



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2024-2025

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Σουζάνας Σωπασουδάκη (Α.Μ.: 2351)

ΕΛΕΓΧΟΣ ΠΕΡΙΕΧΟΜΕΝΟΥ ΑΠΟ ΠΛΑΤΦΟΡΜΕΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑ  
ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ  
CONTENT MODERATION FROM PLATFORMS AND PERSONAL  
DATA PROTECTION

Επιβλέπουσα:

Λίλιαν Μήτρου

Πειραιάς, Ιούνιος 2025



Περιεχόμενα	
<b>ΠΕΡΙΛΗΨΗ</b> .....	5
<b>ABSTRACT</b> .....	7
<b>ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ</b> .....	9
<b>1. ΕΙΣΑΓΩΓΗ - ΤΟ ΣΥΓΧΡΟΝΟ ΨΗΦΙΑΚΟ ΠΕΡΙΒΑΛΛΟΝ ΚΑΙ ΟΙ ΠΡΟΚΛΗΣΕΙΣ ΣΤΗ ΡΥΘΜΙΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ</b> .....	10
<b>2. ΨΗΦΙΑΚΕΣ ΠΛΑΤΦΟΡΜΕΣ ΚΑΙ ΡΥΘΜΙΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ: ΘΕΩΡΗΤΙΚΟ ΚΑΙ ΕΝΝΟΙΟΛΟΓΙΚΟ ΠΛΑΙΣΙΟ</b> .....	13
2.1 Η έννοια των ψηφιακών πλατφορμών .....	13
2.2 Ο Έλεγχος Περιεχομένου στις ψηφιακές πλατφόρμες .....	15
2.2.1 Η έννοια του ελέγχου περιεχομένου.....	15
2.2.2. Αυτορρύθμιση ( <i>self – regulation</i> ) και Συρρύθμιση ( <i>co - regulation</i> ) .....	16
2.2.3 Μηχανισμοί Ελέγχου Περιεχομένου.....	19
2.3 Οι ψηφιακές πλατφόρμες ως φορείς ιδιωτικής αλλά de facto θεσμικής εξουσίας .....	23
<b>3. Ο ΕΛΕΓΧΟΣ ΠΕΡΙΕΧΟΜΕΝΟΥ ΥΠΟ ΤΟ ΠΡΙΣΜΑ ΘΕΜΕΛΙΩΔΩΝ ΔΙΚΑΙΩΜΑΤΩΝ: ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΕΞΙΣΟΡΡΟΠΗΣΗ</b> .....	26
3.1 Η μετάβαση από την τεχνική πρακτική σε θεσμικό πρόβλημα .....	26
3.2 Η ελευθερία της έκφρασης και οι περιορισμοί της στον ψηφιακό λόγο .....	27
3.2.1 Ρητορική Μίσους, Παραπληροφόρηση και Ψευδείς Ειδήσεις ( <i>Fake News</i> ) ως Νομιμοποιητικοί Λόγοι Παρέμβασης .....	29
3.3 Αρχές Εξισορρόπησης: Αναλογικότητα, Αναγκαιότητα και Διαφάνεια Παρέμβασης .....	33
3.4 Η Νομολογία του ΕΔΔΑ και του ΔΕΕ για την προάσπιση της ελευθερίας της έκφρασης στο διαδίκτυο και της ιδιωτικότητας .....	35
<b>4. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ ΓΙΑ ΤΙΣ ΨΗΦΙΑΚΕΣ ΠΛΑΤΦΟΡΜΕΣ</b> .....	38
4.1 Ιστορική και νομοθετική εξέλιξη.....	38
4.2 Κανονισμός 2022/2065 για τις Ψηφιακές Υπηρεσίες ( <i>Digital Services Act - DSA</i> ) .....	39
4.2.1 Η Διαδικασία Ειδοποίησης και Δράσης ( <i>Notice and Action</i> ).....	41
4.2.2 Μηχανισμοί Ενστάσεων και Εξωδικαστική Επίλυση.....	43

4.2.3 Μηχανισμοί Επισήμανσης και Αντιμετώπισης Καταχρηστικών Συμπεριφορών στις Επιγραμμικές Πλατφόρμες.....	44
4.2.4 Διαφάνεια Συστημάτων Συστάσεων και Επιγραμμικής Διαφήμισης.....	45
4.2.5 Οι πολύ μεγάλες επιγραμμικές (online) πλατφόρμες .....	47
4.3 Αξιολόγηση του Κανονισμού 2022/2065 από άποψη προσωπικών δεδομένων..	49
<b>5. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΙΣ ΨΗΦΙΑΚΕΣ ΠΛΑΤΦΟΡΜΕΣ .....</b>	<b>54</b>
5.1 Ο έλεγχος πληροφοριών ως πρακτική επεξεργασίας προσωπικών δεδομένων στις ψηφιακές πλατφόρμες .....	54
5.2 Νομοθετική εξέλιξη της προστασίας προσωπικών δεδομένων σε συνάρτηση με τις ψηφιακές πλατφόρμες.....	57
5.3 Κανονιστική αποτίμηση του ελέγχου περιεχομένου υπό το πρίσμα του Γενικού Κανονισμού Προστασίας Δεδομένων.....	57
5.3.1 Οι ψηφιακές πλατφόρμες ως υπεύθυνοι επεξεργασίας κατά τον έλεγχο περιεχομένου.....	63
5.3.2 Νόμιμες βάσεις επεξεργασίας προσωπικών δεδομένων κατά τον έλεγχο περιεχομένου.....	67
5.3.3 Αρχές επεξεργασίας προσωπικών δεδομένων.....	63
5.3.4 Τα δικαιώματα των χρηστών έναντι των πλατφορμών στο πλαίσιο ελέγχου περιεχομένου.....	68
5.3.5 Το δικαίωμα δικαστικής προστασίας και ο κυρωτικός μηχανισμός του ΓΚΠΔ .....	73
5.4 Ο Ν. 4624/2019 και η εφαρμογή του στις ψηφιακές πλατφόρμες .....	75
<b>6. ΣΥΜΠΕΡΑΣΜΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΠΡΟΚΛΗΣΕΩΝ .....</b>	<b>77</b>
<b>ΒΙΒΛΙΟΓΡΑΦΙΑ .....</b>	<b>83</b>
Ελληνική Βιβλιογραφία - Αρθρογραφία.....	83
Ξενόγλωσση Βιβλιογραφία - Αρθρογραφία .....	84
Διπλωματικές Εργασίες .....	88
Νομοθετικά Κείμενα .....	88
Νομολογία .....	90

## ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία πραγματεύεται το ζήτημα του ελέγχου περιεχομένου από τις ψηφιακές πλατφόρμες υπό το πρίσμα της προστασίας των προσωπικών δεδομένων και της εν γένει διασφάλισης των θεμελιωδών δικαιωμάτων στο σύγχρονο ψηφιακό περιβάλλον. Ειδικότερα, επιχειρεί να αναδείξει τον τρόπο με τον οποίο οι μηχανισμοί φιλτραρίσματος, επισημάνσεων, αφαίρεσης και περιορισμού περιεχομένου, είτε μέσω ανθρώπινης εποπτείας είτε μέσω αλγοριθμικών διαδικασιών, επηρεάζουν το εύρος άσκησης της ελευθερίας της έκφρασης και την ιδιωτικότητα των χρηστών. Το ζήτημα αποκτά ακόμη μεγαλύτερη σημασία, αν ληφθεί υπόψη ότι οι πλατφόρμες, μέσω της συλλογής και επεξεργασίας τεράστιου όγκου προσωπικών δεδομένων, συγκεντρώνουν μια μορφή ιδιωτικής αλλά ουσιαστικά θεσμικής εξουσίας, η οποία δεν υπόκειται πάντοτε σε επαρκή λογοδοσία ή διαφάνεια.

Στο πλαίσιο αυτό, η εργασία αναλύει τα μοντέλα αυτορρύθμισης και συρρύθμισης που έχουν υιοθετηθεί διεθνώς, αξιολογώντας την αποτελεσματικότητά τους σε σχέση με τις αρχές της αναλογικότητας, της αναγκαιότητας και της διαφάνειας. Η μελέτη εστιάζει στη μετάβαση του ζητήματος από μια τεχνική διαδικασία σε ένα θεσμικό πρόβλημα, που αφορά την ίδια τη λειτουργία της δημοκρατίας στο ψηφιακό πεδίο.

Κεντρική θέση στην ανάλυση κατέχει το ευρωπαϊκό ρυθμιστικό πλαίσιο, όπως αυτό διαμορφώνεται από τον Κανονισμό (ΕΕ) 2022/2065 για τις Ψηφιακές Υπηρεσίες (Digital Services Act - DSA), ο οποίος εισάγει νέους κανόνες για τη διαχείριση περιεχομένου, την ευθύνη των παρόχων, τη διαφάνεια των συστημάτων και την προστασία των χρηστών από καταχρηστικές πρακτικές. Παράλληλα, εξετάζεται η σχέση του εν λόγω Κανονισμού με την προστασία προσωπικών δεδομένων, και ιδίως με τον Γενικό Κανονισμό (ΕΕ) 2016/679 (ΓΚΠΔ) και τον ν. 4624/2019, οι οποίοι θέτουν το πλαίσιο για τη νόμιμη επεξεργασία δεδομένων και τα δικαιώματα των υποκειμένων.

Η εργασία βασίζεται σε ανάλυση νομοθετικών και κανονιστικών κειμένων, νομολογίας του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ) και του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ), καθώς και σε επιστημονική βιβλιογραφία που αναδεικνύει τις νομικές και ηθικές διαστάσεις του ζητήματος. Μέσα από αυτήν την πολυεπίπεδη προσέγγιση, επιδιώκεται να αποτυπωθεί η ένταση ανάμεσα στην ανάγκη καταπολέμησης του παράνομου ή επιβλαβούς περιεχομένου και στην υποχρέωση διαφύλαξης των ατομικών ελευθεριών.

Η συνολική αξιολόγηση των δεδομένων οδηγεί στην ανάδειξη της ανάγκης για τη διαμόρφωση ενός συνεκτικού πλαισίου συνεργασίας κράτους, πλατφορμών και ανεξάρτητων αρχών, το οποίο θα συνδυάζει την τεχνολογική καινοτομία με την προστασία των θεμελιωδών δικαιωμάτων. Η ενίσχυση της διαφάνειας, η καθιέρωση σαφών διαδικασιών ελέγχου και ένστασης, καθώς και η συνεκτίμηση των αρχών προστασίας δεδομένων αποτελούν κρίσιμους άξονες για μια πιο δίκαιη και δημοκρατική ψηφιακή διακυβέρνηση. Με αυτόν τον τρόπο, ο έλεγχος περιεχομένου μπορεί να εξελιχθεί από πεδίο σύγκρουσης συμφερόντων σε μηχανισμό ισορροπίας μεταξύ της ελευθερίας της έκφρασης, της ασφάλειας του ψηφιακού χώρου και της προστασίας της ιδιωτικότητας των χρηστών.

## ABSTRACT

This paper addresses the issue of content moderation by digital platforms through the lens of personal data protection and the broader safeguarding of fundamental rights in the contemporary digital environment. In particular, it seeks to highlight the ways in which mechanisms of filtering, flagging, removal, and restriction of content, whether through human supervision or algorithmic processes, affect both the scope of freedom of expression and the privacy of users. The issue becomes even more significant when considering that platforms, through the collection and processing of vast amounts of personal data, concentrate a form of private but de facto institutional power, which is not always subject to sufficient accountability or transparency.

Within this context, the study analyzes the models of self-regulation and co-regulation adopted internationally, assessing their effectiveness in light of the principles of proportionality, necessity, and transparency. The research focuses on the transformation of content moderation from a mere technical process into an institutional challenge, directly related to the functioning of democracy in the digital sphere.

A central position in the analysis is held by the European regulatory framework, as shaped by Regulation (EU) 2022/2065 on Digital Services (Digital Services Act - DSA), which introduces new rules regarding content moderation, provider liability, system transparency, and the protection of users from abusive practices. At the same time, the study explores the relationship between the DSA and the protection of personal data, particularly the General Data Protection Regulation (EU) 2016/679 (GDPR) and Law 4624/2019, which establish the legal framework for the lawful processing of personal data and the rights of data subjects.

The research is based on the analysis of legislative and regulatory texts, the case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECHR), as well as scientific literature that highlights the legal and ethical

dimensions of the issue. Through this multi-layered approach, the study aims to capture the tension between the need to combat illegal or harmful content and the obligation to safeguard individual freedoms.

The overall assessment highlights the need to establish a coherent framework of cooperation between states, platforms, and independent authorities, one that combines technological innovation with the protection of fundamental rights. Strengthening transparency, introducing clear mechanisms of review and appeal, and consistently integrating data protection principles are identified as key pillars for achieving a fairer and more democratic model of digital governance. In this way, content moderation can evolve from a field of conflicting interests into a mechanism of balance between freedom of expression, digital security, and user privacy.

## **ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ**

ΑΠΔΠΧ: Αρχή Προστασίας Δεδομένων Προσωπικού Δεδομένων

Βλ.: Βλέπε

ΓΚΠΔ: Γενικός Κανονισμός Προστασίας Δεδομένων

ΔΕΕ: Δικαστήριο της Ευρωπαϊκής Ένωσης

ΕΔΔΑ: Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου

ΕΕ: Ευρωπαϊκή Ένωση

ΕΕΠΔ: Ευρωπαίος Επόπτης Προστασίας Δεδομένων

ΕΣΔΑ: Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου

ΚτΠ: Κοινωνία της Πληροφορίας

Κλπ: Και λοιπά

Ο.π: Όπως παραπάνω

Παρ.: Παράγραφος

Πχ: Παραδείγματος χάριν

Σελ. : Σελίδα

ΣΛΕΕ: Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης  
ΧΘΔΕΕ: Χάρτης Θεμελιωδών Δικαιωμάτων Ευρωπαϊκής Ένωσης

AVMS: Audiovisual Media Services Directive

DSA: Digital Services Act

European Data Protection Supervisor: EDPS

GDPR: General Data Protection Regulation

VLOPs: Very Large Online Platforms

VLOSEs: Very Large Online Search Engines

## **1. ΕΙΣΑΓΩΓΗ - ΤΟ ΣΥΓΧΡΟΝΟ ΨΗΦΙΑΚΟ ΠΕΡΙΒΑΛΛΟΝ ΚΑΙ ΟΙ ΠΡΟΚΛΗΣΕΙΣ ΣΤΗ ΡΥΘΜΙΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ**

Στην εποχή της ραγδαίας ψηφιακής μετάβασης και της εντατικής χρήσης των μέσων κοινωνικής δικτύωσης, η διαχείριση του περιεχομένου από τις ψηφιακές πλατφόρμες έχει αναδειχθεί σε ένα από τα πλέον κρίσιμα ζητήματα για τη δημοκρατία, την προστασία των ανθρωπίνων δικαιωμάτων και την εύρυθμη λειτουργία του δημόσιου διαλόγου. Ο έλεγχος περιεχομένου (content moderation) αναφέρεται στις διαδικασίες με τις οποίες ψηφιακές πλατφόρμες, όπως το Facebook, το Instagram, το YouTube και το X (πρώην Twitter), αξιολογούν, περιορίζουν ή αφαιρούν αναρτήσεις που θεωρούν ότι παραβιάζουν τους όρους χρήσης ή τη σχετική νομοθεσία, είτε σε ενωσιακό είτε σε εθνικό επίπεδο. Αυτές οι πρακτικές περιλαμβάνουν τόσο αυτοματοποιημένα φίλτρα και τεχνητή νοημοσύνη όσο και τη συμβολή ανθρώπινων ομάδων και επιτροπών που αναλαμβάνουν την αξιολόγηση του περιεχομένου σε συνάρτηση με την εφαρμογή των πολιτικών έκαστης πλατφόρμας και της νομοθεσίας.

Παράλληλα, η προστασία των προσωπικών δεδομένων αποτελεί θεμελιώδες δικαίωμα στην Ευρωπαϊκή Ένωση και βασική αρχή της ψηφιακής διακυβέρνησης. Η αλληλεπίδραση μεταξύ των μηχανισμών ελέγχου και της συλλογής, επεξεργασίας και αποθήκευσης προσωπικών δεδομένων εγείρει σοβαρά νομικά, ηθικά και τεχνολογικά ζητήματα. Όταν μια πλατφόρμα εξετάζει αν ένα περιεχόμενο είναι επιτρεπτό, συχνά στηρίζεται σε βάσεις δεδομένων, το ιστορικό αλληλεπιδράσεων ή ακόμη και στη συμπεριφορική ανάλυση των χρηστών, γεγονός που δύναται να παραβιάζει τις αρχές της αναλογικότητας, της διαφάνειας και της αναγκαιότητας, όπως ορίζονται στον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ).

Η αξία της παρούσας μελέτης αποκτά μεγαλύτερη διάσταση μετά την υιοθέτηση του Κανονισμού για τις Ψηφιακές Υπηρεσίες (Digital Services Act - DSA) το 2022, ο οποίος θεσπίζει νέες υποχρεώσεις διαφάνειας και λογοδοσίας για τις πλατφόρμες, καθώς και μηχανισμούς εποπτείας από εθνικές και ευρωπαϊκές αρχές. Ο συνδυασμός του εν

λόγω Κανονισμού και του Γενικού Κανονισμού Προστασίας Δεδομένων δημιουργεί ένα νέο πλαίσιο λειτουργίας των ψηφιακών υπηρεσιών, το οποίο, ωστόσο, δεν έχει αποφορτιστεί από προκλήσεις και αντιφάσεις, ιδίως ως προς τα όρια μεταξύ της ελευθερίας της έκφρασης, της ιδιωτικότητας και της ευθύνης των πλατφορμών.

Σκοπός της παρούσας εργασίας είναι να κατανοηθεί η νομική και τεχνολογική σχέση μεταξύ του ελέγχου περιεχομένου από ψηφιακές πλατφόρμες και της προστασίας των προσωπικών δεδομένων των χρηστών, ενώ παράλληλα εξετάζονται οι νομοθετικές προβλέψεις της Ευρωπαϊκής Ένωσης, καθώς και οι πρακτικές που υιοθετούνται από τις μεγάλες τεχνολογικές πλατφόρμες, αναλύοντας ταυτόχρονα τις προκλήσεις, τα ηθικά διλήμματα και τις επιπτώσεις στην ελευθερία του λόγου και την ιδιωτικότητα. Η εργασία θα διερευνήσει τα ενδεχόμενα νομικά και κοινωνικά κενά που προκύπτουν από την εφαρμογή των πολιτικών αυτών και θα αναζητήσει λύσεις ή βελτιώσεις για την επίλυση των προκλήσεων που ενδέχεται να δημιουργηθούν στο μέλλον.

Στο πλαίσιο αυτό, η παρούσα μελέτη διαρθρώνεται σε έξι κεφάλαια, τα οποία καλύπτουν το εύρος της εν λόγω θεματικής. Στο πρώτο κεφάλαιο, παρέχεται μια εισαγωγή στο σύγχρονο ψηφιακό περιβάλλον, με ιδιαίτερη έμφαση στις προκλήσεις που αντιμετωπίζουν οι πλατφόρμες στις διαδικασίες ρύθμισης περιεχομένου και προστασίας προσωπικών δεδομένων. Στο δεύτερο κεφάλαιο, αναλύεται το θεωρητικό και εννοιολογικό πλαίσιο γύρω από τις ψηφιακές πλατφόρμες και τη διαδικασία ελέγχου περιεχομένου, με μια εκτενή αναφορά στους μηχανισμούς αυτορρύθμισης και συρρύθμισης, καθώς και στην ιδιωτική εξουσία που ασκούν οι πλατφόρμες αυτές. Στο τρίτο κεφάλαιο, ο έλεγχος περιεχομένου εξετάζεται υπό το πρίσμα των θεμελιωδών δικαιωμάτων. Ειδική έμφαση δίνεται στην ελευθερία της έκφρασης, στους περιορισμούς της στον ψηφιακό λόγο, καθώς και στις νομιμοποιητικές αιτίες παρέμβασης, όπως η ρητορική μίσους και η παραπληροφόρηση. Αναλύονται οι αρχές αναλογικότητας, αναγκαιότητας και διαφάνειας, καθώς και η σχετική νομολογία του ΕΔΔΑ και του ΔΕΕ.

Το τέταρτο κεφάλαιο αναφέρεται στην ευρωπαϊκή νομοθεσία για τις ψηφιακές πλατφόρμες, εστιάζοντας στον Κανονισμό 2022/2065 για τις Ψηφιακές Υπηρεσίες (DSA) και τις βασικές του ρυθμίσεις σχετικά με τη διαφάνεια, την εποπτεία και τη λογοδοσία των πλατφορμών. Αναλύεται η σημασία των νέων ρυθμίσεων στην ενίσχυση της προστασίας των χρηστών και στην προώθηση της διακυβέρνησης των ψηφιακών υπηρεσιών στην Ευρώπη. Στο πέμπτο κεφάλαιο, η μελέτη επικεντρώνεται στην προστασία των προσωπικών δεδομένων, εξετάζοντας τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) και τις επιπτώσεις του στην κανονιστική ρύθμιση του ψηφιακού χώρου. Επιπλέον, διερευνώνται οι νόμιμες βάσεις για την επεξεργασία προσωπικών δεδομένων, οι αρχές επεξεργασίας και οι υποχρεώσεις των πλατφορμών όσον αφορά τα δικαιώματα των χρηστών.

Το έκτο κεφάλαιο συγκεντρώνει τα συμπεράσματα της έρευνας και προτείνει μέτρα για τη βελτίωση των ρυθμιστικών μηχανισμών. Μέσα από συγκριτική θεώρηση των εθνικών πλαισίων, διατυπώνονται προτάσεις για την ενίσχυση της διαφάνειας, της λογοδοσίας και της προστασίας των θεμελιωδών δικαιωμάτων στο πλαίσιο της λειτουργίας των ψηφιακών πλατφορμών.

## 2. ΨΗΦΙΑΚΕΣ ΠΛΑΤΦΟΡΜΕΣ ΚΑΙ ΡΥΘΜΙΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ: ΘΕΩΡΗΤΙΚΟ ΚΑΙ ΕΝΝΟΙΟΛΟΓΙΚΟ ΠΛΑΙΣΙΟ

### 2.1 Η έννοια των ψηφιακών πλατφορμών

Στο σύγχρονο ψηφιακό περιβάλλον, οι πλατφόρμες δεν περιορίζονται πια στον ρόλο μιας ουδέτερης τεχνολογικής υποδομής που απλώς διευκολύνει την ανταλλαγή περιεχομένου μεταξύ χρηστών. Αντιθέτως, εξελίσσονται όλο και περισσότερο σε νέα μέσα μαζικής επικοινωνίας, τα οποία σε μεγάλο βαθμό συμπληρώνουν ή ακόμη και αντικαθιστούν τη λειτουργία του παραδοσιακού Τύπου και της ραδιοτηλεόρασης<sup>1</sup>. Στο πλαίσιο αυτό, οι πλατφόρμες δεν επιτελούν απλώς τεχνικό ρόλο, αλλά ασκούν ουσιαστικό έλεγχο επί της πληροφορίας, λειτουργώντας ως «φύλακες της πύλης» (gatekeepers) του δημόσιου λόγου, ασκώντας παράλληλα έντονη επιρροή στους πολίτες και έχοντας την ευθύνη στη διαμόρφωση της μαζικής ενημέρωσης και στην πρόσβαση τους στο σύστημα της πληροφόρησης.

Μολονότι συνιστούν ένα από τα βασικότερα φαινόμενα του ψηφιακού περιβάλλοντος, καθώς αναδιαμορφώνουν τον τρόπο με τον οποίο αλληλεπιδρούν η πληροφορία, η επικοινωνία, η οικονομία και το δίκαιο, ο όρος «πλατφόρμα» εξακολουθεί να χαρακτηρίζεται από ασάφεια και πολυσημία<sup>2</sup>. Σύμφωνα, με τον ορισμό του Gillespie, οι πλατφόρμες ορίζονται ως διαδικτυακοί τόποι ή υπηρεσίες που «φιλοξενούν, οργανώνουν και κυκλοφορούν το περιεχόμενο ή τις κοινωνικές αλληλεπιδράσεις των χρηστών», χωρίς οι ίδιες να έχουν δημιουργήσει το κύριο μέρος αυτού του περιεχομένου, λειτουργώντας πάνω σε μια υποδομή επεξεργασίας δεδομένων για ποικίλους σκοπούς, όπως η αποκόμιση κέρδους, ενώ ταυτόχρονα

---

<sup>1</sup> Ανθόπουλος Χ. (2021), Η ελευθερία της πληροφόρησης στην εποχή των ψηφιακών πλατφορμών, τεύχος 1 αρ. 1, Επιθεώρηση Δημόσιας Διοίκησης, σελ.2

<sup>2</sup> Barrie Sander (2020), Freedom of expression in the age of online platforms: The promise and pitfalls of human rights - Based approach to content moderation, p. 944 - 945

εποπτεύουν το περιεχόμενο και τη δραστηριότητα των χρηστών<sup>3</sup>. Αντίστοιχα, ο Srnicek τονίζει πως οι πλατφόρμες δεν περιορίζονται στον ρόλο απλών τεχνολογικών υποδομών, αλλά αποτελούν εκφράσεις ενός ιδιαίτερου είδους καπιταλισμού, ο οποίος στηρίζεται στην εκτενή συλλογή, την επεξεργασία και την εμπορική εκμετάλλευση των δεδομένων<sup>4</sup>.

Σημειώνεται ότι οι πλατφόρμες διαφοροποιούνται σημαντικά ως προς τις λειτουργίες τους, καθώς ορισμένες εστιάζουν κυρίως στον διαμοιρασμό βίντεο, όπως το YouTube ή το TikTok, ενώ άλλες λειτουργούν ως κοινωνικά δίκτυα, όπως το Facebook ή το X (πρώην Twitter), δίνοντας έμφαση στην αλληλεπίδραση μεταξύ των χρηστών και την παραγωγή περιεχομένου από το ίδιο το κοινό. Παράλληλα, υπάρχουν πλατφόρμες που βασίζονται σε εμπορικές συναλλαγές, όπως η Amazon, ή στην παροχή υπηρεσιών, όπως το Uber ή το Airbnb, οι οποίες, αν και δεν παράγουν περιεχόμενο με την παραδοσιακή έννοια, συγκεντρώνουν και διαχειρίζονται πληροφορίες με τρόπους που επηρεάζουν τον δημόσιο και ιδιωτικό χώρο.

Η ως άνω κατηγοριοποίηση δεν είναι μόνο λειτουργική, αλλά συνεπάγεται και σημαντικές διαφορές ως προς το είδος και την έκταση του ελέγχου περιεχομένου που δύναται να ασκηθεί. Ειδικότερα, οι πλατφόρμες κοινωνικής δικτύωσης αναλαμβάνουν τον ρόλο ρυθμιστών του περιεχομένου που αναπαράγεται, ασκώντας επιρροή επί του λόγου και της πληροφορίας με τρόπους που επηρεάζουν θεμελιώδη δικαιώματα, όπως την ελευθερία της έκφρασης και το δικαίωμα στην πληροφόρηση. Αντίθετα, οι εμπορικές πλατφόρμες συνήθως διαμορφώνουν κανόνες εποπτείας περιεχομένου με βασικό γνώμονα την οικονομική τους λειτουργία και την προστασία των εμπορικών τους συμφερόντων.

---

<sup>3</sup> Gillespie T. (2018), *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press, p. 18

<sup>4</sup> Srnicek N., (2016), *Platform Capitalism*, Polity Press, p.52

## 2.2 Ο Έλεγχος Περιεχομένου στις ψηφιακές πλατφόρμες

### 2.2.1 Η έννοια του ελέγχου περιεχομένου

Στην εποχή της ψηφιακής επικοινωνίας και της υψηλής διείσδυσης των νέων τεχνολογιών, όπου τα μέσα κοινωνικής δικτύωσης έχουν μετατραπεί σε κεντρικούς χώρους δημόσιας συζήτησης, η έννοια του ελέγχου περιεχομένου έχει αποκτήσει κομβική σημασία. Οι ίδιες οι πλατφόρμες καλούνται να διαχειρίζονται καθημερινά τεράστιες ποσότητες υλικού, το οποίο κυμαίνεται από αναρτήσεις και σχόλια έως φωτογραφίες και βίντεο. Αυτή η διαδικασία εποπτείας, φιλτραρίσματος, ιεράρχησης ή και αφαίρεσης περιεχομένου κρίνεται απαραίτητη, όχι μόνο για την προστασία των χρηστών από υλικό που δύναται να είναι παράνομο, επιβλαβές ή παραπλανητικό, αλλά και για την τήρηση των νομικών υποχρεώσεων με σκοπό την διασφάλιση ενός αξιόπιστου ψηφιακού περιβάλλοντος.

Ωστόσο, ο καθορισμός της εν λόγω έννοιας δεν είναι μονοδιάστατος, αλλά μπορεί να πάρει διαφορετικές μορφές, από τον άμεσο αποκλεισμό ενός επιβλαβούς σχολίου έως την πιο διακριτική ρύθμιση της προβολής περιεχομένου μέσω αλγορίθμων. Εν στενή έννοια, ο έλεγχος περιεχομένου (content moderation) αναφέρεται στην διαδικασία κατά την οποία μια εταιρεία που φιλοξενεί διαδικτυακό περιεχόμενο αξιολογεί την παράνομη φύση ή τη συμβατότητα του περιεχομένου των χρηστών με τους όρους χρήσης της.<sup>5</sup> Στη συνέχεια, βάση αυτής της αξιολόγησης αποφασίζεται εάν το περιεχόμενο αυτό θα υποβαθμιστεί παραμένοντας online με μειωμένη προβολή (shadow banning), αν θα επισημανθεί ως δυνητικά ακατάλληλο ή εσφαλμένο, αν θα απομονωθεί από την εμπορική αξιοποίηση (demonetized)<sup>6</sup> ή αν θα παραμείνει

---

<sup>5</sup> Council of Europe (2021), Content Moderation: Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation (Guidance Note), Adopted by the Steering Committee for Media and Information Society (CDMSI)

<sup>6</sup> Ορισμένες πλατφόρμες επιτρέπουν στον χρήστη να «κερδοσκοπεί» από το περιεχόμενο που αναρτά. Ωστόσο, υπάρχει η δυνατότητα της κατάργησης αυτών των αμοιβών σε ορισμένες

προσβάσιμο ή θα αφαιρεθεί ολικά (take - down). Εν ευρεία έννοια, ο έλεγχος περιεχομένου προσομοιάζει σε ψηφιακή επιμέλεια (content curation), κατά την οποία η διαδικασία επιλογής, διαχείρισης και παρουσίασης της πληροφορίας στους χρήστες περιλαμβάνει προληπτικές ή έμμεσες πρακτικές, ανάλογα με το επιχειρηματικό μοντέλο και το σχεδιασμό της πλατφόρμας<sup>7</sup>. Στόχος είναι η ανάδειξη ποιοτικού και αξιόπιστου περιεχομένου σε έναν υπερκορεσμένο πληροφοριακό χώρο μέσα από αλγοριθμικές ή άλλες μεθόδους. Ενδεικτικά, χρησιμοποιούνται τεχνικές όπως η ομαδοποίηση υλικού σε θεματικές ενότητες, η εξατομίκευση, σύμφωνα με τα ενδιαφέροντα κάθε χρήστη, και η σύνοψη, η οποία βοηθά στην πιο εύκολη κατανόηση των πληροφοριών.

### **2.2.2. Αυτορρύθμιση (self – regulation) και Συρρύθμιση (co - regulation)**

Για την πληρέστερη κατανόηση των ως άνω εννοιών, ήτοι του ελέγχου και της επιμέλειας περιεχομένου, κρίνεται σκόπιμο να τοποθετηθούν μέσα στο γενικότερο πλαίσιο της διακυβέρνησης του ψηφιακού χώρου. Οι τρόποι με τους οποίους οι πλατφόρμες αποφασίζουν ποιο περιεχόμενο προβάλλεται, περιορίζεται ή αφαιρείται δεν είναι τυχαίοι, αλλά συνδέονται άμεσα με το ποιος έχει την εξουσία να θέτει τους κανόνες, πώς αυτοί εφαρμόζονται στην πράξη και ποιος εποπτεύει την όλη διαδικασία. Συνεπώς, οι έννοιες της αυτορρύθμισης και της συρρύθμισης αποκτούν κομβική σημασία, καθώς μας βοηθούν να κατανοήσουμε πώς μοιράζεται η ευθύνη μεταξύ ιδιωτικών εταιρειών και δημόσιων αρχών στη διαχείριση του ψηφιακού περιεχομένου.

---

περιπτώσεις. Π.χ. βλ. πολιτική δημιουργίας εσόδων καναλιού στο YouTube Διαθέσιμο: <https://support.google.com/youtube/answer/6162278> (τελευταία πρόσβαση 22/05/2025)

<sup>7</sup> Council of Europe (2021), Content Moderation: Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation (Guidance Note), ο.π.

Από τη μια μεριά, η αυτορρύθμιση (self - regulation) αναφέρεται στη διαδικασία κατά την οποία, οι ίδιες οι διαδικτυακές πλατφόρμες (όπως πχ. η Meta, το TikTok ή το YouTube) θεσπίζουν τους κανόνες λειτουργίας, τις εσωτερικές πολιτικές και εν γένει τους μηχανισμούς εποπτείας, χωρίς κυβερνητική ενθάρρυνση. Η Οδηγία 2010/13/ΕΕ για τις Οπτικοακουστικές Υπηρεσίες Μέσων (Audiovisual Media Services Directive, στο εξής «AVMS»)<sup>8</sup> της Ευρωπαϊκής Ένωσης παρέχει μια περιγραφή του τι νοείται ως αυτορρύθμιση, χωρίς, ωστόσο, να περιλαμβάνει κάποιο σαφή ορισμό. Έτσι, αναφέρει το εξής «Η αυτορρύθμιση αποτελεί έναν τύπο εθελοντικής πρωτοβουλίας, μέσω της οποίας οικονομικοί φορείς, κοινωνικοί εταίροι, μη κυβερνητικές οργανώσεις και ενώσεις θεσπίζουν κοινές κατευθυντήριες γραμμές, τις οποίες δεσμεύονται να αναπτύξουν, να επιβλέψουν και να εφαρμόσουν». Η πρακτική αυτή βασίζεται, επομένως, στην πεποίθηση ότι οι ίδιες οι εταιρείες έχουν την τεχνογνωσία, την ευελιξία και τα κίνητρα για να ανταποκριθούν άμεσα σε προβλήματα, όπως η παραπληροφόρηση, η ρητορική μίσους ή το επιβλαβές περιεχόμενο. Εκτιμάται ότι δύναται να ενεργούν πιο γρήγορα από τα κρατικά όργανα, προσαρμόζοντας τους κανόνες τους στις ανάγκες των χρηστών και στις αλλαγές της αγοράς.

Ένα παράδειγμα αυτορρύθμισης αποτελεί η πλατφόρμα της ηλεκτρονικής εγκυκλοπαίδειας Wikipedia, η οποία επιτυγχάνει τη διαδικασία ελέγχου του περιεχομένου της μέσω ελεγκτών, γνωστών ως «wikipedians» και ακαδημαϊκών μελών του Wiki Education Foundation<sup>9</sup>. Σημειώνεται, βέβαια, ότι η ανεξαρτησία και η ουδετερότητα των τρίτων ελεγκτών δεν είναι τυχαία. Τούτο διότι, η ανεξαρτησία τους μεταθέτει το βάρος του καταλογισμού σε αυτούς και όχι στην πλατφόρμα κοινωνικής

---

<sup>8</sup> Οδηγία 2010/13/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον συντονισμό ορισμένων νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών σχετικά με την παροχή υπηρεσιών οπτικοακουστικών μέσων (οδηγία για τις υπηρεσίες οπτικοακουστικών μέσων)

<sup>9</sup> Βλ. Wikipedia and fact-checking. Διαθέσιμο στο: [https://en.wikipedia.org/wiki/Wikipedia\\_and\\_fact-checking](https://en.wikipedia.org/wiki/Wikipedia_and_fact-checking) (τελευταία πρόσβαση 25/06/2025)

δικτύωσης, η οποία αποφεύγει την κατηγορία της λογοκρισίας και παρουσιάζεται ως προασπιστής της ελευθερίας του λόγου.

Παρ' όλα αυτά, το μοντέλο αυτό συχνά εγείρει ανησυχίες, καθώς οι αποφάσεις λαμβάνονται χωρίς εξωτερικό έλεγχο, διαφάνεια και δημοκρατική λογοδοσία. Είναι προφανές ότι όταν τα κίνητρα του παρόχου δεν ευθυγραμμίζονται με τα συμφέροντα του ρυθμιστή ή των χρηστών, η αυτορρύθμιση είναι λιγότερο πιθανό να αποδώσει<sup>10</sup>. Σε έναν ψηφιακό κόσμο όπου λίγες μεγάλες πλατφόρμες συγκεντρώνουν τεράστια δύναμη, είναι εύλογος ο φόβος ότι οι αποφάσεις τους καθοδηγούνται, κυρίως, από επιχειρηματικά συμφέροντα και όχι από το κοινό καλό.

Από την άλλη πλευρά, η συρρύθμιση (co-regulation), λειτουργεί ως ένα υβριδικό μοντέλο συνεργασίας ανάμεσα στον κρατικό έλεγχο και την πλήρη αυτονομία των πλατφορμών<sup>11</sup>. Σε αυτό το νομικό πλαίσιο, οι εταιρείες δεν λειτουργούν μόνες τους, αλλά συνεργάζονται με δημόσιες αρχές, ρυθμιστικά σώματα ή ανεξάρτητους φορείς για να ρυθμίσουν τις υποθέσεις τους μέσω κωδίκων δεοντολογίας και να εφαρμόσουν κοινούς κανόνες. Στην ουσία, πρόκειται για μια «ρυθμιζόμενη αυτορρύθμιση», στην οποία υπάρχει διαδραστική σχέση μεταξύ του ρυθμιστή και του ρυθμιζόμενου φορέα<sup>12</sup>.

Ένα ενδεικτικό παράδειγμα αυτής της πρακτικής στην ψηφιακή οικονομία είναι η συνεργασία της Airbnb με πόλεις όπως το Παρίσι και η Κοπεγχάγη για θέματα

---

<sup>10</sup> Council of Europe (2021), Content Moderation: Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation (Guidance Note). Adopted by the Steering Committee for Media and Information Society (CDMSI), p.39

<sup>11</sup> Williams N. J. - Malmgren F. N. (2019), The Platform Policy Puzzle: Forms of Regulating Multi-Sided Platforms in Nine European Cities, MSc Thesis, Copenhagen Business School, p. 102

<sup>12</sup> Finck M. (2017), Digital Revolution: Designing a Supranational Legal Framework for the Platform Economy, LSE Legal Studies Working Paper No. 15/2017, p. 16

φορολόγησης και τήρησης των κανονισμών. Σε αυτές τις περιπτώσεις, διαμορφώνεται ένας μηχανισμός συνεργασίας, στον οποίο εμπλέκονται τόσο οι αρμόδιες δημόσιες αρχές όσο και η ίδια η πλατφόρμα, με στόχο την επίτευξη συγκεκριμένων κανονιστικών στόχων, όπως είναι η είσπραξη του τουριστικού φόρου. Η Airbnb, προσαρμόζοντας το λογισμικό της, ανέλαβε την αυτόματη είσπραξη και απόδοση του φόρου διαμονής για λογαριασμό των ιδιοκτητών, μεταφέροντας έτσι ένα τμήμα της διοικητικής ευθύνης από το δημόσιο προς την ιδιωτική πλατφόρμα. Με αυτόν τον τρόπο, μειώνεται το κόστος για το δημόσιο και παράλληλα ενισχύεται η φορολογική συνέπεια των χρηστών.

Κύριος στόχος της συρρύθμισης είναι, επομένως, να βρεθεί μια ισορροπία μεταξύ της δημοκρατικής εποπτείας και της ευελιξίας του ιδιωτικού τομέα. Παρολ' αυτά, η επιτυχία του ως άνω συστήματος ρύθμισης περιεχομένου έγκειται στη διαφάνεια των διαδικασιών και στο αν οι συμμετέχοντες εκπροσωπούν ισότιμα όλα τα εμπλεκόμενα συμφέροντα, τόσο του ιδιωτικού όσο και του δημοσίου τομέα.

### **2.2.3 Μηχανισμοί Ελέγχου Περιεχομένου**

Η ανάγκη για την εποπτεία και διαχείριση του αναρτώμενου περιεχομένου έχει καταστεί επιτακτική, ιδίως αν λάβουμε υπόψη ότι οι πλατφόρμες κοινωνικής δικτύωσης και ανταλλαγής περιεχομένου έχουν μετατραπεί σε κεντρικά μέσα δημόσιου διαλόγου. Στην πράξη, αυτό επιτυγχάνεται άλλοτε μέσω μηχανισμών αλγοριθμικής ανίχνευσης και άλλοτε μέσω της ανθρώπινης παρέμβασης.

Παρά την αυξανόμενη στροφή προς την αυτοματοποίηση της εποπτείας του ψηφιακού περιεχομένου, η ανθρώπινη εποπτεία εξακολουθεί να αποτελεί κομβικό και αναντικατάστατο στοιχείο των μηχανισμών ελέγχου. Οι επιμελητές περιεχομένου (content moderators) λειτουργούν ως το τελικό στάδιο αξιολόγησης αναρτήσεων που έχουν είτε εντοπιστεί από αλγορίθμους είτε επισημανθεί από χρήστες. Η αρμοδιότητα τους εστιάζει στη χειροκίνητη εξέταση αναρτήσεων,

κειμένων, εικόνων, βίντεο και συνδέσμων, με στόχο την επιβεβαίωση ή μη της παραβίασης των όρων χρήσης της έκαστης πλατφόρμας ή/ και της σχετικής νομοθεσίας. Σε πλατφόρμες, όπως το Facebook ή το Instagram, όταν ένας χρήστης επισημαίνει (report) μια ανάρτηση ως ακατάλληλη, σε πρώτο στάδιο, αυτή ελέγχεται από έναν αυτοματοποιημένο αλγόριθμο φιλτραρίσματος, και έπειτα, σε περίπτωση αμφισβησίας, παραπέμπεται σε έναν ανθρώπινο συντονιστή, ο οποίος καλείται να δράσει με βάση τα συμφραζόμενα και τις εσωτερικές πολιτικές της πλατφόρμας<sup>13</sup>.

Εξίσου σημαντικός είναι και ο ρόλος των οργανισμών επαλήθευσης πληροφοριών (fact-checkers), οι οποίοι λειτουργούν ως εξωτερικοί φορείς επαλήθευσης της εγκυρότητας πληροφοριών που διακινούνται στο διαδίκτυο. Ο έλεγχος αυτός εστιάζει, ως επί το πλείστον, σε θέματα δημόσιου ενδιαφέροντος, όπως η υγεία, η πολιτική, οι κλιματικές αλλαγές κτλ. Για παράδειγμα, το Facebook, το οποίο συνεργάζεται με έναν αριθμό πιστοποιημένων fact-checking οργανισμών, στο πλαίσιο του International Fact-Checking Network (IFCN)<sup>14</sup>, όταν αναπαραχθεί μια ανάρτηση με ψευδή πληροφορία δύναται να την επισημάνει με προειδοποιητική ένδειξη ή να υποβιβάσει την ορατότητά της (downranking).

Στην πραγματικότητα, όμως, μεγάλο μέρος της εποπτείας του περιεχομένου ανατίθεται μέσω εργολαβικών σχέσεων, σε υπεργολάβους που εδρεύουν κυρίως σε τρίτες χώρες, στο πλαίσιο ενός παγκοσμιοποιημένου καταμερισμού ψηφιακής εργασίας<sup>15</sup>. Οι εν λόγω εργαζόμενοι παραμένουν αόρατοι στον δημόσιο λόγο και είναι συχνά ανεπαρκώς αμειβόμενοι και τοποθετημένοι σε αντίξοα περιβάλλοντα στερούμενοι επαρκών υποστηρικτικών μηχανισμών προστασίας. Οι συνθήκες αυτές τείνουν να αυξάνουν την εργασιακή πίεση και το ψυχολογικό φορτίο, γεγονός το

---

<sup>13</sup> Gillespie T. (2018), ο.π., σελ. 91

<sup>14</sup> βλ. <https://www.poynter.org/ifcn/> (τελευταία πρόσβαση 26/06/2025)

<sup>15</sup> Roberts S. T. (2019), Behind the Screen: Content Moderation in the Shadows of Social Media, Yale University Press, p. 203 επ.

οποίο οδηγεί σε δεοντολογικά διλήμματα, καθώς οι αποφάσεις τους αφορούν τον περιορισμό ή την διατήρηση περιεχομένου που δύναται να είναι κοινωνικά ή πολιτικά αμφιλεγόμενο. Συνεπώς, ο ρόλος τους δεν είναι απλώς τεχνικός ή διοικητικός, αλλά άπτεται θεμελιωδών ερωτημάτων περί ελευθερίας της έκφρασης, λογοδοσίας και διαφάνειας.

Σημειώνεται, βέβαια, ότι η αλματώδης αύξηση του όγκου των δεδομένων, σε συνδυασμό με την ταχύτητα μετάδοσης και τη διασυνοριακή φύση των πληροφοριών, έχουν δυσχεράνει την αποκλειστικά ανθρώπινη επιτήρηση του ψηφιακού λόγου. Ως απάντηση στις ως άνω προκλήσεις, οι πλατφόρμες έχουν υιοθετήσει ένα πλέγμα τεχνικών και οργανωτικών μηχανισμών ελέγχου περιεχομένου, που αποτελούνται από αυτοματοποιημένα αλγοριθμικά φίλτρα.

Η μέθοδος της αλγοριθμικής αντιστοίχισης περιεχομένου (content matching) αποτελεί μια από τις κυρίαρχες πρακτικές των πλατφορμών για τον έλεγχο, το φιλτράρισμα και την απομάκρυνση παράνομου ή επιβλαβούς υλικού στο διαδίκτυο. Ειδικότερα, πρόκειται για την αναγνώριση εικόνων ή βίντεο μέσω συστημάτων, όπως το perceptual hashing<sup>16</sup>, δηλαδή την παραγωγή ψηφιακών «αποτυπωμάτων» (hashes) που «χαρτογραφούν» την οπτική ή ακουστική ταυτότητα ενός αρχείου, ώστε να παραμείνει το περιεχόμενο του αναγνωρίσιμο ακόμη και μετά από τροποποιήσεις. Οι πλατφόρμες, μέσω των αλγορίθμων αυτών, συγκρίνουν κάθε νέο αρχείο με υπάρχουσες καταχωρήσεις σε βάσεις δεδομένων απαγορευμένου υλικού, αναζητώντας απόλυτες ή σχετικές ομοιότητες. Χαρακτηριστικό παράδειγμα αποτελεί η τεχνολογία αναγνώρισης εικόνων PhotoDNA, η οποία αξιοποιεί μορφές

---

<sup>16</sup> Barrie Sander (2020), Freedom of expression in the age of online platforms: The promise and pitfalls of human rights - Based approach to content moderation, p. 946

perceptual hashing για τον αυτόματο εντοπισμό υλικού παιδικής σεξουαλικής κακοποίησης ή/και πορνογραφίας (Child Sexual Abuse Material - CSAM)<sup>17</sup>.

Εξίσου σημαντικός μηχανισμός ελέγχου περιεχομένου είναι η αλγοριθμική ταξινόμηση (classification algorithm), η οποία αποτελεί μια μορφή εποπτευόμενης μάθησης (supervised learning), όπου ο αλγόριθμος τροφοδοτείται με ένα σύνολο δεδομένων που έχουν ήδη επισημανθεί (labelled data), ώστε να μάθει επαγωγικά να εξαγάγει μία συνάρτηση, βάσει της οποίας θα προβεί στο μέλλον σε ταξινόμηση άλλων δεδομένων, τα οποία συναντά πρώτη φορά. Με αυτό τον τρόπο, το σύστημα «μαθαίνει» να προβλέπει την ετικέτα ενός νέου δείγματος βάσει των χαρακτηριστικών των δεδομένων εκπαίδευσης. Τέτοιου είδους αλγόριθμοι βρίσκουν εφαρμογή σε ποικίλα πεδία, όπως για παράδειγμα στο φιλτράρισμα ανεπιθύμητου περιεχομένου (spam filtering). Για να μπορέι, δηλαδή, ο αλγόριθμος να προσδιορίσει εάν ένα e-mail είναι ανεπιθύμητο, χρειάζεται να εκπαιδευτεί πρώτα με ένα δείγμα μηνυμάτων που έχουν ήδη χαρακτηριστεί ως ανεπιθύμητα ή μη. Μέσα από αυτά μαθαίνει, λοιπόν, να αναγνωρίζει τα στοιχεία που συνήθως έχει η ανεπιθύμητη αλληλογραφία. Συνεπώς, ένα e-mail θα χαρακτηρίζεται ως ανεπιθύμητο επειδή, θα περιέχει πχ. συγκεκριμένες λέξεις - κλειδιά ή θα έχει σταλεί από έναν συγκεκριμένο τύπο διεύθυνσης.

Τέλος, μια τρίτη μορφή αλγοριθμικού ελέγχου είναι οι αλγόριθμοι κατάταξης (ranking algorithms), οι οποίοι χρησιμοποιούνται για να δημιουργούν σύντομες λίστες επιλέγοντας στοιχεία από ένα μεγαλύτερο σύνολο δεδομένων ή για να ταξινομούν τα στοιχεία σύμφωνα με προκαθορισμένα κριτήρια<sup>18</sup>. Στην ουσία, ρυθμίζουν τη σειρά εμφάνισης των αναρτήσεων, περιορίζοντας τη διάδοση περιεχομένου που θεωρείται

---

<sup>17</sup> Barrie Sander (2020), ο.π.

<sup>18</sup> French Autorité de la concurrence & the German Bundeskartellamt (2019), Algorithms and competition, joint study, p. 6

υψηλού κινδύνου για την κοινότητα<sup>19</sup>. Η προβολή, η ενίσχυση ή η υποβάθμιση μιας ανάρτησης, ακόμη και αν δεν αφαιρεθεί, επηρεάζει άμεσα τη δημόσια ορατότητά της και, συνακόλουθα, τη διάχυσή της στο ψηφιακό οικοσύστημα. Αυτού του τύπου οι αλγόριθμοι χρησιμοποιούνται κυρίως από πλατφόρμες που συγκρίνουν τιμές και προϊόντα, όπως το Skrutz, αλλά και από εφαρμογές, μηχανές αναζήτησης ή ακόμη και από τα κοινωνικά δίκτυα, για να οργανώνουν και να εμφανίζουν το περιεχόμενο στην αρχική σελίδα κάθε χρήστη με βάση τις ανάγκες και την αρέσκεια του.

Η αλληλεπίδραση ανάμεσα σε αλγοριθμικά συστήματα και ανθρώπινους επόπτες περιεχομένου συνιστά μια μορφή συνδυαστικής διακυβέρνησης, η οποία επιδιώκει να εξισορροπήσει τα πλεονεκτήματα της αυτοματοποιημένης αποδοτικότητας με την ανθρώπινη ικανότητα κατανόησης των συμφραζομένων. Ωστόσο, η κατανομή ευθύνης παραμένει προβληματική, καθώς οι πλατφόρμες συχνά αποκρύπτουν το εύρος και τις συνθήκες της ανθρώπινης εποπτείας, προκαλώντας μια εντύπωση τεχνολογικής αυτορρύθμισης<sup>20</sup>. Παράλληλα, η έλλειψη θεσμικού ελέγχου και οι διαφορετικές πολιτισμικές αντιλήψεις για την έννοια της «παραβίασης» οδηγούν σε ασυμμετρικές εφαρμογές, εγείροντας ερωτήματα για την ισονομία και τη διαφάνεια της εποπτείας<sup>21</sup>.

### **2.3 Οι ψηφιακές πλατφόρμες ως φορείς ιδιωτικής αλλά de facto θεσμικής εξουσίας**

Η ανάλυση που προηγήθηκε ανέδειξε τον τρόπο με τον οποίο οι ψηφιακές πλατφόρμες εφαρμόζουν μηχανισμούς ελέγχου περιεχομένου με τεχνολογικά και κανονιστικά εργαλεία. Σημειώνεται, βέβαια, ότι στην πράξη, η δυνατότητα

---

<sup>19</sup> Geiger R. S. (2014), Bots, bespoke, code and the materiality of software platforms: Wikipedia's infrastructure and governance, *Information, Communication & Society*, 17(1), p. 30 - 44

<sup>20</sup> Gillespie T. (2018), ο.π., p. 111 επ.

<sup>21</sup> Suzor N. (2019), *Lawless: The Secret Rules that Govern Our Digital Lives*, Cambridge University Press, p. 165

κατάρτισης κανόνων χρήσης, ο αλγοριθμικός έλεγχος ορατότητας και η απόφαση για τον αποκλεισμό ή διατήρηση περιεχομένου καθιστούν τις πλατφόρμες κανονιστικούς φορείς με χαρακτηριστικά που προσομοιάζουν σε θεσμική εξουσία. Έτσι, από απλοί πάροχοι υποδομών επικοινωνίας, οι πλατφόρμες μετατρέπονται σε καθοριστικούς «διαχειριστές» του δημόσιου λόγου<sup>22</sup>.

Η μετατόπιση αυτή έχει χαρακτηριστεί στη διεθνή βιβλιογραφία ως ιδιωτικοποίηση της ρύθμισης του λόγου (private governance of speech), ενώ παράλληλα γίνεται αναφορά για μια «παράλληλη κανονιστική τάξη»<sup>23</sup>, καθώς οι πλατφόρμες θεσπίζουν όρους και κανόνες κοινότητας (community standards) που λειτουργούν πρακτικά ως κώδικες συμπεριφοράς<sup>24</sup>. Ωστόσο, αυτός ο τρόπος λειτουργίας των πλατφορμών συχνά δεν υπόκειται σε ουσιαστικό δημοκρατικό έλεγχο ούτε συνοδεύεται από ισχυρές συνταγματικές εγγυήσεις, με αποτέλεσμα να γεννιούνται ανησυχίες για το αν προστατεύονται επαρκώς η ελευθερία της έκφρασης και τα προσωπικά δεδομένα των χρηστών. Όπως επισημαίνει ο Balkin, οι πλατφόρμες θα έπρεπε να λειτουργούν ως «θεματοφύλακες της πληροφορίας» (information fiduciaries), φροντίζοντας όχι μόνο τα δικά τους οικονομικά συμφέροντα αλλά και τα δικαιώματα των ανθρώπων που τις χρησιμοποιούν<sup>25</sup>. Στην Ευρωπαϊκή Ένωση, αυτό το πρόβλημα αναγνωρίζεται πλέον ρητά μέσα από τον Κανονισμό για τις Ψηφιακές Υπηρεσίες (DSA), ο οποίος φέρνει νέους κανόνες για περισσότερη διαφάνεια, έλεγχο και υπευθυνότητα απέναντι στην εξουσία των πλατφορμών<sup>26</sup>.

---

<sup>22</sup> Suzor N. (2019), ο.π., σελ. 14 επ.

<sup>23</sup> Klonick K. (2018), The New Governors: The People, Rules, and Processes Governing Online Speech, 131 Harvard Law Review, p. 1650 επ.

<sup>24</sup> Gillespie T. (2018), ο.π., σελ. 47 επ.

<sup>25</sup> Balkin J. (2016), Information Fiduciaries and the First Amendment, 49 UC Davis Law Review 1183, p. 1227

<sup>26</sup> Αιτιολογικές Σκέψεις 25 - 27 και άρθρα 14 -17 του Κανονισμού (ΕΕ) 2022/2065

Συνεπώς, καθίσταται σαφές ότι η συζήτηση για τον έλεγχο περιεχομένου δεν μπορεί να περιοριστεί στη λειτουργία αλγορίθμων ή τεχνικών φίλτρων. Αντιθέτως, απαιτείται μια ευρύτερη θεώρηση που θα αναγνωρίζει τον ρόλο των πλατφορμών ως κεντρικών παραγόντων της ψηφιακής δημόσιας σφαίρας και θα θέτει όρια που να συνάδουν με τις αρχές του κράτους δικαίου.

### 3. Ο ΕΛΕΓΧΟΣ ΠΕΡΙΕΧΟΜΕΝΟΥ ΥΠΟ ΤΟ ΠΡΙΣΜΑ ΘΕΜΕΛΙΩΔΩΝ ΔΙΚΑΙΩΜΑΤΩΝ: ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΕΞΙΣΟΡΡΟΠΗΣΗ

#### 3.1 Η μετάβαση από την τεχνική πρακτική σε θεσμικό πρόβλημα

Η αρωγή των παγκόσμιας εμβέλειας ψηφιακών πλατφορμών στη διασυνοριακή διακίνηση της πληροφορίας και στη διαμόρφωση του δημοσίου λόγου συνοδεύεται με την παράλληλη ανάδυση αναπόφευκτων ζητημάτων ανθρωπίνων δικαιωμάτων. Τούτο διότι, ο έλεγχος του περιεχομένου των πλατφορμών αυτών δεν αποτελεί πλέον μια ουδέτερη ή αμιγώς τεχνική διαδικασία, αλλά ενέχει κριτικές με θεσμικό, νομικό και πολιτικό βάρος, καθώς επηρεάζει άμεσα την ελευθερία της έκφρασης, την πρόσβαση στην πληροφορία, την ιδιωτική ζωή, αλλά και τη δικαιοκρατική διασφάλιση των χρηστών έναντι αυθαιρέτων παρεμβάσεων.

Ειδικότερα, οι ψηφιακές πλατφόρμες, σε οποιαδήποτε μορφή τους, από κοινωνικά δίκτυα έως μηχανές αναζήτησης, δεν αποτελούν πλέον ουδέτερες υποδομές, αλλά ενεργούς διαμορφωτές του δημοσίου λόγου. Παίρνουν κρίσιμες αποφάσεις, όπως το ποιες απόψεις θα αναδειχθούν, ποιες θα αποσιωπηθούν και ποιες θα αφαιρεθούν ως «επιβλαβείς» ή «παραβιαστικές», εφαρμόζοντας όρους χρήσης χωρίς δημοκρατική νομιμοποίηση<sup>27</sup>. Η νομική πρόκληση για την πολιτεία είναι να οριοθετηθεί η εξουσία των πλατφορμών και να διασφαλιστεί ότι η παρέμβαση στον λόγο δεν θα συνεπάγεται με αυθαίρετες ή περιοριστικές πρακτικές, αλλά θα επιτυγχάνεται με γνώμονα την αρχή της διαφάνειας, της αναλογικότητας και της λογοδοσίας, σύμφωνα με τις απαιτήσεις του κράτους δικαίου.

Στο πλαίσιο αυτό, η παρούσα ενότητα επιχειρεί να αναδείξει τα θεμελιώδη δικαιώματα που πλήττονται ή διακυβεύονται κατά την εφαρμογή των ως άνω μηχανισμών ελέγχου περιεχομένου, είτε πρόκειται για αλγοριθμικά συστήματα είτε

---

<sup>27</sup> Balkin J. M. (2018), Free Speech in the Algorithmic Society, UC Davis Law Review, 51(3), p. 1149–1210

για ανθρώπινη εποπτεία. Παράλληλα, εξετάζεται το περίπλοκο έργο της εξισορρόπησης μεταξύ των αντικρουόμενων δικαιωμάτων και συμφερόντων, όπως είναι η ανάγκη για καταπολέμηση της παραπληροφόρησης, της ρητορικής μίσους και των ψευδών ειδήσεων, τα οποία έρχονται αντιμέτωπα με τον κίνδυνο της ελευθερίας της έκφρασης, της ασφάλειας, της έμμεσης λογοκρισίας και της ίσης μεταχείρισης στον ψηφιακό χώρο.

### **3.2 Η ελευθερία της έκφρασης και οι περιορισμοί της στον ψηφιακό λόγο**

Η ελευθερία της έκφρασης αποτελεί θεμελιώδες, όχι μόνο συνταγματικό, αλλά και υπερεθνικό δικαίωμα, το οποίο κατοχυρώνεται τόσο στο Σύνταγμα<sup>28</sup> όσο και σε ευρωπαϊκά και διεθνή νομοθετήματα<sup>29</sup>. Ειδικότερα, το άρθρο 10 της ΕΣΔΑ δεν προστατεύει μόνο το περιεχόμενο και την ουσία των απόψεων αλλά και τον τρόπο και το μέσο της έκφρασης<sup>30</sup>. Αντίστοιχα, στο άρθρο 14 του Συντάγματος, μολονότι αναφέρεται η γραπτή και δια του τύπου έκφραση, κατοχυρώνεται, αναμφίβολα, και η έκφραση γνώμης μέσω του διαδικτύου<sup>31</sup>. Ουσιαστικά, το δικαίωμα αυτό δεν περιλαμβάνει μόνο την ελευθερία διατύπωσης απόψεων, αλλά και την πρόσβαση σε πληροφορίες και τη διάδοσή τους χωρίς περιορισμούς, ανεξαρτήτως μέσου. Σε μια σύγχρονη δημοκρατία, η έκφραση αποτελεί προϋπόθεση για τη δημόσια συμμετοχή, τη λογοδοσία των εξουσιών και την κοινωνική πολυφωνία.

Σημειώνεται, βέβαια, ότι σύμφωνα με τη διεθνή νομολογία και τη πρακτική των κρατών η ελευθερία της έκφρασης δεν είναι απόλυτη. Αντιθέτως, υπόκειται υπό προϋποθέσεις σε περιορισμούς, εφόσον αυτοί προβλέπονται εκ νόμου, εξυπηρετούν

---

<sup>28</sup> Άρθρο 14 του Συντάγματος

<sup>29</sup> Άρθρο 10 της ΕΣΔΑ και Άρθρο 11 του ΧΘΔΕΕ

<sup>30</sup> Σισιλιάνος Λ. Α. (2017), Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου, εκδόσεις Νομική Βιβλιοθήκη, Αθήνα, σελ. 478

<sup>31</sup> Μαντζούφας Π. (2016), Νομικά ζητήματα από την χρήση του διαδικτύου: η ελευθερία της έκφρασης στα ιστολόγια, σελ. 8

θεμιτούς σκοπούς (όπως πχ. η προστασία της εθνικής ασφάλειας, της δημόσιας τάξης, της υγείας), και είναι αναγκαίοι και αναλογικοί σε μια δημοκρατική κοινωνία<sup>32</sup>. Οι αρχές αυτές έχουν επιβεβαιωθεί επανειλημμένα από το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου, το οποίο επισημαίνει ότι ακόμη και ο προσβλητικός ή ενοχλητικός λόγος προστατεύεται, στο μέτρο που συμβάλλει στον δημόσιο διάλογο<sup>33</sup>.

Πάντως, στην εποχή των ψηφιακών πλατφορμών, η ισορροπία μεταξύ της προστασίας της έκφρασης και της ανάγκης για παρέμβαση καθίσταται πιο σύνθετη. Η ρητορική μίσους, η παραπληροφόρηση, η διαδικτυακή παρενόχληση, αλλά και οι ψευδείς ειδήσεις (fake news), εγείρουν ερωτήματα ως προς το ποιες κατηγορίες λόγου επιτρέπεται ή επιβάλλεται να περιοριστούν. Όμως, η έλλειψη ενός κοινού ορισμού της έννοιας «παράνομο περιεχόμενο» οδηγεί τις πλατφόρμες σε σύγχυση, γεγονός που εγκυμονεί κινδύνους υπερβολικών ή αδιαφανών περιορισμών<sup>34</sup>.

Ένα ακόμη φαινόμενο που έχει προκαλέσει ανησυχία είναι αυτό της «αυτολογοκρισίας» (chilling effect), σύμφωνα με το οποίο οι χρήστες αποφεύγουν να διατυπώσουν γνώμες ή να συμμετάσχουν σε διαδικτυακές συζητήσεις υπό τον φόβο αφαίρεσης του περιεχομένου, ακόμη και όταν ο λόγος τους ή η έκφραση τους δεν υπόκειται σε κάποια παρανομία. Παρατηρείται, επομένως, ότι η λειτουργία αλγοριθμικών φίλτρων ή η εφαρμογή ανελαστικών πολιτικών εποπτείας περιεχομένου δύναται να οδηγήσει σε υπερβολική αφαίρεση, δηλαδή την αφαίρεση όχι μόνο παράνομου λόγου, αλλά και νόμιμου, καταστρατηγώντας τη δημοκρατική πολυφωνία<sup>35</sup>.

---

<sup>32</sup> ΕΔΔΑ, Απόφαση της 7ης Δεκεμβρίου 1976, Handyside κατά Ηνωμένου Βασιλείου, No. 5493/72, σκ. 49

<sup>33</sup> ΕΔΔΑ, Απόφαση της 8ης Ιουλίου 1986, Lingens κατά Αυστρίας, No. 9815/82, σκ. 41.

<sup>34</sup> Balkin J. M. (2018), ο.π., p. 1149–1210

<sup>35</sup> Barendt E. (2005), Freedom of Speech, Oxford University Press, p. 35

Συνεπώς, καθίσταται αναγκαίο να διαμορφωθεί ένα σύστημα κανόνων και εγγυήσεων, το οποίο να επιτρέπει την εποπτεία του περιεχομένου χωρίς να καταλύει την έκφραση, ενσωματώνοντας τις αρχές της αναλογικότητας, διαφάνειας, και του δικαιώματος σε προσφυγή. Ταυτόχρονα, πρέπει τα κράτη να λάβουν υπόψη τους ότι όσο πιο επείγουσα είναι η ανάγκη επιβολής περιορισμών, τόσο πιο κρίσιμη είναι η αποτελεσματικότητα και η λογοδοσία αυτών των μέτρων. Οι μηχανισμοί διαφάνειας, επανεξέτασης και προσαρμογής είναι απαραίτητοι και δεν πρέπει να θεωρούνται δευτερεύοντες λόγω του επείγοντος χαρακτήρα των παρεμβάσεων<sup>36</sup>.

### ***3.2.1 Ρητορική Μίσους, Παραπληροφόρηση και Ψευδείς Ειδήσεις (Fake News) ως Νομιμοποιητικοί Λόγοι Παρέμβασης***

Η εμφάνιση και, σταδιακά, η ραγδαία εξάπλωση διαδικτυακών παραβάσεων, όπως η ρητορική μίσους, η παραπληροφόρηση και οι ψευδείς ειδήσεις (fake news) έχει αναδείξει την άμεση ανάγκη για ενεργή παρέμβαση στο ψηφιακό περιεχόμενο, τόσο από τις αρμόδιες κρατικές αρχές όσο και από τις ίδιες τις πλατφόρμες. Τούτο διότι, τα φαινόμενα αυτά θεωρούνται δυνητικά επικίνδυνα για το κράτος δικαίου και τη δημοκρατία. Ωστόσο, η εννοιολογική και νομική τους ασάφεια και η ελλιπής οριοθέτηση δημιουργεί ουσιαστικά και νομικά διλήμματα ως προς την νομιμότητα και την αναλογικότητα των περιορισμών στην ελευθερία του λόγου.

Ειδικότερα, λαμβάνοντας υπόψη ότι το φαινόμενο της ρητορικής μίσους (hate speech) στο διαδίκτυο δεν περιορίζεται σε εθνικά σύνορα, η έλλειψη ενός ενιαίου, διεθνώς αποδεκτού ορισμού της αποτελεί μία από τις σημαντικότερες προκλήσεις όσον αφορά την καταπολέμηση της<sup>37</sup>. Σύμφωνα με έναν θεωρητικό ορισμό, ως

---

<sup>36</sup> Council of Europe (2021), Content Moderation: Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation (Guidance Note). Adopted by the Steering Committee for Media and Information Society (CDMSI)

<sup>37</sup> UNESCO (2021), United Nations Office on Genocide Prevention and the Responsibility to Protect, Addressing hate speech on social media: contemporary challenges, σελ. 3-4.

μισαλλόδοξος λόγος νοείται συνήθως κάθε μορφή προκατάληψης, υποτίμησης ή μίσους έναντι ορισμένων προσώπων ή ομάδας προσώπων λόγω φυλής, χρώματος, εθνικότητας, φύλου, θρησκείας ή άλλων προσωπικών πεποιθήσεων, γλώσσας, σεξουαλικής προτίμησης, σωματικών ή πνευματικών μειονεκτημάτων ή λόγω άλλων διακριτικών χαρακτηριστικών<sup>38</sup>. Σημειώνεται, μάλιστα ότι τόσο το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου όσο και το Δικαστήριο της Ευρωπαϊκής Ένωσης αναγνωρίζουν ότι ο λόγος, ο οποίος συνιστά σαφή προτροπή σε βία ή διακρίσεις παύει να προστατεύεται από την ελευθερία της έκφρασης και μπορεί να περιορίζεται υπό τις προϋποθέσεις της νομιμότητας, της αναγκαιότητας και της αναλογικότητας<sup>39</sup>.

Χαρακτηριστικό παράδειγμα ρητορικής μίσους αποτελεί η προσφυγική κρίση του 2015 - 2016, κατά την οποία σημειώθηκε ραγδαία αύξηση ρητορικών επιθέσεων κατά προσφύγων και μεταναστών στα κοινωνικά δίκτυα. Σύμφωνα με έρευνες της Europol και του European Union Agency for Fundamental Rights (FRA)<sup>40</sup> καταγράφηκαν πλήθος περιπτώσεων προτροπής σε βία, ξενοφοβικού λόγου, ακόμη και επικλήσεων για συγκρότηση ένοπλων πολιτοφυλακών κατά των προσφύγων.

Εξίσου κρίσιμη είναι η επικράτηση του φαινομένου της παραπληροφόρησης (disinformation), η οποία αφορά τη σκόπιμη διάδοση ανακριβών ή παραπλανητικών πληροφοριών, με στόχο τη χειραγώγηση της κοινής γνώμης, την υπονόμηση δημοκρατικών θεσμών και την πρόκληση κοινωνικής διχόνοιας. Πρόκειται για οργανωμένη πρακτική πληροφόρησης, η οποία συχνά σχετίζεται με στρατηγικές

---

<sup>38</sup> Ανθόπουλος Χ. (2000), Προστασία κατά του ρατσισμού και ελευθερία της πληροφόρησης: Ένα συνταγματικό δίλημμα, Αθήνα, σελ. 13

<sup>39</sup> ΕΔΔΑ, Απόφαση της 6ης Ιουλίου 2006, *Erbakan κατά Turkey*, No. 59405/00, σκ. 56–57.

<sup>40</sup> European Union Agency for Fundamental Rights (FRA) (2021), *Hate Speech and Hate Crime against Migrants and Refugees in the EU*. Διαθέσιμο στο: <https://fra.europa.eu/en/publication/2021/hate-speech-and-crime-against-migrants> (τελευταία πρόσβαση: 26/06/2025)

πολιτικής επιρροής<sup>41</sup>. Σημειώνεται δε ότι η παραπληροφόρηση διακρίνεται από την παραπλάνηση χωρίς πρόθεση (misinformation), η οποία, αν και επιζήμια, δεν συνεπάγεται πάντοτε ηθική ή νομική ευθύνη.

Χαρακτηριστικό παράδειγμα παραπληροφόρησης, αποτελούν οι ειδήσεις που είχαν αναπαραχθεί τα έτη 2020 - 2022, κυρίως μέσω πλατφορμών όπως το Facebook και το X (πρώην Twitter), αναφορικά με τον COVID-19, οι οποίες ανέφεραν ότι η πανδημία αποτελεί μια «κατασκευασμένη κρίση» για να επιβληθεί ένας παγκόσμιος έλεγχος και ότι τα εμβόλια κατά του ιού περιείχαν μικροσίπ για την παρακολούθηση των πολιτών<sup>42</sup>. Το περιεχόμενο των ειδήσεων αυτών δεν προερχόταν απλώς από παρανόηση (misinformation), αλλά από στοχευμένη διασπορά πληροφοριών με πολιτικό ή ιδεολογικό κίνητρο (π.χ. από ομάδες κατά των εμβολιασμών).

Περαιτέρω, το φαινόμενο των ψευδών ειδήσεων (fake news), αποτελεί μια μορφή ψευδο-δημοσιογραφίας. Πρόκειται για ένα κατασκευασμένο περιεχόμενο που μιμείται τη μορφή και το ύφος έγκυρων ειδησεογραφικών πηγών, αποσκοπώντας στη σκόπιμη παραπλάνηση ή στην προσέλκυση αναγνωστικού κοινού με clickbait τεχνικές.

Ένα πολύ γνωστό παράδειγμα ψευδής είδησης είναι η υποστήριξη του Πάπα Φραγκίσκο στο Ντόναλντ Τραμπ, κατά την προεκλογική περίοδο των Ηνωμένων Πολιτειών το 2016<sup>43</sup>. Η συγκεκριμένη είδηση μπορεί να μην είχε ουδεμία δόση αλήθειας, όμως δεν ήταν τυχαία. Αντιθέτως, πρόκειται για τη συνήθη πρακτική

---

<sup>41</sup> Wardle C. - Derakhshan H. (2017), Information Disorder: Toward an Interdisciplinary Framework, Council of Europe, p. 20

<sup>42</sup> Brennen J. S. - Simon F. - Howard P. N. - Nielsen R. K. (2020), Types, Sources, and Claims of COVID-19 Misinformation, Reuters Institute for the Study of Journalism, University of Oxford, p.2

<sup>43</sup> Allcott H. - Gentzkow M. (2017), Social Media and Fake News in the 2016 Election, Journal of Economic Perspectives, 31(2), p. 214 -216. Διαθέσιμο στο: <https://doi.org/10.1257/jep.31.2.211> (τελευταία πρόσβαση: 26/06/2025)

παραγωγής κατασκευασμένων ειδήσεων με clickbait τίτλους, με σκοπό, είτε το οικονομικό κέρδος μέσω διαφημιστικών εσόδων, είτε την πολιτική επιρροή και διαμόρφωση συναισθημάτων των ψηφοφόρων.

Σε αντίθεση, όμως, με τη ρητορική μίσους, το ψευδές περιεχόμενο δεν ταυτίζεται εξ ορισμού με παράνομο περιεχόμενο, καθώς συχνά δεν παραβιάζει συγκεκριμένη διάταξη δικαίου, αλλά τίθεται υπό αμφισβήτηση μόνο ως προς την ποιότητα ή την ακρίβεια της πληροφορίας<sup>44</sup>. Αυτό καθιστά την παρέμβαση για την καταπολέμησή του θεσμικά ασταθή και ερμηνευτικά επικίνδυνη, καθώς ενδέχεται να χαρακτηριστεί ως λογοκρισία ή επιλεκτική αφαίρεση. Αντιλαμβανόμενη αυτή τη δυσκολία, η Ευρωπαϊκή Επιτροπή εξέδωσε έναν Ενισχυμένο Κώδικα Ορθής Πρακτικής κατά της Παραπληροφόρησης<sup>45</sup>, ο οποίος βασίζεται ως επί το πλείστον σε ένα μοντέλο συρρύθμισης (co-regulation) μεταξύ ιδιωτικών πλατφορμών, fact-checkers και θεσμικών φορέων παρά στη μονομερή κρατική ρύθμιση.

Πάντως, η γραμμή ανάμεσα στην ψευδή πληροφορία και σε μια διαφορετική, μη καθιερωμένη άποψη συχνά είναι δυσδιάκριτη, ειδικά σε ζητήματα όπου υπάρχει επιστημονική αβεβαιότητα, έντονη πολιτική αντιπαράθεση ή μεγάλη πολιτισμική ποικιλία. Η άνιση εφαρμογή μέτρων ή ο αποκλεισμός περιεχομένου μειονοτικών ή περιθωριακών ομάδων πλήττει την αρχή της ισότητας. Η μεγάλη πρόκληση, λοιπόν, δεν είναι μόνο το πώς θα αντιμετωπιστεί το επιβλαβές περιεχόμενο, αλλά το πώς θα καθοριστούν τα όρια της παρέμβασης με τρόπο θεσμικά ορθολογικό, αναλογικό και στη βάση σαφών, διαφανών και νόμιμων κριτηρίων. Η αξιολόγηση περιεχομένου δεν μπορεί να γίνεται αποσπασματικά, αλλά πρέπει να λαμβάνει υπόψη το νόημα, το πλαίσιο, την πρόθεση του συντάκτη και την αποδεδειγμένη επίδραση στο κοινό. Ο

---

<sup>44</sup> Barendt E. (2005), Freedom of Speech, Oxford University Press, σελ. 164 – 172.

<sup>45</sup> European Commission (2022), Strengthened Code of Practice on Disinformation. Διαθέσιμο στο: <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation> (τελευταία πρόσβαση 26/06/2025)

δημόσιος λόγος, όσο αιχμηρός ή μειοψηφικός και αν είναι, δεν επιτρέπεται να καταστέλλεται προληπτικά, εκτός και αν συνιστά άμεση και σοβαρή απειλή κατά κάποιου άλλου προστατευόμενου αγαθού.

### **3.3 Αρχές Εξισορρόπησης: Αναλογικότητα, Αναγκαιότητα και Διαφάνεια Παρέμβασης**

Όπως ήδη επισημάνθηκε, για να είναι η εποπτεία του ψηφιακού περιεχομένου σύννομη, κρίνεται σκόπιμο να εξισορροπηθούν τα συγκρουόμενα θεμελιώδη δικαιώματα. Αυτή η ισορροπία πρέπει να βασίζεται στην εφαρμογή βασικών κανονιστικών αρχών, όπως η αναλογικότητα, η αναγκαιότητα και η διαφάνεια. Οι αρχές αυτές δεν αποτελούν απλώς θεωρητικές αξιώσεις, αλλά προκύπτουν από τη συνταγματική και διεθνή κατοχύρωση των δικαιωμάτων και λειτουργούν ως ουσιώδες κριτήριο για τη νομιμότητα κάθε παρέμβασης, είτε προέρχεται από τις ίδιες τις ψηφιακές πλατφόρμες είτε από τις δημόσιες αρχές.

Η αρχή της αναλογικότητας, η οποία είναι καθιερωμένη τόσο στη νομολογία του ΕΔΔΑ όσο και στο ενωσιακό δίκαιο, απαιτεί η οποιαδήποτε περιοριστική παρέμβαση στην ελευθερία της έκφρασης να είναι πρόσφορη, δηλαδή να μπορεί να επιφέρει τον σκοπό που επιδιώκει («καταλληλότητα»), να είναι αναγκαία ως προς τον επιδιωκόμενο σκοπό, ο οποίος δεν μπορεί να επιτευχθεί με κάποιο λιγότερο επαχθές μέτρο («αναγκαιότητα») και, τέλος, να μην είναι δυσανάλογη ως προς τον σκοπό αυτόν («εν στενή έννοια αναλογικότητα»)<sup>46</sup>. Στο πλαίσιο της εποπτείας περιεχομένου και κατ' επέκταση των προσωπικών δεδομένων, έκφραση της αρχής αυτής, συνιστά η κατοχύρωση των αρχών επεξεργασίας προσωπικών δεδομένων που καθορίζουν τους όρους και τους τρόπους συλλογής, επεξεργασίας και αποθήκευσης των δεδομένων καλλιεργώντας την εμπιστοσύνη των φυσικών προσώπων και δημιουργώντας πρόσφορο έδαφος για την ανάπτυξη της ψηφιακής οικονομίας στην

---

<sup>46</sup> ΕΔΔΑ, Απόφαση της 26ης Απριλίου 1979, Sunday Times κατά Ηνωμένου Βασιλείου, No. 6538/74, σκ. 62–63.

εσωτερική ευρωπαϊκή αγορά<sup>47</sup>. Κρίνεται, επομένως, σκόπιμη η ύπαρξη διαφοροποιημένων επιπέδων παρέμβασης (π.χ. αφαίρεση, υποβάθμιση, προειδοποίηση, επισήμανση), τα οποία πρέπει να εφαρμόζονται εξατομικευμένα, ανάλογα με τη βαρύτητα και τον κίνδυνο του εκάστοτε περιεχομένου<sup>48</sup>.

Η αρχή της αναγκαιότητας αποτελεί θεμελιώδη δικλείδα εξισορρόπησης ανάμεσα στην ανάγκη εποπτείας του ψηφιακού περιεχομένου και στην προστασία των θεμελιωδών δικαιωμάτων, όπως είναι η ελευθερία έκφρασης και το δικαίωμα στην ιδιωτικότητα. Ειδικότερα, στο πλαίσιο λειτουργίας των ψηφιακών πλατφορμών, η αρχή αυτή επιβάλλει οι παρεμβάσεις για τον έλεγχο και τον περιορισμό περιεχομένου να μην υπερβαίνουν το απολύτως αναγκαίο μέτρο για την επίτευξη του επιδιωκόμενου σκοπού. Η τήρηση της αναγκαιότητας καθίσταται ακόμη πιο κρίσιμη, όταν ο έλεγχος περιεχομένου συνδέεται με την επεξεργασία προσωπικών δεδομένων, καθώς η πρόσβαση σε ευαίσθητα στοιχεία ή η μαζική συλλογή δεδομένων για σκοπούς εποπτείας και ελέγχου εγκυμονεί σοβαρούς κινδύνους για την ιδιωτική σφαίρα των χρηστών. Μάλιστα, όταν πρόκειται για επιβλαβή αλλά όχι παράνομα περιεχόμενα, όπως η παραπληροφόρηση ή ο μισαλλόδοξος λόγος, η αναγκαιότητα πρέπει να αξιολογείται *ad hoc*, με βάση τη συγκεκριμένη απειλή που δημιουργείται και όχι απλώς βάσει γενικών χαρακτηρισμών<sup>49</sup>. Επομένως, κάθε διαδικασία εποπτείας πρέπει να τεκμηριώνεται ως απολύτως αναγκαία, να στηρίζεται σε ελάχιστη επεξεργασία δεδομένων και να συνοδεύεται από επαρκείς εγγυήσεις διαφάνειας και ελέγχου, ώστε να διασφαλίζεται η αναλογική ισορροπία ανάμεσα στην προστασία της δημόσιας τάξης ή άλλων δικαιωμάτων και στον σεβασμό των προσωπικών δεδομένων.

---

<sup>47</sup> Αιτιολογική σκέψη 7 του Κανονισμού (ΕΕ) 2016/679

<sup>48</sup> Douek E. (2021), *Content Moderation as Systems Thinking*, Harvard Journal of Law & Technology, p. 572

<sup>49</sup> Άρθρα 14 - 20 του Κανονισμού (ΕΕ) 2022/2065

Τέλος, η αρχή της διαφάνειας συνιστά βασικό πυλώνα της διασφάλισης της νομιμότητας και της λογοδοσίας στις διαδικασίες ελέγχου περιεχομένου από τις ψηφιακές πλατφόρμες, ιδίως όταν οι πρακτικές αυτές συνεπάγονται την επεξεργασία προσωπικών δεδομένων. Βασική της προϋπόθεση είναι ότι οι χρήστες ενημερώνονται με σαφήνεια και πληρότητα για τους κανόνες που διέπουν την αφαίρεση ή τον περιορισμό περιεχομένου, τα κριτήρια βάσει των οποίων αξιολογείται η νομιμότητα ή η επιβλαβής φύση μιας ανάρτησης, καθώς και για τα τεχνικά ή αλγοριθμικά εργαλεία που χρησιμοποιούνται. Εξάλλου, μόνο μέσα από διαφανείς διαδικασίες μπορεί να διασφαλιστεί η ουσιαστική ισορροπία ανάμεσα στην προστασία της δημόσιας τάξης και την κατοχύρωση της ελευθερίας έκφρασης και της ιδιωτικότητας, ενισχύοντας παράλληλα την εμπιστοσύνη των χρηστών προς τις πλατφόρμες και τις αρμόδιες αρχές.

Ο Κανονισμός για τις Ψηφιακές Υπηρεσίες (DSA), ο οποίος αναλύεται στη συνέχεια, αναγνωρίζει ρητά τις εν λόγω αρχές, ιδίως στα άρθρα 14 - 20, θεσπίζοντας υποχρεώσεις σαφούς αιτιολόγησης αφαίρεσης περιεχομένου, δικαιώματος προσφυγής του χρήστη, και διαφάνειας αλγοριθμικών αποφάσεων. Ταυτόχρονα, προωθείται η ιδέα να εφαρμόζεται μια μεθοδολογία αξιολόγησης του βαθμού επικινδυνότητας και των ευρύτερων συστημικών κινδύνων (risk-based approach), έτσι ώστε οποιαδήποτε παρέμβαση να έχει σαφή συνταγματική και θεσμική βάση και να μην περιορίζεται μόνο σε τεχνικούς ή καθαρά επιχειρησιακούς χειρισμούς.

Συνολικά, είναι σημαντικό οι παρεμβάσεις στο ψηφιακό περιβάλλον να σχεδιάζονται με τρόπο που σέβεται τα θεμελιώδη δικαιώματα και να εφαρμόζονται με σαφή και τεκμηριωμένο τρόπο. Η προστασία των προσωπικών δεδομένων και της ιδιωτικότητας πρέπει να ενσωματώνεται στα μέτρα εποπτείας, ώστε να διασφαλίζεται η ισορροπία ανάμεσα στην αποτελεσματικότητα των ρυθμίσεων και τον σεβασμό των ατομικών ελευθεριών. Η ύπαρξη διαφανούς πλαισίου, λογοδοσίας και ελέγχου συμβάλλει στην ενίσχυση της εμπιστοσύνης των χρηστών και στη

μακροπρόθεσμη βιωσιμότητα ενός δημοκρατικά θεμελιωμένου ψηφιακού οικοσυστήματος.

### **3.4 Η Νομολογία του ΕΔΔΑ και του ΔΕΕ για την προάσπιση της ελευθερίας της έκφρασης στο διαδίκτυο και της ιδιωτικότητας**

Η ανωτέρω θεωρητική εξισορρόπηση αποκτά ρυθμιστικό και πρακτικό περιεχόμενο μέσα από τη νομολογία του Ευρωπαϊκού Δικαστηρίου Ανθρωπίνων Δικαιωμάτων (ΕΔΔΑ) και του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ). Μέσα από τις ήδη εκδοθείσες αποφάσεις τους, έχουν διαμορφωθεί τα όρια της επιτρεπτής παρέμβασης στο διαδίκτυο και καθιερωθεί τα κριτήρια νομιμότητας και αναλογικότητας, τα οποία οφείλουν να λαμβάνουν υπόψη τόσο τα κράτη όσο και οι πλατφόρμες κατά τον έλεγχο περιεχομένου.

Ειδικότερα, σημαντικές αποφάσεις, όπως η Delfi AS κατά Εσθονίας<sup>50</sup> και η Magyar Tartalomszolgáltatók Egyesülete (MTE) και Index.hu Zrt. κατά Ουγγαρίας<sup>51</sup>, ανέδειξαν ότι οι διαδικτυακοί πάροχοι μπορεί να θεωρηθούν υπεύθυνοι για παράνομο ή υβριστικό περιεχόμενο που δημοσιεύουν τρίτοι στις πλατφόρμες τους. Το Δικαστήριο έκρινε ότι η επιβολή ευθύνης σε πάροχο δεν συνιστά κατ' αρχήν παραβίαση του άρθρου 10 της ΕΣΔΑ, εφόσον πληρούνται τα κριτήρια αναλογικότητας, όπως η δυνατότητα πρόληψης ή απομάκρυνσης του επιβλαβούς περιεχομένου και η εξισορρόπηση των εμπλεκόμενων δικαιωμάτων.

Παράλληλα, η νομολογία του ΔΕΕ δίνει ιδιαίτερη έμφαση στη σχέση ανάμεσα στην ελευθερία έκφρασης και στην προστασία δεδομένων προσωπικού χαρακτήρα. Χαρακτηριστική είναι η απόφαση Google Spain SL και Google Inc. κατά AEPD και

---

<sup>50</sup> ΕΔΔΑ, Απόφασης της 16ης Ιουνίου 2015, Delfi AS κατά Εσθονίας, No. 64569/09.

<sup>51</sup> ΕΔΔΑ, Απόφαση της 2ης Φεβρουαρίου 2006, Magyar Tartalomszolgáltatók Egyesülete (MTE) και Index.hu Zrt. κατά Ουγγαρίας, No. 22947/13

González<sup>52</sup>, με την οποία το Δικαστήριο καθιέρωσε το «δικαίωμα στη λήθη» (right to be forgotten), αναγνωρίζοντας το δικαίωμα του ατόμου να ζητά τη διαγραφή συνδέσμων που θίγουν την ιδιωτική του ζωή, εφόσον δεν συντρέχει υπέρτερο δημόσιο συμφέρον στην πρόσβαση στην πληροφορία.

Συνολικά, τόσο το ΕΔΔΑ όσο και το ΔΕΕ αναγνωρίζουν τη σημασία της ύπαρξης σαφών και αναλογικών μηχανισμών για τον έλεγχο του περιεχομένου, ώστε να εξασφαλίζεται η προστασία των θεμελιωδών δικαιωμάτων, ενώ παράλληλα να λαμβάνονται υπόψη οι ανάγκες της δημόσιας τάξης και η προστασία άλλων θεμελιωδών συμφερόντων, όπως η ανθρώπινη αξιοπρέπεια. Όπως επισημαίνουν τα εν λόγω δικαστήρια, κάθε περιορισμός της ελευθερίας της έκφρασης πρέπει να είναι καταρχήν αιτιολογημένος και να προβλέπεται από καθορισμένη νομοθεσία, με στόχο την επίτευξη θεμιτών σκοπών, όπως η αποτροπή της διάδοσης επικίνδυνων ή μισαλλόδοξων ιδεών. Παράλληλα, πρέπει να είναι αυστηρά αναγκαίος και να μη ξεπερνά το απολύτως απαιτούμενο για την επίτευξη του επιδιωκόμενου αποτελέσματος μέτρο. Στο πλαίσιο αυτό, ο έλεγχος κάθε περιορισμού πρέπει να λαμβάνει υπόψη την αναλογικότητά του, ώστε να εξασφαλίζεται ότι οι ενέργειες αυτές δεν θα θέσουν σε κίνδυνο τη δημοκρατική φύση της κοινωνίας.

---

<sup>52</sup> ΔΕΕ, Απόφαση της 13ης Μαΐου 2014, Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12.

## 4. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ ΓΙΑ ΤΙΣ ΨΗΦΙΑΚΕΣ ΠΛΑΤΦΟΡΜΕΣ

### 4.1 Ιστορική και νομοθετική εξέλιξη

Το νομικό υπόβαθρο για τη ρύθμιση των ψηφιακών υπηρεσιών στην Ευρωπαϊκή Ένωση τέθηκε ήδη από το έτος 2000, με την έκδοση της Οδηγίας 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, γνωστής και ως «Οδηγία για το Ηλεκτρονικό Εμπόριο» (e-Commerce Directive). Η εν λόγω Οδηγία αποτέλεσε το πρώτο ρυθμιστικό εγχείρημα για την εδραίωση μιας ενιαίας ψηφιακής ευρωπαϊκής αγοράς, αποσκοπώντας στην άρση των ρυθμιστικών εμποδίων εντός της εσωτερικής αγοράς και στη διευκόλυνση της ελεύθερης παροχής υπηρεσιών της κοινωνίας της πληροφορίας. Ένα από τα θεμελιώδη χαρακτηριστικά του πλαισίου που εισήγαγε η Οδηγία είναι η καθιέρωση του λεγόμενου «καθεστώτος περιορισμένης ευθύνης» (limited liability regime) για τους παρόχους ενδιάμεσων υπηρεσιών. Σύμφωνα με αυτό, οι πάροχοι δεν υπέχουν γενική υποχρέωση παρακολούθησης του περιεχομένου που διακινείται μέσω των υπηρεσιών τους και, υπό προϋποθέσεις, απαλλάσσονται από την ευθύνη για το παράνομο περιεχόμενο που φιλοξενούν, μεταδίδουν ή αποθηκεύουν προσωρινά, εφόσον δεν έχουν πραγματική γνώση της παρανομίας ή ενεργούν αμέσως για την αφαίρεσή του.<sup>53</sup>

Ωστόσο, η αυξημένη χρήση των ψηφιακών υπηρεσιών έχει φέρει στην επιφάνεια νέους κινδύνους και προκλήσεις τόσο για τους αποδέκτες των σχετικών υπηρεσιών, όσο και για την κοινωνία στο σύνολο της. Ενδεικτικά, παρατηρείται ότι οι υπηρεσίες κοινωνικής δικτύωσης χρησιμοποιούνται από τρίτους, με σκοπό τη διάδοση παράνομου ή επιβλαβούς περιεχομένου, όπως διασπορά ψευδών πληροφοριών (fake news) ή πληροφοριών που αφορούν τη ρητορική μίσους (hate speech), τη τρομοκρατία και τη σεξουαλική κακοποίηση/ παρενόχληση παιδιών. Συνεπώς, δεν θα ήταν συνετό

---

<sup>53</sup> Άρθρα 12 - 15 της Οδηγίας 2000/31 ΕΚ

να συνεχίσει να επαφίεται η διαχείριση του περιεχομένου αυτών των υπηρεσιών αποκλειστικά σε όρους χρήσης και συμβατικές ρήτρες που συντάσσονται και εφαρμόζονται, ως επί το πλείστον, μονομερώς από τον εκάστοτε πάροχο μιας τέτοιας υπηρεσίας. Έτσι, η Ευρωπαϊκή Επιτροπή, με τη Σύσταση 2018/334, ενθάρρυνε τα κράτη μέλη να θεσπίσουν μηχανισμούς αναγγελίας παράνομου περιεχομένου και διαδικασίες για την αφαίρεση του.<sup>54</sup>

#### **4.2 Κανονισμός 2022/2065 για τις Ψηφιακές Υπηρεσίες (Digital Services Act - DSA)**

Με την πάροδο του χρόνου η ανάγκη επικαιροποίησης του ρυθμιστικού πλαισίου κατέστη επιτακτική, λόγω των τεχνολογικών εξελίξεων, της ραγδαίας εξάπλωσης των επιγραμμικών (online) πλατφορμών και του όγκου διάχυσης και πρόσληψης της πληροφορίας. Η Οδηγία 2000/31/EK, αν και πρωτοποριακή για την εποχή της, δεν ήταν σε θέση να ανταποκριθεί πλήρως στις σύγχρονες προκλήσεις του ψηφιακού περιβάλλοντος, ήτοι την εξάπλωση παράνομου περιεχομένου, την αδιαφάνεια των αυτοματοποιημένων συστημάτων και τον κίνδυνο προσβολής θεμελιωδών δικαιωμάτων των χρηστών.

Ως απάντηση στις εν λόγω προκλήσεις, η Επιτροπή δημοσίευσε την 15η Δεκεμβρίου 2020 μια Πρόταση Κανονισμού σχετικά με την ενιαία αγορά ψηφιακών υπηρεσιών/ πράξη για τις ψηφιακές υπηρεσίες (Digital Services Act, εφεξής «DSA» ή «Κανονισμός»), η οποία τροποποίησε την ως άνω με αριθμό 2000/31 EK Οδηγία και, η οποία στοχεύει στην δημιουργία ενός ασφαλέστερου, αξιόπιστου και ανοικτού ψηφιακού χώρου, στον οποίο θα προστατεύονται τα θεμελιώδη δικαιώματα των χρηστών των ψηφιακών υπηρεσιών και θα δημιουργούνται ισότιμοι όροι ανταγωνισμού για την ανάπτυξη της καινοτομίας, της επιχειρηματικότητας και της

---

<sup>54</sup> Βλ. Σύσταση (ΕΕ) 2018/334 της Επιτροπής της 1ης Μαρτίου 2018 σχετικά με μέτρα για την αποτελεσματική αντιμετώπιση του παράνομου περιεχομένου στο διαδίκτυο. Διαθέσιμο: <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32018H0334> (τελευταία πρόσβαση: 02/06/2025)

ανταγωνιστικότητας τόσο στην Ευρωπαϊκή Ένωση, όσο και παγκοσμίως.<sup>55</sup> Εισάγεται, έτσι, ένα συνεκτικό ευρωπαϊκό πλαίσιο, το οποίο διατηρεί ορισμένες θεμελιώδεις αρχές της Οδηγίας (όπως η περιορισμένη ευθύνη), αλλά παράλληλα ενσωματώνει νέες υποχρεώσεις για τους παρόχους, ιδίως τις πολύ μεγάλες επιγραμμικές πλατφόρμες (Very Large Online Platforms – VLOPs), επιδιώκοντας μεγαλύτερη διαφάνεια, λογοδοσία και προστασία των χρηστών.<sup>56</sup>

Ειδικότερα, ο Κανονισμός εφαρμόζεται σε παρόχους ενδιάμεσων υπηρεσιών, ανεξαρτήτως μάλιστα του τύπου εγκατάστασής τους<sup>57</sup>. Αυτές οι υπηρεσίες περιλαμβάνουν την «απλή μετάδοση», την «προσωρινή αποθήκευση» και τη «φιλοξενία»<sup>58</sup>, ενώ μία τέταρτη κατηγορία, που ουσιαστικά αποτελεί υποκατηγορία της τελευταίας, είναι οι υπηρεσίες «πλατφόρμας», μέσω της οποίας επιτρέπεται η αποθήκευση των πληροφοριών που παρέχει ο χρήστης και η διάδοσή τους στο κοινό κατόπιν αιτήματος του τελευταίου.

Αφετηρία του χρονοδιαγράμματος του νέου αυτού ρυθμιστικού πλαισίου αποτελεί, ως προαναφέρθηκε, η σχετική πρόταση της Ευρωπαϊκής Επιτροπής, την 15η Δεκεμβρίου 2020. Σημειώνεται δε ότι την 23η Απριλίου 2022 το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο κατέληξαν σε προσωρινή πολιτική συμφωνία σχετικά με την τελική μορφή του νομοθετήματος. Ακολούθως, την 5η Ιουλίου 2022, το Ευρωπαϊκό Κοινοβούλιο ενέκρινε την Πρόταση και την 27η Οκτωβρίου 2022 δημοσιεύθηκε το τελικό κείμενο στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Κατόπιν τούτων, ο Κανονισμός (ΕΕ) 2022/2065 τέθηκε σε ισχύ στις 17 Φεβρουαρίου 2024, γεγονός που

---

<sup>55</sup>Βλ. παράγραφο 3 των Σκέψεων του Κανονισμού. Διαθέσιμο στο: [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32022R2065](https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32022R2065) (τελευταία πρόσβαση: 02/06/2025)

<sup>56</sup> Husovec M. - Peukert A. (2022), *The Digital Services Act: A Legal and Systematic Analysis*, Max Planck Institute for Innovation & Competition Research Paper No. 22-10, p. 370

<sup>57</sup> Αιτιολογική Σκέψη 7 του Κανονισμού (ΕΕ) 2022/2065

<sup>58</sup> Αιτιολογική Σκέψη 5 και άρθρο 3 ζ' του Κανονισμού (ΕΕ) 2022/2065

σηματοδοτεί τη σημαντικότερη αναμόρφωση του νομικού πλαισίου που διέπει τις σύγχρονες ψηφιακές πλατφόρμες.<sup>59</sup>

#### **4.2.1 Η Διαδικασία Ειδοποίησης και Δράσης ( Notice and Action)**

Στο πλαίσιο αυτό, είναι κρίσιμο να εξετάσουμε τις νέες υποχρεώσεις που εισάγει ο Κανονισμός για τους παρόχους υπηρεσιών, καθώς και τον τρόπο με τον οποίο αυτές επηρεάζουν τη σύγχρονη ψηφιακή πραγματικότητα στην Ευρώπη. Ειδικότερα, στα άρθρα 16 - 18 προβλέπονται ειδικές διατάξεις για τους παρόχους υπηρεσιών φιλοξενίας και τους παρόχους επιγραμμικών (online) υπηρεσιών που αφορούν την υποχρέωση για ειδοποίηση και δράση (notice and action) όσον αφορά στην ύπαρξη παράνομου περιεχομένου.

Στην ουσία πρόκειται για μηχανισμούς, οι οποίοι πρέπει να είναι ευκόλως προσβάσιμοι, εύχρηστοι και να παρέχουν τη δυνατότητα υποβολής ειδοποιήσεων αποκλειστικά με ηλεκτρονικά μέσα. Η παράγραφος 2 του άρθρου 16 εξειδικεύει τη γενική υποχρέωση, προσδιορίζοντας τα απαραίτητα στοιχεία που πρέπει να περιλαμβάνει κάθε ειδοποίηση, τα οποία είναι τα εξής: α) επεξήγηση των λόγων για τους οποίους το φυσικό ή νομικό πρόσωπο θεωρεί ότι οι επίμαχες πληροφορίες αποτελούν παράνομο περιεχόμενο, β) σαφή ένδειξη της ηλεκτρονικής τοποθεσίας των εν λόγω πληροφοριών, και ιδίως τον ακριβή URL ή τους ακριβείς URL και, εφόσον είναι απαραίτητο, πρόσθετες πληροφορίες που επιτρέπουν τον προσδιορισμό του παράνομου περιεχομένου, γ) το όνομα και τη διεύθυνση ηλεκτρονικού ταχυδρομείου του φυσικού ή νομικού προσώπου που υποβάλλει την ειδοποίηση, με εξαίρεση την περίπτωση πληροφοριών που θεωρείται ότι αφορούν ένα από τα αδικήματα που αναφέρονται στα άρθρα 3 έως 7 της οδηγίας 2011/93/ΕΕ, δ) δήλωση που επιβεβαιώνει την καλή πίστη του φυσικού ή νομικού προσώπου που υποβάλλει την ειδοποίηση και

---

<sup>59</sup> Ιγγλεζάκης Ι., Προστασία προσωπικών δεδομένων και ελευθερία της έκφρασης στο διαδίκτυο, στο πλαίσιο της εφαρμογής της Πράξης της ΕΕ για τις ψηφιακές υπηρεσίες, Επιθεώρηση Δικαίου Πληροφορικής, Τόμ. 5, Αρ.2, σελ. 2

στην οποία αναφέρεται ότι οι πληροφορίες και οι ισχυρισμοί που περιέχονται σε αυτήν είναι ακριβείς και πλήρεις. Ακολούθως, προβλέπεται ότι ο πάροχος υπηρεσιών φιλοξενίας αποστέλλει παραχρήμα επιβεβαίωση παραλαβής της ειδοποίησης, υπό την προϋπόθεση ότι η ειδοποίηση περιλαμβάνει το όνομα και την ηλεκτρονική διεύθυνση του υποβάλλοντος φυσικού ή νομικού προσώπου<sup>60</sup> και στη συνέχεια, του κοινοποιεί, χωρίς υπαίτια καθυστέρηση, την απόφασή του σχετικά με τις πληροφορίες στις οποίες αναφέρεται η ειδοποίηση, ενημερώνοντάς το σχετικά με τη δυνατότητα προσφυγής κατά της εν λόγω απόφασης<sup>61</sup>. Τέλος, κατόπιν εξέτασης των υποβληθεισών καταγγελιών περιεχομένου, οι πάροχοι υπηρεσιών φιλοξενίας επεξεργάζονται τις ειδοποιήσεις και λαμβάνουν τις αποφάσεις τους, με έγκαιρο, επιμελή και αντικειμενικό τρόπο<sup>62</sup>.

Εξίσου σημαντική ρύθμιση είναι η εισαγωγή σαφούς και συγκεκριμένης αιτιολόγησης των αποφάσεων των παρόχων υπηρεσιών φιλοξενίας, του άρθρο 17, στους θιγόμενους αποδέκτες, όταν ο πάροχος αποφασίζει να αποσύρει ή να απενεργοποιήσει την πρόσβαση σε συγκεκριμένα πληροφοριακά στοιχεία που παρέχονται από τους αποδέκτες της υπηρεσίας. Η εν λόγω υποχρέωση ισχύει ανεξαρτήτως των τεχνικών μέσων ή μηχανισμών που χρησιμοποιεί ο πάροχος για την ανίχνευση, τον εντοπισμό ή την απόσυρση των επίμαχων πληροφοριών ή για την απενεργοποίηση της πρόσβασης σε αυτές, καθώς και ανεξαρτήτως της αιτίας επί της οποίας βασίστηκε η σχετική απόφαση. Οι αποφάσεις αυτές καταχωρίζονται σε δημόσια προσβάσιμη βάση δεδομένων, η οποία τελεί υπό τη διαχείριση της Ευρωπαϊκής Επιτροπής, με την επιφύλαξη της μη συμπερίληψης οποιωνδήποτε προσωπικών δεδομένων. Σύμφωνα με την παράγραφο 3 του άρθρου 17 του εν λόγω Κανονισμού για τις Ψηφιακές Υπηρεσίες, η αιτιολογία της απόφασης πρέπει να

---

<sup>60</sup> Άρθρο 16 παρ.4 του Κανονισμού (ΕΕ) 2022/2065.

<sup>61</sup> Άρθρο 16 παρ.5 του Κανονισμού (ΕΕ) 2022/2065.

<sup>62</sup> Άρθρο 16 παρ.6 του Κανονισμού (ΕΕ) 2022/2065.

περιλαμβάνει τα εξής στοιχεία: α) κατά πόσον η απόφαση συνεπάγεται την απόσυρση των πληροφοριών ή την απενεργοποίηση της πρόσβασης σε αυτές και, κατά περίπτωση, το εδαφικό πεδίο εφαρμογής της απενεργοποίησης της πρόσβασης, β) τα γεγονότα και τις περιστάσεις στις οποίες βασίστηκε η λήψη της απόφασης, συμπεριλαμβανομένου, κατά περίπτωση, του κατά πόσον η απόφαση ελήφθη βάσει ειδοποίησης που υποβλήθηκε σύμφωνα με το άρθρο 16 ή βάσει εθελοντικών αυτεπάγγελτων ερευνών, γ) κατά περίπτωση, πληροφορίες σχετικά με τη χρήση αυτοματοποιημένων μέσων κατά τη λήψη της απόφασης, συμπεριλαμβανομένων περιπτώσεων στις οποίες η απόφαση ελήφθη σε σχέση με περιεχόμενο που ανιχνεύθηκε ή εντοπίστηκε με τη χρήση αυτοματοποιημένων μέσων, δ) όταν η απόφαση αφορά εικαζόμενο παράνομο περιεχόμενο, αναφέρεται ο νομικός λόγος στον οποίο βασίζεται και επεξηγείται γιατί οι πληροφορίες θεωρούνται παράνομο περιεχόμενο βάσει αυτού του λόγου, ε) όταν η απόφαση βασίζεται στην εικαζόμενη ασυμβατότητα των πληροφοριών με τους όρους και τις προϋποθέσεις του παρόχου, αναφέρεται η συμβατική διάταξη στην οποία βασίζεται και επεξηγείται γιατί θεωρείται ότι οι πληροφορίες δεν συνάδουν με την εν λόγω διάταξη, στ) πληροφορίες σχετικά με τις δυνατότητες προσφυγής που διατίθενται στον αποδέκτη της υπηρεσίας σε σχέση με την απόφαση, ιδίως μέσω εσωτερικών μηχανισμών διαχείρισης καταγγελιών, εξωδικαστικής επίλυσης διαφορών και δικαστικής προσφυγής.

#### ***4.2.2 Μηχανισμοί Ενστάσεων και Εξωδικαστική Επίλυση***

Πέραν των υποχρεώσεων για την επεξεργασία ειδοποιήσεων και την αιτιολόγηση των αποφάσεων επί των καταγγελιών, το ρυθμιστικό πλαίσιο του Κανονισμού για τις Ψηφιακές Υπηρεσίες ενισχύεται περαιτέρω μέσω του Τμήματος 3 του Κεφαλαίου III, στο οποίο περιλαμβάνονται ρυθμίσεις για τις επιγραμμικές (online) πλατφόρμες, με εξαίρεση όσες θεωρούνται πολύ μικρές ή μικρές επιχειρήσεις, κατά την έννοια του παραρτήματος της σύστασης 2003/361/ΕΚ.

Σύμφωνα με το άρθρο 20, εισάγεται η υποχρέωση των επιγραμμικών (online) υπηρεσιών να παρέχουν στους αποδέκτες τους πρόσβαση σε αποτελεσματικό εσωτερικό σύστημα διαχείρισης καταγγελιών, το οποίο καθιστά εφικτή τη δωρεάν ηλεκτρονική υποβολή καταγγελιών κατά αποφάσεων που αφορούν την απόσυρση περιεχομένου, την απενεργοποίηση πρόσβασης, την αναστολή ή τον τερματισμό λογαριασμών, ή άλλες περιοριστικές ενέργειες. Όταν μια καταγγελία περιέχει επαρκείς λόγους ώστε ο πάροχος να θεωρήσει ότι είναι αβάσιμη η απόφασή του να μην αναλάβει δράση σχετικά με μία ειδοποίηση ή ότι οι πληροφορίες στις οποίες αναφέρεται η καταγγελία δεν είναι παράνομες ή ασυμβίβαστες με τους όρους και τις προϋποθέσεις του, ή περιέχει πληροφορίες που υποδεικνύουν ότι η συμπεριφορά του καταγγέλλοντος δεν δικαιολογεί το μέτρο που ελήφθη, τότε ο πάροχος της επιγραμμικής πλατφόρμας ανακαλεί την απόφασή του χωρίς αδικαιολόγητη καθυστέρηση<sup>63</sup>.

Ακολούθως, στο άρθρο 21 προβλέπεται η δυνατότητα προσφυγής σε πιστοποιημένους φορείς εξωδικαστικής επίλυσης διαφορών, υπό την προϋπόθεση ότι έχουν πιστοποιηθεί από τον συντονιστή ψηφιακών υπηρεσιών του κράτους μέλους στο οποίο είναι εγκατεστημένο το όργανο εξωδικαστικής επίλυσης διαφορών. Αμφότερα τα μέρη οφείλουν να συνεργάζονται με τους φορείς αυτούς καλόπιστα, αιτιολογώντας σαφώς οποιαδήποτε άρνηση συμμόρφωσης με το αποτέλεσμα της διαδικασίας.

#### ***4.2.3 Μηχανισμοί Επίσημανσης και Αντιμετώπισης Καταχρηστικών Συμπεριφορών στις Επιγραμμικές Πλατφόρμες***

Περαιτέρω, στο άρθρο 22 του παρόντος Κανονισμού εισάγονται οι αξιόπιστες πηγές επίσημανσης παράνομου περιεχομένου (trusted flaggers), οι οποίες αναγνωρίζονται ως τέτοιες από τον αρμόδιο συντονιστή ψηφιακών υπηρεσιών του κράτους μέλους

---

<sup>63</sup> Άρθρο 20 παρ.4 του Κανονισμού (ΕΕ) 2022/2065.

εγκατάστασής τους. Η αναγνώριση αυτή χορηγείται στον αιτούντα εφόσον αποδεδειγμένα διαθέτει την απαραίτητη τεχνογνωσία και ικανότητα, εκπροσωπεί συλλογικά συμφέροντα, είναι ανεξάρτητος από επιγραμμικές πλατφόρμες και ασκεί τις δραστηριότητές τους με ταχύτητα, υπευθυνότητα και αμεροληψία.

Στο άρθρο 23, προβλέπονται μέτρα προστασίας κατά της κατάχρησης των διαδικασιών ειδοποίησης και απόσυρσης περιεχομένου. Οι πάροχοι επιγραμμικών πλατφορμών δύνανται να αναστείλουν τις υπηρεσίες τους απέναντι σε χρήστες που, επανειλημμένα και εντός εύλογου χρονικού διαστήματος, διαδίδουν προδήλως παράνομο περιεχόμενο, υπό την προϋπόθεση ότι έχουν προηγουμένως λάβει σχετική προειδοποίηση. Η ίδια αντιμετώπιση επιφυλάσσεται και για εκείνους που υποβάλλουν συστηματικά προδήλως αβάσιμες ειδοποιήσεις, καθώς τέτοιες πρακτικές μπορούν να υπονομεύσουν την ορθή λειτουργία του μηχανισμού αναφοράς και να πλήξουν θεμελιώδη δικαιώματα, όπως η ελευθερία της έκφρασης.

#### **4.2.4 Διαφάνεια Συστημάτων Συστάσεων και Επιγραμμικής Διαφήμισης**

Περαιτέρω, το άρθρο 25 του Κανονισμού 2022/2065 θεσπίζει πρόσθετες υποχρεώσεις διαφάνειας για τους παρόχους επιγραμμικών πλατφορμών, πέραν των γενικών απαιτήσεων που ισχύουν για όλους τους παρόχους ενδιάμεσων υπηρεσιών, Ειδικότερα, οι εν λόγω πάροχοι καλούνται να δημοσιοποιούν εκθέσεις διαφάνειας αναφορικά με τις πρακτικές τους ως προς τη συγκράτηση, διαχείριση και αφαίρεση περιεχομένου, συμβάλλοντας με τον τρόπο αυτό στην αποτροπή φαινομένων παραπλάνησης και χειραγώγησης των χρηστών<sup>64</sup>.

---

<sup>64</sup> Ρητή απαγόρευση που εισάγεται από τον Κανονισμό ως προς την απαγόρευση χρήσης «παραπλανητικού σχεδιασμού στις επιγραμμικές διεπαφές επιγραμμικών πλατφορμών» (dark patterns). Βλ. σχετικά και Μικρουλέα Α. (2023), Ανταγωνισμός και ρύθμιση στην ψηφιακή οικονομία

Επιπλέον, στο άρθρο 26 του Κανονισμού ρυθμίζεται ένα ιδιαίτερα κρίσιμο πεδίο, αυτό της επιγραμμικής διαφήμισης (online διαφήμιση), το οποίο χαρακτηρίζεται από αυξημένη επικινδυνότητα ως προς τη δυνητική παραβίαση θεμελιωδών δικαιωμάτων<sup>65</sup>. Οι πλατφόρμες υποχρεούνται να παρέχουν σαφείς και κατανοητές πληροφορίες σχετικά με τις αναρτήσεις που φέρουν διαφημιστικό χαρακτήρα, να δηλώνουν το πρόσωπο για λογαριασμό του οποίου προβάλλεται η εκάστοτε διαφήμιση, καθώς και να γνωστοποιούν τις κύριες παραμέτρους βάσει των οποίων καθορίστηκε (στόχευση) ο έκαστος αποδέκτης τους.

Ιδιαίτερη έμφαση δίδεται στον περιορισμό της συμπεριφορικής στόχευσης (behavioural targeting) μέσω της χρήσης ευαίσθητων δεδομένων. Συγκεκριμένα, απαγορεύεται η εμφάνιση διαφημίσεων που βασίζονται στην κατάρτιση προφίλ των χρηστών μέσω της επεξεργασίας ειδικών κατηγοριών προσωπικών δεδομένων, σύμφωνα με το άρθρο 9 του ΓΚΠΔ. Παράλληλα, οι πάροχοι υποχρεούνται να καθιστούν προσβάσιμες, μέσα από τους όρους χρήσης, τις παραμέτρους που χρησιμοποιούνται στα συστήματα συστάσεων, καθώς και τους λόγους επιλογής τους, διασφαλίζοντας έτσι την κατανόηση και τον έλεγχο του χρήστη επί του πληροφοριακού περιβάλλοντός του.<sup>66</sup>

---

<sup>65</sup> Αιτιολογική σκέψη 68 του Κανονισμού 2022/2065: διαφημίσεις που αποτελούν αυτές καθαυτές παράνομο περιεχόμενο και διαφημίσεις που παρέχουν οικονομικά κίνητρα για τη δημοσίευση ή διάδοση παράνομου ή άλλως επιβλαβούς περιεχομένου και δραστηριοτήτων στο διαδίκτυο καθώς και τη μεροληπτική παρουσίαση διαφημίσεων που έχουν επιπτώσεις στην ίση μεταχείριση και στις ίσες ευκαιρίες των πολιτών.

<sup>66</sup>π.χ., η επιγραμμική πλατφόρμα προτείνει, κατατάσσει και ιεραρχεί πληροφορίες με τη χρήση αλγορίθμων, διακρίνει μέσω κειμένου ή άλλων οπτικών αναπαραστάσεων, ή επιμελείται με άλλον τρόπο τις πληροφορίες που παρέχονται από τους αποδέκτες (Αιτ. Σκ. 70 του Κανονισμού)

#### 4.2.5 Οι πολύ μεγάλες επιγραμμικές (online) πλατφόρμες

Το πέμπτο τμήμα του Κανονισμού προβλέπει τις πρόσθετες υποχρεώσεις που εφαρμόζονται στις πολύ μεγάλες επιγραμμικές (online) πλατφόρμες (Very Large Online Platforms - VLOPs) και στις πολύ μεγάλες επιγραμμικές (online) μηχανές αναζήτησης (Very Large Online Search Engines - VLOSEs), ήτοι σε εκείνες που παρέχουν τις υπηρεσίες τους σε αριθμό μέσων μηνιαίων ενεργών αποδεκτών της υπηρεσίας στην Ένωση ίσο ή υψηλότερο από 45 εκατομμύρια.<sup>67</sup>

Σημειώνεται ότι στις 25 Απριλίου 2023 η Ευρωπαϊκή Επιτροπή εξέδωσε τις πρώτες αποφάσεις χαρακτηρισμού, με τις οποίες ορίζονται 17 πολύ μεγάλες επιγραμμικές πλατφόρμες και 2 πολύ μεγάλες επιγραμμικές μηχανές αναζήτησης που έχουν τουλάχιστον 45 εκατομμύρια μηνιαίους ενεργούς χρήστες. Ειδικότερα, ως πολύ μεγάλες επιγραμμικές πλατφόρμες ορίστηκαν οι εξής: Alibaba, AliExpress, Amazon Store, Apple AppStore, Booking, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando. Αντίστοιχα, ως πολύ μεγάλες επιγραμμικές μηχανές αναζήτησης ορίστηκαν οι ακόλουθες : Bing, Google Search<sup>68</sup>. Ο χαρακτηρισμός αυτός των πλατφορμών βασίζεται στις πληροφορίες σχετικά με τον μέσο ανά μήνα αριθμό ενεργών αποδεκτών της υπηρεσίας, τον οποίο έπρεπε να δημοσιεύσουν οι πάροχοι έως τις 17 Φεβρουαρίου 2023.<sup>69</sup>

Οι εν λόγω πάροχοι, λοιπόν, θα πρέπει να εντοπίζουν, αναλύουν και αξιολογούν τυχόν σημαντικούς συστημικούς κινδύνους που απορρέουν από τη λειτουργία και τη

---

<sup>67</sup> Άρθρο 33 του Κανονισμού (ΕΕ) 2022/2065.

<sup>68</sup>Κανονισμός για τις ψηφιακές υπηρεσίες: η Επιτροπή ορίζει τις πρώτες πολύ μεγάλες επιγραμμικές πλατφόρμες και μηχανές αναζήτησης. Διαθέσιμο στο: [https://ec.europa.eu/commission/presscorner/detail/el/ip\\_23\\_2413](https://ec.europa.eu/commission/presscorner/detail/el/ip_23_2413) (Τελευταία πρόσβαση: 13/06/2023)

<sup>69</sup> Άρθρο 24 παρ. 2 του Κανονισμού (ΕΕ) 2022/2065.

χρήση των υπηρεσιών τους στην Ένωση, τουλάχιστον μία φορά ετησίως<sup>70</sup>. Οι κίνδυνοι αυτοί αφορούν τη διάδοση παράνομου περιεχομένου, τυχόν αρνητικές επιπτώσεις ως προς την άσκηση θεμελιωδών δικαιωμάτων (πχ. ανθρωπίνης αξιοπρέπειας, προστασία δεδομένων προσωπικού χαρακτήρα, ελευθερία της έκφρασης κτλ.), τον πολιτικό διάλογο και τις εκλογικές διαδικασίες, καθώς και τη δημόσια ασφάλεια και υγεία. Για την αντιμετώπιση τους, πρέπει να ληφθούν εύλογα, αναλογικά και αποτελεσματικά μέτρα περιορισμού<sup>71</sup>, όπως είναι η προσαρμογή των συστημάτων ελέγχου περιεχομένου ή συστάσεων, μέτρα για τον περιορισμό της προβολής διαφημίσεων, την ενίσχυση των εσωτερικών διαδικασιών ανίχνευσης συστημικών κινδύνων, την έναρξη ή προσαρμογή της συνεργασίας με αξιόπιστες πηγές επισήμανσης παράνομου περιεχομένου. Σε περιόδους κρίσης<sup>72</sup>, η Επιτροπή κατόπιν σύστασης του Συμβουλίου δύναται να εκδώσει απόφαση με την οποία απαιτεί από έναν ή περισσότερους παρόχους πολύ μεγάλων επιγραμμικών πλατφορμών ή πολύ μεγάλων επιγραμμικών μηχανών αναζήτησης να αξιολογήσουν κατά πόσο η λειτουργία και χρήση των υπηρεσιών τους συμβάλλουν σε σοβαρή απειλή, να προσδιορίσουν τα αποτελεσματικά και αναλογικά μέτρα εξάλειψης ή περιορισμού σοβαρής απειλής και να υποβάλουν σχετική έκθεση στην Επιτροπή<sup>73</sup>. Αξίζει να σημειωθεί ότι οι πάροχοι υπόκεινται, με δικά τους έξοδα και τουλάχιστον μια φορά ανά έτος, σε ανεξάρτητους ελέγχους για την αξιολόγηση της συμμόρφωσης με τις υποχρεώσεις του τρίτου κεφαλαίου, τους κώδικες δεοντολογίας και τα πρωτόκολλα διαχείρισης κρίσης<sup>74</sup>. Ακολούθως, επιβάλλονται ακόμη, υποχρεώσεις διαφάνειας αναφορικά με τη χρήση συστημάτων συστάσεων και τη διαδικτυακή διαφήμιση<sup>75</sup>. Περαιτέρω, σύμφωνα με το άρθρο 40 οι πάροχοι πολύ μεγάλων επιγραμμικών

---

<sup>70</sup> Άρθρο 34 του Κανονισμού (ΕΕ) 2022/2065.

<sup>71</sup> Άρθρο 35 του Κανονισμού (ΕΕ) 2022/2065.

<sup>72</sup> Αιτιολογική Σκέψη 91 του Κανονισμού

<sup>73</sup> Άρθρο 36 του Κανονισμού (ΕΕ) 2022/2065

<sup>74</sup> Άρθρο 37 του Κανονισμού (ΕΕ) 2022/2065

<sup>75</sup> Άρθρα 38 - 39 του Κανονισμού (ΕΕ) 2022/2065

πλατφορμών ή πολύ μεγάλων επιγραμμικών μηχανών αναζήτησης παρέχουν στον συντονιστή ψηφιακών υπηρεσιών της χώρας εγκατάστασης ή στην Επιτροπή πρόσβαση σε δεδομένα, τα οποία είναι αναγκαία για την παρακολούθηση και την αξιολόγηση της συμμόρφωσης με τον Κανονισμό. Επιπλέον, θεσπίζουν μια υπηρεσία συμμόρφωσης<sup>76</sup>, ανεξάρτητη από τις επιχειρησιακές τους λειτουργίες και διασφαλίζουν ότι θα συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα που σχετίζονται με τον Κανονισμό<sup>77</sup>. Προκειμένου να διασφαλιστεί η διαθεσιμότητα των πόρων που απαιτούνται για την επαρκή εποπτεία σε επίπεδο Ένωσης δυνάμει του παρόντος κανονισμού, τα κράτη μέλη θα δικαιούνται να επιβάλλουν στους παρόχους που είναι εγκατεστημένοι στην επικράτειά τους εποπτικό τέλος αναφορικά με τα καθήκοντα εποπτείας και επιβολής που ασκούν οι αρχές τους, το ύψος του οποίου θα πρέπει να καθορίζεται σε ετήσια βάση<sup>78</sup>. Τέλος, το έκτο τμήμα εισάγει ρυθμίσεις σχετικά με πρότυπα<sup>79</sup>, κώδικες δεοντολογίας για την online διαφήμιση και την προσβασιμότητα και πρωτόκολλα διαχείρισης κρίσεων ως μορφές αυτορρύθμισης που προωθεί η Επιτροπή και το Συμβούλιο.

#### **4.3 Αξιολόγηση του Κανονισμού 2022/2065 από άποψη προσωπικών δεδομένων**

Ενόψει των όσων εκτέθηκαν ανωτέρω, η ψήφιση του Κανονισμού 2022/2065 για τις Ψηφιακές Υπηρεσίες (Digital Services Act - DSA) από την Ευρωπαϊκή Ένωση σηματοδότησε μια ουσιαστική μεταρρύθμιση του ρυθμιστικού πλαισίου που διέπει τη λειτουργία των επιγραμμικών πλατφορμών, διαθέτοντας εκτενείς προβλέψεις για τις διαδικασίες ρύθμισης περιεχομένου, καλύπτοντας το κενό της Οδηγίας για το ηλεκτρονικό εμπόριο, το οποίο δεν διέθετε ρυθμίσεις για την ειδοποίηση και απόσυρση περιεχομένου. Πέραν τούτου, εισήχθησαν υποχρεώσεις διαφάνειας,

---

<sup>76</sup> όπως ορίζεται στο άρθρο 41 του Κανονισμού 2022/2065

<sup>77</sup> Αιτιολογική Σκέψη 99 και άρθρο 43 του Κανονισμού 2022/2065

<sup>78</sup> Αιτιολογική Σκέψη 101 του Κανονισμού 2022/2065

<sup>79</sup> Άρθρο 44 του Κανονισμού (ΕΕ) 2022/2065.

δέουσας επιμέλειας και λογοδοσίας των παρόχων υπηρεσιών της κοινωνίας της πληροφορίας (ΚΤΠ) που συμβάλλουν σε ένα πιο ασφαλές επιγραμμικό περιβάλλον, αντιμετωπίζοντας τις αδυναμίες του προϋπάρχοντος πλαισίου. Οι νέες αυτές ρυθμίσεις του Κανονισμού είναι, πάντως, διαδικαστικού χαρακτήρα, δεν εκτείνονται σε ρυθμίσεις ουσίας ούτε και υπάρχει νομοθετική παραπομπή στον Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (στο εξής «ΧΘΔΕΕ») και στις αποφάσεις του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου ή των εθνικών Δικαστηρίων.<sup>80</sup> Ο Κανονισμός ουσιαστικά «νομιμοποιεί» και γενικεύει μια ισχύουσα πρακτική, τη ρύθμιση περιεχομένου, δηλαδή θέτει για πρώτη φορά πανευρωπαϊκά κανόνες, όπου προηγουμένως υπήρχε νομολογιακή και de facto ρύθμιση, και περιέχει διατάξεις για τη διαδικασία της ειδοποίησης και απόσυρσης περιεχομένου, προκειμένου να αποφεύγονται καταχρηστικές πρακτικές των παρόχων.

Ωστόσο, το ζήτημα της συμβατότητας των νέων αυτών ρυθμίσεων με το θεμελιώδες δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα εγείρει σημαντικούς προβληματισμούς, καθώς δημιουργείται το ερώτημα αν με τις προβλέψεις αυτές επιβάλλεται ταυτόχρονα ένα γενικευμένο καθεστώς επιτήρησης. Το ερώτημα αυτό είχε απασχολήσει στο παρελθόν το Δικαστήριο της Ευρωπαϊκής Ένωσης, με αφορμή τις υποθέσεις SABAM v. Netlog (C-360/10)<sup>81</sup> και Scarlet Extended v. SABAM<sup>82</sup>, κατά τις οποίες ερευνήθηκε το αν μπορεί να διαταχθεί ένας πάροχος υπηρεσιών φιλοξενίας να θέσει σε λειτουργία, για ολόκληρη την πελατεία του, in abstracto και προληπτικά, με δικά του έξοδα και χωρίς χρονικό περιορισμό, ένα

---

<sup>80</sup> Ιγγλεζάκης Ι. (2024), Προστασία προσωπικών δεδομένων και ελευθερία της έκφρασης στο διαδίκτυο, στο πλαίσιο της εφαρμογής της Πράξης της ΕΕ για τις ψηφιακές υπηρεσίες, Επιθεώρηση Δικαίου Πληροφορικής, Τόμ. 5, Αρ.2, σελ. 13

<sup>81</sup> ΔΕΕ, Απόφαση της 16ης Φεβρουαρίου 2012, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, C-360/10, EU:C:2012:85, σκ. 38

<sup>82</sup> ΔΕΕ, Απόφαση της 24ης Νοεμβρίου 2011, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, EU:C:2011:771, σκ. 25, 40

σύστημα φιλτραρίσματος του μεγαλύτερου μέρους των αποθηκευμένων στους διακομιστές του πληροφοριών προκειμένου να εντοπίζει εκεί ηλεκτρονικά αρχεία που περιέχουν μουσικά, κινηματογραφικά ή οπτικοακουστικά έργα επί των οποίων υφίστανται δικαιώματα πνευματικής ιδιοκτησίας και στη συνέχεια να μπλοκάρει την ανταλλαγή τους. Το Δικαστήριο έκρινε ότι κάτι τέτοιο αποτελεί εκτεταμένη επεξεργασία των πληροφοριών, η οποία επιτρέπει την ταυτοποίηση των χρηστών και κατ' επέκταση την παραβίαση θεμελιωδών δικαιωμάτων. Συνεπώς, δέχθηκε ότι δικαίωμα διανοητικής ιδιοκτησίας δεν υπερέχει του δικαιώματος στην προστασία δεδομένων.

Παρόμοιο προβληματισμό πραγματεύεται και η απόφαση C-401/19 (Πολωνία κατά Κοινοβουλίου και Συμβουλίου)<sup>83</sup>, αναφορικά με την Οδηγία 2019/790<sup>84</sup> για τη διανοητική ιδιοκτησία στην ψηφιακή ενιαία αγορά. Ειδικότερα, το Δικαστήριο απεφάνθη ότι το ειδικό καθεστώς ευθύνης για τους παρόχους επιγραμμικών υπηρεσιών ανταλλαγής περιεχομένου ενέχει περιορισμό της άσκησης του δικαιώματος στην ελευθερία έκφρασης και πληροφόρησης των χρηστών των εν λόγω υπηρεσιών ανταλλαγής περιεχομένου. Ωστόσο, σύμφωνα με το ΔΕΕ ένας τέτοιος περιορισμός, δικαιολογείται μονάχα εφόσον πληρούνται οι όροι του άρθρου 52 παρ. 1 ΧΘΕΕ<sup>85</sup>, καθώς είναι απαραίτητος για την ικανοποίηση της ανάγκης αυτής, δηλαδή νομιμότητα, αναγκαιότητα και αναλογικότητα.

---

<sup>83</sup> ΔΕΕ, Απόφαση της 26ης Απριλίου 2022, Δημοκρατία της Πολωνίας κατά Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της Ευρωπαϊκής Ένωσης, C-401/19, EU:C:2022:297

<sup>84</sup> Οδηγία 219/790 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τα δικαιώματα πνευματικής ιδιοκτησίας και τα συγγενικά δικαιώματα στην ψηφιακή ενιαία αγορά και την τροποποίηση των οδηγιών 96/9/ΕΚ και 2001/29/ΕΚ.

<sup>85</sup> Κάθε περιορισμός στην άσκηση των δικαιωμάτων και ελευθεριών που αναγνωρίζονται στον παρόντα Χάρτη πρέπει να προβλέπεται από το νόμο και να σέβεται το βασικό περιεχόμενο των εν λόγω δικαιωμάτων και ελευθεριών. Τηρουμένης της αρχής της αναλογικότητας, περιορισμοί επιτρέπεται να επιβάλλονται μόνον εφόσον είναι αναγκαίοι και

Σε αυτό το πλαίσιο, μπορεί να εφαρμοστεί η ίδια συλλογιστική και στον Κανονισμό DSA. Οι υποχρεώσεις που επιβάλλονται στους παρόχους να διαθέτουν μηχανισμούς ειδοποίησης και δράσης για την απόσυρση παράνομου περιεχομένου δεν θεωρείται ότι παραβιάζουν την αρχή της αναλογικότητας. Αφενός, δεν επιβάλλεται ένα καθεστώς γενικευμένης επιτήρησης των χρηστών, καθώς παρέμβαση του παρόχου ενεργοποιείται μόνο όταν υπάρχει συγκεκριμένη καταγγελία. Αφετέρου, οι ρυθμίσεις αυτές εξυπηρετούν έναν υπέρτατο σκοπό, ήτοι την προστασία των δικαιωμάτων τρίτων, τα οποία πλήττονται από την παρουσία παράνομων αναρτήσεων στο διαδίκτυο.

Βέβαια, παρά τη θετική αρωγή του DSA στη διαμόρφωση ενός ασφαλούς ψηφιακού οικοσυστήματος, η προστασία των δεδομένων προσωπικού χαρακτήρα δεν αποτελεί κεντρικό άξονα αυτής της νομοθετικής παρέμβασης, καθώς δεν προβλέπει ειδικές εγγυήσεις για την προστασία των δεδομένων κατά τις διαδικασίες ειδοποίησης και δράσης (notice and action), την υποβολή καταγγελιών ή τη χρήση αυτοματοποιημένων εργαλείων ελέγχου.

Ο Ευρωπαϊός Επόπτης Προστασίας Δεδομένων (European Data Protection Supervisor, εφεξής «ΕΕΠΔ» ή «EDPS») είχε εκφράσει, ήδη στο στάδιο της νομοπαρασκευαστικής διαδικασίας (Γνωμοδότηση 1/2021)<sup>86</sup>, ανησυχίες αναφορικά με την ισορροπία που επιχειρεί να επιτύχει ο Κανονισμός DSA μεταξύ διαφάνειας και προστασίας προσωπικών δεδομένων. Ενώ ο Κανονισμός επιδιώκει την ενίσχυση της εμπιστοσύνης στο διαδίκτυο μέσω ανοικτών διαδικασιών, ελλοχεύει ο κίνδυνος τα προσωπικά δεδομένα να διαρρεύσουν ή να υποστούν κατάχρηση, αν δεν προβλέπονται σαφείς περιορισμοί και εγγυήσεις.

---

ανταποκρίνονται πραγματικά σε στόχους γενικού ενδιαφέροντος που αναγνωρίζει η Ένωση ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων.

<sup>86</sup> European Data Protection Supervisor (2021), Opinion 1/2021 on the Proposal of a Digital Services Act

Ελλείψει, λοιπόν, αυτών των ειδικών διατάξεων, τυγχάνουν εφαρμογής οι γενικές διατάξεις του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ)<sup>87</sup>. Πέρα από τις γενικές διατάξεις για τη νομιμότητα της επεξεργασίας που στηρίζεται στη διάταξη του άρθρου 6 παρ. 1 στοιχ. γ' ΓΚΠΔ και αφορά την εκπλήρωση έννομης υποχρέωσης<sup>88</sup>, οι πάροχοι πρέπει να παρέχουν εγγυήσεις για την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων<sup>89</sup> και να εφαρμόζουν την αρχή της προστασίας δεδομένων ήδη από το σχεδιασμό (privacy by design)<sup>90</sup>.

Εν κατακλείδι, η αποτελεσματική προστασία των θεμελιωδών δικαιωμάτων των χρηστών στον ψηφιακό χώρο προϋποθέτει την ορθή και συνεπή εφαρμογή του ΓΚΠΔ παράλληλα με τις διατάξεις του Κανονισμού 2022/2065. Σε αυτό το πλαίσιο, η ενεργός συμμετοχή και ο εποπτικός ρόλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (στο εξής «ΑΠΔΠΧ») καθίσταται κρίσιμος. Η εν λόγω αρχή οφείλει να συμβάλλει καθοριστικά στην ερμηνεία και στην πρακτική εφαρμογή των, κατά τόπους, ασαφών ή ανοιχτών διατάξεων του DSA, ώστε να διασφαλιστεί ότι η ψηφιακή ρύθμιση δεν θα λειτουργήσει εις βάρος των θεμελιωδών ελευθεριών, αλλά ως μηχανισμός ενίσχυσής τους.

---

<sup>87</sup> I. Ιγγλεζάκης (2020), Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679 και ο Εφαρμοστικός Νόμος – Ν. 4624/2019) (γ' έκδοση), σελ. 337

<sup>88</sup> «η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας»

<sup>89</sup> Άρθρα 12 - 22 του Κανονισμού (ΕΕ) 2016/679

<sup>90</sup> Άρθρο 25 του Κανονισμού (ΕΕ) 2016/679

## 5. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΙΣ ΨΗΦΙΑΚΕΣ ΠΛΑΤΦΟΡΜΕΣ

### 5.1 Ο έλεγχος πληροφοριών ως πρακτική επεξεργασίας προσωπικών δεδομένων στις ψηφιακές πλατφόρμες

Η λειτουργία των ψηφιακών πλατφορμών, όπως αναλύθηκε προηγουμένως, δεν εξαντλείται στην παροχή τεχνικών υπηρεσιών φιλοξενίας και μετάδοσης περιεχομένου, αλλά περιλαμβάνει ένα σύνθετο πλέγμα πρακτικών ελέγχου, ιεράρχησης και επιμέλειας της πληροφορίας. Οι πρακτικές αυτές, ανεξαρτήτως του αν ασκούνται μέσω ανθρώπινης εποπτείας ή αυτοματοποιημένων αλγοριθμικών συστημάτων, προϋποθέτουν κατ' ανάγκη τη συλλογή, την ανάλυση και την αξιολόγηση δεδομένων που αφορούν τα υποκείμενα των δεδομένων. Ως εκ τούτου, ο έλεγχος περιεχομένου δεν μπορεί να νοηθεί αποκομμένα από το δίκαιο προστασίας προσωπικών δεδομένων, αλλά συνιστά μορφή επεξεργασίας κατά την έννοια του Γενικού Κανονισμού Προστασίας Δεδομένων.

Η έννοια της «επεξεργασίας»<sup>91</sup> ορίζεται με ιδιαίτερα ευρύ τρόπο και περιλαμβάνει κάθε πράξη ή σειρά πράξεων που πραγματοποιούνται επί προσωπικών δεδομένων, όπως η συλλογή, η καταχώριση, η οργάνωση, η αποθήκευση, η προσαρμογή, η ανάκτηση, η χρήση, η διαβίβαση, η διαγραφή ή η καταστροφή τους. Στο πλαίσιο αυτό, η αξιολόγηση μιας ανάρτησης, η επισήμανσή της ως παραπλανητικής, η υποβάθμιση της προβολής της (downranking), η αφαίρεσή της ή ακόμη και η εξατομικευμένη κατάταξη περιεχομένου, με βάση το προφίλ του χρήστη, συνιστούν αυτοτελείς πράξεις επεξεργασίας προσωπικών δεδομένων.

Ιδιαίτερη σημασία παρουσιάζει το γεγονός ότι τα δεδομένα που υφίστανται επεξεργασία κατά τον έλεγχο περιεχομένου δεν περιορίζονται σε προφανή στοιχεία ταυτοποίησης, όπως το όνομα ή η διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη.

---

<sup>91</sup> Άρθρο 4 παρ. 2 του Κανονισμού (ΕΕ) 2016/679

Αντιθέτως, περιλαμβάνουν δεδομένα συμπεριφοράς, μεταδεδομένα (metadata), δεδομένα λόγου και έκφρασης, καθώς και πληροφορίες που προκύπτουν από την αλληλεπίδραση του χρήστη με το περιεχόμενο και τους μηχανισμούς της πλατφόρμας. Οι πληροφορίες αυτές, είτε μεμονωμένα είτε σε συνδυασμό, δύνανται να σκιαγραφήσουν λεπτομερώς το ψηφιακό προφίλ του υποκειμένου, καθιστώντας το αναγνωρίσιμο και προβλέψιμο ως προς τις προτιμήσεις, τις απόψεις και τη συμπεριφορά του.<sup>92</sup>

Στο σημείο αυτό αναδεικνύεται μια κρίσιμη ιδιαιτερότητα των ψηφιακών πλατφορμών: ο έλεγχος πληροφοριών δεν αποτελεί απλώς αντίδραση σε μεμονωμένα περιστατικά παράνομου ή επιβλαβούς περιεχομένου, αλλά εντάσσεται σε ένα διαρκές και συστηματικό μοντέλο επιτήρησης και αξιολόγησης της δραστηριότητας των χρηστών. Η συνεχής αυτή επεξεργασία μετατοπίζει το βάρος από την εκ των υστέρων αντιμετώπιση παραβάσεων σε μια προληπτική και προβλεπτική λογική, η οποία βασίζεται στη μαζική συλλογή δεδομένων και στην αλγοριθμική ανάλυσή τους.

Υπό το πρίσμα αυτό, ο έλεγχος περιεχομένου αποκτά έντονη κανονιστική διάσταση, καθώς επηρεάζει άμεσα την άσκηση θεμελιωδών δικαιωμάτων, όπως η ελευθερία της έκφρασης και το δικαίωμα στην πληροφόρηση, ενώ ταυτόχρονα εγείρει σοβαρά ζητήματα προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων. Η επεξεργασία δεδομένων στο πλαίσιο της ρύθμισης του ψηφιακού λόγου δεν αποτελεί, συνεπώς, ουδέτερη τεχνική πρακτική, αλλά πράξη με σαφές νομικό και συνταγματικό αποτύπωμα.

## **5.2 Νομοθετική εξέλιξη της προστασίας προσωπικών δεδομένων σε συνάρτηση με τις ψηφιακές πλατφόρμες**

---

<sup>92</sup> Ιγγλεζάκης Ι. (2020), Δίκαιο της Πληροφορίας και της Επικοινωνίας, σελ. 351 επ.

Η προστασία των προσωπικών δεδομένων, ιδίως στο ψηφιακό περιβάλλον, αποτελεί ένα από τα θεμελιώδη, σύγχρονα ζητήματα του ευρωπαϊκού και διεθνούς νομικού πλαισίου. Η ραγδαία εξέλιξη των τεχνολογιών πληροφορίας και επικοινωνίας και η εκτεταμένη χρήση των ψηφιακών πλατφορμών έχουν καταστήσει επιτακτική την ανάγκη για νομική ρύθμιση που να εξασφαλίζει την προστασία των προσωπικών δεδομένων, ενώ παράλληλα να επιτρέπει την ομαλή λειτουργία της ψηφιακής οικονομίας.

Η έκδοση, το 1995, της Οδηγίας 95/46/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου αποτέλεσε την πρώτη σημαντική νομοθετική πρωτοβουλία σε επίπεδο ΕΕ για την προστασία των δεδομένων προσωπικού χαρακτήρα<sup>93</sup>. Παρόλο που η Οδηγία θέσπισε έναν ενιαίο νομικό κανονισμό για τα κράτη-μέλη, η εφαρμογή της παρέμενε σε μεγάλο βαθμό εξαρτώμενη από την εναρμόνιση των εθνικών νομοθεσιών, γεγονός που περιοριζε την αποτελεσματικότητα της προστασίας και καθιστούσε τη συμμόρφωση των ψηφιακών πλατφορμών ευμετάβλητη από χώρα σε χώρα.<sup>94</sup>

Η Ευρωπαϊκή Ένωση, ανταποκρινόμενη στην ασυμμετρία εφαρμογής της Οδηγίας από τα κράτη μέλη και στις σύνθετες προκλήσεις της ταχέως εξελισσόμενης ψηφιακής πραγματικότητας προχώρησε στην θέσπιση του Κανονισμού (ΕΕ) 2016/679 «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/EK» (εφεξής «Γενικός Κανονισμός

---

<sup>93</sup> Οδηγία 95/46/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Διαθέσιμο σε: <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046> (τελευταία πρόσβαση 20/06/2025)

<sup>94</sup> Μήτρου Α. (2004), *Ιδιωτικότητα στο WEB 2.0*. ΔΙΤΕ (π ΔΙΜΕΕ) (3), σελ. 319 επ.

Προστασίας Δεδομένων» ή «ΓΚΠΔ» ή «Κανονισμός»). Ο Κανονισμός αυτός σηματοδοτεί τη μετάβαση από μια προσπάθεια συμμόρφωσης επιμέρους εθνικών διατάξεων σε ένα εναρμονισμένο, ενιαίο και άμεσα εφαρμοστέο ρυθμιστικό πλαίσιο, ενισχύοντας τα δικαιώματα των υποκειμένων και ενσωματώνοντας τις τεχνολογικές εξελίξεις στη νέα ψηφιακή εποχή.

Ιδιαίτερη σημασία για τις ψηφιακές πλατφόρμες έχει το γεγονός ότι ο Κανονισμός ενσωματώνει έννοιες και μηχανισμούς που ανταποκρίνονται στις πρακτικές του σύγχρονου ψηφιακού ελέγχου, όπως η αρχή της λογοδοσίας, η προστασία δεδομένων εξ ορισμού και εξ σχεδιασμού (privacy by design and by default), καθώς και οι ειδικές ρυθμίσεις για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ. Οι διατάξεις αυτές αποκτούν ιδιαίτερη βαρύτητα, όπως αναλύεται και στη συνέχεια, όταν εφαρμόζονται σε περιβάλλοντα όπου η ρύθμιση της πληροφορίας βασίζεται σε αλγοριθμικά συστήματα κατάταξης και φιλτραρίσματος.

Συνολικά, η νομοθετική αυτή εξέλιξη αποτυπώνει μια σαφή μετατόπιση, από την αντίληψη της προστασίας προσωπικών δεδομένων ως αμιγώς ατομικού δικαιώματος προς μια θεώρησή της ως θεμελιώδους πυλώνα της δημοκρατικής ψηφιακής δημόσιας σφαίρας. Στο πλαίσιο αυτό, η επεξεργασία δεδομένων που πραγματοποιείται κατά τον έλεγχο πληροφοριών από τις πλατφόρμες καθίσταται αντικείμενο αυξημένης κανονιστικής προσοχής.

### **5.3. Κανονιστική αποτίμηση του ελέγχου περιεχομένου υπό το πρίσμα του Γενικού Κανονισμού Προστασίας Δεδομένων**

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ), ως το κατεξοχήν δεσμευτικό ενωσιακό πλαίσιο προστασίας της ιδιωτικής ζωής<sup>95</sup> και των προσωπικών δεδομένων,

---

<sup>95</sup> Βλ. σχετικά την ανακοίνωση του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων με αφορμή την τρίτη επέτειο εφαρμογής του ΓΚΠΔ, όπου ο Κανονισμός χαρακτηρίζεται ως μείζον νομοθετικό επίτευγμα για την Ευρώπη και τους πολίτες της, ιδίως ως προς την ανάδειξη του

αποτελεί βασικό κανονιστικό σημείο αναφοράς για την αξιολόγηση της λειτουργίας των ψηφιακών πλατφορμών. Η εφαρμογή του αποκτά ιδιαίτερη σημασία όταν εξετάζεται σε συνάρτηση με τις πρακτικές ελέγχου, ιεράρχησης και επιμέλειας της πληροφορίας, οι οποίες, όπως αναλύθηκε ανωτέρω, στηρίζονται σε συστηματική και συχνά αυτοματοποιημένη επεξεργασία δεδομένων των χρηστών.

Υπό το πρίσμα αυτό, ο έλεγχος περιεχομένου δεν μπορεί να εκλαμβάνεται ως ουδέτερη ή δευτερεύουσα λειτουργία, αλλά ως κανονιστικά κρίσιμη πρακτική, η οποία εγείρει ζητήματα συμμόρφωσης με τις θεμελιώδεις αρχές του Κανονισμού. Ιδίως, ανακύπτουν ερωτήματα ως προς τον προσδιορισμό των ψηφιακών πλατφορμών ως υπευθύνων επεξεργασίας, τη νομιμότητα των επιμέρους μορφών επεξεργασίας που λαμβάνουν χώρα στο πλαίσιο του ελέγχου περιεχομένου, καθώς και τα όρια της επιτρεπτής παρέμβασης όταν αυτή επηρεάζει θεμελιώδη δικαιώματα, όπως η ιδιωτικότητα και η ελευθερία της έκφρασης. Τα ζητήματα αυτά αποτελούν αντικείμενο της κανονιστικής ανάλυσης που ακολουθεί.

### ***5.3.1 Οι ψηφιακές πλατφόρμες ως υπεύθυνοι επεξεργασίας κατά τον έλεγχο περιεχομένου***

Η κανονιστική αξιολόγηση των πρακτικών ελέγχου περιεχομένου προϋποθέτει την αποσαφήνιση του ρόλου που διαδραματίζουν οι ψηφιακές πλατφόρμες στην επεξεργασία των προσωπικών δεδομένων. Οι πλατφόρμες, όπως έχει προαναφερθεί, δύνανται να συλλέγουν συστηματικά, να αναλύουν και να αξιοποιούν προσωπικά δεδομένα χρηστών για σκοπούς εμπορικούς, διαφημιστικούς ή ακόμα και πολιτικής επιρροής<sup>96</sup>. Από νομικής απόψεως, οι πλατφόρμες αυτές εντάσσονται στην έννοια του «υπεύθυνου επεξεργασίας» ή του «εκτελούντος την επεξεργασία», ανάλογα με τον

---

δικαιώματος στην ιδιωτική ζωή και την προστασία των προσωπικών δεδομένων/ Serban A. - Barbosa Teixeira C. (2021) , Data Protection and Digital Services – European Union Perspectives, p. 311

<sup>96</sup> Lynskey O., (2015), The Foundations of EU Data Protection Law, Oxford University Press, p. 260

βαθμό ελέγχου που ασκούν επί των δεδομένων και των σκοπών της επεξεργασίας.<sup>97</sup> Σύμφωνα με τον Κανονισμό<sup>98</sup>, ως υπεύθυνος επεξεργασίας ορίζεται το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ενώ ο εκτελών την επεξεργασία<sup>99</sup> είναι αυτός επεξεργάζεται δεδομένα για λογαριασμό του υπευθύνου. Αμφότεροι υπέχουν σειρά υποχρεώσεων σχετικά με τη διαφάνεια, τη λογοδοσία, τη συμμόρφωση με τις αρχές της ελαχιστοποίησης και της ασφάλειας, αλλά και την προστασία των δικαιωμάτων των υποκειμένων.

Στην περίπτωση των ψηφιακών πλατφορμών, οι πρακτικές ρύθμισης της ορατότητας, της διάδοσης και της αξιολόγησης περιεχομένου παραπέμπουν σε σαφή καθορισμό των σκοπών και των μέσων επεξεργασίας των προσωπικών δεδομένων, γεγονός που θεμελιώνει τον χαρακτηρισμό τους ως υπεύθυνων ή εκτελούντων την επεξεργασία. Επιπλέον, ο εν λόγω χαρακτηρισμός δεν αναιρείται από την ενδεχόμενη ανάθεση επιμέρους λειτουργιών ελέγχου ή τεχνικής υποστήριξης σε τρίτους - υπεργολάβους, καθόσον ο ουσιαστικός καθορισμός των σκοπών και των μέσων της επεξεργασίας παραμένει αδιαπραγμάτευτα στην αρμοδιότητα των ίδιων των πλατφορμών.

Η ανωτέρω προσέγγιση ενισχύεται περαιτέρω από τη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης, η οποία υιοθετεί μια λειτουργική και ευρεία ερμηνεία της έννοιας του υπευθύνου επεξεργασίας, εστιάζοντας όχι στην τυπική κατοχή των δεδομένων, αλλά στην πραγματική επιρροή επί του καθορισμού της επεξεργασίας.

---

<sup>97</sup> Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, WP169.

<sup>98</sup> Άρθρο 4 παρ. 7 του Κανονισμού (ΕΕ) 2016/679

<sup>99</sup> Άρθρο 4 παρ. 8 του Κανονισμού (ΕΕ) 2016/679

Ειδικότερα, στην υπόθεση C-210/16 *Wirtschaftsakademie*<sup>100</sup> το ΔΕΕ αναγνώρισε την ιδιότητα του από κοινού υπευθύνου επεξεργασίας (joint controller)<sup>101</sup> σε διαχειριστή σελίδας κοινωνικού δικτύου, λόγω της συμβολής του στον καθορισμό των παραμέτρων συλλογής και ανάλυσης δεδομένων επισκεπτών. Αντίστοιχα, στην υπόθεση C-40/17 *Fashion ID*<sup>102</sup> κρίθηκε ότι ακόμη και η ενσωμάτωση τεχνολογιών τρίτων (plug-ins), οι οποίες ενεργοποιούν τη συλλογή δεδομένων χρηστών, αρκεί για τη θεμελίωση ευθύνης ως προς τον καθορισμό των σκοπών και των μέσων της επεξεργασίας. Τέλος, η υπόθεση C-131/12 *Google Spain*<sup>103</sup> ανέδειξε ότι η αυτοματοποιημένη ευρετηρίαση, οργάνωση και προβολή πληροφοριών συνιστά αυτοτελή πράξη επεξεργασίας, για την οποία ο φορέας που καθορίζει τη λειτουργία της φέρει την ιδιότητα του υπευθύνου επεξεργασίας.

Κατά συνέπεια, ο χαρακτηρισμός των ψηφιακών πλατφορμών ως υπευθύνων επεξεργασίας κατά τον έλεγχο περιεχομένου δεν αποτελεί απλώς θεωρητική κατασκευή, αλλά προκύπτει από τη λειτουργική πραγματικότητα της ψηφιακής διακυβέρνησης της πληροφορίας. Ως εκ τούτου, οι ψηφιακές πλατφόρμες υπέχουν τις πλήρεις υποχρεώσεις που απορρέουν από τον Κανονισμό, συμπεριλαμβανομένης της τήρησης των θεμελιωδών αρχών της νομιμότητας, της διαφάνειας και της λογοδοσίας, γεγονός που καθιστά αναγκαία τη διερεύνηση των νόμιμων βάσεων επεξεργασίας στις οποίες μπορούν να στηριχθούν οι πρακτικές ελέγχου περιεχομένου.

---

<sup>100</sup> Σκέψη 39

<sup>101</sup> Άρθρο 26 παρ.1 εδ. α' του Κανονισμού (ΕΕ) 2016/679: «Σε περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας, αποτελούν από κοινού υπευθύνους επεξεργασίας»

<sup>102</sup> Σκέψη 96

<sup>103</sup> Σκέψη 41

### *5.3.2 Νόμιμες βάσεις επεξεργασίας προσωπικών δεδομένων κατά τον έλεγχο περιεχομένου*

Η επεξεργασία προσωπικών δεδομένων που λαμβάνει χώρα στο πλαίσιο του ελέγχου περιεχομένου από τις ψηφιακές πλατφόρμες προϋποθέτει την ύπαρξη συγκεκριμένης και έγκυρης νόμιμης βάσης<sup>104</sup>. Ειδικότερα, οι βάσεις επεξεργασίας που τίθενται κατ' αρχήν υπό εξέταση είναι η συγκατάθεση του υποκειμένου των δεδομένων, η αναγκαιότητα για την εκτέλεση σύμβασης και το έννομο συμφέρον του υπευθύνου επεξεργασίας ή τρίτου. Η καταλληλότητα εκάστης εξ αυτών ως θεμελίου για τις πρακτικές ελέγχου περιεχομένου δεν είναι αυτονόητη, αλλά απαιτεί ειδική, ad hoc αξιολόγηση ανάλογα με τη φύση, την έκταση και τη συστηματικότητα της σχετικής επεξεργασίας.

Καταρχάς, η συγκατάθεση<sup>105</sup> του υποκειμένου των δεδομένων (άρθρο 6 παρ. 1 στοιχ. α' ΓΚΠΔ) εμφανίζεται θεωρητικά ως πιθανή βάση επεξεργασίας, ιδίως μέσω της αποδοχής των όρων χρήσης και των πολιτικών περιεχομένου των πλατφορμών. Στην πράξη, ωστόσο, σπανίως πληροί τις αυστηρές προϋποθέσεις του Κανονισμού για έγκυρη συγκατάθεση στο πλαίσιο των συστηματικών πρακτικών ελέγχου περιεχομένου. Τούτο διότι, η σχέση μεταξύ πλατφόρμας και χρήστη χαρακτηρίζεται από έντονη ανισορροπία ισχύος, ενώ η πρόσβαση στις βασικές λειτουργίες της υπηρεσίας συνδέεται συνήθως με την αποδοχή εκτενών και σύνθετων όρων. Υπό αυτές τις συνθήκες, η συγκατάθεση δύσκολα μπορεί να θεωρηθεί ελεύθερη, ειδική και πλήρως ενημερωμένη. Επιπλέον, η δυνατότητα ανάκλησής της θα οδηγούσε πρακτικά στον αποκλεισμό του χρήστη από την υπηρεσία, υπονομεύοντας τον ανακλητό χαρακτήρα της. Για όλους αυτούς τους λόγους, η συγκατάθεση δεν μπορεί να θεωρηθεί πρόσφορη ή ασφαλή νόμιμη βάση επεξεργασίας του ελέγχου περιεχομένου από τις πλατφόρμες.

---

<sup>104</sup> Άρθρο 6 παρ. 1 του Κανονισμού (ΕΕ) 2016/679

<sup>105</sup> Άρθρο 6 παρ. 1 στοιχ. α' του Κανονισμού (ΕΕ) 2016/679

Μία από τις συχνότερα επικαλούμενες βάσεις επεξεργασίας από τις ψηφιακές πλατφόρμες είναι η εκτέλεση της σύμβασης παροχής υπηρεσιών προς τον χρήστη<sup>106</sup>. Οι πλατφόρμες υποστηρίζουν ότι ο έλεγχος περιεχομένου είναι αναγκαίος για τη διασφάλιση της ορθής λειτουργίας της υπηρεσίας, της ασφάλειας του ψηφιακού περιβάλλοντος και της συμμόρφωσης με τους όρους της κοινότητας. Παρολαυτά, η συμβατική βάση πρέπει να ερμηνεύεται στενά. Η απλή πρόβλεψη πρακτικών ελέγχου στους όρους χρήσης δεν αρκεί για να θεωρηθεί ότι κάθε επεξεργασία είναι αναγκαία για την εκτέλεση της σύμβασης. Ιδίως όταν οι πρακτικές αυτές υπερβαίνουν την αντιμετώπιση σαφώς παράνομου περιεχομένου και επεκτείνονται σε αξιολογικές κρίσεις, προληπτική επιτήρηση ή αλγοριθμική ιεράρχηση βάσει προφίλ χρηστών, η σύνδεσή του με την εκτέλεση της σύμβασης καθίσταται αμφίβολη και η επίκληση του άρθρου 6 παρ. 1 στοιχ. β' του Κανονισμού ενδέχεται να οδηγεί σε καταχρηστική διεύρυνση της έννοιας της συμβατικής αναγκαιότητας.

Η πλέον κρίσιμη και ευρέως χρησιμοποιούμενη νόμιμη βάση επεξεργασίας για τον έλεγχο περιεχομένου είναι το έννομο συμφέρον του υπευθύνου επεξεργασίας<sup>107</sup>. Οι πλατφόρμες επικαλούνται, μεταξύ άλλων, την προστασία της επιχειρηματικής τους λειτουργίας, τη διατήρηση ενός ασφαλούς ψηφιακού περιβάλλοντος και την αποτροπή διάδοσης παράνομου ή επιβλαβούς περιεχομένου. Ωστόσο, η επίκληση του έννομου συμφέροντος προϋποθέτει την τήρηση της τριπλής δοκιμασίας της αναγκαιότητας, της καταλληλότητας και της στάθμισης με τα θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Στο πλαίσιο του ελέγχου περιεχομένου, η στάθμιση αυτή αποκτά ιδιαίτερη σημασία, καθώς η επεξεργασία δεν θίγει μόνο την ιδιωτική ζωή, αλλά και την ελευθερία της έκφρασης και το δικαίωμα στην πληροφόρηση. Συνεπώς, η γενική και αφηρημένη επίκληση του έννομου συμφέροντος δεν επαρκεί, αλλά απαιτείται ειδική αιτιολόγηση

---

<sup>106</sup> Άρθρο 6 παρ. 1 στοιχ. β' του Κανονισμού (ΕΕ) 2016/679

<sup>107</sup> Άρθρο 6 παρ. 1 στοιχ. στ' του Κανονισμού (ΕΕ) 2016/679

λαμβάνοντας υπόψη τον χαρακτήρα του περιεχομένου, τον βαθμό παρέμβασης και τις διαθέσιμες εγγυήσεις για τον χρήστη.

Τέλος, σε ορισμένες περιπτώσεις, ο έλεγχος περιεχομένου μπορεί να θεμελιώνεται στην ανάγκη συμμόρφωσης της πλατφόρμας με νομικές υποχρεώσεις<sup>108</sup>, όπως η αφαίρεση προδήλως παράνομου περιεχομένου κατόπιν δικαστικής ή διοικητικής εντολής. Η βάση αυτή παρουσιάζει μεγαλύτερη ασφάλεια δικαίου, καθώς περιορίζεται σε σαφώς προσδιορισμένες υποχρεώσεις και συνοδεύεται από θεσμικές εγγυήσεις. Ωστόσο, η νομική υποχρέωση δεν μπορεί να χρησιμοποιείται ως γενικό θεμέλιο για ευρείες πρακτικές προληπτικού ελέγχου ή αλγοριθμικής επιτήρησης, ιδίως όταν δεν υφίσταται σαφής και συγκεκριμένη νομοθετική πρόβλεψη. Η διάκριση μεταξύ κανονιστικά επιβεβλημένου ελέγχου και ιδιωτικής ρυθμιστικής πρωτοβουλίας των πλατφορμών παραμένει κρίσιμη για την αποφυγή υπέρμετρων παρεμβάσεων στα δικαιώματα των χρηστών.

Συνολικά, η ανάλυση των νόμιμων βάσεων επεξεργασίας καταδεικνύει ότι ο έλεγχος περιεχομένου δεν μπορεί να στηρίζεται σε γενικές ή αδιαφοροποίητες νομικές βάσεις, αλλά απαιτεί εξειδικευμένη και τεκμηριωμένη κανονιστική θεμελίωση. Ο Κανονισμός λειτουργεί, στο πλαίσιο αυτό, όχι μόνο ως εργαλείο προστασίας της ιδιωτικής ζωής, αλλά και ως μηχανισμός περιορισμού της ιδιωτικής κανονιστικής εξουσίας των ψηφιακών πλατφορμών. Για όλους αυτούς τους λόγους, άλλωστε, η ορθή επιλογή και εφαρμογή της νόμιμης βάσης επεξεργασίας αποτελεί κρίσιμο κριτήριο για τη νομιμότητα και τη θεσμική νομιμοποίηση των πρακτικών ελέγχου πληροφοριών στον ψηφιακό χώρο.

### ***5.3.3 Αρχές επεξεργασίας προσωπικών δεδομένων***

Η διαπίστωση της ύπαρξης νόμιμης βάσης επεξεργασίας δεν αρκεί, αφ' εαυτής, για τη νομιμότητα των πρακτικών ελέγχου περιεχομένου. Στο ευρωπαϊκό ρυθμιστικό

---

<sup>108</sup> Άρθρο 6 παρ. 1 στοιχ. γ' του Κανονισμού (ΕΕ) 2016/679

πλαίσιο, η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν εστιάζει αποκλειστικά στην τήρηση επιμέρους κανόνων, αλλά εδράζεται σε ένα συνεκτικό πλέγμα θεμελιωδών αρχών, οι οποίες διαμορφώνουν το ουσιαστικό και ερμηνευτικό υπόβαθρο του Κανονισμού 2016/679 (ΕΕ). Οι αρχές του άρθρου 5 λειτουργούν ως γενικά κριτήρια αξιολόγησης της νομιμότητας και της θεμιτότητας κάθε πράξης επεξεργασίας, ανεξαρτήτως της εκάστοτε επικαλούμενης νόμιμης βάσης.

Στο πλαίσιο της παρούσας μελέτης, η ανάλυση δεν αποσκοπεί στην εξαντλητική παρουσίαση του συνόλου των αρχών επεξεργασίας, αλλά επικεντρώνεται σε εκείνες που αναδεικνύονται ως καίριες σε σχέση με τις πρακτικές ελέγχου περιεχομένου και πληροφοριών από τις ψηφιακές πλατφόρμες. Η επιλογή αυτή δικαιολογείται από το γεγονός ότι ο έλεγχος περιεχομένου προϋποθέτει, κατά κανόνα, τη συστηματική συλλογή, ανάλυση και αξιολόγηση δεδομένων χρηστών, γεγονός που εντείνει τους κινδύνους προσβολής της ιδιωτικότητας και καθιστά ορισμένες αρχές ιδιαίτερας κρίσιμες ως ουσιαστικά όρια της ιδιωτικής ρυθμιστικής εξουσίας των πλατφορμών.

Υπό το πρίσμα αυτό, ιδιαίτερη σημασία αποκτούν οι αρχές της νομιμότητας, της αντικειμενικότητας και της διαφάνειας (lawfulness, fairness and transparency), του περιορισμού του σκοπού (purpose limitation), της ελαχιστοποίησης των δεδομένων (data minimisation), της ακρίβειας (accuracy), του περιορισμού της περιόδου διατήρησης (storage limitation), της ακεραιότητας και εμπιστευτικότητας (integrity and confidentiality), καθώς και της λογοδοσίας (accountability). Οι αρχές αυτές αναλύονται κατωτέρω, καθόσον συνδέονται άμεσα με τις διαδικασίες αξιολόγησης, κατάταξης, υποβάθμισης ή αφαίρεσης περιεχομένου και επηρεάζουν ουσιαστικά τα δικαιώματα των χρηστών.

Καταρχάς, η τριπλή αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας (lawfulness, fairness and transparency) απαιτεί η επεξεργασία να βασίζεται σε προβλεπόμενη νόμιμη βάση<sup>109</sup> κατά τρόπο δίκαιο και προβλέψιμο για το υποκείμενο

---

<sup>109</sup> Άρθρο 6 του Κανονισμού (ΕΕ) 2016/679

των δεδομένων. Στο περιβάλλον των ψηφιακών πλατφορμών, η διαφάνεια συνδέεται άμεσα με την υποχρέωση σαφούς ενημέρωσης των χρηστών σχετικά με τις πρακτικές ελέγχου περιεχομένου και τις συνέπειές τους, ιδίως όταν αυτές βασίζονται σε αυτοματοποιημένες διαδικασίες.

Ιδιαίτερη σημασία παρουσιάζει, περαιτέρω, η αρχή του περιορισμού του σκοπού (purpose limitation)<sup>110</sup>, η οποία επιβάλλει τα δεδομένα να συλλέγονται για συγκεκριμένους και νόμιμους σκοπούς και να μην υφίστανται περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με αυτούς. Στο πλαίσιο του ελέγχου περιεχομένου, η αρχή αυτή θέτει κρίσιμα όρια στη δευτερογενή χρήση δεδομένων που συλλέγονται αρχικώς για σκοπούς ασφάλειας ή συμμόρφωσης, αλλά ενδέχεται να αξιοποιηθούν για τη δημιουργία προφίλ χρηστών (profiling), την κατάταξη ή την προσωποποιημένη προβολή περιεχομένου, κατά τρόπο που υπερβαίνει τις εύλογες προσδοκίες των υποκειμένων.

Συναφώς, η αρχή της ελαχιστοποίησης των δεδομένων (data minimisation)<sup>111</sup>, απαιτεί η επεξεργασία να περιορίζεται στα απολύτως αναγκαία δεδομένα για την επίτευξη των σκοπών του ελέγχου περιεχομένου. Με τον τρόπο αυτό προάγεται μια οικονομία δεδομένων που αποθαρρύνει την αχρείαστη ή υπερβολική συγκέντρωση πληροφοριών. Ωστόσο, οι πλατφόρμες τείνουν να συλλέγουν εκτεταμένα σύνολα συμπεριφορικών δεδομένων, όπως ιστορικό αλληλεπιδράσεων, χρόνος θέασης και μοτίβα χρήσης, γεγονός που εγείρει προβληματισμούς ως προς την αναγκαιότητα και την αναλογικότητα της επεξεργασίας.

Η αρχή της ακρίβειας (accuracy)<sup>112</sup> αποκτά επίσης ιδιαίτερη βαρύτητα, καθώς η χρήση ανακριβών ή ελλιπών δεδομένων στο πλαίσιο αυτοματοποιημένων ή

---

<sup>110</sup> Άρθρο 5 παρ. 1 β) του Κανονισμού (ΕΕ) 2016/679

<sup>111</sup> Άρθρο 5 παρ. 1 γ) του Κανονισμού (ΕΕ) 2016/679

<sup>112</sup> Άρθρο 5 παρ. 1 δ) του Κανονισμού (ΕΕ) 2016/679

ημιαυτοματοποιημένων μηχανισμών ελέγχου μπορεί να οδηγήσει σε εσφαλμένες αποφάσεις. Τέτοιες είναι για παράδειγμα, η λανθασμένη επισήμανση δημοσιεύσεων ως παραπλανητικών, η αδικαιολόγητη υποβάθμιση της προβολής τους ή ακόμη και η επιβολή περιορισμών στους λογαριασμούς χρηστών.

Περαιτέρω, η αρχή του περιορισμού περιόδου διατήρησης (storage limitation)<sup>113</sup> επιβάλλει τη διατήρηση των δεδομένων μόνο για όσο χρονικό διάστημα είναι απολύτως αναγκαίο για την επίτευξη των σκοπών της επεξεργασίας. Η υποχρέωση διαγραφής ή ανωνυμοποίησης των δεδομένων μετά την ολοκλήρωση του ελέγχου περιεχομένου καθίσταται ουσιώδης για τη διασφάλιση της ιδιωτικής ζωής των χρηστών.

Τέλος, η αρχή της λογοδοσίας (accountability)<sup>114</sup>, υποχρεώνει τις ψηφιακές πλατφόρμες να είναι σε θέση να αποδεικνύουν τη συμμόρφωσή τους με τις ανωτέρω αρχές, ιδίως μέσω της τεκμηρίωσης των διαδικασιών ελέγχου περιεχομένου και της αξιολόγησης των κινδύνων για τα δικαιώματα των υποκειμένων των δεδομένων. Πρόκειται για μια αρχή, η οποία αποτελεί ορόσημο στην προστασία των προσωπικών δεδομένων, καθώς μεταθέτει το βάρος απόδειξης στον υπεύθυνο και εκτελούντα την επεξεργασία και τους υποχρεώνει να είναι σε θέση να αποδεικνύουν ότι συμμορφώνονται προς τις διατάξεις περί προστασίας των δεδομένων προσωπικού χαρακτήρα<sup>115</sup>.

Συμπληρωματικά προς τις ως άνω αρχές, ο Κανονισμός καθιερώνει στο άρθρο 25 την προστασία της ιδιωτικότητας εξ ορισμού (privacy by design) και από το σχεδιασμό συστημάτων και εφαρμογών (privacy by default). Οι αρχές αυτές επιβάλλουν στους υπευθύνους επεξεργασίας την ενσωμάτωση κατάλληλων τεχνικών και οργανωτικών

---

<sup>113</sup> Άρθρο 5 παρ. 1 ε) του Κανονισμού (ΕΕ) 2016/679

<sup>114</sup> Άρθρο 5 παρ. 2 του Κανονισμού (ΕΕ) 2016/679

<sup>115</sup> EDPS (2019), Accountability on the Ground: Guidance on Documenting Processing Operations for EU Institutions, Bodies and Agencies.

μέτρων ήδη από τα αρχικά στάδια του σχεδιασμού των συστημάτων και των διαδικασιών επεξεργασίας, με σκοπό τη διασφάλιση της συμμόρφωσης με τις αρχές του άρθρου 5 και την αποτελεσματική προστασία των δικαιωμάτων των υποκειμένων των δεδομένων. Στο περιβάλλον των ψηφιακών πλατφορμών, όπου ο έλεγχος περιεχομένου υλοποιείται κατά κύριο λόγο μέσω αλγοριθμικών μηχανισμών, η προστασία της ιδιωτικότητας δεν μπορεί να αντιμετωπίζεται ως μεταγενέστερη κανονιστική υποχρέωση, αλλά οφείλει να ενσωματώνεται στον ίδιο τον τεχνικό σχεδιασμό των συστημάτων.

Ειδικότερα, τα συστήματα αλγοριθμικού σχεδιασμού (algorithmic design), οι προεπιλεγμένες ρυθμίσεις (default settings) και οι αυτοματοποιημένοι μηχανισμοί φιλτραρίσματος περιεχομένου (automated filtering systems) συνιστούν κρίσιμα πεδία εφαρμογής του άρθρου 25 ΓΚΠΔ. Ο τρόπος με τον οποίο καθορίζονται οι παράμετροι των αλγορίθμων, τα κριτήρια επισήμανσης ή υποβάθμισης περιεχομένου και οι προεπιλεγμένες επιλογές των χρηστών μπορεί να οδηγήσει σε εκτεταμένη επεξεργασία συμπεριφορικών δεδομένων και σε αυτοματοποιημένες αποφάσεις με σημαντικές συνέπειες για την ελευθερία έκφρασης και την ιδιωτική ζωή. Η εφαρμογή της προστασίας δεδομένων εξ ορισμού απαιτεί, συνεπώς, οι πλατφόρμες να περιορίζουν την επεξεργασία στο απολύτως αναγκαίο μέτρο, να αποφεύγουν την υπέρμετρη συλλογή δεδομένων για σκοπούς πρόβλεψης ή κατάταξης και να διασφαλίζουν ότι οι αυτοματοποιημένοι μηχανισμοί ελέγχου περιεχομένου λειτουργούν με διαφανή, αναλογικό και ελεγχόμενο τρόπο, υπό την εποπτεία κατάλληλων μηχανισμών λογοδοσίας<sup>116</sup>.

#### ***5.3.4 Τα δικαιώματα των χρηστών έναντι των πλατφορμών στο πλαίσιο ελέγχου περιεχομένου***

Στο πλαίσιο της λειτουργίας των ψηφιακών πλατφορμών, ο έλεγχος περιεχομένου συνδέεται άρρηκτα με την επεξεργασία προσωπικών δεδομένων των χρηστών,

---

<sup>116</sup> Κανέλλος Λ.(2020) , The GDPR Handbook, εκδόσεις Νομική Βιβλιοθήκη, σελ. 41

γεγονός που καθιστά τα δικαιώματα των υποκειμένων των δεδομένων κρίσιμο αντίβαρο στην άσκηση της κανονιστικής και, εν τοις πράγμασι, θεσμικής ισχύος των πλατφορμών. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων καθιερώνει ένα συνεκτικό πλέγμα δικαιωμάτων, το οποίο αποσκοπεί στην ενδυνάμωση του χρήστη και στη διασφάλιση της διαφάνειας, της λογοδοσίας και του ελέγχου της επεξεργασίας των δεδομένων του, ιδίως σε ψηφιακά περιβάλλοντα όπου λαμβάνονται αποφάσεις που επηρεάζουν άμεσα την ορατότητα, τη διάδοση ή την αφαίρεση ψηφιακού περιεχομένου<sup>117</sup>.

Θεμελιώδη σημασία στο πλαίσιο αυτό έχει το δικαίωμα ενημέρωσης<sup>118</sup>, το οποίο διασφαλίζει ότι ο χρήστης γνωρίζει με σαφήνεια την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας, το είδος των δεδομένων που συλλέγονται, τον σκοπό και τη νόμιμη βάση της επεξεργασίας, καθώς και τη διάρκεια αποθήκευσης των δεδομένων και τους αποδέκτες στους οποίους αυτά ενδέχεται να διαβιβαστούν. Πέραν όμως της γενικής πληροφόρησης για την επεξεργασία δεδομένων, το δικαίωμα αυτό καταλαμβάνει και τη χρήση των δεδομένων στο πλαίσιο των μηχανισμών ελέγχου περιεχομένου, ιδίως όταν αυτά αξιοποιούνται για την αξιολόγηση, την κατάταξη ή την απομάκρυνση περιεχομένου που δημιουργείται ή καταναλώνεται από τον ίδιο τον χρήστη. Η παρεχόμενη ενημέρωση οφείλει να είναι σαφής, κατανοητή και εύκολα προσβάσιμη, ώστε να καθίσταται δυνατή η κατανόηση των κριτηρίων και των διαδικασιών ελέγχου, ιδίως όταν αυτές βασίζονται σε αυτοματοποιημένα συστήματα λήψης αποφάσεων.

Στενά συνδεδεμένο με το δικαίωμα ενημέρωσης είναι το δικαίωμα της πρόσβασης<sup>119</sup>, το οποίο επιτρέπει στον χρήστη να ζητήσει πληροφορίες σχετικά με το αν και κατά πόσον τα δεδομένα του χρησιμοποιούνται στο πλαίσιο διαδικασιών ελέγχου

---

<sup>117</sup> Άρθρο 12 του Κανονισμού (ΕΕ) 2016/679

<sup>118</sup> Άρθρο 13 - 14 του Κανονισμού (ΕΕ) 2016/679

<sup>119</sup> Άρθρο 15 του Κανονισμού (ΕΕ) 2016/679

περιεχομένου, συμπεριλαμβανομένων δεδομένων που προκύπτουν από αναφορές τρίτων χρηστών, από αλγοριθμική ανάλυση συμπεριφοράς ή από συστήματα κατάταξης. Η άσκηση του δικαιώματος αυτού μπορεί να λειτουργήσει ως μηχανισμός ελέγχου της διαφάνειας των πλατφορμών, ιδίως σε περιπτώσεις αφαίρεσης περιεχομένου ή περιορισμού της προβολής του (downranking). Ωστόσο, στην πράξη οι πλατφόρμες συχνά περιορίζονται σε γενικές και τυποποιημένες απαντήσεις, γεγονός που δημιουργεί μια μορφή τυπικής, αλλά όχι ουσιαστικής, διαφάνειας και δυσχεραίνει την αμφισβήτηση των σχετικών αποφάσεων<sup>120</sup>.

Ιδιαίτερη πρακτική σημασία στο περιβάλλον των ψηφιακών πλατφορμών παρουσιάζουν, επίσης, τα δικαιώματα διόρθωσης<sup>121</sup> και διαγραφής<sup>122</sup>. Το δικαίωμα διόρθωσης επιτρέπει την αποκατάσταση ανακριβών ή ελλιπών δεδομένων που ενδέχεται να επηρεάσουν δυσμενώς την αξιολόγηση της συμπεριφοράς ενός χρήστη ή την κατάταξή του από τα συστήματα ελέγχου. Για παράδειγμα, εάν ένα σχόλιο ή μια ανάρτηση κατηγοριοποιηθεί εσφαλμένα ως «παράνομη» από ένα αλγοριθμικό σύστημα ελέγχου, ο χρήστης μπορεί να ζητήσει διόρθωση ώστε η κατηγοριοποίηση να αντανakλά με ακρίβεια το περιεχόμενο και τη σκοπιμότητά του. Αντίστοιχα, το δικαίωμα διαγραφής, γνωστό και ως «δικαίωμα στη λήθη», αποκτά ιδιαίτερη βαρύτητα όταν δεδομένα παρελθούσας δραστηριότητας εξακολουθούν να χρησιμοποιούνται για τη λήψη αποφάσεων ελέγχου περιεχομένου, παρά τη μεταβολή των περιστάσεων. Ωστόσο, το δικαίωμα αυτό δεν είναι απόλυτο<sup>123</sup> και

---

<sup>120</sup> Veale M., Edwards L. (2018), Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling, *Computer Law & Security Review*, p. 399

<sup>121</sup> Άρθρο 16 του Κανονισμού (ΕΕ) 2016/679

<sup>122</sup> Άρθρο 17 του Κανονισμού (ΕΕ) 2016/679

<sup>123</sup> Το Ε.Δ.Δ.Α. στην υπόθεση *Österreichischer Rundfunk κατά Αυστρίας* αναγνώρισε ότι το δικαίωμα στη λήθη υποχωρεί όταν υπάρχει δικαιολογημένο ενδιαφέρον του κοινού για πληροφόρηση

υπόκειται σε περιορισμούς, ιδίως όταν συγκρούεται με λόγους δημοσίου συμφέροντος<sup>124</sup> ή με την ελευθερία της έκφρασης, όπως έχει αναδειχθεί και στη νομολογία του ΔΕΕ στην υπόθεση C-131/12 Google Spain<sup>125</sup>.

Επικουρικά με τα ως άνω, λειτουργεί το δικαίωμα περιορισμού της επεξεργασίας<sup>126</sup>, το οποίο κατοχυρώνει τη δυνατότητα του υποκειμένου των δεδομένων να ζητήσει τον περιορισμό της επεξεργασίας των προσωπικών του δεδομένων υπό συγκεκριμένες προϋποθέσεις. Το δικαίωμα αυτό εφαρμόζεται όταν αμφισβητείται η ακρίβεια των δεδομένων, προκειμένου να παρασχεθεί ο απαραίτητος χρόνος για την επαλήθευσή τους. Ενεργοποιείται, επίσης, όταν η επεξεργασία είναι παράνομη και το υποκείμενο δεν επιθυμεί τη διαγραφή των δεδομένων του, αλλά ζητεί τον περιορισμό της χρήσης τους. Επιπλέον, μπορεί να ασκηθεί όταν τα δεδομένα δεν είναι πλέον αναγκαία για τους σκοπούς της επεξεργασίας από τον υπεύθυνο επεξεργασίας, πλην όμως απαιτούνται από το υποκείμενο για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων. Τέλος, το δικαίωμα περιορισμού της επεξεργασίας υφίσταται και όταν το υποκείμενο έχει αντιταχθεί στην επεξεργασία σύμφωνα με το άρθρο 21 του ΓΚΠΔ,

---

<sup>124</sup> Politou E., Alepis E, Patsakis C. (2018), Forgetting personal data and revoking consent under the GDPR: Challenges and Proposed Solutions, Journal of Cybersecurity, σελ. 11-17.

<sup>125</sup> Χαρακτηριστικά η απόφαση αναφέρει ότι “ο φορέας εκμετάλλευσης μηχανής αναζήτησης υποχρεούται να απαλειφθεί από τον κατάλογο αποτελεσμάτων, ο οποίος εμφανίζεται κατόπιν αναζήτησης προς δημοσιευμένες από τρίτους ιστοσελίδες που περιέχουν πληροφορίες σχετικές με το πρόσωπο αυτό...η υποχρέωση αυτή ισχύει ακόμη και όταν αυτή καθαυτή η δημοσίευση των επίμαχων πληροφοριών στις εν λόγω ιστοσελίδες είναι νόμιμη...”. Ως προς τις προϋποθέσεις εφαρμογής επισημαίνει ότι “...πρέπει να εξετάζεται αν το υποκείμενο των δεδομένων έχει δικαίωμα να πάψει η σχετική με το πρόσωπό του πληροφορία... χωρίς πάντως η αναγνώριση του δικαιώματος αυτού να προϋποθέτει ότι η εμφάνιση της επίμαχης πληροφορίας στον κατάλογο αποτελεσμάτων προκαλεί βλάβη στο υποκείμενο των δεδομένων..”, Γ. Ν. Γιαννόπουλος Γ. Ν. (2018), Εισαγωγή στη Νομική Πληροφορική, Νομική Βιβλιοθήκη, σελ. 90.

<sup>126</sup> Άρθρο 18 του Κανονισμού (ΕΕ) 2016/679

έως ότου ολοκληρωθεί η στάθμιση μεταξύ των εννόμων συμφερόντων του υπευθύνου επεξεργασίας και των δικαιωμάτων ή συμφερόντων του υποκειμένου των δεδομένων.

Ακολουθως, με τον ΓΚΠΔ καθιερώνεται ένα ακόμη καινοτόμο δικαίωμα στην ευρωπαϊκή έννομη τάξη, ήτοι το δικαίωμα στη φορητότητα<sup>127</sup>. Σύμφωνα με αυτό, «το υποκείμενο έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα, όταν: α) η επεξεργασία βασίζεται σε συγκατάθεση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α) ή το άρθρο 9 παράγραφος 2 στοιχείο α) ή σε σύμβαση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο β) και β) η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα». Στο πλαίσιο των ψηφιακών πλατφορμών και του ελέγχου περιεχομένου, το δικαίωμα φορητότητας αποκτά ιδιαίτερο πρακτικό ενδιαφέρον. Επιτρέπει στον χρήστη, για παράδειγμα, να λαμβάνει τα δεδομένα που η πλατφόρμα συλλέγει για το προφίλ του, τη συμπεριφορά του, ή την κατάταξη των δημοσιεύσεών του, όπως δεδομένα σχετικά με likes, σχόλια, ιστορικό προβολών ή αλληλεπιδράσεις με άλλα άτομα. Με αυτόν τον τρόπο, ο χρήστης μπορεί είτε να μεταφέρει τα δεδομένα του σε άλλη πλατφόρμα, είτε να εξετάσει και να αξιολογήσει τον τρόπο με τον οποίο αυτά τα δεδομένα χρησιμοποιούνται για τον έλεγχο του περιεχομένου και την κατάταξη των δημοσιεύσεών του. Στην πράξη, αφορά ψηφιακά προσωπικά δεδομένα όπως φωτογραφίες, διαπροσωπικές επικοινωνίες, δεδομένα αλληλεπίδρασης με

---

<sup>127</sup> Άρθρο του Κανονισμού (ΕΕ) 2016/679

περιεχόμενο, αλλά και μεταδεδομένα που χρησιμοποιούνται για την κατάταξη ή υποβάθμιση δημοσιεύσεων<sup>128</sup>.

Τέλος, κατοχυρώνεται το δικαίωμα να μην υπόκειται το υποκείμενο σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, περιλαμβανομένης της κατάρτισης προφίλ (profiling), εφόσον αυτή παράγει έννομα αποτελέσματα ή επηρεάζει σημαντικά το υποκείμενο<sup>129</sup>. Στο πλαίσιο των ψηφιακών πλατφορμών, η αυτοματοποιημένη επεξεργασία χρησιμοποιείται συχνά για τον έλεγχο περιεχομένου, την κατάταξη δημοσιεύσεων, την υποβάθμιση ή προώθηση αναρτήσεων και την ανάλυση συμπεριφορών των χρηστών. Η εν λόγω πρακτική (profiling), μέσω της δημιουργίας μορφότυπων (profiles), αποσκοπεί στην ταξινόμηση των χρηστών σε συγκεκριμένες ομάδες ή κατηγορίες με βάση μοτίβα συμπεριφοράς, για να ληφθούν αποφάσεις που αφορούν την προβολή ή τον περιορισμό του περιεχομένου τους. Η τεχνική αυτή, αν και προσφέρει λειτουργικά πλεονεκτήματα ιδίως στο πεδίο της εξατομικευμένης παροχής υπηρεσιών και της στοχευμένης διαφήμισης, έχει αποτελέσει αντικείμενο έντονου επιστημονικού και κανονιστικού διαλόγου. Ο πυρήνας της κριτικής εστιάζεται στον κίνδυνο απώλειας του ουσιαστικού ελέγχου από το υποκείμενο επί των δεδομένων του, καθώς και στις ευρύτερες επιπτώσεις που μπορεί να έχει στην ανθρώπινη αξιοπρέπεια και την αυτονομία του προσώπου<sup>130</sup>. Στις ψηφιακές πλατφόρμες, η ομαδοποίηση χρηστών βάσει μοτίβων συμπεριφοράς μπορεί να οδηγήσει σε αθέμιτη μεταχείριση, ενίσχυση προκαταλήψεων ή περιορισμό της ορατότητας συγκεκριμένου περιεχομένου, υπονομεύοντας τον σεβασμό στην ατομικότητα και την ελευθερία έκφρασης. Στο σημείο αυτό αναδεικνύεται και η ανάγκη συμπληρωματικής εφαρμογής των

---

<sup>128</sup> Μήτρου Α. (2017), Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, νέο δίκαιο- νέες υποχρεώσεις- νέα δικαιώματα, εκδόσεις Σάκκουλα, σελ. 136

<sup>129</sup> Άρθρο 22 του Κανονισμού (ΕΕ) 2016/679

<sup>130</sup> Μήτρου Α. (2017), Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, νέο δίκαιο- νέες υποχρεώσεις- νέα δικαιώματα, εκδόσεις Σάκκουλα, σελ. 130

διαδικαστικών εγγυήσεων που προβλέπει ο Κανονισμός για τις Ψηφιακές Υπηρεσίες (DSA), ιδίως ως προς τη δυνατότητα ένστασης και ανθρώπινης επανεξέτασης των αποφάσεων των πλατφορμών.

### **5.3.5 Το δικαίωμα δικαστικής προστασίας και ο κυρωτικός μηχανισμός του ΓΚΠΔ**

Στο πλαίσιο της αρχής της δικαστικής προστασίας και του κράτους δικαίου, τα υποκείμενα των δεδομένων διαθέτουν ένα πλέγμα ένδικων βοηθημάτων και μηχανισμών προσφυγής σε περίπτωση παραβίασης των δικαιωμάτων τους από τις ψηφιακές πλατφόρμες. Οι προβλέψεις αυτές αποσκοπούν στη διασφάλιση της αποτελεσματικής εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων, καθώς και στην ενίσχυση της εμπιστοσύνης των χρηστών ως προς την τήρηση των κανόνων που διέπουν την επεξεργασία προσωπικών δεδομένων σε περιβάλλοντα ελέγχου περιεχομένου, όπως η κατάταξη αναρτήσεων, η υποβάθμιση (downranking) ή η αφαίρεση περιεχομένου.

Σύμφωνα με το άρθρο 77 του Κανονισμού (ΕΕ) 2016/679, κάθε υποκείμενο των δεδομένων διαθέτει το δικαίωμα να υποβάλει καταγγελία σε εποπτική αρχή, εφόσον θεωρεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορά παραβιάζει τις διατάξεις του Κανονισμού. Η καταγγελία μπορεί να υποβληθεί ιδίως στην εποπτική αρχή του κράτους μέλους όπου ο χρήστης έχει τη συνήθη διαμονή του, τον τόπο της εργασίας του ή τον τόπο όπου φέρεται να έλαβε χώρα η παράβαση. Με τον τρόπο αυτό διασφαλίζεται η πρόσβαση σε αποτελεσματικό μηχανισμό διοικητικής προστασίας, ανεξαρτήτως της διασυνοριακής φύσης της επεξεργασίας που πραγματοποιούν οι ψηφιακές πλατφόρμες.

Περαιτέρω, το άρθρο 78 καθιερώνει το δικαίωμα πραγματικής προσφυγής κατά νομικά δεσμευτικής απόφασης εποπτικής αρχής, διασφαλίζοντας τη δυνατότητα δικαστικού ελέγχου των πράξεων ή παραλείψεων της. Επιπλέον, σύμφωνα με το άρθρο 79, κάθε υποκείμενο των δεδομένων διαθέτει δικαίωμα πραγματικής

δικαστικής προσφυγής κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία, όταν θεωρεί ότι τα δικαιώματά του παραβιάστηκαν ως αποτέλεσμα της επεξεργασίας των προσωπικών του δεδομένων<sup>131</sup>. Το δικαίωμα αυτό αποκτά ιδιαίτερη σημασία στο πλαίσιο των ψηφιακών πλατφορμών, όπου οι αποφάσεις ελέγχου περιεχομένου δύνανται να επιφέρουν σοβαρούς περιορισμούς στην ελευθερία έκφρασης και στη διαδικτυακή παρουσία των χρηστών. Στο ίδιο πλαίσιο, κάθε πρόσωπο που υπέστη υλική ή μη υλική ζημία λόγω παραβίασης του Κανονισμού δικαιούται αποζημίωση από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία<sup>132</sup>.

Πέραν της ατομικής δικαστικής προστασίας, ο ΓΚΠΔ ενσωματώνει έναν ισχυρό κυρωτικό μηχανισμό μέσω του άρθρου 83, ο οποίος ρυθμίζει την επιβολή διοικητικών προστίμων από τις εποπτικές αρχές, τα οποία διαβαθμίζονται ανάλογα με τη φύση, τη βαρύτητα και τη διάρκεια της παράβασης. Παραβάσεις που αφορούν, μεταξύ άλλων, τη μη συμμόρφωση με τις υποχρεώσεις διαφάνειας, ενημέρωσης ή τη μη αποτελεσματική άσκηση των δικαιωμάτων των χρηστών από ψηφιακές πλατφόρμες, ενδέχεται να επιφέρουν πρόστιμα έως 10.000.000 ευρώ ή έως 2% του συνολικού ετήσιου παγκόσμιου κύκλου εργασιών. Αντιστοίχως, σοβαρότερες παραβάσεις, όπως η παραβίαση των βασικών αρχών επεξεργασίας ή των δικαιωμάτων των υποκειμένων των δεδομένων, μπορούν να οδηγήσουν στην επιβολή προστίμων έως 20.000.000 ευρώ ή έως 4% του συνολικού κύκλου εργασιών της πλατφόρμας.

Συνοψίζοντας, ο κυρωτικός αυτός μηχανισμός δεν επιτελεί μόνον τιμωρητική λειτουργία, αλλά ιδίως προληπτική και αποτρεπτική, καθώς διαμορφώνει ισχυρά κίνητρα συμμόρφωσης προς το κανονιστικό πλαίσιο προστασίας δεδομένων. Οι εθνικές εποπτικές αρχές, όπως η ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, διαδραματίζουν κρίσιμο ρόλο στην επιτήρηση των

---

<sup>131</sup> Άρθρο 79 του Κανονισμού (ΕΕ) 2016/679

<sup>132</sup> Άρθρο 82 Κανονισμού (ΕΕ) 2016/679

πρακτικών των ψηφιακών πλατφορμών και στην επιβολή κυρώσεων, συμβάλλοντας ουσιαστικά στην προστασία των δικαιωμάτων των χρηστών και στη διασφάλιση υπεύθυνων και διαφανών διαδικασιών ελέγχου περιεχομένου.

#### **5.4 Ο Ν. 4624/2019 και η εφαρμογή του στις ψηφιακές πλατφόρμες**

Σε εθνικό επίπεδο, ο Κανονισμός 2016/679 εφαρμόστηκε με τη θέσπιση του Ν. 4624/2019 «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις» (ΦΕΚ.Α'137/29-08-2019). Σημειώνεται ότι ο νόμος αυτός δεν θεσπίζει αυτοτελές σύστημα προστασίας δεδομένων, αλλά λειτουργεί συμπληρωματικά προς τον Κανονισμό, εξειδικεύοντας ορισμένες από τις προβλέψεις του στο πλαίσιο της ελληνικής έννομης τάξης.

Κεντρικό ρόλο στο εν λόγω κανονιστικό σύστημα διαδραματίζει η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα<sup>133</sup>, η οποία λειτουργεί ως ανεξάρτητη εποπτική αρχή, αρμόδια για την παρακολούθηση της εφαρμογής της νομοθεσίας, την έκδοση κατευθυντήριων οδηγιών και την επιβολή κυρώσεων σε περιπτώσεις παραβίασης της νομοθεσίας περί προστασίας δεδομένων. Η εποπτική αυτή λειτουργία αποκτά ιδιαίτερη σημασία στο περιβάλλον των ψηφιακών πλατφορμών, οι οποίες, ως υπεύθυνοι επεξεργασίας, προβαίνουν σε συστηματική και μεγάλης κλίμακας επεξεργασία προσωπικών δεδομένων χρηστών.

---

<sup>133</sup> Πρωταρχικός σκοπός της Αρχής είναι η προστασία του πολίτη από την παράνομη επεξεργασία των προσωπικών του δεδομένων αλλά και η συνδρομή προς αυτόν σε κάθε περίπτωση διαπίστωσης παραβίασης των σχετικών δικαιωμάτων του. Μήτρου Λ. (1999), Η αρχή προστασίας προσωπικών δεδομένων, εκδόσεις Σάκκουλα

Στο πλαίσιο αυτό, ο Ν. 4624/2019 περιλαμβάνει διατάξεις που αφορούν τις υποχρεώσεις των υπευθύνων επεξεργασίας δεδομένων, τόσο δημόσιων όσο και ιδιωτικών φορέων, με ιδιαίτερη έμφαση στις διαδικασίες συλλογής, επεξεργασίας και διαβίβασης πληροφοριών. Η σημασία του νόμου καθίσταται ιδιαίτερος εμφανής στις ψηφιακές πλατφόρμες, οι οποίες διαχειρίζονται τεράστιους όγκους προσωπικών δεδομένων και πληροφοριών χρηστών και υλοποιούν λειτουργίες ελέγχου περιεχομένου, όπως η αξιολόγηση, η ταξινόμηση, η ιεράρχηση και η προσωποποιημένη προβολή πληροφοριών, συχνά μέσω αυτοματοποιημένων και αλγοριθμικών μηχανισμών.

Παρά την πρόθεση του νομοθέτη να εναρμονιστεί πλήρως με το ευρωπαϊκό πλαίσιο, ο Ν. 4624/2019 έχει προκαλέσει επιστημονική και πρακτική συζήτηση λόγω ορισμένων νομοτεχνικών αδυναμιών. Η Γνωμοδότηση 1/2020 της ΑΠΔΠΧ<sup>134</sup> επισημαίνει ότι ο νόμος σε αρκετά σημεία επαναλαμβάνει διατάξεις του ΓΚΠΔ χωρίς να παρέχει σαφή και λειτουργική εξειδίκευση, γεγονός που ενδέχεται να δημιουργεί ερμηνευτική αβεβαιότητα για τους υπευθύνους επεξεργασίας<sup>135</sup>. Ενδεικτικά, τα άρθρα 6, 7 και 8 του νόμου αναπαράγουν διατάξεις του Κανονισμού σχετικά με τον Υπεύθυνο Προστασίας Δεδομένων (άρθρα 37, 38, 39) χωρίς να καθορίζουν ειδικότερους μηχανισμούς ελέγχου ή λογοδοσίας γεγονός που αποκτά ιδιαίτερη σημασία για τις ψηφιακές πλατφόρμες με πολύπλοκες οργανωτικές και τεχνικές δομές.

Ιδιαίτερο ενδιαφέρον παρουσιάζει το άρθρο 24 παρ. 1 του Ν. 4624/2019, το οποίο επιτρέπει υπό προϋποθέσεις, την επεξεργασία δεδομένων ειδικών κατηγοριών από δημόσιες αρχές, χωρίς ωστόσο να εξειδικεύει επαρκώς τις πρόσθετες εγγυήσεις που απαιτεί ο Κανονισμός. Το ζήτημα αυτό αποκτά πρακτική σημασία για τις ψηφιακές

---

<sup>134</sup> Διαθέσιμο στο [https://www.dpa.gr/sites/default/files/2020-01/gnomodotisi%201\\_2020.pdf](https://www.dpa.gr/sites/default/files/2020-01/gnomodotisi%201_2020.pdf) (τελευταία πρόσβαση: 23/06/2025)

<sup>135</sup> Κανέλλος Α. Ι. (2020), *The GDPR HANDBOOK*, Νομική Βιβλιοθήκη, σελ. 226.

πλατφόρμες, ιδίως όταν αυτές διαχειρίζονται περιεχόμενο που άπτεται ευαίσθητων πτυχών της ιδιωτικής ζωής των χρηστών, όπως δεδομένα υγείας, πολιτικές απόψεις ή θρησκευτικές πεποιθήσεις. Για παράδειγμα, πλατφόρμες κοινωνικής δικτύωσης που εποπτεύουν και προβάλλουν περιεχόμενο σχετικό με ιατρικά ή πολιτικά ζητήματα εφαρμόζουν αλγοριθμικούς μηχανισμούς ταξινόμησης και προσωποποιημένης προβολής, γεγονός που συνεπάγεται αυξημένες απαιτήσεις διαφάνειας, αναλογικότητας και προστασίας των δικαιωμάτων των υποκειμένων των δεδομένων.

Επομένως, ο Ν. 4624/2019, παρά τις νομοτεχνικές του αδυναμίες, θέτει το βασικό εθνικό πλαίσιο εποπτείας της επεξεργασίας προσωπικών δεδομένων από ψηφιακές πλατφόρμες, ενισχύοντας τον ρόλο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ως εγγυητή της νομιμότητας. Η ανάγκη περαιτέρω νομοθετικής και κανονιστικής εξειδίκευσης παραμένει κρίσιμη, προκειμένου να διασφαλιστεί ότι οι διαδικασίες ελέγχου περιεχομένου θα συμμορφώνονται πλήρως με τις αρχές προστασίας προσωπικών δεδομένων, ιδίως σε περιβάλλοντα όπου η επεξεργασία συνδέεται άμεσα με αυτοματοποιημένη λήψη αποφάσεων και προηγμένα αλγοριθμικά συστήματα οργάνωσης της πληροφορίας.

## 6. ΣΥΜΠΕΡΑΣΜΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΠΡΟΚΛΗΣΕΩΝ

Η ανάλυση που προηγήθηκε ανέδειξε ότι η ρύθμιση του ελέγχου περιεχομένου στις ψηφιακές πλατφόρμες, σε συνάρτηση με την προστασία προσωπικών δεδομένων και την κατοχύρωση θεμελιωδών δικαιωμάτων, συνιστά μια πολυεπίπεδη πρόκληση για τον σύγχρονο νομοθέτη και τις αρμόδιες εποπτικές αρχές. Παρά τις σημαντικές τομές που επιφέρει το ενωσιακό πλαίσιο, με πυρήνα τον Κανονισμό 2022/2065 (DSA) και τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ), εξακολουθούν να υφίστανται ζητήματα εφαρμογής, οριοθέτησης αρμοδιοτήτων και διασφάλισης της αρχής της αναλογικότητας. Τούτο διότι, η συγκριτική θεώρηση των εθνικών κανονιστικών πλαισίων αποκαλύπτει σημαντικές διαφοροποιήσεις στην εφαρμογή και ερμηνεία των εν λόγω ρυθμίσεων.

Ενδεικτικά, στη Γερμανία, η εφαρμογή του *Netzwerkdurchsetzungsgesetz (NetzDG)* από το 2017 αποτέλεσε μία από τις πρώτες εθνικές νομοθεσίες που αντιμετώπισαν συστηματικά το ζήτημα της ρητορικής μίσους και της παραπληροφόρησης στο διαδίκτυο<sup>136</sup>. Χαρακτηριστικό του γερμανικού νομοθετικού πλαισίου είναι ότι θέτει αυστηρές προθεσμίες για την απομάκρυνση παράνομου περιεχομένου και προβλέπει σημαντικά πρόστιμα για τις πλατφόρμες που δεν συμμορφώνονται. Ειδικότερα, ο νόμος υποχρεώνει τα κοινωνικά δίκτυα να αφαιρούν «προδήλως παράνομο περιεχόμενο» εντός 24 ωρών ή εντός 7 ημερών όταν η παραβίαση δεν είναι άμεσα πρόδηλη, διαφορετικά κινδυνεύουν να αντιμετωπίσουν πρόστιμα ύψους έως και 50 εκατομμυρίων ευρώ. Υποστηρίζεται δε, ότι οι διαδικτυακές πλατφόρμες έχουν την ευθύνη να αφαιρούν προφανώς παράνομο περιεχόμενο όταν αυτό αναφέρεται από φορείς ή χρήστες των οποίων ο τόπος κατοικίας βρίσκεται στη Γερμανία, ακόμη και αν το περιεχόμενο μεταφορτώθηκε, αναρτήθηκε ή κοινοποιήθηκε από άτομο σε τρίτη

---

<sup>136</sup> Poscher R. (2019), *Germany's NetzDG: Fighting Hate Speech and Fake News in the Digital Age*, *German Law Journal*, 20(5), p. 731–749

χώρα<sup>137</sup>. Ωστόσο, έχει υποστηριχθεί ότι η αυστηρότητα της εφαρμογής ενδέχεται να προκαλέσει φαινόμενα αυτολογοκρισίας, γεγονός που περιορίζει την ελευθερία της έκφρασης. Στο πλαίσιο αυτό, ο Κανονισμός για τις Ψηφιακές Υπηρεσίες επιχειρεί να θέσει ένα ενιαίο, ευρωπαϊκό πλαίσιο που θα αποφεύγει τέτοιες αποκλίσεις, ενώ παράλληλα ενισχύει τη διαφάνεια και τη λογοδοσία των πλατφορμών.

Αντίστοιχα, η βρετανική προσέγγιση, όπως διαφαίνεται από την εφαρμογή του Online Safety Act του 2023, επιβάλλει αυστηρότερους κανόνες για την πρόληψη της διάδοσης επιβλαβούς περιεχομένου και προβλέπει αυξημένη εποπτεία και κυρώσεις για τις πλατφόρμες<sup>138</sup>. Ουσιαστικά, αποτελεί τη βρετανική απάντηση στις προκλήσεις της παραπληροφόρησης, της ρητορικής μίσους, της εκμετάλλευσης παιδιών και άλλων μορφών επιβλαβούς ή παράνομου περιεχομένου και τοποθετείται χρονικά μετά το Brexit και κατ' επέκταση βρίσκεται εκτός του πλαισίου του Κανονισμού DSA. Σημειώνεται, βέβαια, ότι ο βρετανικός νόμος έχει δεχτεί κριτική για ενδεχόμενους περιορισμούς στην ελευθερία της έκφρασης και ελλιπή διασφάλιση των προσωπικών δεδομένων<sup>139</sup>. Σε αντιδιαστολή, η ευρωπαϊκή προσέγγιση, μέσω του Κανονισμού DSA, υιοθετεί μια πιο ισορροπημένη στάση, επιμένοντας στην αρχή της αναλογικότητας και στην ανάγκη διαφάνειας, θέτοντας ως κεντρικό άξονα τη συνεργασία μεταξύ δημοσίων αρχών και πλατφορμών.

Ρυθμιστικός κόμβος του ελέγχου περιεχομένου και της εποπτείας της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) αποτελεί η Ιρλανδία, λόγω της έδρας πολλών μεγάλων τεχνολογικών εταιρειών στο έδαφός της. Η Ιρλανδική Επιτροπή Προστασίας Δεδομένων (Data Protection Commission ή «DPC») έχει

---

<sup>137</sup> Brown A. (2020), Models of governance of online hate speech, Council of Europe, p. 9

<sup>138</sup> UK Parliament (2023), Online Safety Act. Διαθέσιμο στο: <https://bills.parliament.uk/bills/3137> (τελευταία προβολή: 26/06/2026)

<sup>139</sup> Greer C. - McLaughlin E. (2023), Regulating online harms: The Online Safety Act and free speech challenges, International Journal of Law and Technology, 15(2), p. 101 - 123.

αναδειχθεί σε μία από τις πλέον επιδραστικές εποπτικές αρχές της ΕΕ, καθώς καλείται να διαχειριστεί σύνθετες υποθέσεις που αφορούν πολυεθνικούς κολοσσούς όπως η Meta, το Google και το TikTok. Ειδικότερα, η Ιρλανδία έχει προχωρήσει, ήδη από το 2022, στη θέσπιση του Online Safety and Media Regulation Act, ο οποίος επιδιώκει να ενσωματώσει τις ευρωπαϊκές εξελίξεις του DSA, θεσπίζοντας παράλληλα έναν εθνικό Οργανισμό Ρύθμισης των Μέσων και της Ψηφιακής Ασφάλειας (Coimisiún na Meán)<sup>140</sup>. Ο οργανισμός αυτός αναλαμβάνει εποπτικό ρόλο για την απομάκρυνση επιβλαβούς περιεχομένου και την προστασία ανηλίκων, συνδέοντας έτσι την προστασία προσωπικών δεδομένων με την καταπολέμηση της παραπληροφόρησης και της επιβλαβούς ψηφιακής συμπεριφοράς. Ωστόσο, και σε αυτή τη περίπτωση δεν λείπουν οι ανησυχίες αναφορικά με το κατά πόσο διασφαλίζεται επαρκώς η ισορροπία ανάμεσα στον έλεγχο περιεχομένου και την ελευθερία της έκφρασης, ιδίως σε σχέση με τη διαφάνεια των αλγοριθμικών μηχανισμών που χρησιμοποιούν οι πλατφόρμες.

Στην Ελλάδα, η ρύθμιση παραμένει περισσότερο αποσπασματική, με έμφαση στην εφαρμογή του ΓΚΠΔ και του νόμου 4624/2019, ενώ απουσιάζει ειδικό νομοθέτημα που να αντιμετωπίζει ολιστικά την ευθύνη των πλατφορμών για επιβλαβές περιεχόμενο. Στην πράξη, η διαχείριση φαινομένων όπως η ρητορική μίσους ή οι ψευδείς ειδήσεις γίνεται αποσπασματικά, μέσω γενικών ποινικών διατάξεων, αποφάσεων δικαστηρίων ή συστάσεων της Εθνικής Ρυθμιστικής Αρχής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΡΤΤ) και του Εθνικού Συμβουλίου Ραδιοτηλεόρασης (ΕΣΡ). Ωστόσο, οι αρχές αυτές δεν έχουν αρμοδιότητα για την προληπτική εποπτεία των ψηφιακών πλατφορμών. Η εφαρμογή του Κανονισμού 2022/2065 για τις Ψηφιακές Υπηρεσίες (DSA) αναμένεται να καλύψει μέρος αυτού του κενού, καθώς προβλέπει τη σύσταση

---

<sup>140</sup> Irish Government (2022), Online Safety and Media Regulation Act. Διαθέσιμο στο: <https://www.gov.ie/en/department-of-culture-communications-and-sport/publications/online-safety-and-media-regulation-act-2022/#online-safety-and-media-regulation-act> (τελευταία προβολή: 26/06/2025)

εθνικών ψηφιακών συντονιστών και τη συνεργασία με την Ευρωπαϊκή Επιτροπή για την εποπτεία πολύ μεγάλων πλατφορμών. Προκειμένου, λοιπόν, να διασφαλιστεί η ισορροπία ανάμεσα στην ελευθερία της έκφρασης, την προστασία από επιβλαβές περιεχόμενο και την προστασία προσωπικών δεδομένων, καθίσταται η ανάγκη για περαιτέρω νομοθετική εξέλιξη<sup>141</sup>.

Η ανάλυση αυτή υπογραμμίζει την ανάγκη για μια ευρωπαϊκή προσέγγιση που θα ενσωματώνει τις ιδιαίτερες συνθήκες και τις νομικές παραδόσεις κάθε κράτους-μέλους, αλλά ταυτόχρονα θα επιτρέπει την εύκολη προσαρμογή των εθνικών νομοθεσιών σε έναν κοινό ευρωπαϊκό χώρο. Η διαρκής συγκριτική θεώρηση των εθνικών κανονιστικών πλαισίων και η εφαρμογή κοινών αρχών αποτελούν προϋποθέσεις για την οικοδόμηση μιας ενιαίας και αποτελεσματικής ρυθμιστικής στρατηγικής.

Μέσα σε αυτό το δυναμικό και συχνά αντιφατικό περιβάλλον, καθίσταται σαφές ότι η εξισορρόπηση της ελευθερίας έκφρασης, της προστασίας της ιδιωτικότητας και της εύρυθμης λειτουργίας των ψηφιακών υπηρεσιών απαιτεί όχι μόνο νομοθετικές προβλέψεις αλλά και θεσμική και κοινωνική εγρήγορση. Σε αυτό το πλαίσιο, μπορούν να διατυπωθούν ορισμένες κατευθυντήριες προτάσεις με αφετηρία τη θέσπιση ενός εθνικού κανονιστικού πλαισίου συμπληρωματικού προς τον Κανονισμό DSA, το οποίο θα προσαρμόζεται στις ιδιαιτερότητες του ελληνικού ψηφιακού οικοσυστήματος, ενισχύοντας τους μηχανισμούς εποπτείας και την ανεξάρτητη διοικητική αρχή που θα έχει την αρμοδιότητα ελέγχου. Παράλληλα, απαιτείται η ενίσχυση της συνεργασίας μεταξύ δημόσιων αρχών, πλατφορμών και κοινωνίας των πολιτών, μέσω διαρκούς διαβούλευσης και συμμετοχικών διαδικασιών, ώστε να διασφαλίζεται η νομιμοποίηση των παρεμβάσεων και η αποδοχή τους από το κοινό. Εξαιρετικής σημασίας είναι, επίσης, η ενδυνάμωση των

---

<sup>141</sup> Kouroutakis P. (2022), The Digital Landscape in Greece: Challenges and Prospects, Hellenic Journal of Law and Technology 3(1), p.112-130.

ατομικών δικαιωμάτων των χρηστών, με τη βελτίωση των διαδικασιών ενημέρωσης, πρόσβασης, διόρθωσης και διαγραφής προσωπικών δεδομένων, όπως κατοχυρώνονται από τον ΓΚΠΔ, αλλά και η παροχή εύχρηστων και αποτελεσματικών εργαλείων προσφυγής και δικαστικής προστασίας.

Εν κατακλείδι, καθίσταται σαφές ότι ο έλεγχος περιεχομένου από τις ψηφιακές πλατφόρμες και η προστασία των προσωπικών δεδομένων δεν συνιστούν απλώς δύο παράλληλους άξονες κανονιστικής παρέμβασης, αλλά αλληλένδετες όψεις μιας ενιαίας πρόκλησης που αφορά την ουσία της ψηφιακής δημοκρατίας και τη διασφάλιση του σεβασμού των θεμελιωδών δικαιωμάτων στο διαδικτυακό περιβάλλον. Η ισορροπία ανάμεσα στην ανάγκη καταπολέμησης επιβλαβούς ή παράνομου περιεχομένου και στην υποχρέωση διασφάλισης της ιδιωτικότητας και της ελευθερίας της έκφρασης συνιστά τη θεμελιώδη δοκιμασία του σύγχρονου κανονιστικού πλαισίου. Η αποτελεσματική αντιμετώπιση των σύνθετων αυτών ζητημάτων προϋποθέτει σαφή και συνεπή εφαρμογή αρχών, όπως η αναλογικότητα, η αναγκαιότητα και η διαφάνεια, σε συνδυασμό με μια συνεχή συγκριτική θεώρηση των εθνικών και υπερεθνικών προτύπων. Μέσα σε αυτό το πλαίσιο, το εγχείρημα για την οικοδόμηση μιας ψηφιακής τάξης που σέβεται και προστατεύει τα δικαιώματα του ανθρώπου παραμένει διαρκώς επίκαιρο και απαιτεί συνεχή εγρήγορση τόσο σε θεσμικό όσο και σε κοινωνικό επίπεδο, ώστε ο έλεγχος περιεχομένου από πλατφόρμες και η προστασία προσωπικών δεδομένων να συνυπάρχουν ως εγγυήσεις ουσιαστικής ελευθερίας και ασφάλειας στον σύγχρονο ψηφιακό χώρο.

## ΒΙΒΛΙΟΓΡΑΦΙΑ

### Ελληνική Βιβλιογραφία - Αρθρογραφία

1. Ανθόπουλος Χ. (2021), Η ελευθερία της πληροφόρησης στην εποχή των ψηφιακών πλατφορμών, τεύχος 1, αρ. 1, Επιθεώρηση Δημόσιας Διοίκησης. Διαθέσιμο στο: <https://lawjournals.unic.ac.cy/index.php/pareview/article/view/6>
2. Ανθόπουλος Χ. (2000), Προστασία κατά του ρατσισμού και ελευθερία της πληροφόρησης: Ένα συνταγματικό δίλημμα, εκδόσεις Παπαζήση, Αθήνα
3. Γεωργοπούλου Α. και Πολυκαλάς Σπ. (2023), Η ευθύνη των διαδικτυακών πλατφορμών για το περιεχόμενο που αναρτούν οι χρήστες: από την Οδηγία για το ηλεκτρονικό εμπόριο στην Πράξη για τις ψηφιακές υπηρεσίες (DSA), ΔιΜΕΕ, 3/2023 Διαθέσιμο στο: <https://docs.google.com/document/d/1WfqLQt4VfNjNKYIrsQHR99tMWWJlgqY9/edit>
4. Γιαννόπουλος Γ. (2018), Εισαγωγή στη Νομική Πληροφορική, Νομική Βιβλιοθήκη
5. Ιγγλεζάκης, Ι. (2020), Δίκαιο της Πληροφορίας και της Επικοινωνίας, εκδόσεις Σάκκουλα
6. Ιγγλεζάκης Ι. (2020), Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679 και ο Εφαρμοστικός Νόμος – Ν. 4624/2019), 3η εκδόσεις Interactive Books
7. Ιγγλεζάκης Ι. (2024), Προστασία προσωπικών δεδομένων και ελευθερία της έκφρασης στο διαδίκτυο, στο πλαίσιο της εφαρμογής της Πράξης της ΕΕ για τις ψηφιακές υπηρεσίες, Επιθεώρηση Δικαίου Πληροφορικής, ΔιΜΕΕ, 1/2024, Διαθέσιμο στο: <https://ejournals.lib.auth.gr/infolawj>
8. Κανέλλος Λ. (2020), The GDPR Handbook, Αθήνα, εκδόσεις Νομική Βιβλιοθήκη
9. Κοτσαλής Λ. - Μενουδάκος Κ. (επιμ.) (2018), Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων, Νομική διάσταση και πρακτική εφαρμογή

10. Μαντζούφας Π. (2016), Νομικά ζητήματα από την χρήση του διαδικτύου: η ελευθερία της έκφρασης στα ιστολόγια. Διαθέσιμο στο: [https://www.constitutionalism.gr/mantzoufas\\_diadiktyo-eleftheria-ekfrasis](https://www.constitutionalism.gr/mantzoufas_diadiktyo-eleftheria-ekfrasis)
11. Μήτρου Λ. (1999), Η αρχή προστασίας προσωπικών δεδομένων, εκδόσεις Σάκκουλα
12. Μήτρου Λ. (2004), Ιδιωτικότητα στο WEB 2.0. ΔΙΤΕ (π ΔΙΜΕΕ) (3)
13. Μήτρου Λ. (2017), Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων: Νέο δίκαιο – νέες υποχρεώσεις – νέα δικαιώματα, Αθήνα, εκδόσεις Σάκκουλα
14. Μικρουλέα Α. (2023), Ανταγωνισμός και ρύθμιση στην ψηφιακή οικονομία, Αθήνα, εκδόσεις Νομική Βιβλιοθήκη
15. Σισιλιάνος Λ. Α. (2017), Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου, εκδόσεις Νομική Βιβλιοθήκη, Αθήνα

#### **Ξενόγλωσση Βιβλιογραφία - Αρθρογραφία**

1. Allcott H. - Gentzkow M. (2017), Social Media and Fake News in the 2016 Election, Journal of Economic Perspectives, 31(2). Διαθέσιμο στο: <https://doi.org/10.1257/jep.31.2.211>
2. Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, WP169. Διαθέσιμο στο: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf)
3. Balkin J. (2016), Information Fiduciaries and the First Amendment, 49 UC Davis Law Review 1183
4. Balkin J. M. (2018), Free Speech in the Algorithmic Society, UC Davis Law Review, 51(3)
5. Barendt E. (2005), Freedom of Speech, Oxford University Press
6. Barrie Sander (2020), Freedom of expression in the age of online platforms: The promise and pitfalls of human rights - Based approach to content moderation.

7. Brennen J. S. - Simon F. - Howard P. N. - Nielsen R. K. (2020), Types, Sources, and Claims of COVID-19 Misinformation, Reuters Institute for the Study of Journalism, University of Oxford. Διαθέσιμο στο: <https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation>
8. Brown A. (2020), Models of governance of online hate speech, Council of Europe. Διαθέσιμο στο: <https://rm.coe.int/models-of-governance-of-online-hate-speech/16809e671d>
9. Council of Europe (2021), Content Moderation: Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation (Guidance Note). Adopted by the Steering Committee for Media and Information Society (CDMSI).
10. Douek E. (2021), Content Moderation as Systems Thinking, Harvard Journal of Law & Technology
11. EDPS (2019), Accountability on the Ground: Guidance on Documenting Processing Operations for EU Institutions, Bodies and Agencies. Διαθέσιμο στο: [https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2019-07-16-accountability-ground-guidance-documenting-processing-operations-eu-institutions-bodies-and-agencies\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2019-07-16-accountability-ground-guidance-documenting-processing-operations-eu-institutions-bodies-and-agencies_en)
12. European Commission (2022), Strengthened Code of Practice on Disinformation. Διαθέσιμο στο: <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>
13. European Union Agency for Fundamental Rights (FRA) (2021), Hate Speech and Hate Crime against Migrants and Refugees in the EU. Διαθέσιμο στο: <https://fra.europa.eu/en/publication/2021/hate-speech-and-crime-against-migrants>
14. Finck M. (2017), Digital Revolution: Designing a Supranational Legal Framework for the Platform Economy, LSE Legal Studies Working Paper No. 15/2017. Διαθέσιμο στο: <https://eprints.lse.ac.uk/87568/>

15. Flach P. (2012), *Machine Learning: The Art and Science of Algorithms that Make Sense of Data*, Cambridge University Press
16. French Autorité de la concurrence & the German Bundeskartellamt (2019), *Algorithms and competition, Joint Study*. Διαθέσιμο στο: [https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Algorithms and Competition Working-Paper.html](https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Algorithms%20and%20Competition%20Working-Paper.html)
17. Geiger R. S. (2014), *Bots, bespoke, code and the materiality of software platforms: Wikipedia's infrastructure and governance*, *Information, Communication & Society*, 17(1). Διαθέσιμο στο: [https://www.researchgate.net/publication/263115381 Bots bespoke code and the materiality of software platforms](https://www.researchgate.net/publication/263115381_Bots_bespoke_code_and_the_materiality_of_software_platforms)
18. Gillespie T. (2018), *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press. Διαθέσιμο στο: [https://www.researchgate.net/publication/327186182\\_Custodians\\_of\\_the\\_internet\\_Platforms\\_content\\_moderation\\_and\\_the\\_hidden\\_decisions\\_that\\_shape\\_social\\_media](https://www.researchgate.net/publication/327186182_Custodians_of_the_internet_Platforms_content_moderation_and_the_hidden_decisions_that_shape_social_media)
19. Greer C. - McLaughlin E. (2023), *Regulating online harms: The Online Safety Act and free speech challenges*, *International Journal of Law and Technology*, 15(2)
20. Husovec M. - Peukert A. (2022), *The Digital Services Act: A Legal and Systematic Analysis*, Max Planck Institute for Innovation & Competition Research Paper No. 22-10.
21. Katz M. L. - Shapiro C. (1985), *Network Externalities, Competition, and Compatibility: The American Economic Review*, Vol. 75 No. 3. Διαθέσιμο στο: <https://www.jstor.org/stable/1814809>
22. Klonick K. (2018), *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 *Harvard Law Review* 1598
23. Kouroutakis P. (2022), *The Digital Landscape in Greece: Challenges and Prospects*, *Hellenic Journal of Law and Technology* 3(1)

24. Kuner, C. - Bygrave L. A. - Docksey, C. (Eds.) (2020), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press
25. Lyskey O. (2015), *The Foundations of EU Data Protection Law*, Oxford University Press
26. O'Dell A., 2023, *The DSA and Fundamental Rights: A Missed Opportunity for Data Protection*, *European Law Journal*
27. Opinion 1/2021 on the Proposal for a Digital Services Act (2021), European Data Protection Supervisor. Διαθέσιμο στο: [https://www.edps.europa.eu/system/files/2021-02/21-02-10-opinion\\_on\\_digital\\_services\\_act\\_en.pdf](https://www.edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf)
28. Politou E., E. Alepis, C. Patsakis (2018), *Forgetting personal data and revoking consent under the GDPR: Challenges and Proposed Solutions*, *Journal of Cybersecurity*
29. Poscher R. (2019), *Germany's NetzDG: Fighting Hate Speech and Fake News in the Digital Age*, *German Law Journal*, 20(5)
30. Roberts S. T. (2019), *Behind the Screen: Content Moderation in the Shadows of Social Media*, Yale University Press
31. Rochet J.- C. - Tirole J. (2003), *Platform competition in two-sided markets*, *Journal of the European Economic Association*, vol.1 issue 4. Διαθέσιμο στο: <https://academic.oup.com/jeea/article/1/4/990/2280902>
32. Serban A. - Claudio Barbosa Teixeira (2021), *Data Protection and Digital Services – European Union Perspectives*
33. Srnicek N., (2016), *Platform Capitalism*, Polity Press. Διαθέσιμο στο: [https://books.google.gr/books?hl=el&lr=&id=2HdNDwAAQBAJ&oi=fnd&pg=PR3&ots=ntIIKtSn4i&sig=xdsLWGBDJaL4IWvms7zKmaaORvw&redir\\_esc=y#v=onepage&q&f=false](https://books.google.gr/books?hl=el&lr=&id=2HdNDwAAQBAJ&oi=fnd&pg=PR3&ots=ntIIKtSn4i&sig=xdsLWGBDJaL4IWvms7zKmaaORvw&redir_esc=y#v=onepage&q&f=false)
34. Sutton R. S.- Barto A. G. (2018), *Reinforcement Learning: An Introduction* (2nd ed.), MIT Press.

35. Suzor N. (2019), *Lawless: The Secret Rules that Govern Our Digital Lives*, Cambridge University Press.
36. UNESCO (2021), United Nations Office on Genocide Prevention and the Responsibility to Protect, *Addressing hate speech on social media: contemporary challenges*. Διαθέσιμο στο: <https://unesdoc.unesco.org/ark:/48223/pf0000379177>
37. Veale M., Edwards L. (2018), *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling*, *Computer Law & Security Review*
38. Wardle C. - Derakhshan H. (2017), *Information Disorder: Toward an Interdisciplinary Framework*, Council of Europe.

#### **Διπλωματικές Εργασίες**

1. Διπλωματική εργασία της Καπαδούκα Χ. (2023), *Digital Services Act, Digital Markets Act και ζητήματα προστασίας προσωπικών δεδομένων*, Πρόγραμμα Μεταπτυχιακών Σπουδών στο Δίκαιο, Τεχνολογίες Πληροφορικής και Επικοινωνιών, Πανεπιστήμιο Πειραιώς
2. Mazzarda F. (2022) *Pricing algorithms and the risk of tacit collusion*. Bachelor's Degree Thesis, Luiss Guido Carli. Διαθέσιμο στο: <https://tesi.luiss.it/33426/>
3. Williams N. J. - Malmgren F. N. (2019), *The Platform Policy Puzzle: Forms of Regulating Multi-Sided Platforms in Nine European Cities*, MSc Thesis, Copenhagen Business School.

#### **Νομοθετικά Κείμενα**

1. Κανονισμός (ΕΕ) 2017/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός

- Κανονισμός για την Προστασία Δεδομένων). Διαθέσιμο στο: <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679>
2. Κανονισμός (ΕΕ) 2022/2065 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ενιαία αγορά ψηφιακών υπηρεσιών και την τροποποίηση της οδηγίας 2000/31/ΕΚ (πράξη για τις ψηφιακές υπηρεσίες. Διαθέσιμο στο: <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32022R2065>
  3. Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»). Διαθέσιμο στο: <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32000L0031>
  4. Οδηγία 2010/13/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον συντονισμό ορισμένων νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών σχετικά με την παροχή υπηρεσιών οπτικοακουστικών μέσων (οδηγία για τις υπηρεσίες οπτικοακουστικών μέσων). Διαθέσιμο στο: <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32010L0013>
  5. Οδηγία 2019/790/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, για τα δικαιώματα πνευματικής ιδιοκτησίας και τα συγγενικά δικαιώματα στην ψηφιακή ενιαία αγορά και την τροποποίηση των οδηγιών 96/9/ΕΚ και 2001/29/ΕΚ. Διαθέσιμο στο: <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32019L0790>
  6. Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Διαθέσιμο σε: <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046>
  7. Σύσταση (ΕΕ) 2018/334 της Επιτροπής σχετικά με μέτρα για την αποτελεσματική αντιμετώπιση του παράνομου περιεχομένου στο διαδίκτυο.

- Διαθέσιμο: <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32018H0334>
8. Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, ΕΕ C 202 της 7.6.2016. Διαθέσιμο στο <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:12016P/TXT>
9. Irish Government (2022), Online Safety and Media Regulation Act. Διαθέσιμο στο: <https://www.gov.ie/en/department-of-culture-communications-and-sport/publications/online-safety-and-media-regulation-act-2022/>
10. UK Parliament (2023), Online Safety Act. Διαθέσιμο στο: <https://bills.parliament.uk/bills/3137>

## Νομολογία

1. ΔΕΕ, Απόφαση της 13<sup>ης</sup> Μαΐου 2014, (Google Spain SL και Google Inc. κατά Agencia Española de Protección de Datos, AEPD και Mario Costeja González), C-131/12
2. ΔΕΕ, Απόφαση της 16<sup>ης</sup> Φεβρουαρίου 2012, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) κατά Netlog NV, C-360/10
3. ΔΕΕ, Απόφαση της 24<sup>ης</sup> Νοεμβρίου 2011, Scarlet Extended SA κατά Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10
4. ΔΕΕ, Απόφαση της 26<sup>ης</sup> Απριλίου 2022, Δημοκρατία της Πολωνίας κατά Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της Ευρωπαϊκής Ένωσης, C-401/19
5. ΔΕΕ, Απόφαση της 29<sup>ης</sup> Ιουλίου 2019, Fashion ID GmbH & Co. KG κατά Verbraucherzentrale NRW eV, C-40/17
6. ΔΕΕ, Απόφαση της 5<sup>ης</sup> Ιουνίου 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein κατά Wirtschaftsakademie Schleswig-Holstein GmbH, C-210/16
7. ΕΔΔΑ, Απόφασης της 16<sup>ης</sup> Ιουνίου 2015, Delfi AS κατά Εσθονίας, No. 64569/09

8. ΕΔΔΑ, Απόφαση της 2<sup>ης</sup> Φεβρουαρίου 2016, Magyar Tartalomszolgálatók Egyesülete (MTE) και Index.hu Zrt. κατά Ουγγαρίας, No. 22947/13
9. ΕΔΔΑ, Απόφαση της 26<sup>ης</sup> Απριλίου 1979, Sunday Times κατά Ηνωμένου Βασιλείου, No. 6538/74
10. ΕΔΔΑ, Απόφαση της 6<sup>ης</sup> Ιουλίου 2006, Erbakan κατά Turkey, No. 59405/00
11. ΕΔΔΑ, Απόφαση της 7<sup>ης</sup> Δεκεμβρίου 1976, Handyside κατά Ηνωμένου Βασιλείου, No. 5493/72
12. ΕΔΔΑ, Απόφαση της 8<sup>ης</sup> Ιουλίου 1986, Lingens κατά Αυστρίας, No. 9815/82