλειας δεδομένων, όπως η κρυπτογράφηση, η ανωνυμοποίηση και η ψευδωνυμοποίηση, συνιστούν μεθοδολογικά εργαλεία συμμόρφωσης, αφενός με τον GDPR και αφετέρου με τις τεχνικές προδιαγραφές κυβερνοασφάλειας. Εντάσσονται στα τεχνικά

⁶⁹ CJEU, (2019).

⁷⁰ Tufekci, 2015

⁷¹ Επί το πλείστον, βλ. Ferretti A. (2021).

⁷² ECHR, (2017).

⁷³ Mantelero, 2016

και οργανωτικά μέτρα που προβλέπει ο Κανονισμός, για τη διασφάλιση της ακεραιότητας, της Εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων (άρθρα 5 και 32 GDPR).⁷⁴ Εξάλλου, η ψευδωνυμοποίηση ενισχύει τη δυνατότητα χρήσης δεδομένων για σκοπούς ανάλυσης, έρευνας ή ανάπτυξης τεχνολογιών (όπως η Τεχνητή Νοημοσύνη), χωρίς να εκτίθενται άμεσα τα προσωπικά στοιχεία των υποκειμένων, εξισορροπώντας τη χρήση και την προστασία των δεδομένων, συνεπακόλουθα και την ασφάλειά τους.⁷⁵

Σύμφωνα με τις κατευθυντήριες οδηγίες του ENISA (2020), η ψευδωνυμοποίηση ενισχύει την προστασία προσωπικών δεδομένων χωρίς να αφαιρεί την ιδιότητά τους ως προσωπικά. Αποτελεί, επομένως, εργαλείο που μειώνει την έκθεση των δεδομένων σε απειλές, διατηρώντας παράλληλα τη λειτουργική τους αξία για έρευνα και ανάλυση.⁷⁶ Ωστόσο, σε ορισμένες περιπτώσεις, ιδίως σε περιβάλλοντα ποινικής έρευνας ή εθνικής ασφάλειας, η ισχυρή κρυπτογράφηση μπορεί να λειτουργήσει ως εμπόδιο στις δημόσιες αρχές, θέτοντας κρίσιμα διλήμματα μεταξύ απορρήτου και ασφάλειας.⁷⁷

4.3.2 Το αντίκρισμα στην ευρωπαϊκή νομολογία

Ωστόσο, η ατελής εφαρμογή των τεχνικών που εκτέθηκαν αμέσως ανωτέρω εγείρει κινδύνους επαναπροσδιορισμού ταυτότητας (re-identification), γεγονός που ανέδειξε και η απόφαση Breyer εναντίον Γερμανίας, του 2016, του ΔΕΕ. Στην απόφαση αυτή το Δικαστήριο διευκρίνισε ότι ο όρος «ταυτοποίηση» πρέπει να ερμηνεύεται σε ευρύ φάσμα, συμπεριλαμβάνοντας καταστάσεις όπου υπάρχει μερική ταυτοποίηση με δυνατότητα σύνδεσης των δεδομένων με το υποκείμενο, ακόμα και αν δεν είναι πλήρης.⁷⁸

⁷⁴ Τεχνικές κρυπτογράφησης, ανωνυμοποίησης και ψευδωνυμοποίησης, βλ. σχετικές κατευθυντήριες οδηγίες EDPB 1 2022.

⁷⁵ ENISA (2019).

⁷⁶ ENISA (2020), σ. 17–24.

⁷⁷ Abelson, H. et al. (2015)

⁷⁸ CJEU, (2016).

Η νομολογία του ΔΕΕ, μέσα από υποθέσεις όπως η *Breyer*, υπογραμμίζει την αναγκαιότητα της συνεπούς αξιολόγησης του τεχνολογικού και κοινωνικού πλαισίου, όπως και του δυναμικού κινδύνου που προκύπτει από τη χρήση νέων τεχνολογιών στην επεξεργασία δεδομένων, κάτι που συνάδει με την κριτική θεώρηση της υπόθεσης *Breyer* ως πρότυπο μετριασμού κινδύνου στην τεχνολογική συμμόρφωση.

Επιπροσθέτως, το ΔΕΕ με την απόφαση *Schrems II* (C-311/18) επιβεβαίωσε τη σημασία της προστασίας των δεδομένων από την παρακολούθηση τρίτων χωρών κατά τη μεταφορά τους εκτός της ΕΕ, ενισχύοντας το δικαίωμα στην ιδιωτική ζωή και θέτοντας απαραβίαστα όρια στη διασυνοριακή ροή δεδομένων. Το Δικαστήριο αναγνώρισε ότι η προστασία πρέπει να είναι ουσιαστική και όχι απλώς τυπική, κάτι που θα διασφαλίσει την ποιότητα της επεξεργασίας των δεδομένων στο περιβάλλον της ΤΝ και των Big Data.⁷⁹

4.3.3 Καινοτομες προσεγγίσεις στην ασφάλεια δεδομένων

i. Η Τεχνολογία Blockchain ως Ασπίδα Δεδομένων

Το Blockchain, ως αποκεντρωμένη και κρυπτογραφημένη τεχνολογία, παρέχει ένα ασφαλές και αξιόπιστο περιβάλλον αποθήκευσης και διαμοιρασμού πληροφοριών. Ο κατακευκτός χαρακτήρας του περιορίζει την εξάρτηση από κεντρικούς διαχειριστές και ενισχύει την προστασία της ακεραιότητας των δεδομένων.⁸⁰ Μέσω του μοντέλου *self-sovereign identity*, οι χρήστες αποκτούν πλήρη έλεγχο πάνω στην ψηφιακή τους ταυτότητα, επιλέγοντας πότε, πού και σε ποιον κοινοποιούνται τα προσωπικά τους δεδομένα. Η τεχνολογία αυτή μειώνει δραστικά τον κίνδυνο διαρροών και κακόβουλων προσβάσεων.⁸¹

⁷⁹ CJEU, Case C 311/18 – *Schrems II* (2020).

⁸⁰ *CyberNews*, (2024).

⁸¹ Το *Self-Sovereign Identity (SSI)* (Αυτοκυρίαρχη Ταυτότητα) είναι ένα σύστημα διαχείρισης ταυτότητας που δίνει στους χρήστες τον έλεγχο και την ιδιοκτησία της ψηφιακής τους ταυτότητας, χωρίς να εξαρτώνται από τρίτους. Αντί για κεντρικά συστήματα ταυτοποίησης (όπως το *Google Sign-In* ή το *Facebook Connect*), ο χρήστης ελέγχει τα δεδομένα του και αποφασίζει ποιος μπορεί να τα δει και πώς.

Η χρήση του blockchain δημιουργεί ενδιαφέροντες προβληματισμούς σε σχέση με τον GDPR, λόγω της αμεταβλητότητας των δεδομένων και της δυσκολίας εφαρμογής του «δικαιώματος στη λήθη». Ωστόσο, αναπτύσσονται λύσεις όπως το off-chain storage και η χρήση κρυπτογραφημένων hash για την ευθυγράμμιση με τις απαιτήσεις του κανονισμού.⁸²

ii. Η μηδενική εμπιστοσύνη αλλάζει τα δεδομένα στην ασφάλεια των δεδομένων

Παράλληλα με την τεχνολογική καινοτομία, αλλάζει και η φιλοσοφία διαχείρισης της ασφάλειας, όπως δείχνει η αρχιτεκτονική Zero Trust, η οποία βασίζεται στην αρχή «ποτέ εμπιστοσύνη, πάντα επαλήθευση». Αμφισβητείται η παραδοσιακή διάκριση μεταξύ «έμπιστων» και «μη έμπιστων» χρηστών, με κάθε προσπάθεια πρόσβασης να απαιτεί πιστοποίηση και έλεγχο.⁸³ Η πολιτική των ελάχιστων προνομίων (least privilege) περιορίζει την πρόσβαση μόνο στα απολύτως απαραίτητα δεδομένα, από τους απολύτως εξουσιοδοτημένους ρόλους χρηστών. Σε συνδυασμό με πολυπαραγοντικό έλεγχο ταυτότητας (MFA), αυξάνει την ανθεκτικότητα των οργανισμών απέναντι σε παραβιάσεις, τόσο εξωτερικές όσο και εσωτερικές.

iii. Υλοποιήσεις στον Δημόσιο και Ιδιωτικό Τομέα

Η λογική του Zero Trust υιοθετείται ήδη σε ευρεία κλίμακα, ιδιαίτερα από κυβερνητικούς οργανισμούς και πολυεθνικές επιχειρήσεις. Οι οργανισμοί αυτοί επιδιώκουν την προστασία κρίσιμων πληροφοριών και την πρόληψη περιστατικών διαρροής δεδομένων.⁸⁴ Η πανδημία και η στροφή προς την τηλεργασία ενίσχυσαν τη σημασία του Zero Trust. Οι οργανισμοί χρειάζονται πλέον συστήματα που εξασφαλίζουν ασφαλή πρόσβαση ανεξαρτήτως τοποθεσίας, συσκευής ή δικτύου, καθιστώντας το Zero Trust απαραίτητο εργαλείο για την ασφάλεια υβριδικών υποδομών.⁸⁵ Η υιοθέτηση του μοντέλου Zero Trust δεν είναι απλή. Περιλαμβάνει προκλήσεις όπως η ανάγκη για εκτεταμένη χαρτογράφηση των πηγών των

⁸² CyberNews, (2024).

⁸³ MDPI, (2023).

⁸⁴ United Security, (2024).

⁸⁵ MDPI, (2023).

δεδομένων, η διαχείριση των ψηφιακών ταυτοτήτων των υποκειμένων και η συνεχής επιτήρηση του επιπέδου κυβερνοασφάλειας των υποδομών τους. Επιπλέον, απαιτεί ριζικές αλλαγές στους οργανισμούς και συνεχή εκπαίδευση των χρηστών.

4.4 Η ενσωμάτωση της "Privacy by design " στην TN

Η ενσωμάτωση των αρχών *privacy by design* και *privacy by default* στον κύκλο ζωής των συστημάτων TN δεν αποτελεί απλώς νομική υποχρέωση βάσει του άρθρου 25 του GDPR, αλλά προϋποθέτει **μεθοδολογική και οντολογική μεταρρύθμιση** στον τρόπο που σχεδιάζονται, αναπτύσσονται και εφαρμόζονται οι τεχνολογίες. Σε αυτό το πλαίσιο, η αρχή της προληπτικής ρυθμιστικής ενσωμάτωσης (*preventive regulatory embedding*) αναδύεται ως εννοιολογικό εργαλείο, με στόχο τη σύζευξη τεχνολογικού σχεδιασμού με θεμελιώδεις δικαιοτικές και ηθικές αξίες.⁸⁶

Η *privacy by design* επιβάλλει την ενσωμάτωση της προστασίας δεδομένων ήδη από τα πρώτα στάδια της τεχνολογικής αρχιτεκτονικής (*by design*), αλλά και την αυτόματη ενεργοποίηση ρυθμίσεων που ευνοούν την ιδιωτικότητα, χωρίς την ανάγκη παρέμβασης του χρήστη (*by default*). Στο πεδίο της Τεχνητής Νοημοσύνης, οι απαιτήσεις αυτές καθίστανται κρίσιμες, καθώς τα αλγοριθμικά μοντέλα συχνά προϋποθέτουν **μαζική συλλογή, συσχέτιση και προτυποποίηση ευαίσθητων δεδομένων**, με εγγενείς κινδύνους για την ιδιωτικότητα, την αδιαφάνεια και την άνιση μεταχείριση.

Η ενσωμάτωση της *privacy by design* στην TN δεν είναι τεχνικά ουδέτερη, αλλά προϋποθέτει τη συγκρότηση ενός **διατομεακού οικοσυστήματος συνεργασίας** μεταξύ μηχανικών, νομικών, ηθικών επιστημόνων και υπεύθυνων χάραξης πολιτικής. Η ανάπτυξη ενός **κοινού γνωσιακού λεξιλογίου** (*shared epistemic vocabulary*) μεταξύ των επιστημονικών και ρυθμιστικών κοινοτήτων καθίσταται αναγκαία για τη θεμελίωση ενιαίων κριτηρίων λογοδοσίας, επεξηγησιμότητας και διαφάνειας, όπως απαιτείται από την **AI Act**.⁸⁷

⁸⁶ Cavoukian, (2009). · Wachter & Mittelstadt, (2019).

⁸⁷ Veale & Borgesius, (2021).

Η εφαρμογή της αρχής *privacy by design* αποκτά ιδιαίτερη σημασία όταν οι τεχνολογίες ΤΝ αναπτύσσονται σε περιβάλλοντα υψηλού κινδύνου – όπως στο πεδίο της υγείας, της δικαιοσύνης ή της απασχόλησης – όπου τα συστήματα αποφάσεων επηρεάζουν άμεσα δικαιώματα και ευκαιρίες των υποκειμένων. Σε αυτά τα περιβάλλοντα, η διασφάλιση θεσμικών ελέγχων, μηχανισμών εσωτερικής τεκμηρίωσης και *DPIAs* καθίσταται θεμελιώδης προϋπόθεση για τη νομιμοποίηση των εφαρμογών ΤΝ.⁸⁸

Παράλληλα, το νέο ευρωπαϊκό θεσμικό πλαίσιο προτείνει μοντέλα όπως η *co-regulation* και τα *regulatory sandboxes*, εντός των οποίων τα καινοτόμα τεχνολογικά μοντέλα μπορούν να δοκιμάζονται υπό προϋποθέσεις, με έμφαση στη συμμόρφωση με τις αρχές προστασίας δεδομένων και τις απαιτήσεις κοινωνικής αποδοχής.⁸⁹

Η ενσωμάτωση της *privacy by design* στην ΤΝ σηματοδοτεί, εν τέλει, μια **μετάβαση από αμυντικές προς προληπτικές στρατηγικές** προστασίας της ιδιωτικότητας. Απαιτεί τη μετατροπή της προστασίας δεδομένων από παθητικό φραγμό σε ενεργό στοιχείο του τεχνολογικού σχεδιασμού – δηλαδή σε *ενσωματωμένη δημοκρατική αρχή (embedded democratic value)*, η οποία εξασφαλίζει ότι η ΤΝ εξυπηρετεί όχι μόνο την καινοτομία, αλλά και την ανθρώπινη αξιοπρέπεια.

Ειδική βιβλιογραφία κεφαλαίου 4

- Abelson, H. et al. (2015), 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications', MIT CSAIL Report. Διαθέσιμο εδώ: <https://www.usenix.org/conference/enigma2016/conference-program/presentation/rivest>

⁸⁸ EDPB, (2021).

⁸⁹ OECD, (2021)· European Commission, (2020).

- Burrell, J. (2016) 'How the machine "thinks": Understanding opacity in machine learning algorithms', *Big Data & Society*, 3(1). Διαθέσιμο εδώ: <https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512>
- Cadwalladr, C. and Graham-Harrison, E. (2018), 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica', *The Guardian*, 17 March. Διαθέσιμο εδώ: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- Cavoukian, A. (2009) *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario. Διαθέσιμο εδώ: <https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>
- CSC.gr (2023). 9 παραδείγματα εφαρμογών του Blockchain. Διαθέσιμο εδώ: <https://csc.gr/9-paradeigmata-efarmogon-tou-blockchain/>
- CyberNews (2024). Blockchain και κυβερνοασφάλεια. Διαθέσιμο εδώ: <https://cybernews.gr/blockchain/blockchain-kai-kyvernoasfaleia/>
- EDPB, (2022). Adopted - Guidelines 01/2022 on data subject rights - Right of access. Διαθέσιμες εδώ: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf
- EDPB, (2021). Guidelines 01/2021 on Examples regarding Data Breach Notification. Διαθέσιμες εδώ: https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_data_breach_notification_examples_v1_en.pdf
- EDPS. (2020). Opinion 4/2020 on the European strategy for data. Διαθέσιμη εδώ: <https://edps.europa.eu>
- ENISA (2019). Pseudonymisation techniques and best practices. Διαθέσιμο στο: <https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices>

- ENISA (2020), Guidelines on shaping technology according to GDPR provisions. Διαθέσιμο εδώ: <https://www.enisa.europa.eu/sites/default/files/publications/WP2018%20O.2.2.5%20-%20Recomendations%20on%20shaping%20technology%20according%20to%20GDPR%20provisions%20-%20Part%201.pdf>
- ESET (2025). Κυβερνοασφάλεια και Τεχνητή Νοημοσύνη: Τι επιφυλάσσει το 2025. Διαθέσιμο εδώ: <https://www.eset.com/gr/about/newsroom/press-releases-gr-1/kybernoasfaleia-kai-techniti-noimosyni-ti-epifylassei-to-2025/>
- ERT News (2025). Κυβερνοασφάλεια και Τεχνητή Νοημοσύνη. Διαθέσιμο στο: <https://www.ertnews.gr/eidiseis/epistimi/technologia/kyvernoasfaleia-kai-texniti-noimosyni-ti-epifylassei-to-2025/>
- EU AI Act, (2024). Κανονισμός (ΕΕ) 2024/1689. Διαθέσιμος εδώ: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401689
- European Commission (2020). White Paper on Artificial Intelligence: A European Approach to Excellence and Trust. Διαθέσιμο εδώ: https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf
- Ferretti, A. (2021) «Ethics and Governance of Big Data in Health Research and Digital Health Applications». Διαθέσιμο εδώ: file:///C:/Users/a.fafaliou/Downloads/27589_FERRETTIAGATA_2021.pdf
- Gürses, S., Troncoso, C. and Diaz, C. (2011) 'Engineering privacy by design', Computers, Privacy and Data Protection: An Element of Choice.
- Homo Digitalis (2023). Τεχνητή Νοημοσύνη και Κυβερνοασφάλεια: Πραγματικότητα και Υπερβολές. Διαθέσιμο στο: <https://homodigitalis.gr/posts/3752/>

- Mantelero, A. (2016) 'Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection', *Computer Law & Security Review*, 32(2), pp.238–255.
- MDPI (2023). *Artificial Intelligence and Cybersecurity*. Διαθέσιμο εδώ: <https://www.mdpi.com/2079-9292/14/3/581>
- OECD (2021). *Recommendation on Enhancing Access to and Sharing of Data*. Διαθέσιμο εδώ: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463>
- Selbst, A.D. and Barocas, S. (2018) 'The intuitive appeal of explainable machines', *Fordham Law Review*, 87(3). Διαθέσιμο εδώ: <https://par.nsf.gov/servlets/purl/10121294>
- Tene, O. and Polonetsky, J. (2012). *Big Data for All: Privacy and User Control in the Age of Analytics*. *Northwestern Journal of Technology and Intellectual Property*, 11(5), 239–273. Διαθέσιμο εδώ: <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip>
- Tufekci, Z. (2015) 'Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency', *Colorado Technology Law Journal*, 13(203).
- United Security (2024). *Cyber Security with Artificial Intelligence*. Διαθέσιμο εδώ: <https://unitedsecurity.gr/en/cyber-security-ai-vs-humans-en/>
- Veale, M. and Binns, R. (2017). *Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data*. *Big Data & Society*, 4(2), 1–17. Διαθέσιμο εδώ: [εδώ](#).
- Veale, M. & Zuiderveen Borgesius, F. (2021). *Demystifying the Draft EU Artificial Intelligence Act*. *Computer Law Review International*, 22(4). Διαθέσιμο εδώ: <https://www.degruyterbrill.com/document/doi/10.9785/cri-2021-220402/html>

- Wachter, S., Mittelstadt, B. and Floridi, L. (2017) 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation', *International Data Privacy Law*, 7(2), pp.76–99.
- Wachter, S. & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, (2), 494–620. Διαθεσιμο εδώ: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/colb2019&div=15&id=&page=>

Νομολογία

- BVerfG, (2008). Judgment of 27 February 2008, Volkszählungsurteil II. Διαθέσιμη εδώ: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html
- BVwG, (2025). *Entscheidung W108 2274731-1/11E – Noyb v. Clearview AI*. Ολόκληρη η απόφαση διαθέσιμη εδώ: [https://gdprhub.eu/images/8/80/20250131114705867_redacted_\(4\).pdf](https://gdprhub.eu/images/8/80/20250131114705867_redacted_(4).pdf) Η περίληψη της απόφασης στα Αγγλικά διαθέσιμη εδώ: https://gdprhub.eu/index.php?title=BVwG_-_W108_2274731-1/11E
- CJEU, (2020). Case C-311/18. *Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems (Schrems II)*. Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311>
- CJEU, (2016). Case C 582/14 – *Breyer v Germany* (2016): για την έννοια της ταυτοποίησης φυσικών προσώπων. Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0582>

- CJEU, (2019). Case C-136/17 – GC and Others v Commission nationale de l'informatique et des libertés (CNIL): για τη χρήση ευαίσθητων δεδομένων. Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0136>
- CJEU, (2025). -Case C-203/22 - Dun and Bradstreet Austria. Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0203>
- ECHR, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland (2017): για την επεξεργασία δημοσίων δεδομένων. Διαθέσιμη εδώ: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-175121%22%5D%7D>

ΚΕΦΑΛΑΙΟ 5 - ΜΕΛΕΤΕΣ ΠΕΡΙΠΤΩΣΗΣ ΚΑΙ ΕΦΑΡΜΟΓΕΣ

5.1 Ορισμός και Διαχείριση Περιστατικών Παραβίασης Προσωπικών Δεδομένων

Σύμφωνα με τον **GDPR**,⁹⁰ ως περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα (*personal data breach*) ορίζεται: «η παραβίαση της ασφάλειας που οδηγεί τυχαία ή παράνομα σε καταστροφή, απώλεια, μεταβολή, μη εξουσιοδοτημένη γνωστοποίηση ή πρόσβαση σε δεδομένα προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία». Ο ορισμός αυτός καλύπτει τόσο περιστατικά που προκύπτουν από **κακόβουλες ενέργειες** (όπως κυβερνοεπιθέσεις, ransomware, υποκλοπές) όσο και από **ανθρώπινα λάθη** ή **τεχνικές αστοχίες** (όπως αποστολή email σε λάθος παραλήπτη ή απώλεια συσκευής με αποθηκευμένα δεδομένα).

⁹⁰ GDPR, άρθρο 4 (12).

Ο EDPB, μέσω των Κατευθυντήριων Γραμμών 01/2021 σχετικά με τις γνωστοποιήσεις περιστατικών παραβίασης,⁹¹ διευκρινίζει ότι ένα περιστατικό παραβίασης μπορεί να αναφέρεται σε πλήγμα στην **εμπιστευτικότητα**, ήτοι στη μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση (π.χ. hacking), στην **ακεραιότητα**, ήτοι στην μη εξουσιοδοτημένη ή ακούσια τροποποίηση (π.χ. κακόβουλη επεξεργασία), ή και στη **διαθεσιμότητα**, στην απώλεια, δηλαδή, πρόσβασης ή στην καταστροφή δεδομένων (π.χ. ransomware, φυσικές καταστροφές κ.α.).

Ο GDPR προβλέπει ένα **σαφές κανονιστικό πλαίσιο για την αντιμετώπιση** περιστατικών παραβίασης. Αυτό συνίσταται στα εξής:

Εσωτερική Τεκμηρίωση: Όλοι οι υπεύθυνοι επεξεργασίας υποχρεούνται να τηρούν **μητρώο παραβιάσεων**, ανεξαρτήτως του αν η παραβίαση κοινοποιείται στην εποπτική αρχή (Άρθρο 33(5) GDPR).

Ειδοποίηση της Εποπτικής Αρχής: Ο υπεύθυνος επεξεργασίας πρέπει να κοινοποιήσει το περιστατικό στην αρμόδια **Αρχή Προστασίας Δεδομένων εντός 72 ωρών** από τη στιγμή που το αντιλαμβάνεται, εφόσον είναι πιθανόν να προκύψει κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (Άρθρο 33(1) GDPR).

Ενημέρωση των Υποκειμένων των Δεδομένων: Όταν η παραβίαση ενδέχεται να προκαλέσει **υψηλό κίνδυνο** για τα δικαιώματα και τις ελευθερίες των υποκειμένων (όπως απώλεια οικονομικών πόρων ή διαρροή ευαίσθητων στοιχείων), τότε πρέπει να υπάρξει **άμεση και σαφής ενημέρωση των υποκειμένων** (Άρθρο 34 GDPR). Σύμφωνα με τον EU GDPR Handbook της Ευρωπαϊκής Επιτροπής (2018), η υποχρέωση γνωστοποίησης παραβίασης εντός 72 ωρών αποτελεί κρίσιμο εργαλείο έγκαιρης ανταπόκρισης, διαφάνειας και περιορισμού του κινδύνου για τα υποκείμενα των δεδομένων. Το εγχειρίδιο παρέχει επίσης λεπτομερείς οδηγίες για την αξιολόγηση του κινδύνου και τη διαδικασία

⁹¹ EDPB, (2021).

κοινοποίησης, με στόχο τη δημιουργία κοινής ευρωπαϊκής προσέγγισης στην εφαρμογή των άρθρων 33 και 34 του GDPR.

Μέτρα Μετριασμού και Πρόληψης: Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία οφείλουν να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για την αποτροπή μελλοντικών περιστατικών, σύμφωνα με τις αρχές **λογοδοσίας (accountability)** και **ασφάλειας εξ αρχής (security by design)** (Άρθρα 25 και 32 GDPR).

Σημαντικό εργαλείο πρόληψης αποτελεί η **διενέργεια Εκτίμησης Αντικτύπου στην Προστασία Δεδομένων (DPIA)** σε επεξεργασίες υψηλού κινδύνου.⁹²

5.2 Περιπτωσιολογία περιστατικών παραβίασης

Η συχνότητα και η ένταση περιστατικών παραβίασης δεδομένων έχει αυξηθεί αισθητά την τελευταία δεκαετία, αναδεικνύοντας την αδυναμία πολλών κρατικών (ή και μη) φορέων να προσαρμοστούν αποτελεσματικά στις σύγχρονες απειλές του κυβερνοχώρου.⁹³ Ιστότοποι ειδήσεων, πανεπιστημίων, νοσοκομείων, Υπουργείων, ακόμα και ολόκληρων κυβερνήσεων έχουν πέσει θύματα επιθέσεων, με χαρακτήρα άρνησης απόκρισης, συχνά με λυτρισμικό χαρακτήρα, καθώς το ύψος της υπεραξίας είναι τεράστιο.

5.2.1 Διεθνή περιστατικά παραβίασης

Κυβερνοεπίθεση στο Βουλγαρικό Υπουργείο Εσωτερικών (2019)

Ένα εμβληματικό παράδειγμα είναι η Κυβερνοεπίθεση που έπληξε το Υπουργείο Εσωτερικών της Βουλγαρίας το 2019, κατά την οποία εκλάπησαν τα προσωπικά δεδομένα περισσότερων από 5 εκατομμύρια πολιτών. Το περιστατικό αυτό αποκάλυψε σοβαρές ελλείψεις στα τεχνικά και οργανωτικά μέτρα ασφαλείας, καθώς και στην εφαρμογή των διατάξεων του GDPR και της Οδηγίας NIS.⁹⁴ Η απάντηση των βουλγαρικών αρχών

⁹² EDPB, (2021).

⁹³ EDPB, (2021).

⁹⁴ New York Times, (2019).

περιελάμβανε την επιβολή χρηματικών κυρώσεων και την αναθεώρηση της εθνικής στρατηγικής κυβερνοασφάλειας. Παράλληλα, η Εποπτική Αρχή της χώρας αναβάθμισε τον μηχανισμό ελέγχου και παρακολούθησης συμμόρφωσης των δημόσιων φορέων.⁹⁵

AT&T – Διαρροή Δεδομένων 86 Εκατομμυρίων Χρηστών (2025)

Τον Μάιο του 2025, η AT&T βρέθηκε αντιμέτωπη με μία από τις μεγαλύτερες διαρροές δεδομένων στην ιστορία της, καθώς διέρρευσαν προσωπικές πληροφορίες περίπου 86 εκατομμυρίων χρηστών, μεταξύ των οποίων αριθμοί κοινωνικής ασφάλισης (SSN), ημερομηνίες γέννησης και διευθύνσεις. Τα δεδομένα αυτά αναρτήθηκαν σε δημοφιλή φόρουμ του dark web, δημιουργώντας έντονες ανησυχίες για κλοπές ταυτότητας. Η εταιρεία επιβεβαίωσε την παραβίαση και προσέφερε δωρεάν υπηρεσίες παρακολούθησης ταυτότητας στους πληγέντες, ενώ παράλληλα συνεργάστηκε με τις αρμόδιες αρχές για τη διερεύνηση του περιστατικού.⁹⁶

Headero – Παραβίαση σε Εφαρμογή Γνωριμιών (2025)

Η εφαρμογή γνωριμιών Headero υπέστη σοβαρή παραβίαση ασφαλείας τον Μάιο του 2025, όταν αποκαλύφθηκε ότι ευαίσθητα δεδομένα περίπου 350.000 χρηστών, συμπεριλαμβανομένων προσωπικών μηνυμάτων, διευθύνσεων email και τοποθεσιών GPS, ήταν προσβάσιμα λόγω εσφαλμένης ρύθμισης βάσης δεδομένων. Αν και η εταιρεία ανέφερε ότι δεν διαπιστώθηκε μαζική κατάχρηση των δεδομένων, η διαρροή ανέδειξε την ανάγκη για ισχυρότερες πρακτικές ασφαλείας στις εφαρμογές κοινωνικής διασύνδεσης. Η Headero προέβη άμεσα σε διορθωτικά μέτρα και ενημέρωσε τις εποπτικές αρχές προστασίας δεδομένων.⁹⁷

Cyberattacks σε Αλυσίδες Λιανικής – Marks & Spencer, Co-op & Whole Foods (2025)

Κατά το πρώτο εξάμηνο του 2025, γνωστές αλυσίδες λιανικής του Ηνωμένου Βασιλείου και των ΗΠΑ, όπως οι Marks & Spencer, Co-op και Whole Foods, βρέθηκαν στο στόχαστρο

⁹⁵ ENISA, (2021).

⁹⁶ hackread.com, (2025).

⁹⁷ Dailysecurityreview.com, (2025).

οργανωμένων κυβερνοεπιθέσεων που προκάλεσαν σημαντικές διαταραχές στις αλυσίδες εφοδιασμού τους. Οι επιθέσεις είχαν ως αποτέλεσμα την προσωρινή αναστολή παραδόσεων και την ανάρτηση προειδοποιητικών σημειωμάτων σε άδεια ράφια καταστημάτων. Οι εταιρείες συνεργάστηκαν με ειδικούς κυβερνοασφάλειας, αναβαθμίζοντας τα συστήματά τους και εισάγοντας πολιτικές Zero Trust για την προστασία από μελλοντικά περιστατικά.⁹⁸

Washington Post – Στοχευμένη Επίθεση σε Email Δημοσιογράφων (2025)

Τον Ιούνιο του 2025, η εφημερίδα *Washington Post* επιβεβαίωσε ότι δημοσιογράφοι της που καλύπτουν την Κίνα υπέστησαν στοχευμένη κυβερνοεπίθεση, με αποτέλεσμα την παραβίαση των email τους. Οι επιθέσεις αποδόθηκαν σε κρατικά υποκινούμενους δράστες και θεωρήθηκαν μέρος ευρύτερης εκστρατείας επιτήρησης του Τύπου. Η εφημερίδα προέβη σε υποχρεωτική αλλαγή όλων των σχετικών κωδικών πρόσβασης, ενώ η διεύθυνση ενίσχυσε τα πρωτόκολλα ασφαλείας για τις διεθνείς ανταποκρίσεις της.⁹⁹

“Mother of All Breaches” – 26 Δισεκατομμύρια Εγγραφές (2024)

Στις αρχές του 2024, διεθνή μέσα και ερευνητές κυβερνοασφάλειας ανέφεραν μία γιγαντιαία συγκεντρωτική παραβίαση δεδομένων, γνωστή ως “Mother of All Breaches” (MOAB), που περιελάμβανε πάνω από 26 δισεκατομμύρια εγγραφές από πλατφόρμες όπως Twitter, Canva, Dropbox, LinkedIn, και άλλες. Η συλλογή των δεδομένων προήλθε από συνδυασμό προηγούμενων διαρροών και πιθανόν νέων παραβιάσεων. Το γεγονός αυτό αποκάλυψε την αδυναμία επαρκούς ανωνυμοποίησης δεδομένων και τόνισε την ανάγκη για διαλειτουργικά πρότυπα ασφαλείας. Η ανάλυση συνεχίζεται από διεθνείς οργανισμούς.¹⁰⁰

National Public Data (NPD) – Κατάρρευση μετά από Παραβίαση (2024)

Η εταιρεία Jerico Pictures, διαχειρίστρια της βάσης δεδομένων *National Public Data* (NPD), υπέστη συντριπτική κυβερνοεπίθεση που οδήγησε σε έκθεση περίπου 2,9 δισεκατομμυρίων εγγραφών πολιτών από τις ΗΠΑ, τον Καναδά και το Ηνωμένο Βασίλειο. Η διαρροή, που

⁹⁸ [Apnews.com](#), (2025). & [theguardian.com](#), (2025).

⁹⁹ [Reuters.com](#),(2025).

¹⁰⁰ [Cybernews.com](#) (2024)

περιελάμβανε στοιχεία ταυτότητας, οικονομικά δεδομένα και ποινικά μητρώα, είχε ως συνέπεια τη διακοπή λειτουργίας της εταιρείας και την έναρξη ποινικών ερευνών. Το περιστατικό αποτέλεσε αντικείμενο διεθνούς συζήτησης περί ευθύνης ιδιωτικών data brokers.¹⁰¹

Change Healthcare / UnitedHealth – Εκτεταμένο Ransomware (2025)

Τον Φεβρουάριο του 2025, η θυγατρική της UnitedHealth, *Change Healthcare*, υπέστη σοβαρή ransomware επίθεση από την ομάδα BlackCat/ALPHV, με εκτιμώμενο αντίκτυπο σε πάνω από 100 εκατομμύρια ιατρικά αρχεία. Η εταιρεία αναγκάστηκε να διακόψει τη λειτουργία συστημάτων τιμολόγησης και φαρμακευτικής χορήγησης, με αποτέλεσμα καθυστερήσεις στην περίθαλψη και τεράστιο οικονομικό κόστος, που εκτιμάται άνω των 2,4 δισ. δολαρίων. Η αποκατάσταση περιελάμβανε πληρωμές λύτρων, ενεργοποίηση ασφαλιστικών ρητρών και εμπλοκή της κυβέρνησης των ΗΠΑ.¹⁰²

Internet Archive – Διαρροή Χρηστών (2024)

Το *Internet Archive*, πλατφόρμα που φιλοξενεί τη “Wayback Machine”, ανακοίνωσε ότι υπήρξε διαρροή προσωπικών δεδομένων 31 εκατομμυρίων χρηστών, εξαιτίας κακόβουλου JavaScript και επίθεσης DDoS. Η διαρροή αφορούσε email και hashed passwords. Οι υπεύθυνοι της πλατφόρμας απέκλεισαν την κακόβουλη δραστηριότητα και ενημέρωσαν τους χρήστες να αλλάξουν τα διαπιστευτήριά τους, ενώ ενίσχυσαν τα συστήματα ασφαλείας και επιβεβαίωσαν ότι δεν υπήρξε πρόσβαση σε περιεχόμενο χρηστών.¹⁰³

Sepah Bank – Ισάβ (2025)

Τον Μάρτιο του 2025, ο κρατικός ιρανικός τραπεζικός οργανισμός *Sepah Bank* φέρεται να υπέστη κυβερνοεπίθεση που είχε ως αποτέλεσμα τη διαρροή δεδομένων περίπου 42 εκατομμυρίων πελατών, μεταξύ των οποίων στρατιωτικοί και κρατικοί λειτουργοί. Οι επιτιθέμενοι διέρρευσαν τα δεδομένα σε φόρουμ του dark web, απειλώντας με επιπλέον

¹⁰¹ Ibm.com, (2024).

¹⁰² Aha.org, (2025).

¹⁰³ BleepingComputer, (2024).

διαρροές εκτός αν καταβληθούν λύτρα. Η ιρανική κυβέρνηση αρνήθηκε την ευθύνη παραβίασης και υποστήριξε ότι η βάση δεδομένων ήταν ψευδής, ενώ παράλληλα διενεργήθηκαν έρευνες από ανεξάρτητους φορείς.¹⁰⁴

5.2.2 Περιστατικά παραβίασης στην Ελλάδα

Επίθεση DDoS στο Δημόσιο Δίκτυο «Σύζευξις» (Ιανουάριος 2025)

Τον Ιανουάριο του 2025, καταγράφηκε εκτεταμένη επίθεση άρνησης υπηρεσίας (DDoS) στο δημόσιο τηλεπικοινωνιακό δίκτυο «Σύζευξις», το οποίο συνδέει κρίσιμες δημόσιες υπηρεσίες, συμπεριλαμβανομένων φορέων ταυτοποίησης και αυθεντικοποίησης. Η επίθεση προερχόταν από κατανεμημένα botnets που χρησιμοποιούσαν IP από ευρωπαϊκές και τρίτες χώρες, περιλαμβανομένης και της Ρωσίας. Στόχος αποτέλεσε η υπερφόρτωση του δικτύου με μαζική κακόβουλη κυκλοφορία. Η Εθνική Αρχή Κυβερνοασφάλειας και το CERT του Υπουργείου Ψηφιακής Διακυβέρνησης ενεργοποίησαν άμεσα πρωτόκολλα αντίδρασης σε συνεργασία με τον ΟΤΕ, περιλαμβάνοντας φιλτράρισμα της κυκλοφορίας, αναβάθμιση της ανθεκτικότητας των υπηρεσιών και ενεργή παρακολούθηση για αποφυγή παραβίασης εμπιστευτικών δεδομένων. Το περιστατικό δεν φαίνεται να προκάλεσε απώλεια δεδομένων, ωστόσο αναδείχθηκε η ανάγκη ενίσχυσης των δυνατοτήτων αποτροπής δικτυακών επιθέσεων σε επίπεδο εθνικής υποδομής.¹⁰⁵

Περιστατικό Παραβίασης στην Υπηρεσία Κτηματολογίου (Ιούλιος 2024)

Το καλοκαίρι του 2024, το Ελληνικό Κτηματολόγιο αποτέλεσε στόχο σειράς συντονισμένων ψηφιακών επιθέσεων, με περισσότερες από 400 απόπειρες μέσα σε μία εβδομάδα. Από τις επιθέσεις αυτές εκλάπησαν περίπου 1,2 GB δεδομένων, κυρίως εσωτερικά λειτουργικά αρχεία και όχι προσωπικά στοιχεία πολιτών. Η διαχείριση του περιστατικού περιελάμβανε την άμεση απενεργοποίηση των ενεργών VPN συνδέσεων, την επαναρύθμιση όλων των διαπιστευτηρίων πρόσβασης, την επιβολή πολυπαραγοντικού ελέγχου ταυτότητας (2FA), και την ενίσχυση των μεθόδων διαδικτυακής θωράκισης. Το Κτηματολόγιο διαβεβαίωσε πως

¹⁰⁴Iranwire, (2025).

¹⁰⁵ Protothema.gr, 2(2025).

δεν επηρεάστηκε η επιχειρησιακή του λειτουργία, ενώ η Αρχή Προστασίας Δεδομένων και το Εθνικό Κέντρο Κυβερνοασφάλειας ενημερώθηκαν επισήμως.¹⁰⁶

Υποκλοπές μέσω Predator – Εθνική Κρίση Ιδιωτικότητας (2022–2024)

Το καλοκαίρι του 2022, μια σειρά καταγγελιών γνωστών πολιτικών και δημοσιογράφων σχετικά με παρακολουθήσεις των επικοινωνιών τους από κατασκοπευτικό λογισμικό ήρθε στο προσκήνιο στην Ελλάδα, με αφορμή δύο λογισμικά κατασκοπείας, το Pegasus και το Predator. Το ζήτημα πήρε τέτοιες διαστάσεις, λόγω της ιδιότητας των παρακολουθουμένων, που στην κοινή γνώμη ταυτίστηκε με το ελληνικό Watergate, καθώς οι παρακολουθήσεις έγιναν από την Εθνική Υπηρεσία Πληροφοριών (εφεξής η «ΕΥΠ»). Η υπόθεση προκάλεσε πολιτικές αναταράξεις και οδήγησε στην απομάκρυνση ανώτερων στελεχών της ΕΥΠ. Η ΑΠΔΠΧ ξεκίνησε αυτεπάγγελτη έρευνα, ενώ η υπόθεση ερευνήθηκε και από την Ευρωπαϊκή Επιτροπή LIBE, εγείροντας ερωτήματα για την κρατική εποπτεία, το απόρρητο των επικοινωνιών και την εφαρμογή του Άρθρου 8 της ΕΣΔΑ.¹⁰⁷ Τον Μάρτιο του 2024, ο πρώην διοικητής της ΕΥΠ κατέθεσε ενώπιον δικαστηρίου ότι δεν χρησιμοποιήθηκε «παράνομο malware» – παρά τις αποδείξεις παρουσίας Predator σε συσκευές πολιτικών και δημοσιογράφων.¹⁰⁸ Την ίδια στιγμή, η ΑΠΔΠΧ εντόπισε πάνω από 350 μηνύματα SMS απόπειρας εγκατάστασης του Predator και ξεκίνησε έρευνες, εξέδωσε διαταγές και επέβαλε πρόστιμα για μη συνεργασία.

Από νομοθετική σκοπιά, η Ελλάδα έχει προβεί σε επιμέρους παρεμβάσεις μετά την κρίση που προκάλεσε η υπόθεση Predator, όπως η ψήφιση του Ν. 5002/2022 για την τροποποίηση του πλαισίου των επισυνδέσεων¹⁰⁹ και η ενίσχυση της ΑΠΔΠΧ με αρμοδιότητες σχετικές με

¹⁰⁶ CyberMaterial.com (2024).

¹⁰⁷ Euractiv.com, (2023).

¹⁰⁸ reuters.com, (2024).

¹⁰⁹ [Νόμος 5002/2022, ΦΕΚ Α' 228/09.12.2022](#). Η νομοθετική πρωτοβουλία που μετουσιώθηκε στον Ν. 5002/2022 είχε ως στόχους “τη θωράκιση και τον εκσυγχρονισμό της διαδικασίας άρσης του απορρήτου των επικοινωνιών σύμφωνα με το δεύτερο εδάφιο της παρ.1 του άρθρου 19 του Συντάγματος, τη βελτιστοποίηση της δράσης της Εθνικής Υπηρεσίας Πληροφοριών, την προστασία

την εμπορία κατασκοπευτικού λογισμικού. Ωστόσο, η παραβίαση της ιδιωτικότητας από παράνομο λογισμικό θα μπορούσε να είχε αποφευχθεί –ή έστω μετριαστεί σημαντικά– μέσω της ενίσχυσης της εθνικής κυβερνοανθεκτικότητας. Ο GDPR επιβάλλει αρχές όπως η λογοδοσία και η ασφάλεια εξ αρχής, ενώ η Οδηγία NIS2 και ο πρόσφατος Ν. 5019/2023 καθιστούν υποχρεωτική την εφαρμογή τεχνικών και οργανωτικών μέτρων σε κρίσιμους φορείς. Η ύπαρξη ενός λειτουργικού Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), η χρήση μηχανισμών εντοπισμού κακόβουλου λογισμικού, η έγκαιρη γνωστοποίηση περιστατικών και η εφαρμογή πολιτικών ταυτοποίησης θα μπορούσαν να αποτελέσουν σημαντικά αναχώματα. Εντέλει, το σκάνδαλο ανέδειξε το κενό μεταξύ της θεσμικής προστασίας και της επιχειρησιακής ετοιμότητας, υπενθυμίζοντας ότι η τεχνολογική ασφάλεια και η προστασία της ιδιωτικότητας είναι ζητήματα όχι μόνο νομικά αλλά και στρατηγικής δημόσιας πολιτικής.

5.3 Καλές Πρακτικές Προστασίας Δεδομένων σε Εταιρείες Τεχνολογίας

Οι μεγάλες πολυεθνικές εταιρείες τεχνολογίας όπως **Microsoft**, **Google** και **Apple** έχουν εξελίξει στρατηγικές διαχείρισης κινδύνου και προστασίας προσωπικών δεδομένων που συχνά υπερβαίνουν τις ελάχιστες κανονιστικές απαιτήσεις.

Η **Microsoft**, μέσω του **Trust Center** της, εφαρμόζει πολιτικές ασφάλειας που βασίζονται σε risk-based frameworks και διαφάνεια, ενώ παράλληλα παρέχει στους πελάτες της εργαλεία συμμόρφωσης και λογοδοσίας (Microsoft, n.d.). Η **Google**, από την πλευρά της, έχει αναπτύξει προηγμένα user dashboards, παρέχοντας granular έλεγχο στα δεδομένα και τη συγκατάθεση (consent management). Η **Apple** έχει υιοθετήσει πολιτικές edge computing και τοπικής επεξεργασίας δεδομένων σε συσκευές, περιορίζοντας την αποστολή δεδομένων σε

του απορρήτου των επικοινωνιών από λογισμικά παρακολούθησης, την οργανική και λειτουργική αναβάθμιση του επιπέδου κυβερνοασφάλειας στη χώρα, και την αποτελεσματικότερη προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.”

εξωτερικούς διακομιστές, ενισχύοντας έτσι την ιδιωτικότητα βάσει της αρχής της ελαχιστοποίησης.¹¹⁰

Παρά αυτές τις βέλτιστες πρακτικές, οι εταιρείες έχουν αποτελέσει αντικείμενο νομικών ελέγχων, όπως στην υπόθεση **Schrems II**, στην οποία το Δικαστήριο της ΕΕ ακύρωσε το Privacy Shield με το σκεπτικό ότι το αμερικανικό δίκαιο δεν προσέφερε ισοδύναμες εγγυήσεις με τον GDPR για τη μεταφορά προσωπικών δεδομένων.¹¹¹ Η υπόθεση αυτή σηματοδότησε μια καμπή για τη διεθνή διακυβέρνηση δεδομένων, τονίζοντας την ανάγκη για συμβατότητα μεταξύ των επί μέρους εθνικών νομικών πλαισίων και για τεκμηριωμένες TIAS στις διασυνοριακές διαβιβάσεις δεδομένων.

Η ανάγκη για αυξημένη επιμέλεια καθίσταται ακόμη πιο έντονη όταν πρόκειται για τεχνολογικούς παρόχους **εκτός του δυτικού δικαιοκ και θεσμικού πλαισίου**, όπως για παράδειγμα εταιρείες προερχόμενες από την **Κίνα**. Παρά την αυξανόμενη παρουσία κινεζικών πλατφορμών και τεχνολογιών στον παγκόσμιο ψηφιακό χάρτη (όπως η Huawei, η TikTok και η Alibaba Cloud), σοβαρά ερωτήματα παραμένουν ως προς την ανεξαρτησία των εταιρειών αυτών από τις κρατικές δομές ασφαλείας. Επομένως, η συζήτηση για τις πολυεθνικές πλατφόρμες δεν περιορίζεται στην εφαρμογή τεχνικών μέτρων, αλλά αγγίζει τον πυρήνα της **ψηφιακής κυριαρχίας** και της **θεσμικής συμβατότητας** μεταξύ των εθνικών πλαισίων προστασίας δεδομένων και των εμπορικών πρακτικών των τεχνολογικών κολοσσών.

Στον πίνακα που ακολουθεί αποτυπώνονται σχηματικά τα πεδία εφαρμογής και οι αποδέκτες των βασικών εργαλείων κανονιστικής συμμόρφωσης για την προστασία των προσωπικών δεδομένων και την κυβερνοασφάλεια.

¹¹⁰ EDPB, (2021).

¹¹¹ CJEU, (2020).

Πλαίσιο	Πεδίο Εφαρμογής	Τύπος Υποχρεώσεων	Ελεγκτικός Μηχανισμός	Αποδέκτες
GDPR	Προστασία προσωπικών δεδομένων	Νομικές, οργανωτικές, τεχνικές	Εποπτικές Αρχές (π.χ. ΑΠΔΠΧ)	Δημόσιοι και ιδιωτικοί φορείς
NIS 2	Κυβερνοασφάλεια κρίσιμων υποδομών	Οργανωτικές, τεχνικές	Εθνικές Αρχές Κυβερνοασφάλειας	Οργανισμοί κρίσιμης σημασίας
ISO/IEC 27001	Διαχείριση ασφάλειας πληροφοριών	Τεχνικές, οργανωτικές	Εσωτερικός και εξωτερικός έλεγχος	Εθελοντική εφαρμογή

Πίνακας 1: Συγκριτική Ανάλυση Κανονιστικών Πλαισίων προστασίας προσωπικών δεδομένων και κυβερνοασφάλειας.

5.4 Από την Κανονιστική Αρχή στην Πρακτική Εφαρμογή: Η Ασφάλεια Εξ Αρχής και το Παράδειγμα της Ελλάδας

Η αρχή της **ασφάλειας εξαρχής (security by design)** συνιστά πλέον βασικό πυλώνα της προστασίας δεδομένων και της συμμόρφωσης με τον GDPR, ο οποίος ρητά επιβάλλει την ενσωμάτωση της κυβερνοασφάλειας σε όλα τα στάδια της επεξεργασίας (άρθρα 25 και 32 GDPR). Η αρχή της ασφάλειας εξ αρχής, όπως ερμηνεύεται από τη θεωρητική βιβλιογραφία,¹¹² απαιτεί την ενσωμάτωση της προστασίας δεδομένων σε κάθε στάδιο του σχεδιασμού συστημάτων και διαδικασιών, μετατρέποντας την τεχνική συμμόρφωση σε κανονιστικό καθήκον. Παράλληλα, το πρότυπο **ISO/IEC 27001** αποτελεί διεθνώς

¹¹² Kuner et al., (2020).

αναγνωρισμένο πλαίσιο για τη δημιουργία και συντήρηση ενός **Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS)**, το οποίο περιλαμβάνει μηχανισμούς για την αναγνώριση, εκτίμηση και μετριασμό κινδύνων, τη διαχείριση συμβάντων και τη συνεχή βελτίωση.¹¹³

Επιπλέον, η εφαρμογή των αρχών **security και privacy by default** υποστηρίζεται και από άλλα πρότυπα, όπως το ISO/IEC 27701, το οποίο λειτουργεί ως επέκταση του ISO 27001 για την ενίσχυση της προστασίας προσωπικών δεδομένων.¹¹⁴ Η διαλειτουργικότητα των παραπάνω προτύπων ενισχύει την ικανότητα ανταπόκρισης στις απαιτήσεις διαφάνειας, λογοδοσίας και τεχνικής επάρκειας του GDPR και της οδηγίας NIS2. Η κανονιστική συμμόρφωση βάσει των προαναφερθέντων προτύπων φωτίζεται από soft law κείμενα, όπως ο *Good Practices Guide for ISMS Implementation* του ENISA (2021), ο οποίος προσφέρει βέλτιστες πρακτικές για τη δημιουργία και διατήρηση ενός αποδοτικού Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών στον δημόσιο και ιδιωτικό τομέα. Ο ENISA, στο πλαίσιο των καθηκόντων του βάσει της **Cybersecurity Act**, τονίζει τη σημασία της εφαρμογής risk-based προσεγγίσεων, αξιολόγησης αντικτύπου και διαλειτουργικότητας μεταξύ των ευρωπαϊκών οργανισμών.

Στην Ελλάδα, παρατηρείται σταδιακή αλλά ουσιώδης στροφή προς την **πιστοποίηση φορέων του δημόσιου τομέα** κατά τα ανωτέρω πρότυπα. Η **Ανεξάρτητη Αρχή Δημοσίων Εσόδων (ΑΑΔΕ)**, ενδεικτικά, δρομολόγησε ήδη από το 2023 διαδικασία πλήρους συμμόρφωσης με το ISO/IEC 27001, στο πλαίσιο της ευρύτερης ψηφιακής στρατηγικής του ελληνικού Δημοσίου.¹¹⁵

Παράλληλα, **ιδιωτικοί πάροχοι κρίσιμων υποδομών** (ενέργεια, τηλεπικοινωνίες, υγεία) υποχρεούνται από το 2024, σύμφωνα με τον νέο Ν. 5002/2022 και την ενσωμάτωση της NIS 2

¹¹³ ISO, (2022).

¹¹⁴ ISO, (2019).

¹¹⁵ Gov.gr, (2023).

μέσω του Ν. 5019/2023,¹¹⁶ να εφαρμόζουν **ελάχιστες απαιτήσεις κυβερνοασφάλειας**, βάσει τεχνικών και οργανωτικών μέτρων που αντικατοπτρίζονται σε διεθνή πρότυπα και, φυσικά, στην ίδια την Οδηγία NIS2.

Η θεσμική τάση είναι σαφής: η **ασφάλεια και η προστασία της ιδιωτικότητας δεν είναι πλέον προαιρετική πολιτική επιλογή, αλλά θεσμική επιταγή**, εναρμονισμένη με ευρωπαϊκές στρατηγικές όπως η Στρατηγική της ΕΕ για την Ψηφιακή δεκαετία και ο GDPR. Η υλοποίηση της αρχής “*Security by Design*” στο ελληνικό διοικητικό και επιχειρησιακό περιβάλλον, παρότι σε πρόωρο στάδιο, συγκροτεί το βασικό εργαλείο μετάβασης προς ένα **ασφαλές, λειτουργικό και διαφανές ψηφιακό κράτος**.

Ειδική βιβλιογραφία κεφαλαίου 5

- Aha.org (American Hospital Association), (2024). Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field. Διαθέσιμο εδώ: <https://www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and?>

¹¹⁶ Ο Ν. 5019/2023 (ΦΕΚ 27/Α/14-2-2023) αφορά τη θέσπιση ελάχιστων απαιτήσεων ασφαλείας για παρόχους κρίσιμων υποδομών, στο πλαίσιο της ψηφιακής στρατηγικής και της προστασίας συστημάτων που υποστηρίζουν δημόσιες λειτουργίες, την υγεία, την ενέργεια, τις μεταφορές και τις τηλεπικοινωνίες. Η συνδρομή του στο πλαίσιο της NIS 2 είναι σημαντική, καθώς θέτει τις βάσεις για οργανωτικά και τεχνικά μέτρα ασφαλείας, θεσπίζει υποχρεώσεις συμμόρφωσης για ιδιωτικούς και δημόσιους φορείς που χαρακτηρίζονται ως φορείς παροχής βασικών υπηρεσιών, δηλαδή όσοι εμπíπτουν και στο πεδίο εφαρμογής της NIS 2 και προβλέπει ελεγκτικούς μηχανισμούς, ρυθμιστική εποπτεία και δυνατότητα επιβολής διοικητικών κυρώσεων σε περιπτώσεις παραβίασης των υποχρεώσεων ασφαλείας.

- Apnews.com,(2025). With retail cyberattacks on the rise, customers find orders blocked and shelves empty. Διαθέσιμο εδώ: <https://apnews.com/article/cyberattack-retail-whole-foods-victorias-secret-ms-9105458e6ef45152b065e623d0bf06fd>
- BleepingComputer, (2024). Internet Archive hacked, data breach impacts 31 million users. Διαθέσιμο εδώ: <https://www.bleepingcomputer.com/news/security/internet-archive-hacked-data-breach-impacts-31-million-users/>
- CyberMaterial.com (2024). *Greek Land Registry under cyberattack: incident response underway.* [online] Διαθέσιμο εδώ: <https://cybermaterial.com>
- Cybernews.com (2024). Mother of all breaches reveals 26 billion records: what we know so far. Διαθέσιμο εδώ: <https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/>
- CJEU, Case C-311/18 – *Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems (Schrems II)*, ECLI:EU:C:2020:559. Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:62018CJ0311>
- Dailisecurity.com, (2025). **Headero App Data Leak Exposes Over Four Million Sensitive User Records, Including GPS and Sexual Preferences.** Διαθέσιμο εδώ: <https://dailysecurityreview.com/security-spotlight/headero-app-data-leak-exposes-over-four-million-sensitive-user-records-including-gps-and-sexual-preferences/>
- EDPB (2021), *Overview of national enforcement actions under the GDPR.* European Data Protection Board. Διαθέσιμο εδώ: <https://edpb.europa.eu>
- EDPB (2021), *Guidelines 01/2021 on Examples regarding Data Breach Notification under the GDPR, Version 2.0.* European Data Protection Board. Διαθέσιμο σε: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-data-breach_en
- ENISA (2021), *Good Practices Guide for ISMS Implementation.* European Union Agency for Cybersecurity. Διαθέσιμο σε: <https://www.enisa.europa.eu>

- EU AI Act, (2024). Κανονισμός (ΕΕ) 2024/1689. Διαθέσιμος εδώ: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401689
- Euractiv.com, (2023). EXCLUSIVE: EU Prosecutor probes Greek ‘Predatorgate’. Διαθέσιμο εδώ: <https://www.euractiv.com/section/politics/news/exclusive-eu-prosecutor-probes-greek-predatorgate/>
- European Commission (2018), EU GDPR Handbook – Data Breach Notification, Brussels: Publications Office of the European Union. Διαθέσιμο εδώ: https://www.edps.europa.eu/sites/default/files/publication/18-12-05_guidelines_data_breach_en_0.pdf
- Gov.gr (2023), Πιστοποίηση ISO της ΑΑΔΕ για την Ασφάλεια Πληροφοριακών Συστημάτων. Διαθέσιμο εδώ: https://www.aade.gr/sites/default/files/2023-11/diakirixi_anaptyxi_plaisiou_asfaleias_pliροφοριων.pdf?
- hackread.com, (2025). Hackers Leak 86 Million AT&T Records with Decrypted SSNs. Διαθέσιμο εδώ: <https://hackread.com/hackers-leak-86m-att-records-with-decrypted-ssns/?>
- ibm.com, (2024). National Public Data breach publishes private data of 2.9B US citizens. Διαθέσιμο εδώ: <https://www.ibm.com/think/news/national-public-data-breach-publishes-private-data-billions-us-citizens?>
- iranwire.com, (2025). Hackers Claim Access to 42 Million Sepah Bank Records, Bank Denies Breach. Διαθέσιμο εδώ: <https://iranwire.com/en/news/139996-hackers-claim-access-to-42-million-sepah-bank-records-bank-denies-breach/?>
- ISO/IEC (2022), 27001:2022 – *Information security, cybersecurity and privacy protection – Information security management systems*. Geneva: International Organization for Standardization. Διαθέσιμο εδώ: <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en>
- ISO/IEC (2019), 27701:2019 – *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*. Geneva: International Organization for Standardization. Διαθέσιμο εδώ: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en>

- Kuner, C., Bygrave, L.A. & Docksey, C. (eds.) (2021) *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford: Oxford University Press. Διαθέσιμη εδώ: https://web.archive.org/web/20210509231556id_/https://fdslive.oup.com/www.oup.com/academic/pdf/law/GDPRCommentary_ArticleUpdates.pdf
- New York Times, (2019). "5 Million Bulgarians Have Their Personal Data Stolen in Hack". Διαθέσιμο εδώ: <https://www.nytimes.com/2019/07/17/world/europe/bulgaria-hack-cyberattack.html>
- Protothema.gr, 2(2025). Νέα κυβερνοεπίθεση στο δίκτυο «ΣΥΖΕΥΞΙΣ» - Λειτουργήσαν άμεσα οι μηχανισμοί άμυνας. Διαθέσιμο εδώ: <https://www.protothema.gr/greece/article/1589076/nea-kuvernoepithesi-sto-diktuo-suzeuxis/>
- Reuters.com, (2025). Washington Post investigating cyberattack on journalists' email accounts, source says. Διαθέσιμο εδώ: <https://www.reuters.com/world/us/washington-post-investigating-cyberattack-journalists-wsj-reports-2025-06-15/?>
- ¹ reuters.com, (2024). Greece's former spy boss tells judges service did not use illegal malware in 2019-22. Διαθέσιμο εδώ: <https://www.reuters.com/world/europe/greeces-former-spy-boss-tells-judges-service-did-not-use-illegal-malware-2019-22-2024-07-27/?>
- Theguardian.com, (2025). M&S 'praying for sun' but full recovery from cyber-attack unlikely this summer. Διαθέσιμο εδώ: <https://www.theguardian.com/business/2025/jun/14/m-and-s-cyber-attack-recovery-summer-clothing-online-services?>
- Νόμος 5019/2023 - ΦΕΚ 27/Α/14-2-2023. Διαθέσιμος εδώ: <https://www.e-nomothesia.gr/sunegoros-tou-katanalote/n-5019-2023.html>

- [Νόμος 5002/2022, ΦΕΚ Α' 228/09.12.2022. Διαθέσιμος εδώ: https://www.kodiko.gr/nomothesia/document/844300/nomos-5002-2022](https://www.kodiko.gr/nomothesia/document/844300/nomos-5002-2022)

ΚΕΦΑΛΑΙΟ 6 – ΣΥΜΠΕΡΑΣΜΑΤΙΚΕΣ ΣΚΕΨΕΙΣ

- ΔΕΟΝΤΟΛΟΓΙΑ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ: ΠΡΟΣ

ΕΝΑ ΔΗΜΟΚΡΑΤΙΚΟ ΨΗΦΙΑΚΟ ΜΕΛΛΟΝ

Η παρούσα Διπλωματική Εργασία επεχείρησε να καταδείξει με το πλέον γλαφυρό τρόπο τον πολυπαραγοντικό χαρακτήρα της προστασίας προσωπικών δεδομένων και της κυβερνοασφάλειας στο σημερινό ευρωπαϊκό κανονιστικό και τεχνολογικό περιβάλλον. Η ανάλυση ανέδειξε τη διαλεκτική σχέση ανάμεσα στις νομικές, τεχνικές και οργανωτικές διαστάσεις, γεγονός που καθιστά αναγκαία την προώθηση συνεκτικών και ολιστικών πολιτικών παρεμβάσεων.¹¹⁷

6.1 Η προσέγγιση από πλευράς Δικαίου

Κατ' αρχάς, η ενίσχυση της κανονιστικής συνοχής στην ΕΕ αποτελεί επιτακτική ανάγκη. Η αλληλεπικάλυψη μεταξύ του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), της Οδηγίας NIS 2, του Κανονισμού DORA και του Κανονισμού για την Τεχνητή Νοημοσύνη (AI Act), έχει δημιουργήσει ερμηνευτικές και πρακτικές δυσκολίες στους φορείς συμμόρφωσης.¹¹⁸ Η ΕΕ οφείλει να προχωρήσει στην έκδοση εναρμονισμένων κατευθυντήριων γραμμών για την κοινή εφαρμογή των ρυθμιστικών αυτών εργαλείων,¹¹⁹ ενώ κρίνεται σκόπιμη η ίδρυση ενός ευρωπαϊκού παρατηρητηρίου ρυθμιστικής συνοχής με

¹¹⁷ European Commission, (2020).

¹¹⁸ Veale & Borgesius, (2021).

¹¹⁹ Article 29 Working Party, (2018).

αρμοδιότητα τον συντονισμό και την παρακολούθηση της εφαρμογής των κανονισμών από τους οργανισμούς.

Παράλληλα, η αναβάθμιση των δεξιοτήτων και των διαθέσιμων πόρων των δημοσίων οργανισμών αναδεικνύεται ως βασικός πυλώνας ενίσχυσης της κυβερνοανθεκτικότητας. Η ανά χειράς εργασία ανέδειξε τις αδυναμίες των δημοσίων φορέων, ιδιαίτερα των τοπικών αρχών, σε ό,τι αφορά την προστασία δεδομένων και τη διαχείριση περιστατικών παραβίασης.¹²⁰ Η δημιουργία ενός σταθερού μηχανισμού χρηματοδότησης για την υιοθέτηση τεχνικών μέτρων και την ομοιογενή και ταυτόχρονη πιστοποίηση σε όλα τα κράτη-μέλη κατά ISO/IEC 27001 είναι κρίσιμη.¹²¹ Παράλληλα, η θεσμοθέτηση υποχρεωτικής συνεχούς εκπαίδευσης για κρίσιμες ειδικότητες του δημόσιου τομέα, όπως οι Υπεύθυνοι Προστασίας Δεδομένων (DPOs) και οι IT managers, αποτελεί απαραίτητη προϋπόθεση προσαρμογής στις εξελισσόμενες απειλές.

Σε επίπεδο εποπτείας των μεγάλων πολυεθνικών ψηφιακών πλατφορμών, έχει αναδειχθεί ήδη η ανάγκη για πιο δραστικές και συντονισμένες παρεμβάσεις. Η ενίσχυση του μηχανισμού «one-stop shop» του GDPR πρέπει να συνοδευτεί από θεσμικές ασφαλιστικές δικλίδες, ώστε να αποφευχθούν καθυστερήσεις ή στρεβλώσεις στη διασυνοριακή εποπτεία. Παράλληλα, η υποχρεωτική δημοσίευση ετήσιων απολογιστικών εκθέσεων από εταιρείες με περισσότερους από 10 εκατομμύρια χρήστες στην ΕΕ,¹²² θα ενίσχυε τη διαφάνεια και τη λογοδοσία στην ψηφιακή οικονομία.

Καθώς η Τεχνητή Νοημοσύνη αποκτά κεντρική θέση στα πληροφοριακά συστήματα, και το Blockchain μετατρέπει το πρότυπο εμπιστοσύνης από το κεντρικό στο αποκεντρωμένο, τα παραδοσιακά νομικά σχήματα βρίσκονται σε κατάσταση επιταχυνόμενης αναθεώρησης. Η θεσμική προσαρμογή προσπαθεί να «κρατήσει βήμα» με τις εξελίξεις, μέσα από

¹²⁰ EDPB, (2021).

¹²¹ ENISA, (2021).

¹²² EDPS, (2024).

πρωτοβουλίες όπως η NIS 2, ο GDPR, η Data Act, αλλά και μέσω ενός διαρκώς διευρυνόμενου διεθνούς διαλόγου για την "ψηφιακή κυριαρχία" και την "ηθική της πληροφορίας".

Η τεχνητή νοημοσύνη μετασχηματίζει ριζικά το οικοσύστημα πληροφορίας και συνεπώς απαιτείται μια συστημική και προληπτική ρύθμιση. Η ενσωμάτωση αρχών λογοδοσίας και επεξηγησιμότητας σε όλες τις δημόσιες συμβάσεις σχετικές με εφαρμογές της ΤΝ, βάσει του άρθρου 9 της AI Act, αποτελεί αναγκαίο βήμα. Επιπλέον, η ενίσχυση ανεξάρτητων ηθικών εποπτικών φορέων με ρόλο την έκδοση δεσμευτικών γνωμοδοτήσεων πριν από την θέση σε ισχύ συστημάτων υψηλού κινδύνου ενδυναμώνει τη δημοκρατική νομιμοποίηση της τεχνολογίας.¹²³

Στην κατεύθυνση της προώθησης ενός δεδομενοκεντρικού προσανατολισμού της τεχνολογικής καινοτομίας, η ενίσχυση εργαλείων όπως τα «data sandboxes» και τα πρότυπα λογισμικού με προεπιλεγμένη συμμόρφωση (privacy-by-default code) είναι ιδιαίτερα σημαντική.¹²⁴ Τέτοιες πρακτικές ενισχύουν τη συνεργασία μεταξύ ρυθμιστικών αρχών και ιδιωτικού τομέα, μειώνοντας παράλληλα τον κίνδυνο παραβιάσεων.

Εν κατακλείδι, κεντρική σημασία έχει η καλλιέργεια ψηφιακής συνείδησης στους πολίτες. Η ένταξη της ψηφιακής ηθικής και της προστασίας προσωπικών δεδομένων στα προγράμματα δευτεροβάθμιας και τριτοβάθμιας εκπαίδευσης συνιστά μια επένδυση στο δημοκρατικό μέλλον της ΕΕ.¹²⁵ Συμπληρωματικά, η υλοποίηση ευρωπαϊκής καμπάνιας ενημέρωσης για τα ψηφιακά δικαιώματα των πολιτών, σε συνεργασία με τις Αρχές Προστασίας Δεδομένων και την κοινωνία των πολιτών, θα ενίσχυε τη συμμετοχή και την εμπιστοσύνη στο ψηφιακό κράτος.¹²⁶ Το θεμελιώδες που πρέπει να καλλιεργηθεί τα επόμενα χρόνια είναι πως η κυβερνοασφάλεια και η προστασία των προσωπικών δεδομένων δεν συνιστούν απλώς τεχνικές ή νομικές προκλήσεις, αλλά αποτελούν θεμελιώδη ζητήματα δημοκρατίας και

¹²³ Binns, (2018).

¹²⁴ OECD, (2021).

¹²⁵ Bashar, U. and Naaz, I, (2024).

¹²⁶ EDPB, (2022).

κράτους δικαίου. Η αντιμετώπισή τους απαιτεί διαρκή θεσμικό αναστοχασμό, ενδυνάμωση όλων των εμπλεκόμενων φορέων και προσήλωση σε ένα ψηφιακό μοντέλο διακυβέρνησης που θέτει στο επίκεντρο τον άνθρωπο και τα δικαιώματά του.

6.2 Μία φιλοσοφική θεώρηση

Η ταχύτατη διείσδυση της τεχνολογίας στις δομές της καθημερινής ζωής και της διοίκησης θέτει εκ νέου το ζήτημα των ηθικών ορίων της τεχνολογικής εξουσίας. Οι ψηφιακές τεχνολογίες δεν είναι ουδέτερα εργαλεία· ενσωματώνουν αξίες, προτεραιότητες και, συχνά, ασύμμετρες δυναμικές σχέσεις. Το διακύβευμα της προστασίας των προσωπικών δεδομένων και της κυβερνοασφάλειας δεν είναι απλώς νομικό ή τεχνικό, αλλά βαθιά φιλοσοφικό: ποιος ορίζει το ψηφιακό υποκείμενο και υπό ποιες συνθήκες;

Ο John Rawls, στο κλασικό του έργο *A Theory of Justice* (1971), ανέπτυξε την έννοια της «δικαιοσύνης ως θεμελιώδους αρετής των κοινωνικών θεσμών», προτάσσοντας δύο αρχές: την ισότητα των βασικών ελευθεριών και την αρχή της διαφοράς – σύμφωνα με την οποία ανισότητες δικαιολογούνται μόνον όταν ωφελούν τους λιγότερο ευνοημένους.¹²⁷ Στο ψηφιακό περιβάλλον, η εφαρμογή αυτής της συλλογιστικής επιβάλλει έναν σχεδιασμό των τεχνολογιών που προάγει την καθολική πρόσβαση, τη διαφάνεια, τη λογοδοσία και τη μη διάκριση – δηλαδή την «ηθική της ένταξης» στον πυρήνα της τεχνολογικής αρχιτεκτονικής.

Η Hannah Arendt είχε ήδη προειδοποιήσει για τον κίνδυνο απώλειας του πολιτικού χώρου λόγω της τεχνικής κυριαρχίας, σημειώνοντας ότι «ο κόσμος γίνεται ακατανόητος όταν η πράξη υποκαθίσταται από τη διαχείριση».¹²⁸ Αντίστοιχα, ο Habermas υπογράμμισε την ανάγκη να διαμορφώνεται η νομιμοποίηση των τεχνολογικών ρυθμίσεων μέσα από συμμετοχικές διαδικασίες επικοινωνιακής δράσης και ορθολογικού διαλόγου.¹²⁹ Όπως τονίζει ο Habermas, η αυτονομία των θεσμών σε ένα δημοκρατικό πολίτευμα δεν είναι δυνατή χωρίς ουσιαστική πρόσβαση του πολίτη στη δημόσια σφαίρα. Σε έναν ψηφιακό

¹²⁷ Rawls, J. (1999).

¹²⁸ (Arendt, H. (1958).

¹²⁹ Habermas, J. (1996).

κόσμο που κυριαρχείται από ιδιωτικές πλατφόρμες, η απώλεια κυριαρχίας επί των δεδομένων ισοδυναμεί με υπονόμηση της πολιτικής συμμετοχής και της πληροφόρησης. Η αρχή της ψηφιακής κυριαρχίας εμπεριέχει έτσι και μία **δεοντολογική διάσταση**, που συνδέεται με τη θεωρία του John Rawls περί «ίσων βασικών ελευθεριών». Ο έλεγχος της πληροφορίας αποτελεί προϋπόθεση για ουσιαστική ισότητα και συμμετοχή· αλλιώς, η τεχνολογία δεν ενισχύει τη δημοκρατία, αλλά αναπαράγει ανισότητες. Αυτό καθιστά επιτακτική τη θέσπιση μηχανισμών δημοκρατικής λογοδοσίας στην ψηφιακή διακυβέρνηση.¹³⁰

Σε αυτό το πλαίσιο, ο ψηφιακός συνταγματισμός δεν μπορεί να περιορίζεται στον νομικό φορμαλισμό, αλλά πρέπει να ενσωματώνει ουσιαστικά κριτήρια κοινωνικής νομιμοποίησης και διαφάνειας. Η ιδέα του informational self-determination,¹³¹ που εμπεδώνεται και στο ευρωπαϊκό νομικό κεκτημένο,¹³² συνιστά πυλώνα αυτής της δεοντολογικής συγκρότησης: το άτομο πρέπει να έχει ουσιαστικό έλεγχο επί των δεδομένων του, και η τεχνολογία να σχεδιάζεται με προτεραιότητα την προστασία του προσώπου. Όπως παρατηρεί ο Paul Ricoeur, η ταυτότητα του ατόμου δεν είναι στατική, αλλά διαλογική και ερμηνευτική: κάθε σύστημα επεξεργασίας δεδομένων επεμβαίνει στην αφήγηση του εαυτού, άρα επιβάλλεται η μέγιστη ευθύνη στην αρχιτεκτονική αυτών των τεχνολογιών.¹³³

Στον ορίζοντα της ψηφιακής εποχής, λοιπόν, η προστασία των προσωπικών δεδομένων και η κυβερνοασφάλεια δεν αποτελούν πλέον απλώς τεχνικές ή νομικές συντεταγμένες, αλλά τα θεμέλια μιας αναδυόμενης ψηφιακής πολιτειότητας. Η εργασία αυτή ανέδειξε πως η σχέση μεταξύ των δύο εννοιών δεν είναι μόνο αλληλοσυμπληρούμενη αλλά και διαλεκτική, μια σχέση εντάσεων και συγκλίσεων, μεταβαλλόμενη καθώς η τεχνολογία και η κοινωνία μετασχηματίζονται.

¹³⁰ Floridi, 2019).

¹³¹ Westin, A.F. (1967

¹³² BVerfG, (1983)

¹³³ Ricoeur, P.(1992).

Πέρα από το τεχνοκρατικό λεξιλόγιο των ρυθμιστικών πλαισίων, το κρίσιμο διακύβευμα είναι η δημοκρατία του 21ου αιώνα: αν ο πολίτης παραμένει κύριος της πληροφορίας που τον αφορά ή αν μετατρέπεται σε αντικείμενο αδιάκοπης επιτήρησης και ψηφιακής εμπορευματοποίησης. Σε αυτό το σταυροδρόμι, η λογοδοσία των τεχνολογιών, η ερμηνευσιμότητα των αλγορίθμων, και η εμπέδωση της αρχής του πληροφοριακού αυτοκαθορισμού δεν είναι απλώς θεσμικές απαιτήσεις, αλλά πράξεις ψηφιακής αξιοπρέπειας. Ίσως το μέλλον δεν ανήκει μόνο σε εκείνους που επεξεργάζονται περισσότερα δεδομένα, αλλά σε εκείνους που τα επεξεργάζονται με σεβασμό, διαφάνεια και σκοπό. Η προστασία των προσωπικών δεδομένων δεν είναι τροχοπέδη στην καινοτομία – είναι ο ηθικός της οδηγός.

Ειδική βιβλιογραφία κεφαλαίου 6

- Arendt, H. (1958). *The Human Condition*. Chicago: University of Chicago Press. Διαθέσιμο εδώ:
[https://books.google.gr/books?hl=el&lr=&id=bGlwDwAAOBAJ&oi=fnd&pg=PR5&dq=%E2%80%A2%09Arendt,+H.+\(1958\).+The+Human+Condition.+Chicago:+University+of+Chicago+Press.&ots=3onpqIxSAV&sig=D-ExHAjdLn4_xYDqkx2WPV7I7rs&redir_esc=y#v=onepage&q=%E2%80%A2%09Arendt%2C%20H.%20\(1958\).%20The%20Human%20Condition.%20Chicago%3A%20University%20of%20Chicago%20Press.&f=false](https://books.google.gr/books?hl=el&lr=&id=bGlwDwAAOBAJ&oi=fnd&pg=PR5&dq=%E2%80%A2%09Arendt,+H.+(1958).+The+Human+Condition.+Chicago:+University+of+Chicago+Press.&ots=3onpqIxSAV&sig=D-ExHAjdLn4_xYDqkx2WPV7I7rs&redir_esc=y#v=onepage&q=%E2%80%A2%09Arendt%2C%20H.%20(1958).%20The%20Human%20Condition.%20Chicago%3A%20University%20of%20Chicago%20Press.&f=false)
- Article 29 Working Party (2018). *Guidelines on Transparency under Regulation 2016/679*. Brussels: European Commission. Διαθέσιμο εδώ:
https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf
- BVerfG, (1983). Judgment of 15 December 1983, *Volkszählungsurteil I*. Διαθέσιμη εδώ:
https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs1_9831215_1bvr020983en.html

- Bashar, U. and Naaz, I, (2024). DIGITAL LITERACY: THE IMPORTANCE, INITIATIVES AND CHALLENGES”. Διαθέσιμο εδώ: <file:///C:/Users/a.fafaliou/Downloads/IRJMETS60500157224-may.pdf>
- Binns, R. (2018). ‘Algorithmic accountability and public reason’, *Philosophy & Technology*, 31(4), 543–556. Διαθέσιμο εδώ: <https://link.springer.com/article/10.1007/s13347-017-0263-5>
- EDPB (2021). *Guidelines 01/2021 on Examples regarding Data Breach Notification*. Brussels: European Data Protection Board. Διαθέσιμο εδώ: https://www.edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf
- ENISA (2021). *Cybersecurity for Public Administrations: Good Practices and Recommendations*. Athens: European Union Agency for Cybersecurity. Διαθέσιμο εδώ: <https://www.enisa.europa.eu>
- European Commission (2020). *White Paper on Artificial Intelligence: A European approach to excellence and trust*. COM(2020) 65 final. Διαθέσιμο εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0065>
- European Commission (2018). *EU GDPR Handbook – Data Breach Notification*. Brussels: Publications Office of the European Union. Διαθέσιμο εδώ: https://www.edps.europa.eu/sites/default/files/publication/18-12-05_guidelines_data_breach_en_0.pdf
- EDPB (2022). *Statement on Digital Sovereignty and Citizens’ Rights in the EU*. Brussels: EDPB. Διαθέσιμο εδώ: <https://europeanmovement.eu/policy/digital-sovereignty-and-citizens-rights-2/>
- EDPS, (2024). *European Data Protection Supervisor;s 2024 annual report*. Διαθέσιμο εδώ: https://www.edps.europa.eu/system/files/2025-04/edps_annual_report-2024_en.pdf

- Floridi, L. (2019). *The Logic of Information: A Theory of Philosophy as Conceptual Design*. Oxford University Press. Διαθέσιμο εδώ: [https://books.google.gr/books?hl=el&lr=&id=nYZUEAAAOBAJ&oi=fnd&pg=PP1&dq=Floridi,+L.+\(2019\).+The+Logic+of+Information:+A+Theory+of+Philosophy+as+Conceptual+Design.+Oxford+University+Press.&ots=uxqLuJ_YHN&sig=rwY7FR93HH_rIcfT9TDoeW0D5k&redir_esc=y#v=onepage&q=Floridi%2C%20L.%20\(2019\).%20The%20Logic%20of%20Information%3A%20A%20Theory%20of%20Philosophy%20as%20Conceptual%20Design.%20Oxford%20University%20Press.&f=false](https://books.google.gr/books?hl=el&lr=&id=nYZUEAAAOBAJ&oi=fnd&pg=PP1&dq=Floridi,+L.+(2019).+The+Logic+of+Information:+A+Theory+of+Philosophy+as+Conceptual+Design.+Oxford+University+Press.&ots=uxqLuJ_YHN&sig=rwY7FR93HH_rIcfT9TDoeW0D5k&redir_esc=y#v=onepage&q=Floridi%2C%20L.%20(2019).%20The%20Logic%20of%20Information%3A%20A%20Theory%20of%20Philosophy%20as%20Conceptual%20Design.%20Oxford%20University%20Press.&f=false)
- Habermas, J. (1996). *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*. Cambridge: MIT Press. Διαθέσιμο εδώ: [https://books.google.gr/books?hl=el&lr=&id=4SK1CgAAQBAJ&oi=fnd&pg=PT7&dq=%E2%80%A2%09Habermas,+J.+\(1996\).+Between+Facts+and+Norms:+Contributions+to+a+Discourse+Theory+of+Law+and+Democracy.+Cambridge:+MIT+Press.&ots=4zm2IeOZgy&sig=FXU1LDIvV8Jli8Gw2p3WnycPscx&redir_esc=y#v=onepage&q&f=false](https://books.google.gr/books?hl=el&lr=&id=4SK1CgAAQBAJ&oi=fnd&pg=PT7&dq=%E2%80%A2%09Habermas,+J.+(1996).+Between+Facts+and+Norms:+Contributions+to+a+Discourse+Theory+of+Law+and+Democracy.+Cambridge:+MIT+Press.&ots=4zm2IeOZgy&sig=FXU1LDIvV8Jli8Gw2p3WnycPscx&redir_esc=y#v=onepage&q&f=false)
- OECD (2021). *Recommendation on Enhancing Access to and Sharing of Data*. Διαθέσιμο εδώ: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463>
- Rawls, J. (1999). *A Theory of Justice (revised edition of A Theory of Justice, 1971)*. Cambridge, MA: Harvard University Press. Διαθέσιμο εδώ: <https://giuseppicapograssi.wordpress.com/wp-content/uploads/2014/08/rawls99.pdf>
- Ricoeur, P. (1992). *Oneself as Another*. Chicago: University of Chicago Press. Διαθέσιμο εδώ: [https://books.google.gr/books?hl=el&lr=&id=uCZSOYcB_CIC&oi=fnd&pg=PP11&dq=%E2%80%A2%09Ricoeur,+P.+\(1992\).+Oneself+as+Another.+Chicago:+University+of+Chicago+Press.&ots=FjJEkxQbXt&sig=1tL4BYbqUOpzvq2c-CLJytfRpYY&redir_esc=y#v=onepage&q=%E2%80%A2%09Ricoeur%2C%20P.%20\(1992\).%20Oneself%20as%20Another.%20Chicago%3A%20University%20of%20Chicago%20Press.&f=false](https://books.google.gr/books?hl=el&lr=&id=uCZSOYcB_CIC&oi=fnd&pg=PP11&dq=%E2%80%A2%09Ricoeur,+P.+(1992).+Oneself+as+Another.+Chicago:+University+of+Chicago+Press.&ots=FjJEkxQbXt&sig=1tL4BYbqUOpzvq2c-CLJytfRpYY&redir_esc=y#v=onepage&q=%E2%80%A2%09Ricoeur%2C%20P.%20(1992).%20Oneself%20as%20Another.%20Chicago%3A%20University%20of%20Chicago%20Press.&f=false)

- Veale, M., & Borgesius, F. Z. (2021). 'Demystifying the Draft EU Artificial Intelligence Act', *Computer Law Review International*, 22(4), 97–112. Διαθέσιμο εδώ: <https://doi.org/10.9785/cri-2021-220402>
- Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum – Review to tis book by DAVID L. Ross, *Washington and Lee Law Review*, *Washington and Lee Law Review*”, Spring 3-1-1968. Διαθέσιμο εδώ:
- <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr>

ΠΑΡΑΡΤΗΜΑ 1: ΠΙΝΑΚΑΣ

ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

Συντομογραφία	Όρος
AI/TN	Artificial Intelligence/Τεχνητή Νοημοσύνη
AI Act	Artificial Intelligence Act
ΑΑΔΕ	Ανεξάρτητη Αρχή Δημοσίων Εσόδων
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
BCR	Binding Corporate Rules
BVerfG	Bundesverfassungsgericht
BVwG	Bundesverwaltungsgericht
CERT	Computer Emergency Response Team
CJEU/ΔΕΕ	Court of Justice of the European Union
CSIRT	Computer Security Incident Response Team
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECHR	European Court of Human Rights

ECISO	European CyberSecurity Organisation
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ΕΕ	Ευρωπαϊκή Ένωση
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου
GDPR	General Data Protection Regulation
ISMS	Information Security Management System
MFA	Multi-Factor Authentication
NIS 2	Οδηγία για την Ασφάλεια Δικτύων και Πληροφοριών, αναθεωρημένη (2022)
SCCs	Standard Contractual Clauses
TIA	Transfer Impact Assessment
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών
ΧΘΔΕΕ	Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

ΠΑΡΑΡΤΗΜΑ 2: ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ ΚΑΙ ΕΙΚΟΝΩΝ

Αρίθμηση	Τίτλος	Σελίδα
Εικόνα 1	Θεματική διάρθρωση προστασίας προσωπικών δεδομένων και κυβερνοασφάλειας	22
Διάγραμμα 1	Διάγραμμα σχέσης κυβερνοασφάλειας και προστασίας δεδομένων	83

ΠΙΝΑΚΑΣ ΒΙΒΛΙΟΓΡΑΦΙΚΩΝ ΑΝΑΦΟΡΩΝ

Ξενόγλωσση Βιβλιογραφία

- Abelson, H. et al. (2015), 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications', MIT CSAIL Report. Διαθέσιμο εδώ: <https://www.usenix.org/conference/enigma2016/conference-program/presentation/rivest>
- advisera.com, (2022). ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide. Διαθέσιμο εδώ: <https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/?com>
- Aha.org (American Hospital Association), (2024). Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field. Διαθέσιμο εδώ: <https://www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and?>
- Apnews.com,(2025). With retail cyberattacks on the rise, customers find orders blocked and shelves empty. Διαθέσιμο εδώ: <https://apnews.com/article/cyberattack-retail-whole-foods-victorias-secret-ms-9105458e6ef45152b065e623d0bf06fd>
- Arendt, H. (1958). The Human Condition. Chicago: University of Chicago Press. Διαθέσιμο εδώ: [https://books.google.gr/books?hl=el&lr=&id=bGlwDwAAQBAJ&oi=fnd&pg=PR5&dq=%E2%80%A2%09Arendt,+H.+\(1958\).+The+Human+Condition.+Chicago:+University+of+Chicago+Press.&ots=3onpqIxSAV&sig=D-ExHAjdLn4 xYDqkx2WPV7l7rs&redir_esc=y#v=onepage&q=%E2%80%A2%09Arendt%2C%20H.%20\(1958\).%20The%20Human%20Condition.%20Chicago%3A%20University%20of%20Chicago%20Press.&f=false](https://books.google.gr/books?hl=el&lr=&id=bGlwDwAAQBAJ&oi=fnd&pg=PR5&dq=%E2%80%A2%09Arendt,+H.+(1958).+The+Human+Condition.+Chicago:+University+of+Chicago+Press.&ots=3onpqIxSAV&sig=D-ExHAjdLn4 xYDqkx2WPV7l7rs&redir_esc=y#v=onepage&q=%E2%80%A2%09Arendt%2C%20H.%20(1958).%20The%20Human%20Condition.%20Chicago%3A%20University%20of%20Chicago%20Press.&f=false)

- Article 29 Working Party (2018). Guidelines on Transparency under Regulation 2016/679. Brussels: European Commission. Διαθέσιμο εδώ: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf
- Burrell, J. (2016) 'How the machine "thinks": Understanding opacity in machine learning algorithms', Big Data & Society, 3(1). Διαθέσιμο εδώ: <https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512>
- Bashar, U. and Naaz, I, (2024). DIGITAL LITERACY: THE IMPORTANCE, INITIATIVES AND CHALLENGES". Διαθέσιμο εδώ: <file:///C:/Users/a.fafaliou/Downloads/IRJMETS60500157224-may.pdf>
- Binns, R. (2018). 'Algorithmic accountability and public reason', Philosophy & Technology, 31(4), 543–556. Διαθέσιμο εδώ: <https://link.springer.com/article/10.1007/s13347-017-0263-5>
- BleepingComputer, (2024). Internet Archive hacked, data breach impacts 31 million users. Διαθέσιμο εδώ: <https://www.bleepingcomputer.com/news/security/internet-archive-hacked-data-breach-impacts-31-million-users/>
- Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press. Διαθέσιμο εδώ: <file:///C:/Users/a.fafaliou/Downloads/ssrn-2770634-1.pdf>
- Bygrave, L. A. (2014). Data Privacy Law: An International Perspective. Oxford University Press. Διαθέσιμο στο: <https://academic.oup.com/book/27114>
- Cadwalladr, C. and Graham-Harrison, E. (2018), 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica', The Guardian, 17 March. Διαθέσιμο εδώ: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

- Cavoukian, A. (2009) Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario. Διαθέσιμο εδώ: <https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>
- Convention of Budapest on Cybercrime, (2001). Council of Europe ETS No. 185/2001). Διαθέσιμη εδώ: <https://rm.coe.int/1680081561>. Συγκεντρωμένα τα κείμενα της Σύμβασης και των δύο Προσθετων Πρωτοκόλλων της εδώ: <https://eur-lex.europa.eu/EL/legal-content/summary/convention-on-cybercrime.html>
- Creemers, R. (2018). Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century. Journal of Contemporary China. Διαθέσιμο εδώ: <https://www.tandfonline.com/doi/full/10.1080/10670564.2016.1206281#d1e103>
- CSC.gr (2023). 9 παραδείγματα εφαρμογών του Blockchain. Διαθέσιμο εδώ: <https://csc.gr/9-paradeigmata-efarmogon-tou-blockchain/>
- CyberMaterial.com (2024). Greek Land Registry under cyberattack: incident response underway. [online] Διαθέσιμο εδώ: <https://cybermaterial.com>
- Cybernews.com (2024). Mother of all breaches reveals 26 billion records: what we know so far. Διαθέσιμο εδώ: <https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/>
- CyberNews.com, (2024). Blockchain και κυβερνοασφάλεια. Διαθέσιμο εδώ: <https://cybernews.gr/blockchain/blockchain-kai-kyvernoasfaleia/>
- Dailisecurity.com, (2025). Headero App Data Leak Exposes Over Four Million Sensitive User Records, Including GPS and Sexual Preferences. Διαθέσιμο εδώ: <https://dailysecurityreview.com/security-spotlight/headero-app-data-leak-exposes-over-four-million-sensitive-user-records-including-gps-and-sexual-preferences/>
- Dpa.gr. Ο επίσημος ιστότοπος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ΑΠΔΠΧ: <https://www.dpa.gr/>

- ECSCO, (2025). White Paper - NIS2 Implementation: Challenges & Priorities. Διαθέσιμο εδώ: <https://ecs-org.eu/ecso-uploads/2025/01/ECSCO-White-Paper-NIS2-Implementation.pdf>
- EDPB, (2021). Guidelines 01/2021 on Examples regarding Data Breach Notification. Διαθέσιμες εδώ: https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_data_breach_notification_examples_v1_en.pdf
- EDPB (2021), Overview of national enforcement actions under the GDPR. European Data Protection Board. Διαθέσιμο εδώ: <https://edpb.europa.eu>
- EDPB, (2022). Adopted - Guidelines 01/2022 on data subject rights - Right of access. Διαθέσιμες εδώ: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf
- EDPB (2022). Statement on Digital Sovereignty and Citizens' Rights in the EU. Brussels. Διαθέσιμο εδώ: <https://europeanmovement.eu/policy/digital-sovereignty-and-citizens-rights-2/>
- EDPS. (2020). Opinion 4/2020 on the European strategy for data. Διαθέσιμη εδώ: <https://edps.europa.eu>
- EDPS, (2024). European Data Protection Supervisor;s 2024 annual report. Διαθέσιμο εδώ: https://www.edps.europa.eu/system/files/2025-04/edps_annual_report-2024_en.pdf
- ENISA (2019). Pseudonymisation techniques and best practices. Διαθέσιμο στο: <https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices>
- ENISA (2020), Guidelines on shaping technology according to GDPR provisions. Διαθέσιμο εδώ: <https://www.enisa.europa.eu/sites/default/files/publications/WP2018%20O.2.2.5%20->

[%20Recomendations%20on%20shaping%20technology%20according%20to%20GDPR%20provisions%20-%20Part%201.pdf](#)

- ENISA (2021), Good Practices Guide for ISMS Implementation. European Union Agency for Cybersecurity. Διαθέσιμο σε: <https://www.enisa.europa.eu>
- ENISA (2021). Public-private partnerships for cybersecurity: evaluation and good practices. European Union Agency for Cybersecurity. Διαθέσιμο εδώ: <https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/national-cybersecurity-strategies-0/public-private>
- ENISA (2021). Cybersecurity for Public Administrations: Good Practices and Recommendations. Athens: European Union Agency for Cybersecurity. Διαθέσιμο εδώ: <https://www.enisa.europa.eu>
- ENISA (2022). Cybersecurity Threat Landscape Report. European Union Agency for Cybersecurity. Διαθέσιμο εδώ: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202022.pdf>
- ENISA, (2023). Interoperable EU Risk Management Framework. Διαθέσιμο εδώ: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report-Interoperable%20EU%20Risk%20Management%20Framework_Updated.pdf
- ENISA, (2023). Cybersecurity and Data Protection by Design. Διαθέσιμο στο: <https://www.enisa.europa.eu/publications/data-protection-engineering>
- ENISA, (2025). NIS2 Technical Implementation Guidance. Διαθέσιμο εδώ: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

- ERT News (2025). Κυβερνοασφάλεια και Τεχνητή Νοημοσύνη. Διαθέσιμο στο: <https://www.ertnews.gr/eidiseis/epistimi/technologia/kyvernoasfaleia-kai-texniti-noimosyni-ti-epifylassei-to-2025/>
- ESET (2025). Κυβερνοασφάλεια και Τεχνητή Νοημοσύνη: Τι επιφυλάσσει το 2025. Διαθέσιμο εδώ: <https://www.eset.com/gr/about/newsroom/press-releases-gr-1/kyvernoasfaleia-kai-techniti-noimosyni-ti-epifylassei-to-2025/>
- EU AI Act, (2024). Κανονισμός (ΕΕ) 2024/1689. Διαθέσιμος εδώ: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401689
- EU Data Act (2020). Κανονισμός (ΕΕ) 2020/2854. Διαθέσιμος εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1749730466674>
- EU Data Governance Act, (2022). Κανονισμός (ΕΕ) 2022/868. Διαθέσιμος εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868>
- EU Directive NIS2, (2022). Οδηγία (ΕΕ) 2022/2555. Διαθέσιμη εδώ: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>
- EU DORA Regulation, (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Διαθέσιμος εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554>
- EU Cyber Resilience Act (2024). Κανονισμός (ΕΕ) 2024/2847. Διαθέσιμος εδώ: <https://www.european-cyber-resilience-act.com/>
- EU Cybersecurity Act, (2019). Κανονισμός (ΕΕ) 2019/881. Διαθέσιμο στο: <https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng>
- EU-US Data Privacy Framework, (2024). Διαθέσιμο εδώ: https://privacyshielddev.blob.core.windows.net/publicsiteassets/Full%20Text_EU-U.S.%20DPF.pdf

- Euractiv.com, (2023). EXCLUSIVE: EU Prosecutor probes Greek ‘Predatorgate’. Διαθέσιμο εδώ: <https://www.euractiv.com/section/politics/news/exclusive-eu-prosecutor-probes-greek-predatorgate/>
- European Commission (2018), EU GDPR Handbook – Data Breach Notification, Brussels: Publications Office of the European Union. Διαθέσιμο εδώ: https://www.edps.europa.eu/sites/default/files/publication/18-12-05_guidelines_data_breach_en_0.pdf
- European Commission, (2020). Europe's Digital Decade. Διαθέσιμο στο: <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>
- European Commission (2020). Shaping Europe’s Digital Future. Brussels: COM(2020) 67 final. Διαθέσιμο εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0067>
- European Commission (2020). White Paper on Artificial Intelligence: A European Approach to Excellence and Trust. Διαθέσιμο εδώ: https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf
- European Commission (2022). Proposal for a Regulation on the European Health Data Space (EHDS), COM(2022) 197 final. Διαθέσιμο εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0197>
- European Data Strategy, (2020). Διαθέσιμη εδώ: https://ec.europa.eu/commission/presscorner/api/files/attachment/862109/European_data_strategy_en.pdf
- Ferretti, A. (2021) «Ethics and Governance of Big Data in Health Research and Digital Health Applications». Διαθέσιμο εδώ: file:///C:/Users/a.fafaliou/Downloads/27589_FERRETTIAGATA_2021.pdf

- Floridi, L. (2019). The Logic of Information: A Theory of Philosophy as Conceptual Design. Oxford University Press. Διαθέσιμο εδώ: [https://books.google.gr/books?hl=el&lr=&id=nYZUEAAAOBAJ&oi=fnd&pg=PP1&dq=Floridi,+L.+\(2019\).+The+Logic+of+Information:+A+Theory+of+Philosophy+as+Conceptual+Design.+Oxford+University+Press.&ots=uxqLuJ_YHN&sig=rwY7FR93HH_rIcfT9TDoeW0D5k&redir_esc=y#v=onepage&q=Floridi%2C%20L.%20\(2019\).%20The%20Logic%20of%20Information%3A%20A%20Theory%20of%20Philosophy%20as%20Conceptual%20Design.%20Oxford%20University%20Press.&f=false](https://books.google.gr/books?hl=el&lr=&id=nYZUEAAAOBAJ&oi=fnd&pg=PP1&dq=Floridi,+L.+(2019).+The+Logic+of+Information:+A+Theory+of+Philosophy+as+Conceptual+Design.+Oxford+University+Press.&ots=uxqLuJ_YHN&sig=rwY7FR93HH_rIcfT9TDoeW0D5k&redir_esc=y#v=onepage&q=Floridi%2C%20L.%20(2019).%20The%20Logic%20of%20Information%3A%20A%20Theory%20of%20Philosophy%20as%20Conceptual%20Design.%20Oxford%20University%20Press.&f=false)
- GDPR, (2016). (Regulation (EU) 2016/679.). Διαθέσιμος εδώ: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- Gov.gr (2023), Πιστοποίηση ISO της ΑΑΔΕ για την Ασφάλεια Πληροφοριακών Συστημάτων. Διαθέσιμο εδώ: https://www.aade.gr/sites/default/files/2023-11/diakirixi_anaptyxi_plaisiou_asfaleias_pliroforion.pdf?
- Greenleaf, G. (2021). Global Tables of Data Privacy Laws and Bills (7th Ed, January 2021). Διαθέσιμο εδώ: <file:///C:/Users/a.fafaliou/Downloads/ssrn-3836261.pdf>
- Gürses, S., Troncoso, C. and Diaz, C. (2011) 'Engineering privacy by design', Computers, Privacy and Data Protection: An Element of Choice.
- Habermas, J. (1996). Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy. Cambridge: MIT Press. Διαθέσιμο εδώ: [https://books.google.gr/books?hl=el&lr=&id=4SK1CgAAQBAJ&oi=fnd&pg=PT7&dq=%E2%80%A2%09Habermas,+J.+\(1996\).+Between+Facts+and+Norms:+Contributions+to+a+Discourse+Theory+of+Law+and+Democracy.+Cambridge:+MIT+Press.&ots=4zm2IeOZgy&sig=FXU1LDIvV8Jli8Gw2p3WnycPsrc&redir_esc=y#v=onepage&q&f=false](https://books.google.gr/books?hl=el&lr=&id=4SK1CgAAQBAJ&oi=fnd&pg=PT7&dq=%E2%80%A2%09Habermas,+J.+(1996).+Between+Facts+and+Norms:+Contributions+to+a+Discourse+Theory+of+Law+and+Democracy.+Cambridge:+MIT+Press.&ots=4zm2IeOZgy&sig=FXU1LDIvV8Jli8Gw2p3WnycPsrc&redir_esc=y#v=onepage&q&f=false)
- hackread.com, (2025). Hackers Leak 86 Million AT&T Records with Decrypted SSNs. Διαθέσιμο εδώ: <https://hackread.com/hackers-leak-86m-att-records-with-decrypted-ssns/?>

- Homo Digitalis (2023). Τεχνητή Νοημοσύνη και Κυβερνοασφάλεια: Πραγματικότητα και Υπερβολές. Διαθέσιμο στο: <https://homodigitalis.gr/posts/3752/>
- ibm.com, (2024). National Public Data breach publishes private data of 2.9B US citizens. Διαθέσιμο εδώ: <https://www.ibm.com/think/news/national-public-data-breach-publishes-private-data-billions-us-citizens?>
- International Standardisation Organisation ISO, ISO/IEC 27001 και ISO/IEC 27701, διαθέσιμα εδώ: <https://www.iso.org/standard/27001> και εδώ: <https://www.iso.org/standard/71670.html>
- iranwire.com, (2025). Hackers Claim Access to 42 Million Sepah Bank Records, Bank Denies Breach. Διαθέσιμο εδώ: <https://iranwire.com/en/news/139996-hackers-claim-access-to-42-million-sepah-bank-records-bank-denies-breach/?>
- ISO/IEC (2019), 27701:2019 – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Geneva: International Organization for Standardization. Διαθέσιμο εδώ: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en>
- ISO/IEC (2022), 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems. Geneva: International Organization for Standardization. Διαθέσιμο εδώ: <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en>
- Kuner, C., Bygrave, L.A. & Docksey, C. (eds.) (2021) The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press. Διαθέσιμη εδώ: https://web.archive.org/web/20210509231556id_/https://fdslive.oup.com/www.oup.com/academic/pdf/law/GDPRCommentary_ArticleUpdates.pdf
- Mantelero, A. (2016) 'Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection', Computer Law & Security Review, 32(2), pp.238–255.

- MDPI (2023). Artificial Intelligence and Cybersecurity. Διαθέσιμο εδώ: <https://www.mdpi.com/2079-9292/14/3/581>
- New York Times, (2019). “5 Million Bulgarians Have Their Personal Data Stolen in Hack”. Διαθέσιμο εδώ: <https://www.nytimes.com/2019/07/17/world/europe/bulgaria-hack-cyberattack.html>
- Nissenbaum, H. (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press. Διαθέσιμο εδώ: https://web.archive.org/web/20220629220601id_/https://watermark.silverchair.com/jinfo_poli_1_2011
- OECD (2021). Recommendation on Enhancing Access to and Sharing of Data. Διαθέσιμο εδώ: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463>
- ¹ OECD, (2022). Enhancing Digital Security and Privacy in Policy Making. [Online] Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf
<https://www.oecd.org/digital/enhancing-digital-security-and-privacy.pdf>
- Protothema.gr, 2(2025). Νέα κυβερνοεπίθεση στο δίκτυο «ΣΥΖΕΥΞΙΣ» - Λειτουργήσαν άμεσα οι μηχανισμοί άμυνας. Διαθέσιμο εδώ: <https://www.protothema.gr/greece/article/1589076/nea-kuvernoepithesi-sto-diktuo-suzeuxis/>
- Rawls, J. (1999). A Theory of Justice (revised edition of A Theory of Justice, 1971). Cambridge, MA: Harvard University Press. Διαθέσιμο εδώ: <https://giuseppicapograssi.wordpress.com/wp-content/uploads/2014/08/rawls99.pdf>
- ¹ reuters.com, (2024). Greece's former spy boss tells judges service did not use illegal malware in 2019-22. Διαθέσιμο εδώ:

<https://www.reuters.com/world/europe/greeces-former-spy-boss-tells-judges-service-did-not-use-illegal-malware-2019-22-2024-07-27/>

- Reuters.com, (2025). Washington Post investigating cyberattack on journalists' email accounts, source says. Διαθέσιμο εδώ: <https://www.reuters.com/world/us/washington-post-investigating-cyberattack-journalists-wsj-reports-2025-06-15/>
- Ricoeur, P. (1992). *Oneself as Another*. Chicago: University of Chicago Press. Διαθέσιμο εδώ: [https://books.google.gr/books?hl=el&lr=&id=uCZSOYcB_CIC&oi=fnd&pg=PP11&dq=%E2%80%A2%09Ricoeur,+P.+\(1992\).+Oneself+as+Another.+Chicago:+University+of+Chicago+Press.&ots=FjJEkxQbXt&sig=1tL4BYbqUOpzvq2c-CLJytfRpYY&redir_esc=y#v=onepage&q=%E2%80%A2%09Ricoeur%2C%20P.%20\(1992\).%20Oneself%20as%20Another.%20Chicago%3A%20University%20of%20Chicago%20Press.&f=false](https://books.google.gr/books?hl=el&lr=&id=uCZSOYcB_CIC&oi=fnd&pg=PP11&dq=%E2%80%A2%09Ricoeur,+P.+(1992).+Oneself+as+Another.+Chicago:+University+of+Chicago+Press.&ots=FjJEkxQbXt&sig=1tL4BYbqUOpzvq2c-CLJytfRpYY&redir_esc=y#v=onepage&q=%E2%80%A2%09Ricoeur%2C%20P.%20(1992).%20Oneself%20as%20Another.%20Chicago%3A%20University%20of%20Chicago%20Press.&f=false)
- Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, (2022). Διαθέσιμο εδώ: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22023A0228\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22023A0228(01))
- Selbst, A.D. and Barocas, S. (2018) 'The intuitive appeal of explainable machines', *Fordham Law Review*, 87(3). Διαθέσιμο εδώ: <https://par.nsf.gov/servlets/purl/10121294>
- Tene, O. and Polonetsky, J. (2012). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, 11(5), 239–273. Διαθέσιμο εδώ: <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njt>
- Theguardian.com, (2025). M&S 'praying for sun' but full recovery from cyber-attack unlikely this summer. Διαθέσιμο εδώ:

<https://www.theguardian.com/business/2025/jun/14/m-and-s-cyber-attack-recovery-summer-clothing-online-services?>

- Tufekci, Z. (2015) 'Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency', *Colorado Technology Law Journal*, 13(203).
- United Security (2024). Cyber Security with Artificial Intelligence. Διαθέσιμο εδώ: <https://unitedsecurity.gr/en/cyber-security-ai-vs-humans-en/>
- US Cybersecurity Framework (CSF), σε επίσημη, εγκεκριμένη από τον NIST ελληνική μετάφραση. Διαθέσιμο εδώ: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.gre.pdf>
- Veale, M. and Binns, R. (2017). Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. *Big Data & Society*, 4(2), 1–17. Διαθέσιμο [εδώ](#).
- Veale, M. & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4). Διαθέσιμο εδώ: <https://www.degruyterbrill.com/document/doi/10.9785/cri-2021-220402/html>
- Wachter, S., Mittelstadt, B. and Floridi, L. (2017) 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation', *International Data Privacy Law*, 7(2), pp.76–99.
- Wachter, S. & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, (2), 494–620. Διαθέσιμο εδώ: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/colb2019&div=15&id=&page=>
- Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum – Review to tis book by DAVID L. Ross, *Washington and Lee Law Review*, *Washington and Lee Law Review*,

Spring

3-1-1968.

Διαθέσιμο

εδώ:

<https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr>

- Yogosha.com, (2024). NIS2 vs DORA: what differences and which legislation prevails? Διαθέσιμο εδώ: <https://yogosha.com/blog/nis2-vs-dora/>
- Επίσημος ιστοχώρος της CISA (Cybersecurity and Infrastructure Security Agency): <https://www.cisa.gov/>
- Επίσημος ιστοχώρος της Cyberspace Administration of China (CAC): <https://www.cac.gov.cn/>
- Επίσημος ιστοχώρος του CERT-EU: <https://cert.europa.eu/>
- Επίσημος ιστοχώρος του EU NIS Cooperation Group: <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>
- Επίσημος ιστοχώρος του NIST (National Institute of Standards and Technology): <https://www.nist.gov/>

Ευρωπαϊκή Νομολογία

- Bundesverfassungsgericht, (1983). Judgment of 15 December 1983, Volkszählungsurteil I. Διαθέσιμη εδώ: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html
- Bundesverfassungsgericht, (2008). (Judgment of 27 February 2008, Volkszählungsurteil II. Διαθέσιμη εδώ: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html
- Bundesverwaltungsgericht, (2025). *Entscheidung W108 2274731-1/11E – Noyb v. Clearview AI*. Ολόκληρη η απόφαση διαθέσιμη εδώ: [https://gdprhub.eu/images/8/80/20250131114705867_redacted_\(4\).pdf](https://gdprhub.eu/images/8/80/20250131114705867_redacted_(4).pdf) Η περίληψη

της απόφασης στα Αγγλικά διαθέσιμη εδώ:
<https://gdprhub.eu/index.php?title=BVwG - W108 2274731-1/11E>

- Court of Justice of the European Union, 2015. Case C-362/14, Maximilian Schrems v. Data Protection Commissioner (Schrems I). Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362>
- Court of Justice of the European Union, (2016). Case C 582/14 – Breyer v Germany. Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0582>
- Court of Justice of the European Union, (2019). Case C-136/17 – GC and Others v Commission nationale de l'informatique et des libertés (CNIL). Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0136>
- Court of Justice of the European Union, (2020). Case C-311/18. Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems (Schrems II). Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311>
- Court of Justice of the European Union, (2020). Joined Cases C-511/18, C-512/18 and C-520/18 – La Quadrature du Net and Others Premier ministre and Others. Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0511>
- Court of Justice of the European Union, (2025). -Case C-203/22 - Dun and Bradstreet Austria. Διαθέσιμη εδώ: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0203>
- European Court of Human Rights, (2008). Liberty and Others v. United Kingdom, Judgment of 1 July 2008. Διαθέσιμη εδώ: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22%3A%5B%22001-87207%22%5D%7D>
- European Court of Human Rights, (2017). Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland (2017): για την επεξεργασία δημοσίων δεδομένων. Διαθέσιμη εδώ: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22%3A%5B%22001-175121%22%5D%7D>

- European Court of Human Rights, (2021). Big Brother Watch and Others v. the United Kingdom. Διαθέσιμη εδώ: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-210077%22%5D%7D>

Ελληνόγλωσση Βιβλιογραφία

- Υπουργείο Ψηφιακής Διακυβέρνησης (2020). *Εθνική Στρατηγική Κυβερνοασφάλειας 2020–2025*. Αθήνα: Εθνικός Φορέας Κυβερνοασφάλειας. Διαθέσιμο σε: <https://mindigital.gr>

Ελληνική Νομοθεσία

- Νόμος 4411/2016 (ΦΕΚ 142/Α/3-8-2016). Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών. Διαθέσιμος εδώ: <https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/nomos-4411-2016.html>
- Νόμος 4624/2019 (ΦΕΚ Α΄ 137/29.08.2019). Μέτρα εφαρμογής του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) και της Οδηγίας (ΕΕ) 2016/680. Διαθέσιμος εδώ: <https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-phkek-137a-29-8-2019.html>
- Νόμος 5002/2022, ΦΕΚ Α΄ 228/09.12.2022. Διαθέσιμος εδώ: <https://www.kodiko.gr/nomothesia/document/844300/nomos-5002-2022>
- Νόμος 5019/2023 - ΦΕΚ 27/Α/14-2-2023. Διαθέσιμος εδώ: <https://www.e-nomothesia.gr/sunegoros-tou-katanalote/n-5019-2023.html>

- Νόμος 5188/2025 – (ΦΕΚ 49/Α/28-3-2025). Διαθέσιμος εδώ: <https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/n-5188-2025.html>
- Π.Δ. 82/2021 (ΦΕΚ Α' 195/30.11.2021). Οργανισμός του Υπουργείου Ψηφιακής Διακυβέρνησης και σύσταση Εθνικού Φορέα Κυβερνοασφάλειας. Διαθέσιμο εδώ: <https://www.e-nomothesia.gr/kat-astynomikos-astynomia/kriseis-proagoges/proedriko-diatagma-82-2021-phek-201a-30-10-2021.html>

Όλοι οι παρατιθέμενοι σύνδεσμοι προσπελάστηκαν εσχάτως στις 30/09/2025.