



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ  
Εθνικόν και Καποδιστριακόν  
Πανεπιστήμιον Αθηνών  
— ΙΔΡΥΘΕΝ ΤΟ 1837 —

**ΝΟΜΙΚΗ ΣΧΟΛΗ**

Π.Μ.Σ.: ΕΜΠΟΡΙΚΟΥ ΔΙΚΑΙΟΥ  
ΕΙΔΙΚΕΥΣΗ: ΑΪΛΛΑ ΑΓΑΘΑ ΚΑΙ ΑΝΤΑΓΩΝΙΣΜΟΣ  
ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΕΤΟΣ: 2021-2022

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

**της Ελένης Σπυρίδωνος Χριστοπούλου**

**A.M.: 7340122101021**

**«Παράβαση Προσωπικών Δεδομένων και Δίκαιο Ανταγωνισμού:  
Υπόθεση Facebook»**

**Επιβλέπουσα Καθηγήτρια και Τριμελής Επιτροπή:**

Αναπληρώτρια Καθηγήτρια, κ. Μικρούλεα Π. Αλεξάνδρα (επιβλέπουσα)

Επίκουρη Καθηγήτρια, κ. Ευθυμία Ι. Κινινή

Επίκουρος Καθηγητής, κ. Εμμανουήλ Π. Μαστρομανώλης

**Αθήνα, Οκτώβριος 2022**

*Αφιερώνεται σε όλα τα αγαπημένα μου πρόσωπα*

*Copyright © Χριστοπούλου Ελένη, 2022*

*Με επιφύλαξη παντός δικαιώματος. All rights reserved.*

*Απαγορεύεται η αντιγραφή, αποθήκευση και η διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα.*

*Οι απόψεις και θέσεις που περιέχονται σε αυτήν την εργασία εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών.*

## Ευχαριστίες

*Θα ήθελα να ευχαριστήσω θερμά την κ. Μικρουλέα Αλεξάνδρα, Αναπληρώτρια Καθηγήτρια Εμπορικού Δικαίου, στο Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών και επιβλέπουσα της παρούσας μελέτης, για την πολύτιμη βοήθεια και καθοδήγηση. Η συμβολή της υπήρξε σπουδαία, διότι με τις γνώσεις και την προθυμία της να με υποστηρίξει και να με κατευθύνει, υλοποιήθηκε η παρούσα έρευνα, στα πλαίσια της αποπεράτωσης των σπουδών μου, στο Πρόγραμμα Μεταπτυχιακών Σπουδών. Επιπλέον, θα ήθελα να ευχαριστήσω, και τα άλλα δύο μέλη της τριμελούς επιτροπής, την κ. Κινινή Ευθυμία, Επίκουρη Καθηγήτρια Εμπορικού Δικαίου και τον κ. Μαστρομανώλη Εμμανουήλ, Επίκουρο Καθηγητή του Εμπορικού Δικαίου, για τη μελέτη της διπλωματικής μου εργασίας, αλλά και όλους τους Καθηγητές μου, οι οποίοι υπήρξαν σπουδαίοι δάσκαλοι και μεταλαμπάδευσαν τις γνώσεις τους, σε εμένα και τους συμφοιτητές μου, οδηγώντας τη σκέψη μας σε νέους ορίζοντες.*

## ΠΕΡΙΕΧΟΜΕΝΑ

Συντομογραφίες.....	09
Περίληψη.....	10
Abstract.....	11
Εισαγωγή.....	12
<b>ΚΕΦΑΛΑΙΟ 1: Τα Δεδομένα Προσωπικού Χαρακτήρα.....</b>	<b>14</b>
1.1 Εννοιολογική προσέγγιση.....	14
1.1.1 Τα προσωπικά δεδομένα.....	14
1.1.2 Η έννοια της ιδιωτικότητας.....	16
1.1.3 Η επεξεργασία των δεδομένων και η έννοια της συγκατάθεσης.....	19
1.2 Τα προσωπικά δεδομένα στις ψηφιακές πλατφόρμες.....	21
1.2.1 Τα προσωπικά δεδομένα στα μέσα κοινωνικής δικτύωσης.....	21
1.2.2 Ηλεκτρονικές εμπορικές συναλλαγές και δεδομένα των πλατφορμών.....	22
1.2.3 Καταπάτηση δικαιωμάτων χρηστών στο διαδίκτυο.....	24
1.3 Δικαιώματα των υποκειμένων των προσωπικών δεδομένων.....	25
1.3.1 Το δικαίωμα της πρόσβασης του υποκειμένου.....	26
1.3.2 Το δικαίωμα φορητότητας.....	27
1.3.3 Το δικαίωμα διόρθωσης και το δικαίωμα προβολής αντιρρήσεων.....	27
1.3.4 Το δικαίωμα διαγραφής- δικαίωμα στη «λήθη».....	28
1.3.5 Το δικαίωμα του υποκειμένου αναφορικά με την αυτοματοποιημένη λήψη αποφάσεων.....	30
<b>ΚΕΦΑΛΑΙΟ 2: Το νομικό πλαίσιο σε εθνικό και υπερεθνικό επίπεδο.....</b>	<b>31</b>
2.1 Το θεσμικό πλαίσιο προστασίας των δεδομένων προσωπικού χαρακτήρα.....	31
2.1.1 Το ισχύον δίκαιο στην Ελλάδα.....	31
α) Στο Σύνταγμα.....	31
β) Στον Αστικό Κώδικα.....	32
γ) Στο Ποινικό Δίκαιο.....	32
2.1.2 Το θεσμικό πλαίσιο στην Ευρώπη.....	33
α) Κανονισμοί και Οδηγίες.....	33

β) Ο Γενικός Κανονισμός Προσωπικών Δεδομένων (GDPR).....	35
2.1.3 Η προστασία των δεδομένων στις ΗΠΑ.....	38
2.2 Η παραβίαση των δεδομένων προσωπικού χαρακτήρα.....	40
2.2.1 Η γνωστοποίηση της παραβίασης στην εποπτική αρχή.....	41
2.2.2 Η ανακοίνωση της παραβίασης στο υποκείμενο των προσωπικών δεδομένων.....	43

### **ΚΕΦΑΛΑΙΟ 3: Νομικό Πλαίσιο: Ο Κανονισμός DMA, πλατφόρμες και προσωπικά δεδομένα.....**

3.1 Ιστορικό πλαίσιο του Digital Markets Act (DMA).....	45
3.2 Αιτιολόγηση της πρότασης.....	46
3.3 Στόχοι του DMA.....	47
3.4 Πεδίο εφαρμογής του DMA.....	48
3.4.1 Οι πλατφόρμες ως ρυθμιστές πρόσβασης .....	49
3.4.2 Υποχρεώσεις των ρυθμιστών πρόσβασης.....	50
3.5 Μόχλευση και περικάλυψη (Leverage and envelopment).....	51
3.6 Συνέπειες από τη μη συμμόρφωση των ρυθμιστών πρόσβασης με τους κανόνες της DMA.....	52
3.7 Η σχέση της DMA με την DSA.....	53
3.8 Η πράξη Eu Data act.....	54
3.8.1 Το ιστορικό πλαίσιο της πρότασης.....	55
3.8.2 Τα μέτρα που περιλαμβάνονται στο νόμο περί δεδομένων.....	55
3.8.3 Τα αποτελέσματα της πράξης Eu Data Act.....	56

### **ΚΕΦΑΛΑΙΟ 4: Η Γερμανική Υπόθεση “Facebook”- C-252/21.....**

4.1 Η ανάλυση της υπόθεσης.....	57
4.1.1 Εισαγωγή.....	57
4.1.2 Η γερμανική υπόθεση Facebook.....	58
4.1.3 Ιστορικό της υποθέσεως.....	59
4.2 Τα πραγματικά περιστατικά και το διαδικαστικό υπόβαθρο.....	62
4.3 Το νομικό πλαίσιο στη C-252/21.....	64
4.3.1 Το δίκαιο της Ένωσης.....	65
4.3.2 Το γερμανικό δίκαιο.....	65

4.4 Αίτηση για την έκδοση προδικαστικής απόφασης από το Oberlandesgericht Düsseldorf (Γερμανία)- Facebook Inc. και άλλοι κατά Bundeskartellamt.....	66
4.4.1 Προδικαστικά ερωτήματα.....	66
4.4.1 α) Ο ρόλος του Bundeskartellamt.....	66
4.4.1 β) Η επεξεργασία «ευαίσθητων» προσωπικών δεδομένων από την ίδια και η συσχέτιση αυτών με πληροφορίες άλλων εταιριών.....	67
4.4.1 γ) Επιχειρήματα και δικαιολογητική βάση της επεξεργασίας και της συσχέτισης, δυνάμει των άρθρων του Κανονισμού GDPR.....	68
4.4.1 δ) Οι σκοποί της επεξεργασίας ως έννομα συμφέροντα κατά το άρθρο 6 παρ. 1, στοιχείο στ' του GDPR.....	68
4.4.1 ε) Δικαιολογητική βάση της επεξεργασίας για νόμιμους σκοπούς.....	69
4.4.1 στ) Δήλωση συγκατάθεσης χρήστη προς την επιχείρηση που κατέχει δεσπό- ζουσα θέση στην αγορά.....	69
4.4.1 ζ) Ο ρόλος της εποπτικής αρχής κατά τις διατάξεις του ΓΚΠΔ.....	70
4.5 Απαντήσεις επί των προδικαστικών ερωτημάτων.....	70
4.5.1 Απάντηση του πρώτου προδικαστικού ερωτήματος.....	70
4.5.2 Απάντηση του δεύτερου προδικαστικού ερωτήματος.....	71
4.5.3 Απάντηση του τρίτου, τέταρτου και πέμπτου προδικαστικού ερωτήματος.....	72
4.5.4 Απάντηση του έκτου προδικαστικού ερωτήματος.....	73
4.5.5 Απάντηση του έβδομου προδικαστικού ερωτήματος.....	74
4.6 Προτάσεις του γενικού εισαγγελέα Α. Ράντου.....	75

<b>ΚΕΦΑΛΑΙΟ 5: Η Γερμανική Υπόθεση Facebook- C-252/21 και η ανάλυσή της υπό το πρίσμα του Δικαίου του Ανταγωνισμού.....</b>	<b>78</b>
5.1 Η σχετική αγορά στην υπόθεση Facebook.....	78
5.2 Η καταχρηστική εκμετάλλευση δεσπόζουσας θέσης.....	79
5.2.1 Νομικό Πλαίσιο.....	79
5.2.2 Η έννοια της κατάχρησης.....	80
5.2.3 Η πρακτική της καταχρηστικής εκμετάλλευσης στην υπόθεση Facebook.....	81
5.3 Η θεωρία της βλάβης (theory of harm) στα πλαίσια της αναλύσεως της..... γερμανικής υποθέσεως.....	83
5.4 Η σχέση μεταξύ Δικαίου Ανταγωνισμού και του Νόμου για την προστασία των προσωπικών δεδομένων.....	85
5.5 Εξέταση πτυχών της προστασίας δεδομένων.....	85

5.6 Συμβατότητα με τις αξίες του GDPR.....	86
5.7 Η συγκατάθεση των χρηστών της πλατφόρμας.....	87
5.7.1 Η παραβίαση της ιδιωτικότητας ως βλάβη των καταναλωτών- χρηστών της Πλατφόρμας του Facebook.....	87
5.8 Συμπεράσματα από την απόφαση.....	88
5.9 Σχολιασμός και αξιολόγηση της απόφασεως.....	88

## **ΚΕΦΑΛΑΙΟ 6: Η παραβίαση των προσωπικών δεδομένων στις πλατφόρμες... 90**

6.1 Ψηφιακές πλατφόρμες και Δίκαιο του Ανταγωνισμού.....	90
6.1.1 Τα δεδομένα προσωπικής και μη προσωπικής ταυτοποίησης των χρηστών του διαδικτύου.....	94
6.2 Παραβάσεις των πλατφορμών.....	97
6.2.1 α) Google.....	98
β) Facebook.....	101
6.2.2 Ζητήματα ιδιωτικότητας στο διαδίκτυο (Internet Privacy Issues).....	102
6.2.3 Η παραβίαση των προσωπικών δεδομένων των υποκειμένων, μέσω των “cookies”.....	105
6.2.4 Συνέπειες από την παραβίαση των δεδομένων στις πλατφόρμες.....	107

## **ΚΕΦΑΛΑΙΟ 7: Πλατφόρμες κοινωνικής δικτύωσης και Facebook Cases..... 109**

7.1 Οι ιστοσελίδες κοινωνικής δικτύωσης (social media) και τα δεδομένα προσωπικού χαρακτήρα.....	109
7.2 Η εφαρμογή του “Facebook” και τα προσωπικά δεδομένα.....	110
7.2.1 Οι υποχρεώσεις των παρόχων.....	113
7.2.2 Ευθύνη μεσαζόντων στην παροχή των υπηρεσιών του διαδικτύου.....	115
7.2.3 Facebook και Διαφήμιση στην πλατφόρμα.....	118
7.2.4 Το δικαίωμα της ελευθερίας της έκφρασης στην πλατφόρμα με τη χρήση ψευδωνύμου.....	120
7.2.5 Η διαρροή των προσωπικών δεδομένων από την πλατφόρμα κοινωνικής δικτύωσης του “Facebook”.....	121
7.2.6 Η ανάλυση της υπόθεσης “Facebook”.....	122
α) Υπόθεση Cambell v. Facebook Inc.....	122
β) Υπόθεση παραβίασης δεδομένων προσωπικού χαρακτήρα μέσω Facebook fanpage.....	124



γ) Υπόθεση Max Schrems κατά Facebook.....	126
δ) Sponsored Stories.....	127
<b>ΚΕΦΑΛΑΙΟ 8: Τρόποι προστασίας, Δικαιώματα και Κυρώσεις.....</b>	<b>129</b>
8.1 Νέες Τεχνολογίες και τρόποι προστασίας των προσωπικών δεδομένων στον κυβερνοχώρο.....	129
8.2 Δικαίωμα άσκησης μέσω έννομης προστασίας.....	132
8.3 Οι κυρώσεις σε περιπτώσεις παραβάσεων.....	133
α) Διοικητικές κυρώσεις.....	133
β) Ποινικές κυρώσεις.....	134
<b>Συμπεράσματα.....</b>	<b>135</b>
<b>Βιβλιογραφία και Ηλεκτρονικές Πηγές.....</b>	<b>137</b>
<b>ΠΑΡΑΡΤΗΜΑ Ι.....</b>	<b>149</b>
Νομοθεσία.....	149
<b>ΠΑΡΑΡΤΗΜΑ ΙΙ.....</b>	<b>154</b>
Νομολογία.....	154

## Συντομογραφίες

<b>ΑΚ</b>	Αστικός Κώδικας
<b>ΑΠΔΠΧ</b>	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
<b>Βλ</b>	Βλέπε
<b>ΓΚΠΔ</b>	Γενικός Κανονισμός Προσωπικών Δεδομένων (GDPR)
<b>ΕΕ</b>	Ευρωπαϊκή Ένωση
<b>ΕΕ</b>	Ευρωπαϊκή Επιτροπή
<b>ΕΚ</b>	Ευρωπαϊκό Κοινοβούλιο
<b>ΕΜΑ</b>	Επιτροπή Μονίμων Αντιπροσώπων
<b>ΕΣΔΑ</b>	Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου
<b>ΟΟΣΑ</b>	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
<b>ΠΚ</b>	Ποινικός Κώδικας
<b>Σ</b>	Σύνταγμα
<b>ΣΕΕ</b>	Συνθήκη για την Ευρωπαϊκή Ένωση
<b>ΣΛΕΕ</b>	Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης
<b>ΕισΝΑΚ</b>	Εισαγωγικός Νόμος του Αστικού Κώδικα
<b>ΥΠΔ</b>	Υπεύθυνος Προστασίας Δεδομένων (DPO)
<b>CAPs</b>	Content Applications and Services Providers
<b>GWB</b>	Gesetz gegen Wettbewerbsbeschränkungen
<b>DMA</b>	Digital Markets Act
<b>DPO</b>	Data Protection Officer
<b>DSA</b>	Data Services Act
<b>FTC</b>	Federal Trade Commission
<b>FB</b>	Facebook
<b>GDPR</b>	General Data Protection Regulation
<b>ISPs</b>	Internet Service Providers
<b>OECD</b>	Organisation for Economic Co-operation and Development

## Περίληψη

Η παρούσα μελέτη αφορά το θέμα της παράβασης των δεδομένων προσωπικού χαρακτήρα, αλλά και τη σχέση του ζητήματος αυτού, με το δίκαιο του ανταγωνισμού. Σε αυτά τα πλαίσια, γίνεται αναφορά και στις ψηφιακές πλατφόρμες, οι οποίες στη σύγχρονη εποχή αποτελούν τη λεγόμενη «ψηφιακή οικονομία» και οι οποίες χαρακτηρίζονται από αποτελέσματα δικτύου (*network effects*), πολύ μεγάλες αποδόσεις κλίμακας (*extreme returns to scale*) και δεδομένα μεγάλου όγκου (*big data*). Αυτά τα δεδομένα, αλλά και η χωρητικότητα των διαδικτυακών πλατφορμών, δημιουργούν τις συνθήκες για την κάλυψη πλήθους καταναλωτικών αναγκών. Οι καταναλωτές επιδιώκουν την εκτέλεση των εργασιών τους σε διαδικτυακούς τόπους, σε χαμηλότερο κόστος, σε λιγότερο χρόνο και αποκομίζοντας περισσότερα οφέλη, συγκριτικά με την εκτέλεση των ίδιων εργασιών, δίχως την χρήση των ψηφιακών πλατφορμών. Κατανοούμε ότι η χρήση των συστημάτων αυτών, αφορά πλήθος δραστηριοτήτων, όπως είναι η εκτέλεση χρηματικών συναλλαγών μέσω ηλεκτρονικής πλατφόρμας (*e-banking*), η αγορά προϊόντων από εταιρίες, αλλά και οι υπηρεσίες επικοινωνίας. Η εξέλιξη των αγορών αυτών, έχει ωστόσο προκαλέσει την τάση προς ενίσχυση των παρεμβατικών μηχανισμών, προκειμένου να υπάρξει προστασία του ελεύθερου ανταγωνισμού.

Στο σύστημα αυτό, της «ψηφιακής οικονομίας», βρίσκεται μεγάλος αριθμός δεδομένων, τα οποία θα πρέπει οπωσδήποτε να παραμείνουν προστατευμένα από οποιαδήποτε προσβολή ή προσπάθεια υποκλοπής. Ο αριθμός των προσωπικών δεδομένων που φιλοξενούνται στο διαδίκτυο είναι υπερβολικά μεγάλος, λόγω του γεγονότος ότι χρήστες από όλο τον κόσμο, δραστηριοποιούνται στις πλατφόρμες και στον «κυβερνοχώρο». Οποιαδήποτε «διαρροή» τέτοιου ηλεκτρονικού υλικού, καθιστά προσβολή και παράβαση των προσωπικών δεδομένων των χρηστών και τιμωρείται από το νόμο. Αυτό συμβαίνει, διότι κάθε ιστότοπος, με συγκεκριμένη λειτουργία και σκοπό δημιουργίας, έχει προηγουμένως δεσμευτεί να προστατεύει τα προσωπικά δεδομένα των χρηστών, οι οποίοι μάλιστα, είναι εντοπισμένοι σε παγκοσμίου εκτάσεως κλίμακα. Τέτοιο παράδειγμα «διαρροής» υλικού, αποτελεί η υπόθεση του Facebook, με τα δεδομένα που υπήρχαν σε αυτό, να ξεπερνούν τα εκατομμύρια, λόγω της δημοφιλίας της πλατφόρμας σε παγκόσμιο επίπεδο.

**Λέξεις-κλειδιά: προσωπικά δεδομένα, δίκαιο ανταγωνισμού, Facebook**

## **Abstract**

*The present study refers to the issue of personal data violation and its relation, to the law of competition. In this context, digital platforms, are also mentioned. Moreover, in modern times, they are the so -called "digital economy" and they are characterized by network effects, extreme returns to scale and big data. These data, as well as the capacity of online platforms, create the conditions to meet a large number of consumer needs. Consumers are seeking to perform their work on websites, at a lower cost, in less time and reaping more benefits than the same work, without the use of digital platforms. We understand that the use of these systems concerns a number of activities, such as e-banking, buying products from companies and communication services. The evolution of these markets, however, has caused the tendency to strengthen intervention mechanisms in order to protect free competition.*

*In this system, of the "digital economy", there is a large number of data, which should definitely remain protected from any infringement or attempt of spying. The number of personal data hosted online is too large, due to the fact that users from all over the world are active on platforms and cyberspace. Any "leak" of such electronic material makes an infringement of users' personal data and this action is punished by the law. This happens, because each website, with a specific function and purpose of creation, has previously been committed to protect the personal data of users, who are even located on a world -class scale. Such an example of "leakage" material is Facebook's case, with the data that existed in it, exceeding millions, due to the popularity of the platform worldwide.*

***Keywords: Personal Data, Competition Law, Facebook***

## Εισαγωγή

Στη σύγχρονη εποχή παρατηρείται ολοένα και περισσότερο η χρήση των διαδικτυακών πλατφορμών σε όλους τους τομείς της καθημερινής ζωής των πολιτών για τη διεκπεραίωση πλήθος δραστηριοτήτων, οι οποίες μάλιστα, αφορούν τόσο την οικονομική όσο και την κοινωνική ζωή.

Σε αυτά τα πλαίσια, είναι ουσιώδες να αναφερθεί ότι η εύκολη πρόσβαση στον κυβερνοχώρο, αποτελεί μία δυνατότητα την οποία εκμεταλλεύεται ο πολίτης, χρησιμοποιώντας κάθε φορά το ουσιαστικό δικαίωμά του στην πρόσβαση στην κυκλοφορία των πληροφοριών, αλλά εκμεταλλευόμενος, αντίστοιχα και την αντίστοιχη υποχρέωση του κράτους προς αυτή την κατεύθυνση. Τόσο η εύκολη πρόσβαση, όσο το χαμηλό κόστος, σε συνδυασμό με το γεγονός ότι πρόκειται για ανοιχτό αλλά και παγκόσμιο δίκτυο χωρίς όρια και σύνορα, δημιουργεί την ανάγκη των πολιτών για την χρησιμοποίηση των πλατφορμών, αλλά και την ανταλλαγή των πληροφοριών με τα μέλη της διαδικτυακής «κοινότητας».

Παράλληλα, υπό το πρίσμα της άσκησης των υποχρεώσεων μιας επιχείρησης, η ταχύτητα, η ελευθερία και η οικονομική ανεξαρτησία του Διαδικτύου, αποτελούν χαρακτηριστικά, τα οποία χρειάζεται οπωσδήποτε μια εταιρεία για την ομαλή λειτουργία της, αλλά και για την αποτελεσματικότερη επικοινωνία μεταξύ των μελών της, προκειμένου να συνδεθεί σε παγκόσμιες αγορές, να έρθει σε επαφή με πλήθος νέων καταναλωτών ανά τον κόσμο και να προσφέρει νέες, καινοτόμες και διαφορετικές δυνατότητες, τις οποίες υπό άλλες συνθήκες δεν θα μπορούσε να υλοποιήσει αποτελεσματικά.

Ακόμη, οι επιχειρήσεις χρησιμοποιούν ολοένα και περισσότερο το ηλεκτρονικό εμπόριο προκειμένου να ικανοποιήσουν τους καταναλωτές τους, με την παροχή των προϊόντων τους, αλλά και των υπηρεσιών τους, ενώ πλέον, παρατηρείται το φαινόμενο να εμφανίζονται περισσότερα ηλεκτρονικά καταστήματα, τα οποία δεν διαθέτουν αντίστοιχο φυσικό κατάστημα για τους καταναλωτές τους, αλλά αντίθετα, χρησιμοποιούν τον κυβερνοχώρο, τόσο για να διαφημίσουν τα προϊόντα τους, όσο για να προσφέρουν και να πωλήσουν στους καταναλωτές τους μεγάλες ποσότητες προϊόντων και να διαμορφώσουν μία ισχυρή δυναμική στην αγορά.

Με αυτό τον τρόπο επιτυγχάνεται ο σκοπός της επιχείρησης, να αποκομίσει κέρδη και οφέλη μέσω της χρήσης του διαδικτύου, αλλά και των σύγχρονων

συναλλαγών, με αποτέλεσμα να πραγματοποιούνται εύκολες και ασφαλείς διαδικτυακές αγορές, σε γρήγορο χρόνο, με αμεσότητα και με πολύ λίγα έξοδα για την ίδια. Αναφορικά με τα ηλεκτρονικά καταστήματα, τα οποία, ειδικότερα, δεν διαθέτουν φυσικό κατάστημα, τα οικονομικά τους οφέλη από τις ηλεκτρονικές συναλλαγές τείνουν αυξάνονται σημαντικά εξ αυτού του λόγου.

Κατανοούμε λοιπόν ότι στη σύγχρονη εποχή, το διαδίκτυο ενώνει τους καταναλωτές με τις επιχειρήσεις και διευκολύνει με κάθε δυνατό τρόπο την μεταξύ τους επικοινωνία, προκειμένου να επιτευχθούν ασφαλώς οι εμπορικές συναλλαγές και να επιτευχθεί ο οικονομικός σκοπός της εκάστοτε επιχείρησης. Παράλληλα, στο σύστημα της κοινωνικής ζωής, κατά τον ίδιο τρόπο, διευκολύνεται η σχέση και η επαφή μεταξύ των ατόμων, χάρη στη ραγδαία αύξηση και χρήση της τεχνολογίας και των προϊόντων- μέσων της.

Θα πρέπει, ωστόσο, να αναφερθεί το γεγονός, ότι κατά τη διαδικασία ανταλλαγής πληροφοριών κατά τη διεκπεραίωση των εμπορικών συναλλαγών, μέσω των ηλεκτρονικών συστημάτων και των σύγχρονων υπολογιστικών μέσων και πλατφορμών, γίνεται επεξεργασία πλήθους προσωπικών δεδομένων και πληροφοριών οικονομικού χαρακτήρα, αλλά και ατομικών στοιχείων, τα οποία οι καταναλωτές, δεν θα ήθελαν να διαρρεύσουν ή να τύχουν μετέπειτα επεξεργασίας από την επιχείρηση και τα μέλη της, αλλά να σταματήσει η χρήση τους, ύστερα από τη λήξη της εμπορικής συναλλαγής τους, ή έστω, έπειτα από ένα μικρό χρονικό διάστημα από την τελευταία χρήση της διαδικτυακής πλατφόρμας, η οποία χρησιμοποιήθηκε κατά τη συναλλαγή.

Αυτές οι πληροφορίες, είναι πιθανό να αφορούν τόσο ατομικά χαρακτηριστικά, όπως για παράδειγμα, ονοματεπώνυμο, διεύθυνση κατοικίας ή στοιχεία επικοινωνίας του καταναλωτή, όσο και οικονομικά στοιχεία, όπως είναι στοιχεία της τραπεζικής κάρτας ή ο εξατομικευμένος λογαριασμός του χρήστη, ο οποίος χρησιμοποιείται για την εκπλήρωση της ενοχικής του υποχρέωσης, που προκύπτει από τη συναλλαγή με το ηλεκτρονικό κατάστημα.

Σε κάθε περίπτωση, είναι απαραίτητη η δέσμευση του κατόχου προσωπικών δεδομένων των καταναλωτών από την επιχείρηση ή τρίτο, είτε πρόκειται για ηλεκτρονική επικοινωνία, είτε για άμεση σχέση, να φυλάσσουν τα δεδομένα προσωπικού χαρακτήρα που τους εμπιστεύονται οι καταναλωτές.

# ΚΕΦΑΛΑΙΟ 1

## Τα Δεδομένα Προσωπικού Χαρακτήρα

### 1.1 Εννοιολογική προσέγγιση

#### 1.1.1 Τα προσωπικά δεδομένα

Τα προσωπικά δεδομένα αποτελούν μία ευρεία κατηγορία δεδομένων, η οποία μάλιστα, παρουσιάζει διαφοροποιήσεις ανάμεσα σε χώρες του κόσμου, αλλά και ταξινομείται διαφορετικά με βάση, τόσο τη φύση, όσο και το είδος των δεδομένων αυτών. Αυτό το γεγονός, συμβαίνει διότι σε κάθε κράτος, ο όρος της ιδιωτικής ζωής ή της ιδιωτικότητας διαφέρει, αντίστοιχα.

Σύμφωνα με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), τα δεδομένα προσωπικού χαρακτήρα είναι όλες εκείνες οι πληροφορίες, οι οποίες αφορούν ένα πρόσωπο ταυτοποιημένο ή ταυτοποιήσιμο, το οποίο ονομάζεται μάλιστα, υποκείμενο των δεδομένων. Αυτές οι πληροφορίες είναι εξατομικευμένες, ξεχωριστές και διαφορετικές για κάθε άτομο. Πρόκειται για πληροφορίες που αφορούν το ονοματεπώνυμο, τη διεύθυνση, τα στοιχεία επικοινωνίας, τον αριθμό δελτίου ταυτότητας (Α.Δ.Τ.) ή διαβατηρίου, το εισόδημα, το ιατρικό ιστορικό, τον κωδικό πρωτοκόλλου διαδικτύου (IP) και το πολιτιστικό προφίλ.<sup>1</sup>

Καθεμία από τις παραπάνω πληροφορίες αποτελεί χαρακτηριστικό του προσώπου, το οποίο περιγράφει και ξεχωρίζει από τα υπόλοιπα μέλη της κοινωνίας. Αυτά τα δεδομένα, είναι απαραίτητο να προστατεύονται από την πολιτεία, αλλά κι από άτομα ή οργανισμούς και φορείς, τα οποία τα συλλέγουν, τα αποθηκεύουν και έπειτα τα επεξεργάζονται για κάποιο συγκεκριμένο σκοπό και για ορισμένο χρονικό διάστημα. Τα παραπάνω δεδομένα, αποτελούν απλές εκφάνσεις της έννοιάς τους, ενώ υπάρχουν και τα καλούμενα ως «ευαίσθητα» προσωπικά δεδομένα, που αποτελούν τον πυρήνα του δικαιώματος του κάθε ατόμου.

Επιπλέον, είναι αξιοσημείωτο να αναφερθεί ότι η επεξεργασία των προσωπικών δεδομένων δεν επιτρέπεται, ειδικά στα ιδιαίτερα και ευαίσθητα στοιχεία

---

<sup>1</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm)

ή χαρακτηριστικά της ιδιωτικής ζωής του προσώπου, σχετικά με τα πολιτικά φρονήματα, τον σεξουαλικό προσανατολισμό, την καταγωγή, τις θρησκευτικές πεποιθήσεις, την συμμετοχή σε συνδικαλιστικές οργανώσεις, τα δεδομένα υγείας και τα στοιχεία εκείνα που αφορούν ποινικές καταδίκες ή αδικήματα τα οποία έχουν τελεστεί από τον πολίτη κάθε κράτους.<sup>2</sup>

Επιπρόσθετα, είναι σπουδαίο να αναφερθεί το γεγονός, ότι τα «απλά» προσωπικά δεδομένα, όπως αναφέρθηκαν παραπάνω, αφορούν όλη την διαδικασία της συλλογής, αλλά και της επεξεργασίας των προσωπικών δεδομένων, η οποία γίνεται με απλή προφορική συγκατάθεση του ατόμου και γνωστοποίηση στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΧΠΔ). Ωστόσο για τα «ευαίσθητα» προσωπικά δεδομένα απαγορεύεται η επεξεργασία τους εξ αρχής. Είναι βέβαια, πολύ σημαντική η εξαίρεση ως προς την γενική απαγόρευση, καθώς υπάρχει η δυνατότητα να ληφθεί σχετική άδεια από την αρμόδια Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΧΠΔ).<sup>3,4</sup>

Σύμφωνα με το νόμο, προκειμένου να υπάρξει άδεια από την ΑΠΧΠΔ, θα πρέπει να συντρέχουν συγκεκριμένοι λόγοι, οι οποίοι αναφέρονται ενδεικτικά στο άρ.7 του νόμου 2472/1997. Ως τέτοιος λόγος, αναφέρεται η ρητή και γραπτή συγκατάθεση του υποκειμένου των δεδομένων, η εθνική ασφάλεια, η προστασία της δημόσιας υγείας (άρ. 34 ν. 2915/2001), ή η τέλεση κάποιας έρευνας, στον τομέα της επιστήμης, με προγενέστερη επιπρόσθετη ενέργεια προληπτικού ελέγχου, αναφορικά με την τήρηση των προσωπικών δεδομένων (ν.2472/1997).

Προκειμένου να γίνει αντιληπτό ποια άτομα παρακολουθούν ή επεξεργάζονται τα προσωπικά δεδομένα, θα πρέπει να αναλυθεί ο τρόπος επεξεργασίας και να προσδιοριστούν τα άτομα, οι επιχειρήσεις και οι οργανισμοί, οι οποίοι τα συλλέγουν. Σε αυτό το πλαίσιο, μπορούμε να εντοπίσουμε δύο βασικά

---

<sup>2</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm).

<sup>3</sup>Αλεξανδροπούλου-Αιγυπτιάδου Ευγενία, « Προσωπικά δεδομένα: Η νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους», Εκδ. Αντ. Ν. Σάκκουλας, 2007

<sup>4</sup>Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015



προφίλ, τα οποία έχουν ως αρμοδιότητα την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

Αρχικά, πρόκειται για τον υπεύθυνο επεξεργασίας (ΥΠΔ) και τον εκτελούντα την επεξεργασία. Ο πρώτος είναι υπεύθυνος να αποφασίσει τον σκοπό, αλλά και τον τρόπο, με τον οποίο θα γίνει η επεξεργασία, ενώ ο δεύτερος είναι υπεύθυνος για την φύλαξη και την επεξεργασία τους για λογαριασμό του πρώτου. Ειδικότερα, ο υπεύθυνος προστασίας δεδομένων, έχει οριστεί από την εκάστοτε επιχείρηση, έτσι ώστε να είναι αρμόδιος για την παρακολούθηση, την επεξεργασία, αλλά και την ενημέρωση των υπολοίπων υπαλλήλων προκειμένου εκείνοι να τελέσουν τις υποχρεώσεις τους. Επιπλέον, συνεργάζεται με την ΑΠΔΠΧ και αποτελεί τον σύνδεσμο μεταξύ αυτής και των ατόμων.<sup>5</sup>

### **1.1.2 Η έννοια της ιδιωτικότητας**

Η ιδιωτικότητα ενός ατόμου νοείται ως το θεμελιώδες και αναφαίρετο ανθρώπινο δικαίωμα, με το οποίο το άτομο μπορεί να αποφασίζει για το είδος των πληροφοριών αλλά και το χρόνο κατά τον οποίο επιθυμεί να διαβιβαστούν πληροφορίες του και προσωπικά, ατομικά του στοιχεία σε τρίτους.<sup>6</sup>

Συνδέεται άρρηκτα με το δικαίωμα της προσωπικότητας, αλλά και το δικαίωμα του ιδιωτικού βίου, κατά το οποίο κάθε άτομο έχει δικαίωμα να δρα και να λειτουργεί στην προσωπική του ζωή με το δικό του τρόπο, δίχως να διαρρέουν πληροφορίες και προσωπικά του δεδομένα σε άλλους. Η προστασία της προσωπικότητας και του ιδιωτικού βίου είναι απαραίτητες σε μία δημοκρατική κοινωνία.

Οι εκφάνσεις της ποικίλουν, ανάλογα με το είδος του δικαιώματος. Ενδεικτικά αναφέρεται, το απόρρητο της επικοινωνίας, το ιατρικό απόρρητο, η προστασία της ιδιωτικής ζωής των εργαζομένων, αλλά και η ιδιωτικότητα κατά την πλοήγηση στο διαδίκτυο και στις ψηφιακές πλατφόρμες. Παράλληλα, είναι απαραίτητο να αναφερθεί το γεγονός ότι κάθε ιδιώτης έχει το δικαίωμα να αποτρέψει

---

<sup>5</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm).

<sup>6</sup> Longman Dictionary of Contemporary English, “Privacy-Definition”, Pearson, 2014

αδικαιολόγητες παρεμβάσεις, όπως για παράδειγμα τον σωματικό έλεγχο ή την διαρροή των προσωπικών του στοιχείων τα οποία παραβιάζουν την ιδιωτική του σφαίρα και τον εκθέτουν σε μεγάλο αριθμό ατόμων του δημοσίου βίου. Κάθε είδους καταπάτηση του απορρήτου της ιδιωτικής σφαίρας της ζωής ενός πολίτη τιμωρείται από το νόμο.<sup>7</sup>

Πρόκειται για συνταγματικά κατοχυρωμένο δικαίωμα και κάθε κράτος πρέπει να εισάγει νόμους οι οποίοι θα έχουν ως βάση την προστασία των πολιτών, την προάσπιση των δικαιωμάτων, τους αλλά και της σφαίρας της ιδιωτικότητας τους. Αυτή η μέριμνα αφορά το κράτος και τους πολίτες του, οι οποίοι θα πρέπει να είναι ενημερωμένοι και να μην επιτρέπουν οποιαδήποτε παραβίαση των προσωπικών τους δεδομένων και εν γένει των συνταγματικά κατοχυρωμένων δικαιωμάτων τους.

Επιπρόσθετα, η ιδιωτικότητα αναφέρεται και ως το δικαίωμα του ατόμου στην απομόνωση, την ελευθερία, την αυτονομία και τη λιγότερη δυνατή έκθεσή του στην δημόσια προσοχή.<sup>8</sup> Ιδιαίτερα στις Ηνωμένες Πολιτείες Αμερικής, οι έννοιες των προσωπικών δεδομένων και της ιδιωτικότητας θεωρούνται ταυτόσημες, ενώ αντίθετα στην ευρωπαϊκή ήπειρο, η έννοια των δεδομένων προσωπικού χαρακτήρα (personal data), χρησιμοποιείται περισσότερο.<sup>9</sup>

Παράλληλα, η έννοια της ιδιωτικότητας δεν αφορά μόνο τη σφαίρα του ιδιωτικού βίου και τις πληροφορίες που υπάρχουν για τον κάθε πολίτη ξεχωριστά και εξατομικευμένα στην κοινωνική ζωή, αλλά τοποθετήθηκε και στο πεδίο του κυβερνοχώρου, του διαδικτύου δηλαδή, όπου γίνεται λόγος για τη διαδικτυακή ιδιωτικότητα (internet privacy). Συγκεκριμένα, πρόκειται για εκατομμύρια δεδομένα χρηστών των ψηφιακών πλατφορμών, στις οποίες, μάλιστα, αποθηκεύονται, μετατρέπονται και διατίθενται σε τρίτους, μέσω διαδικτύου.<sup>10</sup>

---

<sup>7</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

<sup>8</sup> Longman Dictionary of Contemporary English, “Privacy-Definition”, Pearson, 2014

<sup>9</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

<sup>10</sup> Clarke Roger, “Information privacy on the Internet”, 1998

Επιπλέον, γίνεται λόγος για την καλούμενη «ιδιωτικότητα των πληροφοριών» (information privacy). Αυτό σημαίνει ότι τα άτομα, τα οποία χρησιμοποιούν το διαδίκτυο, επιθυμούν οι πληροφορίες και τα προσωπικά τους στοιχεία να μην διατίθενται σε τρίτους, δίχως την άδεια και την συγκατάθεσή τους. Έτσι, κατά την πλοήγηση στο διαδίκτυο, οι χρήστες αφήνουν τα διαδικτυακά τους αποτυπώματα στις ψηφιακές πλατφόρμες, καταχωρούν τα προσωπικά του στοιχεία, απαντούν σε ερωτήματα, συμπληρώνουν τα στοιχεία τους σε ηλεκτρονικές αιτήσεις και αλληλεπιδρούν με άλλους χρήστες στις ψηφιακές πλατφόρμες, οι οποίες, στη συνέχεια, γίνονται αντικείμενο επεξεργασίας από τρίτους, που δύνανται να διαχειριστούν κακόβουλα τα δεδομένα που έχουν λάβει από το εκάστοτε λογισμικό και να βλάψουν τους χρήστες των διαδικτυακών τόπων. Η δυνατότητα αυτή, να ασκούν τρίτοι μεγάλο έλεγχο στα προσωπικά δεδομένα άλλων, τους δίνει μεγάλη εξουσία στην διαχείριση των πληροφοριών που αντλούνται από τις ψηφιακές πλατφόρμες.<sup>11</sup>

Επιπλέον, είναι πολύ σημαντικό να τονιστεί το γεγονός ότι η ιδιωτικότητα αφορά και την ιδιωτική σφαίρα του καταναλωτή, εν γένει (consumer privacy). Ο καταναλωτής επιδιώκει την διεκπεραίωση χρηματικών συναλλαγών μέσω της ψηφιακής πλατφόρμας e-banking ή ακόμη, την χρήση άλλων ιστοσελίδων προκειμένου να πραγματοποιήσει κάποια εμπορική συναλλαγή με κάποια εμπορικό κατάστημα και καταχωρεί προσωπικά του στοιχεία στον κυβερνοχώρο.<sup>12</sup> Ωστόσο, απαγορεύεται με κάθε τρόπο η μη εξουσιοδοτημένη συλλογή των πληροφοριών, αλλά και η χρήση τους από τρίτους.<sup>13</sup>

Βέβαια, αυτή η καταχώρηση των προσωπικών πληροφοριών κατά τις εμπορικές συναλλαγές, μπορεί να συμβεί και δίχως τη χρήση του διαδικτύου ή των ηλεκτρονικών καταστημάτων αλλά και σε διάφορες άλλες άμεσες συναλλαγές της καθημερινή ζωής.

---

<sup>11</sup> Clarke Roger, "Information privacy on the Internet", 1998

<sup>12</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

<sup>13</sup> Wang H., M.K.O. Lee, and C. Wang, "Consumer Privacy Concerns about Internet Marketing", 1998

### 1.1.3 Η επεξεργασία των δεδομένων και η έννοια της συγκατάθεσης

Η Ευρωπαϊκή Ένωση έχει θεσπίσει κανόνες αναφορικά με την προστασία των προσωπικών δεδομένων και την επεξεργασία τους. Η επεξεργασία θα πρέπει να γίνει με τρόπο θεμιτό, αλλά και σύννομο, για έναν ορισμένο και νόμιμο σκοπό και να καλύπτει μόνο τα στοιχεία εκείνα τα οποία είναι απαραίτητα και αναγκαία προκειμένου να επιτευχθεί ο σκοπός αυτός.<sup>14</sup>

Σε περίπτωση που κάποιο άτομο επιδιώκει να επεξεργαστεί προσωπικά δεδομένα θα πρέπει πρώτα να διασφαλίσει εάν πληρούνται ορισμένοι όροι και κριτήρια. Αρχικά, δεν είναι αναγκαίο να πληρούνται όλοι οι όροι, αλλά αρκεί να πληρούται έστω και ένας από αυτούς. Τέτοιος όρος είναι, για παράδειγμα, η συγκατάθεση του υποκειμένου των προσωπικών δεδομένων, δηλαδή, η έμπρακτη και ρητή συναίνεση του ατόμου. Ένας άλλος όρος σχετικά με την επεξεργασία, είναι να χρειάζεται τα δεδομένα αυτός που τα επεξεργάζεται, προκειμένου να εκπληρώσει κάποια νομική υποχρέωση ή για να προστατεύσει ζωτικά συμφέροντα του υποκειμένου. Ένας επιπλέον όρος, είναι η διεκπεραίωση δημοσίου συμφέροντος ή η ενέργεια προς όφελος των νόμιμων συμφερόντων της επιχείρησης του επεξεργάζοντος (DPO) τα προσωπικά δεδομένα τρίτου. Σε περίπτωση ωστόσο, που τα δικαιώματα του υποκειμένου υπερσχύουν των συμφερόντων της εταιρείας, δεν υπάρχει δυνατότητα επεξεργασίας των προσωπικών του δεδομένων. Εάν λοιπόν, υπάρχει έστω και ένας από τους παραπάνω όρους, δίνεται η δυνατότητα στο άτομο που χρειάζεται να επεξεργαστεί τα προσωπικά δεδομένα τρίτων, να το πράξει.<sup>15</sup>

Επιπρόσθετα, έχει πολύ μεγάλη σημασία να υπάρχει η δυνατότητα της παροχής διάφανων πληροφοριών. Πιο συγκεκριμένα, το άτομο, το οποίο επεξεργάζεται τα προσωπικά δεδομένα να παρέχει στα υποκείμενά τους, σαφείς πληροφορίες, αναφορικά με το πρόσωπο που τα επεξεργάζεται, αλλά και τον λόγο που αυτό προχωρά σε αυτού του είδους την επεξεργασία. Θα πρέπει δηλαδή, να παρέχονται συγκεκριμένες πληροφορίες στο υποκείμενο.

---

<sup>14</sup> [https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm)

<sup>15</sup> [https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm)

Αυτές οι πληροφορίες, αφορούν το πρόσωπο που επεξεργάζεται τα δεδομένα, την αιτία αυτής της επεξεργασίας, τη νομική βάση της και το άτομο που πρόκειται να λάβει τα δεδομένα, εάν αυτό υπάρχει. Υπάρχει επίσης δυνατότητα, σε συγκεκριμένες περιπτώσεις, να δίνονται περαιτέρω πληροφορίες, όπως για παράδειγμα, τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων (ΥΠΔ), το χρονικό διάστημα της αποθήκευσης των δεδομένων, τα μέτρα που ισχύουν, το νόμιμο συμφέρον της επιχείρησης, τα δικαιώματα του υποκειμένου περί διόρθωσης, περιορισμού διαγραφής, απαγόρευσης χρήσης, της δυνατότητα απορρόφησης, της συγκατάθεσης, αλλά και τις επιπτώσεις από την συγκεκριμένη συγκατάθεση. Θα πρέπει αυτές οι πληροφορίες να δίνονται σε σαφή και κατανοητή γλώσσα στο άτομο στο οποίο απευθύνονται.<sup>16</sup>

Αναφορικά με την συγκατάθεση του υποκειμένου για την προστασία των προσωπικών του δεδομένων και την επεξεργασία τους, ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) έχει ορίσει αυστηρούς κανόνες για αυτή τη διαδικασία. Στόχος αυτού του Κανονισμού είναι να διασφαλιστεί ότι το άτομο που παρέχει την συγκατάθεσή του έχει πλήρη γνώση και κατανόηση για τον σκοπό της συναίνεσής του. Η συγκατάθεση είναι απαραίτητο να δίνεται με καταφατική πράξη, όπως για παράδειγμα, την επιλογή πλήκτρου στην ιστοσελίδα ή την υπογραφή της δήλωσης, ενώ παράλληλα, είναι απαραίτητο η συναίνεση αυτή να δίνεται με σαφήνεια και ορισμένο τρόπο, με ελευθερία στην βούληση και με δήλωση απλή στην διατύπωση και γλώσσα κατανοητή. Σε περίπτωση που δοθεί συγκατάθεση από το υποκείμενο των δεδομένων για την επεξεργασία του, το άτομο που πρόκειται να επεξεργαστεί τα δεδομένα, δικαιούται να προχωρήσει στην επεξεργασία, μόνο για εκείνους τους σκοπούς, για τους οποίους δόθηκε η συναίνεση. Επιπλέον, θα πρέπει να υπάρχει δυνατότητα να αποσυρθεί η συγκατάθεση από το υποκείμενο σε περίπτωση που αλλάξει γνώμη και μάλιστα, αυτό θα πρέπει να το γνωρίζει εκ των προτέρων.<sup>17</sup>

---

<sup>16</sup> [https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm)

<sup>17</sup> [https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm)

## 1.2 Τα προσωπικά δεδομένα στις ψηφιακές πλατφόρμες

### 1.2.1 Τα προσωπικά δεδομένα στα μέσα κοινωνικής δικτύωσης

Αποτελεί γεγονός της σύγχρονης πραγματικότητας η ολοένα και αυξανόμενη χρήση του διαδικτύου και των ψηφιακών πλατφορμών από εκατομμύρια χρήστες παγκοσμίως. Η χρήση αυτή του κυβερνοχώρου έχει επεκταθεί και σε πλατφόρμες επικοινωνίας, όπου οι χρήστες μπορούν σε αυτό το διαδικτυακό τόπο να έρθουν σε επικοινωνία με όποιο άτομο επιθυμούν ανά τον κόσμο, άμεσα, σε λιγιστό χρόνο και χωρίς κανένα χρηματικό κόστος.

Τέτοιες δυνατότητες επικοινωνίας παρέχονται στους χρήστες μέσω των ιστοσελίδων κοινωνικής δικτύωσης, όπως είναι το Facebook, το Instagram, το LinkedIn και το Twitter. Ήδη από το 2003 ξεκίνησε η εμφάνιση μίας προσωπικής σελίδας με την ονομασία “MySpace”, η οποία αποτέλεσε ένα ιδιαίτερο και δημοφιλές εργαλείο στα χέρια χιλιάδων χρηστών του διαδικτύου, οι οποίοι δημοσίευαν κατά την βούλησή τους το περιεχόμενο που εκείνοι επιθυμούσαν.<sup>18, 19</sup>

Έπειτα, εμφανίστηκε το Facebook, το 2004 και άρχισε να χρησιμοποιείται από πλήθος ανθρώπων παγκοσμίως.<sup>20</sup> Κατά τα τελευταία χρόνια μάλιστα, άρχισε να επεκτείνεται η χρήση των λεγομένων “social media” σε πολύ μεγάλα ποσοστά.<sup>21, 22</sup>

Από αυτή την εκτεταμένη χρήση, ωστόσο, προκύπτουν ζητήματα ιδιωτικότητας και παραβίασης των προσωπικών δεδομένων των χρηστών με την έκθεση εκατομμυρίων ευαίσθητων δεδομένων τους. Δεν είναι λίγες οι περιπτώσεις

---

<sup>18</sup> Boyd M. and N.B. Ellison, “Social network Sites: Definition, History and Scholarship”, Journal of Computer-Mediated Communication, 2007

<sup>19</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

<sup>20</sup> Kirkpatrick D., “The Facebook effect: The inside story of the company that is connecting the world, Simon and Schuster/ Virgin Books, New York, 2010

<sup>21</sup> Yeager J.B. and R.K Sisson, “USER BEWARE: Maximizing the Possibilities, Minimizing the Risks of using Social Media, 33-OCT, Pa. Law.26., 2011

<sup>22</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

άλλωστε, κατά τις οποίες οι χρήστες έχουν βρεθεί εκτεθειμένοι, βέβαια στα προσωπικά τους δεδομένα να έχουν διαρρεύσει και να έχουν προσφύγει στα δικαστήρια προκειμένου να επιλύσουν την μεταξύ τους διαφορά. Είναι δυνατόν δηλαδή, να εκτεθούν τα ευαίσθητα προσωπικά δεδομένα των χρηστών ανά πάσα στιγμή και με εύκολο σχετικά τρόπο.

Είναι αξιοσημείωτο να αναφερθεί, ότι σε σχετική έρευνα η οποία διεξήχθη σε μεγάλο αριθμό χρηστών παρατηρήθηκε το φαινόμενο ότι υπήρχε η δυνατότητα άντλησης ευαίσθητων προσωπικών δεδομένων, μέσω των προτιμήσεων των χρηστών στην πλατφόρμα του Facebook και πιο συγκεκριμένα μέσα από την δήλωση της προτίμησής τους, από τα λεγόμενα “Facebook Likes”.<sup>23</sup> Δεδομένα, όπως για παράδειγμα, το θρήσκευμα, η οικογενειακή κατάσταση, η καταγωγή, το φύλο.<sup>24</sup>

Γίνεται λοιπόν αντιληπτό, ότι με τη χρήση του διαδικτύου και συγκεκριμένα με τα μέσα κοινωνικής δικτύωσης (social media), διευκολύνεται η επικοινωνία με χιλιάδες άτομα, ωστόσο καταγράφονται προσωπικά στοιχεία, αλλά και συνομιλίες των ατόμων μεταξύ τους μέσα στις ψηφιακές πλατφόρμες. Κάθε προσωπικό στοιχείο θα πρέπει να είναι προστατευμένο, ωστόσο, δεν είναι λίγες οι φορές όπου έχουν παραβιαστεί τα προσωπικά δεδομένα των χρηστών και έχουν διαρρεύσει δίχως την συναίνεση των υποκειμένων.

### **1.2.2 Ηλεκτρονικές εμπορικές συναλλαγές και δεδομένα των πλατφορμών**

Στις ψηφιακές πλατφόρμες δραστηριοποιούνται επιχειρήσεις, οι οποίες κινούνται διαδικτυακά και έχουν ως σκοπό την πραγματοποίηση εμπορικών συναλλαγών με τους καταναλωτές, έτσι ώστε να αυξήσουν το κέρδος και να πωλήσουν τα προϊόντα ή τις υπηρεσίες τους. Κατά την διαδικασία αυτή, βέβαια, συλλέγουν και επεξεργάζονται έναν πολύ μεγάλο αριθμό δεδομένων και πληροφοριών. Ο στόχος αυτής της συλλογής είναι η βελτιστοποίηση και η τελειοποίηση της εμπειρίας των χρηστών στη σελίδα, αλλά και η ικανοποίηση των

---

<sup>23</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

<sup>24</sup> Kosinski et al., “Private traits and attributes are predictable from digital networks of human behavior”, 5802-5805 PNAS, 2013

διαφημιστών, οι οποίοι την χρηματοδοτούν. Η πρόσβαση στην ιδιωτικότητα των χρηστών και η καταχώρηση των προσωπικών τους δεδομένων στις ψηφιακές πλατφόρμες, γίνεται συνήθως με τη μορφή ενός διαδικτυακού εργαλείου, το οποίο ονομάζεται “cookies”, έτσι ώστε να καταφέρουν οι χρήστες να αποκτήσουν πρόσβαση σε μία ηλεκτρονική- ιντερνετική υπηρεσία.<sup>25</sup>

Όπως προαναφέρθηκε, βέβαια, τίθεται το ζήτημα της σύγκρουσης των δικαιωμάτων της ελευθερίας της έκφρασης από τη μία πλευρά και των δικαιωμάτων του χρήστη από την άλλη πλευρά. Η στάθμιση αυτή, θα πρέπει να γίνεται, λαμβανομένου υπ’ όψιν του γεγονότος ότι σε περίπτωση που υπερισχύουν τα δικαιώματα του καταναλωτή δεν υπάρχει δυνατότητα από την ηλεκτρονική επιχείρηση να εισβάλει σε αυτά, δίχως τη συγκατάθεσή του. Οφείλει μάλιστα, να σεβαστεί την ιδιωτική του σφαίρα και το δικαίωμά τους στην προσωπικότητα.

Το πιο ορθό θα ήταν σε αυτή την περίπτωση, να υπάρχει μία δυνατότητα ρύθμισης μέσω προληπτικής παρέμβασης, πράγμα που σημαίνει ότι θα μπορεί να ενθαρρύνεται η καινοτομία και η δημιουργικότητα των εταιρειών, δίχως να βλάπτουν τα συμφέροντά τους, αλλά παράλληλα, θα προωθείται η προστασία των προσωπικών δεδομένων των χρηστών.<sup>26</sup>

Σε πολλές περιπτώσεις, οι καταναλωτές, οι οποίοι επικοινωνούν με τις επιχειρήσεις προκειμένου να αγοράσουν ένα προϊόν ή να τους παρασχεθεί κάποια υπηρεσία από αυτές, δίνουν πολύ μεγάλη έμφαση στον τρόπο με τον οποίο θα μπορούσαν, ίσως, οι ίδιοι να ελέγχουν άμεσα τα δεδομένα τους, αλλά και στο γεγονός ότι θα επιθυμούσαν να έχουν γνώση περί της επακριβούς χρήσης αυτών.<sup>27</sup> Ο μόνος τρόπος με τον οποίο οι καταναλωτές προσπαθούν να ελέγχουν την διαχείριση των προσωπικών τους δεδομένων είναι μέσω της επιλογής των επιχειρήσεων ή των οργανισμών που επιλέγουν να εμπιστευθούν.<sup>28</sup>

---

<sup>25</sup> Χατζόπουλος Β., Η οικονομία των πλατφορμών (“platform economy”) και η εσωτερική αγορά της ΕΕ, ΕυΔικ 4/2019

<sup>26</sup> Τάσσης Σ., ΔΕΕ – δύο θεμελιώδεις αποφάσεις για τα προσωπικά μας δεδομένα και τα ηλεκτρονικά δίκτυα: Απόφαση C-131/12 (Google) και συνεκδικαζόμενες C-293/12 και C-594/12 (νομιμότητα υποχρεωτικής διατήρησης τηλεπικοινωνιακών δεδομένων), ΔΙΜΕΕ 1/2014

<sup>27</sup> Malhotra N. K., Kim S. S., and Agarwal J., “Internet users’ information privacy concerns (IUIPC): The construct, the scale and a casual model”, Information Systems Research, 2004, p.336-355

<sup>28</sup> Tsai et al., “The Effect of Online Private Information on Purchasing Behavior”, Information Systems Research 22, 2011, p. 254-268



### 1.2.3 Καταπάτηση δικαιωμάτων χρηστών στο διαδίκτυο

Ένα ιδιαίτερα σημαντικό ζήτημα που αντιμετωπίζουν οι χρήστες του διαδικτύου και ιδιαίτερα, όσοι εμπιστεύονται ατομικά τους στοιχεία, προκειμένου να πραγματοποιήσουν κάποιου είδους εμπορική χρηματική συναλλαγή με επιχειρήσεις, είναι η ανησυχία σχετικά με το πόσο εύκολα μπορούν να παραβιαστούν τα προσωπικά τους δεδομένα, αλλά και τις συνέπειες που μπορεί να έχει για εκείνους, η παραβίαση αυτή.

Οι συνέπειες της παραβίασης, θα μπορούσαν να διαχωριστούν σε διαφορετικά επίπεδα, με βάση την αξία και την σπουδαιότητά της. Η βλάβη, δηλαδή, που προκαλείται σε εκείνους, από τρίτους, οι οποίοι χρησιμοποιούν κακόβουλα τις πληροφορίες που λαμβάνουν από το λογισμικό των ψηφιακών πλατφορμών, μπορεί να διαφέρει και να κατηγοριοποιηθεί σε επιμέρους επίπεδα.

Εάν πρόκειται για βλάβη, η οποία είναι μικρής σχετικά αξίας, θα μπορούσε να τοποθετηθεί στο χαμηλότερο επίπεδο παραβίασης. Τέτοιο παράδειγμα αποτελεί η αλλαγή των κωδικών των στοιχείων της τραπεζικής κάρτας στο e-banking, ή των κωδικών των μέσων κοινωνικής δικτύωσης (social media/ networks), προκειμένου να επιτευχθεί η διασφάλιση του περιεχομένου τους.<sup>29</sup>

Εάν η βλάβη είναι μεγαλύτερης βαρύτητας, τότε γίνεται λόγος για το επόμενο επίπεδο, κατά το οποίο οι ανεπιθύμητες συνέπειες αφορούν την απώλεια οικονομικών στοιχείων της περιουσίας του ατόμου, ή σε ακόμη χειρότερη περίπτωση, γίνεται λόγος για το ακόμα υψηλότερο επίπεδο βλάβης, με αποτέλεσμα την απώλεια της ζωής του ατόμου ή την πρόκληση κάποιας βαριάς μορφής σωματικής βλάβης.<sup>30</sup>

Σε κάθε περίπτωση, γίνεται αντιληπτό, ότι οι συνέπειες από μία τέτοια παραβίαση, πέραν του γεγονότος ότι δεν αποτελούν μία πράξη ηθικής, είναι και κάτι, που τιμωρείται από το νόμο και για το οποίο, έχουν θεσπιστεί κανονισμοί τόσο σε εθνικό, όσο και υπερεθνικό επίπεδο, προκειμένου να αντιμετωπιστούν ζητήματα και

---

<sup>29</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

<sup>30</sup> NIST, National Institute of Standards and Technology Special Publication, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)- Recommendations of the National Institute of Standards and Technology”, 2010

ανησυχίες, αναφορικά με την ιδιωτικότητα των ατόμων, τόσο όταν δραστηριοποιούνται στο διαδίκτυο, όσο και εκτός του κυβερνοχώρου, έτσι ώστε να αποφευχθεί οποιαδήποτε παραβίαση και διαρροή προσωπικών δεδομένων σε τρίτους δίχως την συναίνεση των υποκειμένων τους.

### **1.3 Δικαιώματα των υποκειμένων των προσωπικών δεδομένων**

Όπως προαναφέρθηκε, όταν πρόκειται για συλλογή και επεξεργασία προσωπικών δεδομένων, υπάρχουν ειδικοί κανόνες, οι οποίοι βασίζονται στα θεμελιώδη και συνταγματικώς κατοχυρωμένα δικαιώματα των ατόμων- υποκειμένων των προσωπικών δεδομένων.

Φυσικά, θα πρέπει να υπάρχει ρητή συγκατάθεση, σχετικά με τη χρήση και τη διαβίβασή τους σε τρίτους. Το ίδιο βέβαια, θα πρέπει να ισχύει και για την συλλογή και αποθήκευση προσωπικών δεδομένων των ανήλικων, όπου ο εκτελών την επεξεργασία, οφείλει να λάβει τη συγκατάθεση από τον γονέα ή κηδεμόνα του ανήλικου. Αυτό συμβαίνει, προκειμένου να προστατευθεί το ανήλικο τέκνο από οποιαδήποτε παραβίαση των προσωπικών του δεδομένων και κατ' επέκταση για την εν γένει προστασία του, ως ατόμου.

Έχουν θεσπιστεί ορισμένοι κανόνες, τόσο σε εθνικό, όσο και σε υπερεθνικό επίπεδο, οι οποίοι έχουν ως βάση τους, αυτή την ανάγκη προστασίας των ατόμων της κοινωνίας. Οι συγκεκριμένοι νόμοι, στηρίζονται στα δικαιώματα των ατόμων, αναφορικά με την προσωπικότητα, την ιδιωτικότητα και την αξιοπρέπειά τους. Η πολιτεία οφείλει να προστατεύει και να σέβεται όλα τα δικαιώματα των μελών της.

Αναφορικά λοιπόν, με τα δικαιώματα που προκύπτουν, ως προς την επεξεργασία των προσωπικών δεδομένων, θα μπορούσαμε να σημειώσουμε τις παρακάτω κατηγορίες δικαιωμάτων<sup>31</sup>: α) Αρχικά, το δικαίωμα πρόσβασης και φορητότητας των δεδομένων.

β) Έπειτα, το δικαίωμα διορθώσεως και προβολής αντιρρήσεων του υποκειμένου.

---

<sup>31</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm)

γ) Μία επόμενη κατηγορία, είναι το δικαίωμα της διαγραφής ή διαφορετικά, το αποκαλούμενο και ως δικαίωμα στη «λήθη».

δ) Επιπρόσθετα, σε άλλη κατηγορία εντάσσεται το δικαίωμα του υποκειμένου, να μην υπόκειται σε οποιαδήποτε απόφαση που βασίζεται σε αυτοματοποιημένη λήψη αποφάσεων επεξεργασίας των προσωπικών του στοιχείων.

Όλα αυτά τα δικαιώματα αποτελούν τη βάση, πάνω στην οποία στηρίχθηκαν οι κανονισμοί, ενώ παράλληλα, η διαφύλαξή τους αποτελεί προτεραιότητα της πολιτείας, όπως ήδη έχει τονιστεί.<sup>32</sup>

### 1.3.1 Το δικαίωμα της πρόσβασης του υποκειμένου

Το δικαίωμα του υποκειμένου στην πρόσβαση των προσωπικών του δεδομένων είναι θεμελιώδες. Κάθε επιχείρηση ή οργανισμός οφείλει να διασφαλίζει ότι κάθε υποκείμενο μπορεί να έχει γνώση και ενημέρωση, αναφορικά με τα προσωπικά του στοιχεία, δωρεάν και άμεσα. Το υποκείμενο υποβάλλει σχετικό αίτημα στην επιχείρηση ή τον οργανισμό, αναφορικά με την επιθυμία του να έχει πρόσβαση στα προσωπικά του δεδομένα.

Σε αυτή την περίπτωση, το άτομο που συλλέγει τα προσωπικά δεδομένα οφείλει να ενημερώσει το υποκείμενο, σχετικά με το εάν υπάρχει επεξεργασία των δεδομένων του ή όχι και να του δώσει περαιτέρω πληροφορίες. Εάν υποθεθεί ότι υπάρχει, πράγματι, επεξεργασία, η επιχείρηση θα πρέπει να πληροφορήσει το πρόσωπο, σχετικά με τον σκοπό ή τις κατηγορίες των προσωπικών δεδομένων, αλλά και να του παράσχει άμεσα, αντίγραφο των δεδομένων που υπόκειται σε επεξεργασία σε προσβάσιμο μορφότυπο.<sup>33</sup>

Αυτό το δικαίωμα δίνει τη δυνατότητα στο υποκείμενο να έχει πλήρη γνώση και έλεγχο στα προσωπικά του δεδομένα, να αισθάνεται ασφάλεια και να αποτρέπει με οποιοδήποτε τρόπο τις ανεπιθύμητες ενέργειες τρίτων στα ατομικά του στοιχεία.

---

<sup>32</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm).

<sup>33</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm).

### 1.3.2 Το δικαίωμα φορητότητας

Το δικαίωμα στη φορητότητα των δεδομένων αποτελεί επίσης, σημαντικό θεμέλιο, με το οποίο πραγματοποιείται ο έλεγχος του υποκειμένου στα προσωπικά του δεδομένα.

Έτσι, όταν τα δεδομένα υπόκεινται σε επεξεργασία και εκείνη βασίζεται είτε σε σύμβαση, είτε σε συγκατάθεση του υποκειμένου, το τελευταίο, έχει τη δυνατότητα να αιτηθεί την επιστροφή των προσωπικών του δεδομένων ή τη διαβίβασή τους σε κάποια άλλη επιχείρηση. Η επιχείρηση ή ο οργανισμός, οφείλει να διαβιβάσει τα προσωπικά δεδομένα, σύμφωνα με την επιθυμία του υποκειμένου και να ενεργήσει με βάση την βούλησή του και όχι αντίθετα από αυτήν. Τα δεδομένα αυτά, θα πρέπει να παρέχονται σε έναν μηχαναγνώσιμο μορφότυπο, οποίος μάλιστα, χρησιμοποιείται ευρέως.<sup>34</sup>

Κατανοούμε λοιπόν, ότι το συγκεκριμένο δικαίωμα διευκολύνει το υποκείμενο των δεδομένων τόσο, ως προς το να ελέγχει, όσο και ως προς το να έχει πρόσβαση στα ατομικά του στοιχεία, αλλά και να αιτείται τη μεταφορά τους σε οποιοδήποτε άλλο οργανισμό ή επιχείρηση.

### 1.3.3 Το δικαίωμα διόρθωσης και το δικαίωμα προβολής αντιρρήσεων

Το δικαίωμα στη διόρθωση των προσωπικών δεδομένων του υποκειμένου, λειτουργεί ιδιαίτερα επιβοηθητικά, τόσο ως προς το ίδιο το άτομο, όσο και ως προς την επιχείρηση, η οποία οφείλει να διορθώνει και να μεταβάλει τα στοιχεία των υποκειμένων, σε περίπτωση που εκείνα είναι εσφαλμένα, παρουσιάζουν ελλείψεις, ή ανακρίβειες.

Το δικαίωμα αυτό, συνίσταται στην αίτηση διορθώσεως ή συμπληρώσεως των προσωπικών δεδομένων, η οποία υποβάλλεται από το υποκείμενό του, χωρίς ωστόσο, να υπάρχουν καθυστερήσεις κατά τη διαδικασία, από τους αρμόδιους στην εκάστοτε επιχείρηση. Αντίθετα, η τελευταία, οφείλει να προβεί σε ενημέρωση όλων

---

<sup>34</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm)

των παραληπτών των προσωπικών δεδομένων, αλλά και σε κοινοποίηση του γεγονότος ότι έχουν υπάρξει μεταβολές ή διαγραφές στα προγενέστερα προσωπικά δεδομένα του ατόμου. Επιπλέον, σε περίπτωση που υπήρξε εσφαλμένη διαβίβαση προσωπικών δεδομένων, η εταιρεία οφείλει να ενημερώσει σχετικά με τις διενεργηθείσες μεταβολές, οποιονδήποτε τα έλαβε ή τα είδε, χωρίς ωστόσο, αυτό να προϋποθέτει μεγάλες και δυσανάλογες προσπάθειες ή βάρος για την επιχείρηση ή τον οργανισμό.<sup>35</sup>

Επιπρόσθετα, το υποκείμενο έχει το δικαίωμα να αντιταχθεί, οποιαδήποτε στιγμή επιθυμεί, στην επεξεργασία των δεδομένων του. Πρόκειται για το δικαίωμα προβολής αντιρρήσεων, κατά το οποίο, το άτομο εφόσον διαφωνεί με την επεξεργασία των δεδομένων του, η επιχείρηση οφείλει να διακόψει την επεξεργασία, εκτός εάν έχει νόμιμο συμφέρον, το οποίο υπερισχύει, συγκριτικά με τα συμφέροντα του υποκειμένου.

Βέβαια, το ίδιο το υποκείμενο μπορεί να ζητήσει να σταματήσει ή να περιοριστεί η επεξεργασία των δεδομένων του, εφόσον τα δικά του συμφέροντα υπερισχύουν εκείνων της επιχείρησης. Σε περίπτωση όμως, άμεσης εμπορικής προώθησης, η επιχείρηση οφείλει να διακόψει την επεξεργασία, εφόσον υπάρχει αίτηση από το υποκείμενο.<sup>36</sup>

Με τα δύο δικαιώματα αυτά, δίνεται η δυνατότητα στο υποκείμενο να ελέγχει την επεξεργασία των δεδομένων του, να παρεμβαίνει σε περίπτωση διόρθωσης των στοιχείων του αιτούμενος την αλλαγή τους, αλλά και να προβάλει αντιρρήσεις, όποτε θεωρεί ότι είναι απαραίτητο.

### **1.3.4 Το δικαίωμα διαγραφής- δικαίωμα στη «λήθη»**

Υπάρχουν αρκετές περιπτώσεις, κατά τις οποίες, το υποκείμενο επιθυμεί τη διαγραφή των προσωπικών του δεδομένων, από τα αρχεία της επιχείρησης, είτε πρόκειται για ψηφιακές πλατφόρμες, είτε για έντυπα αρχεία. Το συγκεκριμένο δικαίωμα διαγραφής, ονομάζεται και δικαίωμα στη «λήθη» (right to be forgotten).

---

<sup>35</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm).

<sup>36</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm)

Πολλές φορές, λοιπόν, τα υποκείμενα ζητούν από τον υπεύθυνο επεξεργασίας, να τα διαγράψει, εφόσον έχουν επιτελέσει τον σκοπό τους και δεν υπάρχει άλλος λόγος παραμονής, συλλογής και αποθήκευσής τους από την εκάστοτε επιχείρηση. Αυτή η δυνατότητα, παρέχεται εκ του νόμου στο υποκείμενο, προκειμένου να μπορεί να ασκεί πλήρη έλεγχο στις πληροφορίες που αφορούν το ίδιο, είτε αυτά διακινούνται στο διαδίκτυο, είτε επεξεργάζονται από την επιχείρηση.<sup>37</sup>

Ωστόσο, η επιχείρηση μπορεί να μην το πράξει, εφόσον συντρέχουν οι εξής προϋποθέσεις:

α) Αρχικά, εάν η επεξεργασία αποτελεί προϋπόθεση για την τήρηση της ελευθερίας της έκφρασης ή της πληροφόρησης, θα πρέπει τα στοιχεία να παραμείνουν αποθηκευμένα, παρά την αίτηση διαγραφής από το υποκείμενο.

β) Ακόμη, εάν υπάρχει υποχρέωση συμμόρφωσης με κάποια συγκεκριμένη νομική υποχρέωση, η επιχείρηση οφείλει να αποθηκεύσει αυτά τα προσωπικά δεδομένα.

γ) Ένας άλλος λόγος, που η επιχείρηση δεν υποχρεούται να πράξει κάτι τέτοιο, αποτελεί η αποθήκευση των προσωπικών δεδομένων, προκειμένου να εγερθεί μετέπειτα κάποια νομική αξίωση

δ) ή τέλος, εάν υπάρχουν λόγοι δημοσίου συμφέροντος, που υπαγορεύουν την αποθήκευση ή την συλλογή τους.<sup>38</sup>

Αξίζει να σημειωθεί, ότι το δικαίωμα στη «λήθη» αποτελεί έκφανση του δικαιώματος στην ιδιωτική ζωή, ωστόσο, είναι ιδιαίτερα δύσκολο, μία πληροφορία να διαγραφεί ολοσχερώς από τον κυβερνοχώρο, καθώς κατά πάσα πιθανότητα, η πληροφορία αυτή, διακινείται από τρίτους, χωρίς να υπάρχει δυνατότητα να σταματήσει η κυκλοφορία της.

---

<sup>37</sup> Ξανθούλης Ν., «Το δικαίωμα στη λήθη υπό το φως των ανθρωπίνων δικαιωμάτων», ΔΙΜΕΕ 2/2013, σελ. 178

<sup>38</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm).

### **1.3.5 Το δικαίωμα του υποκειμένου αναφορικά με την αυτοματοποιημένη λήψη αποφάσεων**

Τέλος, το υποκείμενο έχει το δικαίωμα να μη δεχθεί να υπόκειται σε απόφαση, η οποία εδράζεται σε αυτοματοποιημένη επεξεργασία. Λαμβάνοντας βέβαια, υπ' όψιν την εξαίρεση, κατά την οποία το άτομο έχει δώσει τη ρητή του συγκατάθεση γι' αυτού του είδους την επεξεργασία, η επιχείρηση οφείλει να δίνει τη δυνατότητα στο υποκείμενο να ενημερώνεται, αναφορικά με αυτή την αυτοματοποιημένη λήψη, να μπορεί να την εξετάζει, αλλά και να την αμφισβητεί. Δηλαδή το άτομο, σε περίπτωση που διαφωνεί με την αυτοματοποιημένη απόφαση μπορεί να την αμφισβητήσει και να ζητήσει ανθρώπινη παρέμβαση.<sup>39</sup>

Με βάση όλα όσα αναφέρθηκαν, κατανοούμε ότι τα δικαιώματα των υποκειμένων προσωπικών δεδομένων, σχετίζονται με το δικαίωμα στην προσωπικότητα, την ιδιωτικότητα και την προστασία της αξιοπρέπειάς τους. Η προστασία τους από την πολιτεία καθίσταται αδήριτης και πρωταρχικής σημασίας, καθότι ο ίδιος ο νόμος δίνει το περιθώριο και τη δυνατότητα σε κάθε πολίτη να ελέγχει, να ενημερώνεται, να αμφισβητεί και να έχει πρόσβαση σε κάθε πληροφορία και στοιχείο που τον αφορά.

---

<sup>39</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm).

## ΚΕΦΑΛΑΙΟ 2

### Το νομικό πλαίσιο σε εθνικό και υπερεθνικό επίπεδο

#### 2.1 Το θεσμικό πλαίσιο προστασίας των δεδομένων προσωπικού χαρακτήρα

##### 2.1.1 Το ισχύον δίκαιο στην Ελλάδα

Στην Ελλάδα, θεμελιώνεται ένα ειδικό σύστημα κανονισμών, που αφορούν την προστασία των προσωπικών δεδομένων. Αυτοί οι κανόνες, που τίθενται στην ελληνική έννομη τάξη, αφορούν και τους δύο χώρους, τον «κυβερνοχώρο» και τον φυσικό χώρο.

##### α) Σύνταγμα

Το ζήτημα της προστασίας των προσωπικών δεδομένων, αλλά και της συλλογής, της αποθήκευσης και της επεξεργασίας τους, είναι κατοχυρωμένο, ως θεμελιώδες και απαραβίαστο δικαίωμα, στο Σύνταγμα. Ειδικότερα, το άρθρο 2 παρ. 1, αναφέρεται στο σεβασμό και την προστασία της αξίας του ανθρώπου, η οποία μάλιστα, αποτελεί την πρωταρχική υποχρέωση της πολιτείας. Επίσης, στο άρθρο 5 παρ. 1 του Συντάγματος, γίνεται αναφορά στην ελευθερία της προσωπικότητας και τη συμμετοχή του ατόμου στην οικονομική, κοινωνική και πολιτική ζωή της χώρας, εφόσον βέβαια, δεν παραβιάζεται το Σύνταγμα και τα χρηστά ήθη. Στο άρθρο 9 παρ. 1 και 19 παρ.1 Σ., γίνεται λόγος για την ιδιωτική και οικογενειακή ζωή του ατόμου και για το απόρρητο των επιστολών και της επικοινωνίας αντίστοιχα, ενώ επίσης, στο άρθρο 9Α του Συντάγματος, κατοχυρώθηκε το δικαίωμα προστασίας από τη συλλογή αποθήκευση και χρήση, κυρίως μέσω του διαδικτύου των προσωπικών δεδομένων. Ακόμη, συμπληρώνεται, ότι η προστασία τους διασφαλίζεται από ανεξάρτητη αρχή, η οποία λειτουργεί και συγκροτείται, σύμφωνα με όσα ορίζει ο νόμος.<sup>40</sup>

---

<sup>40</sup> Γιαννοπούλου Σ., «Προστασία Προσωπικών Δεδομένων στον Εργασιακό Χώρο», Διπλωματική Εργασία Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών (Δ.Π.Μ.Σ.) «Δίκαιο και Οικονομία», Πανεπιστήμιο Πειραιώς, 2017



## **β) Αστικός Κώδικας**

Στον Αστικό Κώδικα, το άρθρο 57ΑΚ αναφέρεται στο δικαίωμα της προσωπικότητας, σύμφωνα με το οποίο, κάθε άτομο το οποίο προσβάλλεται έχει δικαίωμα να άρει την προσβολή και να αιτηθεί τη μη επανάληψή της στο μέλλον. Ύστερα βέβαια, εισήχθη νόμος για την προστασία των προσωπικών δεδομένων (Ν.2472/1997).

## **γ) Ποινικός Κώδικας**

Παράλληλα, στον Ποινικό Κώδικα, βρίσκονται διατάξεις, οι οποίες αφορούν την προστασία των προσωπικών δεδομένων και σχετίζονται ιδιαίτερα, με την παραβίαση των απορρήτων. Τέτοια άρθρα, είναι το 370 ΠΚ και το 370 Α ΠΚ, σχετικά με την παραβίαση του απορρήτου των επιστολών και της τηλεφωνικής επικοινωνίας αντίστοιχα. Τα άρθρα 370 Β και 370 Γ του Ποινικού Κώδικα, αναφέρονται στην παραβίαση στοιχείων του δημοσίου ή του ιδιωτικού τομέα, ενώ το 370 Γ του ΠΚ, στην αντιγραφή ή παράνομη χρήση ηλεκτρονικών υπολογιστών ή την πρόσβαση σε αρχεία. Το άρθρο 371 ΠΚ, επίσης, αναφέρεται στην παραβίαση της εχεμύθειας στα επαγγέλματα.<sup>41</sup>

Οι συγκεκριμένοι νόμοι εκδόθηκαν, αποσκοπώντας στην προσπάθεια να εναρμονιστεί αυτή η ελληνική νομοθεσία με όσα ρυθμίζονται από τις Οδηγίες 95/46/ΕΚ και 2002/58/ΕΚ. Το περιεχόμενο των συγκεκριμένων συμπληρώθηκε με Αποφάσεις και Κανονιστικές Πράξεις της από ΑΠΔΠΧ και της Ευρωπαϊκής Επιτροπής.<sup>42</sup>

Με βάση την χρονολογία τους από το παλαιότερο στο νεότερο, γίνεται παρακάτω, μια αναφορά στα επιμέρους νομοθετικά κείμενα, ως εξής:

Αρχικά, ο Ν. 2472/1997, θεσπίστηκε αναφορικά με την προστασία του ατόμου έναντι της επεξεργασίας των προσωπικών δεδομένων. Στη συνέχεια, ο Νόμος 3471/2006, αφορούσε την προστασία των δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ενώ ο μετέπειτα Νόμος 3783/2009,

---

<sup>41</sup> Γιαννοπούλου Σ., «Προστασία Προσωπικών Δεδομένων στον Εργασιακό Χώρο», Διπλωματική Εργασία Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών (Δ.Π.Μ.Σ.) «Δίκαιο και Οικονομία», Πανεπιστήμιο Πειραιώς, 2017

<sup>42</sup> Σιδηρόπουλος Θ., «Το Δίκαιο του Διαδικτύου, Εκδόσεις Αντ. Σάκκουλα, Αθήνα, 2008

αναφερόταν στην ταυτοποίηση των ατόμων που κατέχουν και χρησιμοποιούν εξοπλισμό και υπηρεσίες κινητής τηλεφωνίας και άλλες διατάξεις. Επιπλέον, ο Νόμος 3917/2011 αναφερόταν στα συστήματα επιτήρησης, καταγραφής του ήχου και της εικόνας, σε δημόσιους χώρους και συναφείς διατάξεις. Επιπρόσθετα ο Ν.4070/2012 αφορούσε τις ρυθμίσεις των ηλεκτρονικών επικοινωνιών και μάλιστα, περιλαμβάνει τις πρόσφατες τροποποιήσεις του Νόμου 3471/2006. Τέλος, ο Νόμος 3051/ 2002 αναφερόταν στις αρχές λειτουργίας της Ανεξάρτητης Αρχής Προστασίας των Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).<sup>43</sup>

## **2.1.2 Το θεσμικό πλαίσιο στην Ευρώπη**

### **α) Κανονισμοί και Οδηγίες**

Σε υπερεθνικό επίπεδο, η Ευρωπαϊκή Ένωση, προκειμένου να καλύψει την αρχική ανάγκη προστασίας της ιδιωτικής ζωής, διατυπώνει τη Σύμβαση της Ρώμης, στις 4 Νοεμβρίου 1950.

Η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ), η οποία κυρώθηκε με νομοθετικό διάταγμα του 1974, αναφέρεται στο δικαίωμα κάθε ατόμου, να γίνεται σεβαστή η οικογενειακή και ιδιωτική του ζωή, ο τόπος κατοικίας, αλλά και η αλληλογραφία του. Στο ίδιο πλαίσιο, του ίδιου άρθρου, της ΕΣΔΑ, στο άρθρο 8 της Σύμβασης, αναφέρεται και το δικαίωμα προστασίας της ελεύθερης επαγγελματικής δραστηριότητας.<sup>44</sup>

Η Ευρωπαϊκή Ένωση, προς αυτό το σκοπό, έχει συναγάγει έναν Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), ο οποίος είναι παγκόσμιας εμβέλειας και εξέδωσε, μάλιστα, το έτος 1980 κατευθυντήριες αρχές, οι οποίες διέπουν την προστασία της ιδιωτικότητας και της διασυννοριακές ροές προσωπικών δεδομένων. Πρόκειται για κείμενο με μη δεσμευτικό χαρακτήρα, το οποίο περιλαμβάνει συγκεκριμένες αρχές, όπως για παράδειγμα, αυτή της περιορισμένης

---

<sup>43</sup> Γιαννοπούλου Σ., «Προστασία Προσωπικών Δεδομένων στον Εργασιακό Χώρο», Διπλωματική Εργασία Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών (Δ.Π.Μ.Σ.) «Δίκαιο και Οικονομία», Πανεπιστήμιο Πειραιώς, 2017

<sup>44</sup> Ως ανωτέρω, βλ. υπ. 43

συγκέντρωσης, συλλογής και αποθήκευσης των δεδομένων, της αρχής του ορισμένου σκοπού, της αρχής της διαφάνειας και της αρχής της ευθύνης.

Το 1981, θεσπίστηκε Σύμβαση του Συμβουλίου της Ευρώπης για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία των δεδομένων τους. Πρόκειται για τη Σύμβαση 108/28.1.1981. Η σύμβαση αυτή μάλιστα, υπογεγραμμένη στο Στρασβούργο, απαγορεύει ρητά και με κάθε τρόπο την επεξεργασία ευαίσθητων πληροφοριών και δεδομένων για τη ζωή των ατόμων, όπως για παράδειγμα, το φύλο, την ηλικία, το θρήσκευμα και το ποινικό μητρώο τους. Μάλιστα, στη συγκεκριμένη σύμβαση, προβλέπεται και το δικαίωμα της διορθώσεως. Παράλληλα, περιορισμοί του δικαιώματος είναι δυνατοί, μόνο στην περίπτωση κατά την οποία, το κράτος τίθεται σε κίνδυνο η υφίσταται πολύ σπουδαία ανάγκη.<sup>45</sup>

Επιπλέον, θεσπίστηκε η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24<sup>ης</sup> Οκτωβρίου 1995, αναφορικά με την προστασία των φυσικών προσώπων στην επεξεργασία των προσωπικών τους δεδομένων, αλλά και την ελεύθερη κυκλοφορία των πληροφοριών αυτών.

Έπειτα, η Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 10<sup>ης</sup> Ιουλίου 2002, αναφερόταν στην επεξεργασία δεδομένων και την προστασία της ιδιωτικής σφαίρας σε ό,τι αφορά τις ηλεκτρονικές επικοινωνίες. Ουσιαστικά, το αντικείμενό της ήταν η προσπάθεια προστασίας, με κάθε τρόπο, των δεδομένων των υποκειμένων, στα πλαίσια παροχής υπηρεσιών επικοινωνιών σε δημόσια δίκτυα.

Παράλληλα, ο Κανονισμός 45/2001/ΕΚ αφορούσε αυτή την προστασία των δεδομένων από τα όργανα και τους οργανισμούς της κοινότητας και την ελεύθερη κυκλοφορία όλων των δεδομένων και των πληροφοριών.

Έπειτα, ο Κανονισμός ΕΕ 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, αφορούσε στην προστασία των φυσικών προσώπων απέναντι στην επεξεργασία των δεδομένων τους, στην ελεύθερη κυκλοφορία των δεδομένων αυτών, αλλά παράλληλα και στην κατάργηση της

---

<sup>45</sup> Γιαννοπούλου Σ., «Προστασία Προσωπικών Δεδομένων στον Εργασιακό Χώρο», Διπλωματική Εργασία Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών (Δ.Π.Μ.Σ.) «Δίκαιο και Οικονομία», Πανεπιστήμιο Πειραιώς, 2017

Οδηγίας 95/ 46/ ΕΚ. Πρόκειται για τον Γενικό Κανονισμό για την Προστασία των Δεδομένων, το καλούμενο GDPR.<sup>46</sup>

## **β) Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) - GDPR**

Ο Γενικός Κανονισμός Προστασίας Δεδομένων αποτελεί ένα πολύ σημαντικό κείμενο, το οποίο καθορίζει με λεπτομέρεια, όλα όσα απαιτούνται, αναφορικά με τη συλλογή, την αποθήκευση, αλλά και τη διαχείριση των δεδομένων από οργανισμούς, αλλά και επιχειρήσεις.

Όλες αυτές οι απαιτήσεις, έχουν ισχύ για οργανισμούς της Ευρωπαϊκής Ένωσης, οι οποίοι μάλιστα, επεξεργάζονται τα προσωπικά δεδομένα και τα ατομικά στοιχεία των πολιτών στην ΕΕ, αλλά και για εκείνους, εκτός της ΕΕ, έχουν όμως, ως στόχο τους πολίτες, οι οποίοι διαβιούν εκτός της Ευρωπαϊκής Ένωσης.<sup>47</sup>

Αναφορικά με το πεδίο εφαρμογής του ΓΚΠΔ, θα πρέπει να αναφερθούν συγκεκριμένα στοιχεία. Ο Κανονισμός αυτός, εφαρμόζεται, στην περίπτωση που η επιχείρηση, η οποία εκτελεί την επεξεργασία των δεδομένων, έχει την έδρα της στην Ευρωπαϊκή Ένωση, ανεξαρτήτως από το εάν ο τόπος εκείνος, είναι πράγματι, ο τόπος επεξεργασίας των δεδομένων.

Ακόμη μία άλλη περίπτωση εφαρμογής του Κανονισμού, αφορά στην περίπτωση, κατά την οποία η επιχείρηση εδρεύει εκτός συνόρων της ΕΕ, ωστόσο, έχει επικοινωνία με τα άτομα τα οποία βρίσκονται εντός των συνόρων της, επεξεργάζεται τα προσωπικά δεδομένα, που αφορούν την παροχή υπηρεσιών ή προϊόντων στα άτομα αυτά, ή ακόμη παρακολουθεί τη συμπεριφορά των ατόμων που ζουν στα εδάφη της ΕΕ.<sup>48</sup>

---

<sup>46</sup> Γιαννοπούλου Σ., «Προστασία Προσωπικών Δεδομένων στον Εργασιακό Χώρο», Διπλωματική Εργασία Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών (Δ.Π.Μ.Σ.) «Δίκαιο και Οικονομία», Πανεπιστήμιο Πειραιώς, 2017

<sup>47</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm).

<sup>48</sup> Ως ανωτέρω βλ. υπ. 47

Είναι αξιοσημείωτο, ότι οι επιχειρήσεις, οι οποίες δεν έχουν την έδρα τους εντός της ΕΕ, αλλά μπορούν να επεξεργάζονται τα ατομικά στοιχεία των πολιτών της Ένωσης, οφείλουν να διορίζουν κάποιον ως εκπρόσωπο στην ΕΕ.<sup>49</sup>

Κατανοούμε λοιπόν, ότι σε όλες αυτές τις περιπτώσεις, ο ΓΚΠΔ, έχει την εφαρμογή του και ισχύουν όλες οι διατάξεις, οι οποίες αφορούν τα προσωπικά δεδομένα και την προστασία τους. Ωστόσο, υπάρχουν περιπτώσεις, κατά τις οποίες δεν τίθεται εφαρμογή.

Οι περιπτώσεις αυτές, αφορούν το υποκείμενο των προσωπικών δεδομένων και συγκεκριμένα, εάν πρόκειται για υποκείμενο το οποίο είναι νεκρό ή για υποκείμενο που είναι νομικό πρόσωπο, δεν τίθεται εφαρμογή ο Γενικός Κανονισμός Προσωπικών Δεδομένων. Επιπλέον, δεν εφαρμόζεται, εάν η επεξεργασία αυτή, γίνεται από άτομο, το οποίο ενεργεί για διαφορετικούς σκοπούς, πέραν του εμπορικού, επαγγελματικού πεδίου ή του επιχειρηματικού.<sup>50</sup>

Σύμφωνα με το άρθρο 1 του Κανονισμού, ο ΓΚΠΔ θεσπίζει κανόνες, οι οποίοι αφορούν στην προστασία των φυσικών προσώπων απέναντι στην επεξεργασία των προσωπικών τους δεδομένων, αλλά και κανονισμούς, οι οποίοι αφορούν την ελεύθερη κυκλοφορία αυτών. Παράλληλα, προστατεύονται θεμελιώδη ανθρώπινα δικαιώματα, αλλά και ελευθερίες των φυσικών προσώπων και πιο συγκεκριμένα, κάθε δικαίωμα στην προστασία των ατομικών τους στοιχείων (άρθρο 1 του ΓΚΠΔ).

Έπειτα, στο άρθρο 5 του ΓΚΠΔ, γίνεται αναφορά σε όλες εκείνες τις αρχές, οι οποίες αφορούν την επεξεργασία αυτών των δεδομένων, προσδιορίζονται όλες οι προϋποθέσεις, οι οποίες πρέπει να πληρούνται, προκειμένου να θεωρείται η επεξεργασία νόμιμη, ενώ στο άρθρο 12 ΓΚΠΔ, προσδιορίζονται τα δικαιώματα του υποκειμένου και στο άρθρο 24, οι υποχρεώσεις του υπεύθυνου επεξεργασίας (ΥΠΔ).

Αξιοσημείωτο επίσης, είναι το άρθρο 17 του Κανονισμού, στο οποίο γίνεται λόγος για το δικαίωμα διαγραφής ή διαφορετικά, το αποκαλούμενο και ως δικαίωμα στη «λήθη», για το οποίο έχει γίνει λόγος ήδη πιο πάνω, στην παρούσα μελέτη. Στο δικαίωμα αυτό, περιγράφονται όλες οι διαδικασίες, κατά τις οποίες, το άτομο ζητά τη διαγραφή των δεδομένων προσωπικού χαρακτήρα και την αντίστοιχη απάντηση της

---

<sup>49</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm).

<sup>50</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm)

επιχείρησης και των αρμοδίων σχετικά με την άμεση και χωρίς καθυστερήσεις διαγραφή όλων των στοιχείων, τα οποία επιθυμεί το υποκείμενο να διαγραφούν.<sup>51</sup>

Επιπρόσθετα είναι πολύ σημαντικό να αναφερθεί, ότι κάθε κράτος-μέλος της Ευρωπαϊκής Ένωσης, διασφαλίζει ότι υπάρχει μία ή περισσότερες ανεξάρτητες αρχές, δημόσιες, οι οποίες έχουν ως καθήκον τους, την παρακολούθηση της εφαρμογής του συγκεκριμένου Κανονισμού, η οποία αφορά την προστασία όλων αυτών των κατοχυρωμένων δικαιωμάτων των πολιτών. Οι αρχές αυτές, ονομάζονται εποπτικές (άρθρο 51 του ΓΚΠΔ) και στη συνέχεια, καθορίζονται όλα τα καθήκοντα και υποχρεώσεις αυτών των εποπτικών αρχών.<sup>52</sup>

Επιπλέον, σύμφωνα με το κείμενο του Κανονισμού, γίνεται μεγάλη αναφορά στις ροές των προσωπικών δεδομένων από και προς χώρες, εκτός της ΕΕ και διεθνείς οργανισμούς, οι οποίες ροές, βέβαια, είναι απαραίτητες για την επέκταση του εμπορίου και της διεθνούς συνεργασίας. Ωστόσο, λόγω της ραγδαίας ανάπτυξης της τεχνολογίας και των ηλεκτρονικών συστημάτων, αλλά και της διόγκωσης αυτών των ροών, τα προσωπικά δεδομένα, τα οποία διαβιβάζονται από την ΕΕ, σε τρίτες χώρες και διεθνείς οργανισμούς, μπορούν να πραγματοποιούνται αποκλειστικά με πλήρη συμμόρφωση, προς όλες τις διατάξεις του Κανονισμού.

Αξιοσημείωτο είναι επίσης, ότι ο Κανονισμός δε θίγει όλες τις διεθνείς συμφωνίες, οι οποίες έχουν συναφθεί μεταξύ της ΕΕ, αλλά και τρίτων χωρών, που διέπουν και αφορούν τη διαδικασία διαβίβασης των ατομικών στοιχείων, αλλά προβλέπουν ασφάλεια και εγγυήσεις για την προστασία των υποκειμένων των δεδομένων (Κείμενο Κανονισμού Προσωπικών Δεδομένων-GDPR).

Επομένως, κατανοούμε ότι τα κράτη μέλη, έχουν την δυνατότητα να συνάπτουν διεθνείς συμφωνίες, σχετικά με τη διαβίβαση αυτών των στοιχείων, σε τρίτες χώρες, ή σε διεθνείς οργανισμούς, ωστόσο στο σημείο και στο βαθμό που οι συγκεκριμένες συμφωνίες που συνάπτονται, δε θίγουν όλες τις διατάξεις του Κανονισμού ή γενικότερα του Δικαίου της Ευρωπαϊκής Ένωσης, αλλά και να περιλαμβάνουν ένα συγκεκριμένο επίπεδο προστασίας και ασφάλειας για τα κατοχυρωμένα δικαιώματα των υποκειμένων.

---

<sup>51</sup> Γιαννοπούλου Σ., «Προστασία Προσωπικών Δεδομένων στον Εργασιακό Χώρο», Διπλωματική Εργασία Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών (Δ.Π.Μ.Σ.) «Δίκαιο και Οικονομία», Πανεπιστήμιο Πειραιώς, 2017

<sup>52</sup> Ως ανωτέρω βλ. υπ. 51

Επίσης, σύμφωνα με τις αρχές που διέπουν την ΕΕ, σε ό,τι αφορά κυρίως την προστασία των ανθρωπίνων δικαιωμάτων, η Επιτροπή, θα πρέπει να αξιολογήσει την τρίτη χώρα, κατά πόσο σέβεται το κράτος δικαίου την πρόσβαση στη δικαιοσύνη, αλλά και τους διεθνείς θεσμούς και όλες τις διατάξεις για τα δικαιώματα του ανθρώπου, αλλά και γενικότερες αρχές όπως την προστασία της δημόσιας ασφάλειας, της εθνικής ασφάλειας, της άμυνας και το ποινικό δίκαιο.<sup>53</sup>

Κατανοούμε λοιπόν, ότι έχει προκύψει οικονομική, αλλά και κοινωνική ολοκλήρωση, αναφορικά με την λειτουργία της εσωτερικής αγοράς και αυτό, έχει ως αποτέλεσμα, την πολύ σημαντική αύξηση των σημαντικών διασυνοριακών ροών των προσωπικών δεδομένων.

Η ανταλλαγή αυτή, των δεδομένων, μεταξύ φυσικών προσώπων δημοσίων και ιδιωτικών φορέων επιχειρήσεων, αλλά και ενώσεων σε ολόκληρη την ΕΕ έχει αυξηθεί. Αυτό σημαίνει ότι κάθε εθνική αρχή του Κανονισμού των κρατών-μελών της ΕΕ, καλείται από το Ευρωπαϊκό Δίκαιο, να εφαρμόζει τις αρχές της συνεργασίας και της ανταλλαγής των δεδομένων, έτσι ώστε να μπορούν να εκτελούν όλες τις υποχρεώσεις και τα καθήκοντά τους, για την αρχή κάποιου άλλου κράτους –μέλους.<sup>54</sup>

Παράλληλα, η μη τήρηση των κανόνων του Γενικού Κανονισμού Προστασίας Δεδομένων, θα μπορούσε να έχει ως αποτέλεσμα την επιβολή μεγάλων προστίμων, τα οποία θα μπορούσαν να φτάσουν έως και τα 20 εκατομμύρια € ή το 4% του κύκλου εργασιών της επιχείρησης συνολικά, για ορισμένες παραβάσεις τις οποίες τέλεσε. Η ΑΠΔΠΧ έχει τη δυνατότητα επιπλέον, να επιβάλει διορθωτικά μέτρα, συμπληρωματικού χαρακτήρα, όπως για παράδειγμα, να διατάξει να διακοπεί η επεξεργασία των δεδομένων, από τους αρμόδιους επεξεργασίας τους.<sup>55</sup>

### **2.1.3 Η προστασία των δεδομένων στις ΗΠΑ**

Το νομοθετικό πλαίσιο στις ΗΠΑ διαφέρει σε μεγάλο βαθμό από εκείνο των κρατών-μελών της Ευρωπαϊκής Ένωσης, σε ό,τι αφορά το ζήτημα της προστασίας

---

<sup>53</sup> Κείμενο Κανονισμού Προσωπικών Δεδομένων-GDPR.

<sup>54</sup> Ως ανωτέρω βλ. υπ. 53

<sup>55</sup>[https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm).

των προσωπικών δεδομένων και της προσπάθειας αποτροπής παραβιάσεων τόσο στο φυσικό χώρο, όσο και στο διαδίκτυο.<sup>56</sup> Οι διαφορές εντοπίζονται τόσο, αναφορικά με τα δικαιώματα των υποκειμένων, όσο και ως προς τις πρακτικές που χρησιμοποιούνται προκειμένου να διασφαλίσουν την προστασία τους.<sup>57</sup>

Αξιοσημείωτο είναι το γεγονός, ότι δεν υπάρχει ενιαία εφαρμογή σε όλες τις πολιτείες, αλλά η κάθε πολιτεία ρυθμίζει μόνη της τα νομοθετικό πλαίσιο, το οποίο αφορά στη νομοθέτηση του θέματος των προσωπικών δεδομένων. Βέβαια, υπάρχουν διατάξεις, οι οποίες ρυθμίζουν κάποιες δραστηριότητες του ιδιωτικού τομέα, όπως για παράδειγμα, ο νόμος για την προστασία των δεδομένων προσωπικού χαρακτήρα στον πιστωτικό τομέα (Fair Credit Reporting Act).<sup>58</sup>

Γενικότερα, το σύστημα των ΗΠΑ, έχει ως βάση την απαγόρευση της υποκλοπής και την αποτροπή κοινοποίησης οποιασδήποτε επικοινωνίας, την προστασία της ιδιωτικότητας του ηλεκτρονικού ταχυδρομείου (e-mail),<sup>59</sup> αλλά και την πολύ προστατευμένη ανάπτυξη ασφαλών πρακτικών και πολιτικών στον κυβερνοχώρο για τους ανήλικους χρήστες του διαδικτύου. Θεσπίστηκε μάλιστα, νομοσχέδιο κατά το οποίο οι εταιρείες Google, Microsoft και Yahoo, αποτελούν δεσμευμένες επιχειρήσεις, έτσι ώστε να είναι υπεύθυνες για την παροχή στους χρήστες του ίντερνετ, την «Τεχνολογία μη Παρακολούθησης» (“Do not track technology”).<sup>60</sup>

---

<sup>56</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

<sup>57</sup> S. Scheindlin and D. Carpa, “The Sedona Conference, Electronic Discovery and Digital Evidence, Thomson Reuters, 2009, p.204

<sup>58</sup> Ιγγλεζάκης Ι, Προστασία προσωπικών δεδομένων στις υπηρεσίες κοινωνικής δικτύωσης, Σνήγορος 86/2011

<sup>59</sup> S. Scheindlin and D. Carpa, “The Sedona Conference, Electronic Discovery and Digital Evidence, Thomson Reuters, 2009, p.204

<sup>60</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015



Πρόκειται για νομοσχέδιο, το οποίο αφορά αμιγώς τα προσωπικά δεδομένα και κάθε πληροφορία που μπορεί να οδηγήσει στην αναγνώριση κάποιου ορισμένου ατόμου ή στην άμεση ταυτοποίησή του.<sup>61</sup>

Είναι ιδιαίτερα σημαντικό, να χρησιμοποιούνται πολιτικές ιδιωτικότητας (privacy policies) από τις επιχειρήσεις προς τους καταναλωτές, ιδιαίτερα όταν αφορά ιστοσελίδες, προκειμένου να μπορέσουν να ενημερωθούν σχετικά με τις υπηρεσίες, αλλά και τα προσωπικά δεδομένα που πρόκειται να χρησιμοποιηθούν, το χρόνο στον οποίο θα παραμείνουν στην πλατφόρμα, αλλά και την κάθε δυνατότητα ή επιλογή που θα έχουν, σχετικά με την χρήση των πληροφοριών τους.<sup>62, 63</sup>

Αυτό, δίνει τη δυνατότητα στους χρήστες να μπορούν να επιλέγουν τις από ιστοσελίδες τους, τις επιχειρήσεις με τις οποίες θα επικοινωνήσουν, με βάση τις πολιτικές ιδιωτικότητας (privacy policies) που παρέχονται.<sup>64</sup> Οι περισσότερες ιστοσελίδες και επιχειρήσεις, χρησιμοποιούν πολιτικές ιδιωτικότητας<sup>65</sup> ωστόσο τα άτομα σπανίως τις μελετούν<sup>66,67</sup>

## **2.2 Η παραβίαση των δεδομένων προσωπικού χαρακτήρα**

Η παραβίαση των δεδομένων προσωπικού χαρακτήρα συμβαίνει, όταν σημειώνεται μία πράξη, αναφορικά με την ασφάλεια των δεδομένων, για τα οποία ευθύνεται η επιχείρηση ή ο οργανισμός, το οποίο έχει ως αποτέλεσμα, να παραβιάζονται τα απόρρητα, η διαθεσιμότητα, και η ακεραιότητα. Σε περίπτωση που

---

<sup>61</sup> Elinor Mills, “Obama unveils Consumer Privacy Bill of Rights”, 2012

<sup>62</sup> Federal Trade Commission, 2000

<sup>63</sup> Cavoukian A. and Hamilton T., “Privacy Pay-off”, Mc Graw -Hill, 2002

<sup>64</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

<sup>65</sup> Adkinson, W.F., Eisenach, J.A., and Lenard, T.M., “Privacy online: A report on the information practices and policies of commercial websites, The Progress and Freedom Foundation, 2002

<sup>66</sup> Privacy Leadership Initiative, 2001

<sup>67</sup> Culcan, M.J., Bies R.J., “ Consumer Privacy: Balancing Economic and Justice Considerations”, Journal of Social Issues, 2003, p.323-342

κάτι τέτοιο συμβεί, υπάρχει πιθανότητα αυτή η παραβίαση να επηρεάσει τα δικαιώματα, αλλά και τις ελευθερίες των φυσικών προσώπων.

Έτσι, η επιχείρηση ή ο οργανισμός οφείλει να ειδοποιήσει την εποπτική αρχή, χωρίς να καθυστερήσει περαιτέρω αδικαιολογήτως και μάλιστα, μέσα σε χρονικό περιθώριο εντός 72 ωρών, το αργότερο, από τη στιγμή που έλαβαν γνώση σχετικά με την παραβίαση.<sup>68</sup>

Σε περίπτωση επίσης, που η επιχείρηση εκτελεί η ίδια την επεξεργασία, θα πρέπει να ενημερώνει και τον υπεύθυνο επεξεργασίας, αναφορικά με το συμβάν. Φυσικά, υπάρχει και η περίπτωση, η διαρροή των προσωπικών δεδομένων να έχει λάβει μεγάλες προεκτάσεις και να θέτει σε πολύ μεγάλο κίνδυνο τα συμφέροντα των φυσικών προσώπων, τα οποία επηρεάζονται. Τότε, θα πρέπει να ενημερωθεί καθένας από εκείνους, πολλώ δε μάλλον, εάν δεν υπάρχει κάποιο αποτελεσματικό μέτρο προστασίας από την επιχείρηση.

Βέβαια, οφείλουμε να ομολογήσουμε ότι είναι πολύ δύσκολο να διαγραφούν τα προσωπικά δεδομένα, ιδιαίτερα από τις ηλεκτρονικές πλατφόρμες, όπου η διαχείρισή τους είναι πολύ δύσκολη, από τη στιγμή που εκείνα έχουν διαρρεύσει, διότι η κυκλοφορία τις πληροφορίας στο διαδίκτυο των αρχείων είναι χαοτική και πολύ παγκοσμίου εμβέλειας. Αυτό συμβαίνει, διότι κάθε πληροφορία που διαρρέει, υπάρχει πιθανότητα να χρησιμοποιηθεί από χρήστες κακόβουλους, οι οποίοι επεξεργάζονται το λογισμικό των ηλεκτρονικών μέσων, λαμβάνεται χωρίς την συναίνεση τους και την χρησιμοποιούν προκειμένου να αποκομίσουν ίδιον όφελος. Πρόκειται για παραβίαση των προσωπικών δεδομένων, των αρχών της προστασίας προσωπικότητας αλλά και προσβολής της ιδιωτικής σφαίρας των ατόμων.

### **2.2.1 Η γνωστοποίηση της παραβίασης στην εποπτική αρχή**

Στο άρθρο 33 του Γενικού Κανονισμού Προστασίας Δεδομένων γίνεται αναφορά στη γνωστοποίηση αυτής της παραβίασης στην εποπτική αρχή. Έτσι, σε περίπτωση που συμβεί κάτι τέτοιο, ο υπεύθυνος επεξεργασίας οφείλει να

---

<sup>68</sup>[https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach\\_el](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_el)

γνωστοποιήσει αμελλητί εντός 72 ωρών, την εποπτική αρχή, η οποία είναι αρμόδια όπως ορίζεται στο άρθρο 55 του ΓΚΠΔ (άρθρο 33 παρ.1 ΓΚΠΔ).

Εάν, αυτή η παραβίαση δεν υπάρχει πιθανότητα να προκαλέσει κάποιο πρόβλημα ή κίνδυνο για οποιονδήποτε, ή την ελευθερία των φυσικών προσώπων, τότε υπάρχει η δυνατότητα να μη γνωστοποιηθεί άμεσα στην εποπτική αρχή. Σε κάθε άλλη περίπτωση, εάν η γνωστοποίηση δεν πραγματοποιηθεί, εντός του χρονικού πλαισίου που ορίζεται, θα πρέπει να συνοδεύεται από γραπτή αιτιολόγηση, σχετικά με τους λόγους της καθυστέρησης της γνωστοποίησης (άρθρο 33 παρ. 1 του ΓΚΠΔ).<sup>69</sup>

Παράλληλα το φυσικό πρόσωπο που εκτελεί την επεξεργασία, θα πρέπει να ενημερώνει τον υπεύθυνο κατευθείαν, μόλις λάβει γνώση της παραβίασης. Σύμφωνα με την γνωστοποίηση που αναφέρεται στην παράγραφο 1 του άρθρου 33 ΓΚΠΔ, θα πρέπει να περιγράφεται το είδος και η φύση της παραβίασης, στη συνέχεια να ανακοινώνεται το όνομα, αλλά και κάθε στοιχείο επικοινωνίας των αρμοδίων, προκειμένου να υπάρχει δυνατότητα τα υποκείμενα των δεδομένων, να επικοινωνήσουν με τους αρμόδιους. Επιπλέον, θα πρέπει να περιγράφεται κάθε ενδεχόμενη συνέπεια από το συμβάν, αλλά και τα προτεινόμενα ή τα άμεσα ληφθέντα μέτρα από την επιχείρηση ή τον οργανισμό, έτσι ώστε να μειωθούν οι πιθανότητες ενδεχόμενων δυσμενών αποτελεσμάτων και συνεπειών (άρθρο 33 παρ.2 και 3 του ΓΚΠΔ).<sup>70</sup>

Αξιοσημείωτο είναι επίσης να αναφερθεί, ότι εάν δεν είναι δυνατόν να δοθούν άμεσα και παράλληλα στον ίδιο χρόνο, όλες οι πληροφορίες, υπάρχει η δυνατότητα να παρέχονται σταδιακά, χωρίς ωστόσο να υπάρχει λόγος για καθυστέρηση και μάλιστα δίχως αιτιολόγηση (άρθρο 33 παρ.4 ΓΚΠΔ).

Ο υπεύθυνος για την επεξεργασία είναι αρμόδιος για την τεκμηρίωση κάθε παραβίασης. Η ιδιότητά του συνίσταται στην αναφορά των πραγματικών περιστατικών, στις ένομες συνέπειες, αλλά και τα διορθωτικά μέτρα, τα οποία λαμβάνει η επιχείρηση. Σκοπός αυτών των αρμοδιοτήτων είναι να επαληθευτεί από

---

<sup>69</sup>[https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach\\_el](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_el)

<sup>70</sup> <https://eur-lex.europa.eu/legal-content>

την εποπτική αρχή, η συμμόρφωση προς τα άρθρα και τις διατάξεις του Κανονισμού (άρθρο 33 παρ.5 ΓΚΠΔ).<sup>71</sup>

### **2.2.2 Η ανακοίνωση της παραβίασης στο υποκείμενο των προσωπικών Δεδομένων**

Πέραν των όσων αναφέρθηκαν στο άρθρο 33 του ΓΚΠΔ, αναφορικά με την γνωστοποίηση στην εποπτική αρχή, θα πρέπει να γίνει και ανακοίνωση της παραβίασης και στο υποκείμενα των δεδομένων, τα οποία υφίστανται την οποιαδήποτε είδους προσβολή.<sup>72</sup>

Αυτή η ανακοίνωση αναφέρεται στο άρθρο 34 του Κανονισμού και οι επιχειρήσεις ή οι οργανισμοί οφείλουν να συμμορφωθούν με τις διατάξεις και τα άρθρα του Κανονισμού. Όπως ήδη αναφέρθηκε, στην περίπτωση πρόκλησης υψηλού κινδύνου και ύπαρξης μεγάλης βλάβης στα φυσικά πρόσωπα, ο υπεύθυνος οφείλει να ανακοινώσει αμελλητί την παραβίαση (άρθρο 34 παρ.1 ΓΚΠΔ).

Οι ανακοινώσεις στα άτομα που αποτελούν τα υποκείμενα των προσωπικών στοιχείων που παραβιάστηκαν θα πρέπει να είναι συγκεκριμένες. Αρχικά, να γίνεται εκτενής περιγραφή, με σαφήνεια και ακρίβεια η φύση και το είδος των παραβιάσεων που υπέστησαν, αλλά και η ενημέρωση και τα μέτρα που αναφέρθηκαν στο άρθρο 33 παρ.3, β, γ και δ (άρθρο 34 παρ.2 ΓΚΠΔ).

Φυσικά υπάρχει και η πιθανότητα να μην πραγματοποιηθεί η ακόλουθη ανακοίνωση στο υποκείμενο των δεδομένων, για το λόγο ότι ο υπεύθυνος επεξεργασίας κατάφερε να εφαρμόσει τα κατάλληλα μέτρα προστασίας ή ότι χάρη σε αυτά τα μέτρα, δεν τίθενται σε υψηλό κίνδυνο τα δικαιώματα των φυσικών προσώπων. Παράλληλα εάν προϋποτίθενται πολύ μεγάλες και δυσανάλογες προσπάθειες, η επιχείρηση ή ο οργανισμός μπορεί να προβεί σε δημόσια ανακοίνωση, προκειμένου να ενημερωθούν με αποτελεσματικό τρόπο τα φυσικά πρόσωπα που υπέστησαν την παραβίαση (άρθρο 34 παρ.3 ΓΚΠΔ).<sup>73</sup>

Επιπλέον, εάν η εποπτική αρχή ενημερωθεί ότι ο υπεύθυνος δεν έχει προβεί στην ανακοίνωση, τον καλεί να συμμορφωθεί με τις διατάξεις του Κανονισμού και να

---

<sup>71</sup> <https://eur-lex.europa.eu/legal-content>.

<sup>72</sup> <https://eur-lex.europa.eu/legal-content>.

<sup>73</sup> <https://eur-lex.europa.eu/legal-content>.

το πράξει άμεσα. Μπορεί βέβαια και να εξετάσει τους παραπάνω λόγους, κατά τους οποίους υπάρχει η δυνατότητα λόγω των διορθωτικών μέτρων να μην υπάρξει κλήση και ανακοίνωση των υποκειμένων των προσωπικών δεδομένων (άρθρο 34 παρ.4 ΓΚΠΔ).<sup>74</sup>

---

<sup>74</sup> <https://eur-lex.europa.eu/legal-content>

## ΚΕΦΑΛΑΙΟ 3

### Νομικό Πλαίσιο: Ο Κανονισμός DMA, πλατφόρμες και προσωπικά δεδομένα

#### 3.1 Ιστορικό πλαίσιο του Digital Markets Act (DMA)

Τον Δεκέμβριο του 2020, παρουσιάστηκε από την Ευρωπαϊκή Επιτροπή μία δέσμη μέτρων, αναφορικά με τις ψηφιακές υπηρεσίες και τις πράξεις για τις ψηφιακές αγορές.<sup>75</sup> Ύστερα από κάποιους μήνες, στις 25 Νοεμβρίου 2021, τα κράτη-μέλη ομόφωνα, προχώρησαν στην έγκριση των θέσεων του Συμβουλίου.<sup>76</sup> Έπειτα, στις 24 Μαρτίου του 2022, μετά από την πραγματοποίηση τεσσάρων συνεδριάσεων, επετεύχθη συμφωνία, η οποία είχε προσωρινό χαρακτήρα.

Επιπλέον, στις 11 Μαΐου 2022, η επιτροπή των Μονίμων Αντιπροσώπων (EMA), η οποία μάλιστα, αποτελεί το κυριότερο όργανο του Συμβουλίου για προπαρασκευαστικές πράξεις, προχώρησε σε έγκριση του κειμένου, το οποίο, θα πρέπει στη συνέχεια, να περάσει από έγκριση και από το Κοινοβούλιο, προκειμένου να τεθεί σε ισχύ. Ο χρόνος συμμόρφωσης διαρκεί μέχρι τις αρχές του 2024.<sup>77</sup>

Παράλληλα, συμφωνήθηκε ότι στο πλαίσιο της πράξεως για τις ψηφιακές αγορές (DMA), επρόκειτο να συμφωνηθεί και η πράξη για τις ψηφιακές υπηρεσίες (DSA), αναφορικά με τις οικονομικές και κοινωνικές επιπτώσεις από τη συλλογή των δεδομένων από τους ρυθμιστές της πρόσβασης.

Η συγκεκριμένη πράξη, μαζί με την DMA, αποτελούν δύο πυλώνες ρύθμισης στην ψηφιακή οικονομία, διότι βασίζονται στις Ευρωπαϊκές αρχές και δημιουργούν τα όρια της δράσης των ψηφιακών πλατφορμών με μεγάλη δυναμική στην αγορά.<sup>78</sup>

---

<sup>75</sup><https://www.consilium.europa.eu/el/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/#>

<sup>76</sup>Ως ανωτέρω, βλ. υπ. 75

<sup>77</sup><https://www.consilium.europa.eu/el/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/#>

<sup>78</sup>Ως ανωτέρω, βλ. υπ. 77

### 3.2 Αιτιολόγηση της πρότασης

Η Ευρωπαϊκή Ένωση, τα τελευταία 10 χρόνια, έχει επιβάλει μεγάλα πρόστιμα σε εταιρίες, λόγω των αντιανταγωνιστικών και επιβλαβών πρακτικών τους στην ψηφιακή οικονομία.<sup>79</sup>

Με την πράξη DMA, η οποία αποτελεί πλέον Κανονισμό, δίνεται η δυνατότητα να απαγορευτούν άμεσα αυτές οι πρακτικές, αλλά και να καθοριστούν τα όρια για ένα πιο δίκαιο και διεκδικήσιμο χώρο στην οικονομία, τόσο για τις επιχειρήσεις που δραστηριοποιούνται στον ευρωπαϊκό χώρο, όσο και για τους νέους φορείς.<sup>80</sup>

Με βάση αυτή την αιτιολόγηση, οι κανόνες που τέθηκαν, κατανοούμε ότι είναι ιδιαίτερα σημαντικοί και ουσιώδεις για την ενίσχυση των αγορών στην ψηφιακή οικονομία, αλλά και για την απελευθέρωση των αγορών. Παράλληλα, ενισχύεται η ελευθερία των καταναλωτών, έτσι ώστε να μπορούν να επιλέγουν χωρίς κωλήματα τις υπηρεσίες και τα προϊόντα, που εκείνοι επιθυμούν στην ψηφιακή αγορά, αλλά παράλληλα, κατανέμεται η αξία στην ψηφιακή οικονομία και δίνονται κίνητρα για καινοτομίες. Η συγκεκριμένη πράξη, που αφορά τις ψηφιακές αγορές (DMA), ορίζει κανόνες, οι οποίοι είναι σαφείς, σχετικά με τις μεγάλες επιγραμμικές πλατφόρμες.<sup>81</sup>

Ο Υφυπουργός Ψηφιακών Υποθέσεων της Γαλλίας, Cedric, ανέφερε συγκεκριμένα, ότι η Ευρωπαϊκή Ένωση είναι η πρώτη, η οποία προτείνει κάτι τέτοιο και το εφαρμόζει, ενώ παράλληλα τονίζει ότι το ίδιο παράδειγμα θα ήταν καλό να το ακολουθήσουν και άλλες χώρες.<sup>82</sup>

Επιπρόσθετα, ένα μεγάλο μέρος ψηφιακών επιχειρήσεων δρουν ολοένα και περισσότερο ως ρυθμιστές της πρόσβασης, ανάμεσα σε επιχειρηματικούς χρήστες και τελικούς χρήστες, έχοντας μάλιστα, σταθερή θέση.<sup>83</sup> Συχνά, δημιουργούνται οικοσυστήματα ομίλων, γύρω από τις υπηρεσίες που προσφέρονται, πράγμα, το οποίο δημιουργεί φραγμούς-εμπόδια εισόδου στην αγορά, με αποτέλεσμα να ασκείται έλεγχος επί της πρόσβασης, την κατοχή παγιωμένης θέσης στις αγορές της ψηφιακής

---

<sup>79</sup><https://www.consilium.europa.eu/el/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/#>

<sup>80</sup> Ως ανωτέρω βλ. υπ. 79

<sup>81</sup> Ως ανωτέρω βλ. υπ. 79

<sup>82</sup> Ως ανωτέρω βλ. υπ. 79

<sup>83</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52020PC0842&from=en>

οικονομίας, την εξάρτηση των επιχειρηματικών χρηστών από αυτούς τους ρυθμιστές της πρόσβασης και κατ' επέκταση να δημιουργείται αθέμιτη συμπεριφορά, έναντι αυτών των επιχειρηματικών χρηστών.<sup>84</sup>

Καθίσταται, λοιπόν, αδήριτη ανάγκη ανάληψης δράσης σε επίπεδο ευρωπαϊκό, διότι μόνο με τις κανονιστικές πρωτοβουλίες, τις οποίες αναλαμβάνουν τα κράτη-μέλη, δεν θα μπορούσαν να αντιμετωπιστούν αυτές οι αρνητικές επιπτώσεις και κατά πάσα πιθανότητα, θα οδηγούσαν σε κατακερματισμό της εσωτερικής αγοράς.

Το γεγονός ότι υπάρχει ανάγκη αντιμετώπισης όλων αυτών των προβλημάτων, δημιούργησε την εφαρμογή αυτών των κανόνων από την Ευρωπαϊκή Ένωση, έτσι ώστε σε αυτά τα πλαίσια, να υπάρχει εξασφάλιση ότι οι αγορές που έχουν μεγάλες πλατφόρμες, οι οποίες επιδρούν πολύ σημαντικά στα δίκτυα και ενεργούν μάλιστα ως ρυθμιστές της πρόσβασης να μπορούν να παραμένουν δίκαιες και προσπελάσιμες για τους νεοεισερχόμενους στην αγορά, για τις εταιρείες, αλλά και για τους φορείς της οικονομίας.<sup>85</sup>

Κατανοούμε λοιπόν, ότι με βάση αυτή την αιτιολόγηση τέθηκε σε ισχύ το νομικό πλαίσιο της DMA για τις ψηφιακές αγορές, όπως επίσης αποφασίστηκε και το DSA για τις ψηφιακές υπηρεσίες.

### **3.3 Στόχοι του DMA**

Όπως ήδη αναφέρθηκε, η DMA πλέον έχει τεθεί σε ισχύ και έχει ως στόχο να απαγορεύσει τις μονοπωλιακές και αντιανταγωνιστικές πρακτικές επιχειρήσεων, οι οποίες αποκαλούνται «digital gatekeepers». Αυτές οι εταιρίες είναι οι γνωστοί ψηφιακοί κολοσσοί της Google, Meta κ.ά.<sup>86</sup>

Ο σκοπός αυτής της πράξης της Ευρωπαϊκής Ένωσης είναι να ενισχύσει τις start-ups επιχειρήσεις να προχωρήσουν σε καινοτομίες, να είναι περισσότερο ανταγωνιστικές, αλλά παράλληλα και να δοθούν περισσότερες επιλογές και ευκαιρίες στους καταναλωτές. Ειδικότερα, ο σκοπός είναι όλοι αυτοί οι στόχοι της DMA να πραγματοποιηθούν, τόσο σε ευρωπαϊκή, όσο και σε παγκόσμια κλίμακα και οι

---

<sup>84</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52020PC0842&from=en>

<sup>85</sup> Ως ανωτέρω βλ. υπ. 83

<sup>86</sup> <https://marketingweek.gr/dma-i-archi-mias-epochis/>



«digital gatekeepers» να υιοθετήσουν όλους αυτούς τους κανόνες που τίθενται από την DMA.<sup>87</sup>

Ένα σημαντικό στοιχείο που αφορά, άλλωστε και την προστασία των δεδομένων προσωπικού χαρακτήρα των χρηστών των πλατφορμών, είναι και η απαγόρευση της καταγραφής των δραστηριοτήτων των καταναλωτών στην πλατφόρμα για την προώθηση στοχευμένων διαφημίσεων, χωρίς να υπάρχει έγγραφη και ρητή συγκατάθεση τους, αλλά και η απαγόρευση εγκατάστασης λογισμικού σε υπολογιστές που έχουν σκοπό το αποκαλούμενο «web-tracking» δηλαδή, την παρακολούθηση των χρηστών του διαδικτύου, με σκοπό τη συλλογή και επεξεργασία των προσωπικών δεδομένων του για χρήση άλλη, από εκείνη για την οποία έχουν συναινέσει οι χρήστες. Οι επιχειρήσεις «digital gatekeepers» έχουν στη διάθεσή τους έξι μήνες για να συμμορφωθούν με το μέτρο αυτό που τίθεται από την DMA.<sup>88</sup>

Ο σκοπός δηλαδή, είναι να διασφαλιστεί ότι καμία μεγάλη επιγραμμική πλατφόρμα, η οποία αποτελεί ρυθμιστή της πρόσβασης δε θα καταχραστεί τη θέση αυτή, που της δίνεται, εις βάρος άλλων εταιρειών ή χρηστών.<sup>89</sup> Να απαγορευθεί, δηλαδή η καταχρηστική εκμετάλλευση δεσπόζουσας θέσης των επιχειρήσεων που λειτουργούν ως ρυθμιστές πρόσβασης και καθορίζουν εμπόδια εισόδου στην αγορά της ψηφιακής οικονομίας.

Επιπλέον, στόχος αυτής της πρότασης, είναι να υπάρχει η δυνατότητα στις πλατφόρμες να αξιοποιούν το δυναμικό τους, έτσι ώστε, τόσο η τελικοί, όσο και οι επιχειρηματικοί χρήστες να ωφελούνται οικονομικά από τις ψηφιακές πλατφόρμες, σε ένα περιβάλλον, το οποίο θα είναι διεκδικήσιμο και δίκαιο προς όλους.<sup>90</sup>

### 3.4 Πεδίο εφαρμογής του DMA

Αναφορικά με τα πεδία εφαρμογής του DMA, θα πρέπει να αναφέρουμε ότι πρόκειται για τις βασικές υπηρεσίες των ψηφιακών πλατφορμών, οι οποίες παρέχονται από τους ρυθμιστές της πρόσβασης σε χρήστες επιχειρήσεων, οι οποίοι

---

<sup>87</sup> <https://marketingweek.gr/dma-i-archi-mias-epochis/>

<sup>88</sup> <https://marketingweek.gr/dma-i-archi-mias-epochis/>

<sup>89</sup> <https://www.consilium.europa.eu/el/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/#>

<sup>90</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52020PC0842&from=en>

έχουν ως τόπο εγκατάστασης την Ευρωπαϊκή Ένωση, ή σε τελικούς χρήστες, που είτε βρίσκονται στην Ένωση, είτε είναι εγκατεστημένοι σε αυτήν, χωρίς να παίζει ρόλο ο τόπος εγκατάστασης και διαμονής των ρυθμιστών της πρόσβασης.<sup>91</sup>

Πιο συγκεκριμένα, στο άρθρο 3 παράγραφος 1 και 2 του Κανονισμού, αναφέρονται συγκεντρωμένα, όλα εκείνα τα χαρακτηριστικά των πλατφορμών που εμπίπτουν στο πεδίο εφαρμογής του και αποτελούν δηλαδή, ρυθμιστές πρόσβασης. Αυτό σημαίνει ότι πρέπει να υπάρχουν βασικές υπηρεσίες πλατφόρμας (“Core Platform Services”)<sup>92</sup> όπως αυτές ορίζονται από τον Κανονισμό.<sup>93</sup>

### 3.4.1 Οι πλατφόρμες ως ρυθμιστές πρόσβασης

Είναι αξιοσημείωτο να αναφερθεί το είδος των πλατφορμών, οι οποίες θεωρούνται ως ρυθμιστές της πρόσβασης (gatekeepers). Σε αυτά τα πλαίσια, το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο, συμφώνησαν ότι θα πρέπει, κατ’ αρχάς, μία τέτοια πλατφόρμα να έχει τα τελευταία τρία χρόνια, κύκλο εργασιών ανά έτος τουλάχιστον 7,5 δις εντός της ΕΕ. Διαφορετικά θα πρέπει να έχει τουλάχιστον 10.000 επιχειρηματικούς χρήστες, οι οποίοι θα βρίσκονται εγκατεστημένοι στην Ευρωπαϊκή Ένωση, ή η πλατφόρμα να έχει χρηματιστηριακή αξία τουλάχιστον 75 δις ευρώ.<sup>94</sup>

Επιπρόσθετα, ένα βασικό χαρακτηριστικό μιας τέτοιας πλατφόρμας, είναι να έχει μία ή περισσότερες βασικές υπηρεσίες (Core Platform Services) σε τουλάχιστον τρία κράτη μέλη. Τέτοιες υπηρεσίες, μπορεί να είναι τα κοινωνικά δίκτυα, τα web-browsers και οι μηχανές αναζήτησης.<sup>95</sup>

Αυτά τα ιδιαίτερα χαρακτηριστικά, κάνουν τις πλατφόρμες να λειτουργούν ως “gatekeepers” και να ρυθμίζουν ουσιαστικά την πρόσβαση και κατ’ επέκταση, να δημιουργούν εμπόδια εισόδου στην ψηφιακή αγορά, δημιουργώντας, κατ’ αυτό τον

---

<sup>91</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52020PC0842&from=en>

<sup>92</sup> <https://www.consilium.europa.eu/el/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/#>

<sup>93</sup> <https://www.consilium.europa.eu/media/56086/st08722-xx22.pdf>

<sup>94</sup> <https://www.consilium.europa.eu/el/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/#>

<sup>95</sup> <https://www.consilium.europa.eu/el/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/#>

τρόπο, δεσπόζουσα θέση στην ψηφιακή οικονομία, θέση, μάλιστα, την οποία χρειάζονται, έτσι ώστε να αποκτήσουν μεγάλα οικονομικά οφέλη.

Γι' αυτό το λόγο, ο Κανονισμός διευκρινίζει το είδος των πλατφορμών που λειτουργούν ως ρυθμιστές πρόσβασης και διαχωρίζει όλες τις επιβεβλημένες υποχρεώσεις των επιχειρήσεων “gatekeepers” στην ψηφιακή οικονομία, έτσι ώστε να δημιουργηθεί ένα δίκαιο και διεκδικήσιμο περιβάλλον στην αγορά, απαγορεύοντας τις αντιανταγωνιστικές πρακτικές που τις καθιερώνουν σε αυτήν.

### **3.4.2 Υποχρεώσεις των ρυθμιστών πρόσβασης**

Οι επιχειρήσεις που λειτουργούν ως “gatekeepers” έχουν υποχρεώσεις, οι οποίες απορρέουν από τον Κανονισμό και τις οποίες, οι επιχειρήσεις είναι υποχρεωμένες να τηρούν και να συμμορφώνονται με όσα επιβάλλονται από τους κανόνες που έχουν οριστεί από την Ευρωπαϊκή Ένωση.

Ειδικότερα, είναι απαραίτητο να ενημερώνουν την Ευρωπαϊκή Επιτροπή για τις εξαγορές ή οποιεσδήποτε συγχωνεύσεις πραγματοποιούνται.<sup>96</sup> Αυτή η υποχρέωση γνωστοποίησης είναι απαραίτητη, έτσι ώστε η Ευρωπαϊκή Επιτροπή να είναι σε θέση να κρίνει την κατάσταση των ρυθμιστών πρόσβασης και την θέση τους στην ψηφιακή οικονομία.

Επιπλέον, έχουν την υποχρέωση να παρέχουν στους πολίτες την πρόσβαση σε όλες εκείνες τις πληροφορίες, που αφορούν τους ίδιους ή τις επιδόσεις τους, αναφορικά με τις διαφημίσεις στην πλατφόρμα ή την εμπορική προώθηση των προϊόντων και των υπηρεσιών τους σε αυτές.<sup>97</sup> Αυτή η υποχρέωση απορρέει από το δικαίωμα των ατόμων στην ενημέρωση, αναφορικά με τις προσωπικές τους πληροφορίες, οι οποίες είναι καταχωρημένες ως δεδομένα στις ψηφιακές πλατφόρμες.

Επιπρόσθετα, θα πρέπει να επιτρέπουν την διακοπή της εγγραφής από αυτές τις βασικές υπηρεσίες, σε οποιονδήποτε επιθυμεί να ασκήσει αυτό το δικαίωμα, σε οποιαδήποτε χρονική στιγμή.<sup>98</sup> Κατανοούμε, ότι αυτό το δικαίωμα απορρέει, επίσης,

---

<sup>96</sup><https://www.consilium.europa.eu/el/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/#>

<sup>97</sup> Ως ανωτέρω βλ. υπ. 96

<sup>98</sup> Ως ανωτέρω βλ. υπ. 96

από τις διατάξεις για την προστασία των δεδομένων προσωπικού χαρακτήρα και το δικαίωμα του χρήστη στην διακοπή της εγγραφής των προσωπικών του πληροφοριών στην πλατφόρμα.

Μία ακόμη υποχρέωση, αφορά τα λογισμικά, τα οποία εγκαθίστανται αυτόματα στην πλατφόρμα και τα οποία, πολλές φορές, οι χρήστες δεν επιθυμούν. Πρόκειται δηλαδή, για browsers, τα οποία ο χρήστης δεν έχει επιλέξει, αλλά στην πραγματικότητα, εμφανίζονται και εγκαθίστανται στο λογισμικό του, χωρίς τη συναίνεσή του.<sup>99</sup>

Επιπρόσθετα, έχουν την υποχρέωση να διασφαλίζουν τη διαλειτουργικότητα αυτών των υπηρεσιών και να επιτρέπουν στους προγραμματιστές τους να έχουν την πρόσβαση σε αυτές.<sup>100</sup> Η υποχρέωση διαλειτουργικότητας υπογραμμίζεται στο άρθρο 7 του DMA και στην ουσία, αφορά την παροχή των απαραίτητων τεχνικών διεπαφών ή λύσεων, ύστερα από αίτηση και φυσικά, χωρίς χρηματικό κόστος.<sup>101</sup>

Παράλληλα, το άρθρο 14 αφορά στη γνωστοποίηση, ύστερα από τη συλλογή δεδομένων στην πλατφόρμα, πράγμα που σημαίνει ότι ο “gatekeeper” πρέπει να ενημερώσει την Επιτροπή, μέσα σε δύο μήνες από την υλοποίηση της συγκέντρωσης, ενώ επίσης, το άρθρο 15 αφορά στην υποχρέωση υποβολής περιγραφής όλων των τεχνικών χαρακτηριστικών της κατάρτισης ενός προφίλ του καταναλωτή στην Επιτροπή, μέσα σε προθεσμία έξι μηνών, από τον ορισμό του ως “gatekeeper”, όπως περιγράφεται στο άρθρο 3 του Κανονισμού.<sup>102</sup>

### **3.5 Μόχλευση και περικάλυψη (Leverage and envelopment)**

Η στρατηγική της μόχλευσης, την οποία χρησιμοποιούν οι επιχειρήσεις προκειμένου να αποκτήσουν μεγάλα οικονομικά οφέλη, απαιτεί δύο βασικά στοιχεία.

Αρχικά, η πλατφόρμα, η οποία είναι κυρίαρχη θα πρέπει να έχει τη δυνατότητα να αξιοποιήσει όλους τους πελάτες της κύριας αγοράς σε νέες αγορές.

---

<sup>99</sup> Ως ανωτέρω βλ. υπ. 96

<sup>100</sup> Ως ανωτέρω βλ. υπ. 96

<sup>101</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52020PC0842&from=en>

<sup>102</sup> Ως ανωτέρω βλ. υπ. 101

Με αυτό τον τρόπο, θα μπορέσει να αποκτήσει οφέλη από αποτελέσματα δικτύου μεγάλου βεληνεκούς, όταν εισέρχεται σε νέες αγορές. Αυτά τα δίκτυα μπορεί να είναι πολύ μεγαλύτερου μεγέθους από αυτά που απολαμβάνει ο συμμετέχων.<sup>103</sup>

Το δεύτερο στοιχείο, αποτελεί το γεγονός της ύπαρξης κοινών στοιχείων ή ενοτήτων με πιθανές επιπτώσεις αποκλεισμού των βασικών υπηρεσιών από την πλατφόρμα. Πιο συγκεκριμένα, στις ψηφιακές αγορές, αυτή η συγκεκριμένη μέθοδος μπορεί να έχει ως βάση της το απόρρητο των καταναλωτών και των χρηστών της πλατφόρμας, μέσω της συναίνεσής τους για την εγγραφή τους σε αυτή. Αυτό πραγματοποιείται μέσω της επιλογής του πλήκτρου της αποδοχής του απορρήτου ή των όρων και των προϋποθέσεων, που επιτρέπουν τη χρήση των δεδομένων των καταναλωτών σε όλες τις πλατφόρμες.<sup>104</sup>

Τα θετικά και τα αρνητικά αυτής της στρατηγικής ποικίλουν. Αρχικά, η θετική πλευρά δίνει τη δυνατότητα στην πλατφόρμα, η οποία κυριαρχεί στην αγορά να απολαμβάνει μεγάλα έσοδα, αλλά και οι πελάτες της να είναι πλήρως ικανοποιημένοι, ενώ παράλληλα συμβάλλει στον αυξημένο ανταγωνισμό μεταξύ των πλατφορμών.<sup>105</sup>

Ωστόσο η αρνητική πλευρά, αφορά τον αποκλεισμό των ανταγωνιστών, οι οποίοι είναι εξίσου αποτελεσματικοί, αλλά δεν έχουν τόσο μεγάλη βάση χρηστών ή μπορεί να δραστηριοποιούνται σε αγορές διαφορετικές. Αυτό έχει ως αποτέλεσμα, να μην προάγεται ο αποτελεσματικός ανταγωνισμός, η πρακτική να είναι αντιανταγωνιστική και να μην προωθείται η καινοτομία στην ψηφιακή οικονομία.<sup>106</sup>

### **3.6 Συνέπειες από τη μη συμμόρφωση των ρυθμιστών πρόσβασης με τους κανόνες της DMA**

Σε περίπτωση που ένας “gatekeeper” δε συμμορφώνεται με τους κανόνες που έχουν επιβληθεί από τον Κανονισμό και τους παραβιάζει, θα εφαρμοστούν οι διατάξεις του άρθρου 26 παρ.1 αναφορικά με τη μη συμμόρφωση από δόλο ή

---

<sup>103</sup>[https://cerre.eu/wp-content/uploads/2020/11/CERRE\\_DMA\\_Making-economic-regulation-of-platforms-fit-for-the-digital-age\\_Full-report\\_December2020.pdf](https://cerre.eu/wp-content/uploads/2020/11/CERRE_DMA_Making-economic-regulation-of-platforms-fit-for-the-digital-age_Full-report_December2020.pdf)

<sup>104</sup> Ως ανωτέρω βλ. υπ. 103

<sup>105</sup> Ως ανωτέρω βλ. υπ. 103

<sup>106</sup> Ως ανωτέρω βλ. υπ. 103

αμέλεια. Ειδικότερα, θα επιβληθεί πρόστιμο έως 10%, το οποίο, σε περίπτωση υποτροπής μετατρέπεται σε 20% του συνολικού κύκλου εργασιών.<sup>107</sup>

Στο άρθρο 26 παρ. 2 η χρηματική ποινή επιβάλλεται σε επιχειρήσεις, συμπεριλαμβανομένων φυσικά και των “gatekeepers”, σε περιπτώσεις, κατά τις οποίες, δολίως παραλείπουν να παράσχουν πληροφορίες ή αυτές είναι παραπλανητικές και το ποσό που καλείται να αποδώσει φτάνει έως το 1% του συνολικού κύκλου εργασιών.<sup>108</sup>

Τέλος, σύμφωνα με το άρθρο 27 παρ. 1, οι χρηματικές ποινές που επιβάλλονται με απόφαση, έτσι ώστε οι επιχειρήσεις να συμμορφωθούν με τα άρθρα 8, 18, 21, 23 φτάνει έως και το 5% του μέσου ημερήσιου κύκλου εργασιών.<sup>109</sup>

Αξιοσημείωτο είναι να αναφερθεί ότι σε περιπτώσεις, κατά τις οποίες παραβιάζεται συνεχώς ο Κανονισμός, τουλάχιστον τρεις φορές σε οκτώ έτη, δίνει τη δυνατότητα στην Ευρωπαϊκή Επιτροπή να κινήσει έρευνα στην αγορά ή να επιβάλει τα σχετικά διορθωτικά μέτρα. Η Επιτροπή αποτελεί τον αρμόδιο φορέα, ο οποίος είναι υπεύθυνος για την επιβολή του Κανονισμού και για τον έλεγχο της τήρησης αυτού.<sup>110</sup>

### 3.7 Η σχέση της DMA με την DSA

Το DMA, μαζί με το νόμο για τις ψηφιακές υπηρεσίες (DSA), αποτελεί τη σημαντικότερη αναθεώρηση του ψηφιακού ρυθμιστικού τοπίου που έχει πραγματοποιηθεί έως και σήμερα.<sup>111</sup> Ο κανονισμός DMA αφορά τους κανόνες που έχουν επιβληθεί από την Ευρωπαϊκή Ένωση, προκειμένου να αποτελέσει έναν ρυθμιστικό πυλώνα στην ψηφιακή οικονομία, ερειζόμενο σε αυτές τις αξίες που προβάλλει η Ένωση και να απαγορεύσει τις αντισταγωνιστικές πρακτικές στο πλαίσιο της ψηφιακής οικονομίας.<sup>112</sup>

---

<sup>107</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52020PC0842&from=en>

<sup>108</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52020PC0842&from=en>

<sup>109</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52020PC0842&from=en>

<sup>110</sup> <https://www.consilium.europa.eu/el/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/#>

<sup>111</sup> [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4109299](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4109299)

<sup>112</sup> <https://www.consilium.europa.eu/el/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/#>

Οι οικονομικές επιπτώσεις, οι οποίες προέρχονται από τη συλλογή και την επεξεργασία των προσωπικών δεδομένων από τους ρυθμιστές της πρόσβασης (“gatekeepers”) αποτελούν το ρυθμιστικό πλαίσιο της DMA.

Η DSA (Digital Services Act όμως, αφορά όλες τις κοινωνικές επιπτώσεις και πρόκειται για τον Κανονισμό για τις ψηφιακές υπηρεσίες.<sup>113</sup> Αποτελεί ρυθμιστικό πυλώνα, ο οποίος μαζί με την DMA, έχουν ως στόχο τον καθορισμό πλαισίων και ορίων, μέσα στα όποια θα υπάρχει ένα δίκαιο και ανταγωνιστικό ψηφιακό περιβάλλον.

### **3.8 Η πράξη Eu Data act**

Στις 22 Φεβρουαρίου 2022, η Ευρωπαϊκή Επιτροπή πρότεινε κανόνες, οι οποίοι είναι νέοι και αφορούν τη δυνατότητα που έχουν τα πρόσωπα να μπορούν να χρησιμοποιούν και να έχουν πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, τα οποία παράγονται στην Ευρωπαϊκή Ένωση, σε όλους τους τομείς της οικονομίας.<sup>114</sup> Όλες αυτές οι προτάσεις, αφορούν το νόμο περί δεδομένων και αποτελούν στην πραγματικότητα έναν ψηφιακό μετασχηματισμό, διότι παρέχουν ευκαιρίες και καινοτομίες, κάνοντας το ψηφιακό περιβάλλον ακόμη πιο ανταγωνιστικό, με βάση το δεδομένο, άλλωστε ότι τα δεδομένα των χρηστών βρίσκονται στο διαδίκτυο σε πάρα πολύ μεγάλο όγκο, ο οποίος μάλιστα, αυξάνεται συνεχώς δυναμικά.

Ο συγκεκριμένος νόμος, ο οποίος αφορά τα δεδομένα προσωπικού χαρακτήρα των χρηστών, τα οποία κατοχυρώνονται στις πλατφόρμες και χρησιμοποιούνται στην ψηφιακή οικονομία, αντιμετωπίζει τα ζητήματα κάθε φύσης που οδηγούν σε μη επαρκή χρήση αυτών των δεδομένων. Οι νέοι αυτοί κανόνες λοιπόν, θα καταστήσουν ακόμη περισσότερα δεδομένα στη διάθεσή τους, έτσι ώστε να μπορούν να επαναχρησιμοποιηθούν.<sup>115</sup>

---

<sup>113</sup><https://www.consilium.europa.eu/el/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/#>

<sup>114</sup> [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_1113](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113)

<sup>115</sup> [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_1113](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113)

### 3.8.1 Το ιστορικό πλαίσιο της πρότασης

Η πρόταση από την Ευρωπαϊκή Επιτροπή, στις 22 Φεβρουαρίου 2022, αποτελεί τη δεύτερη κύρια νομοθετική πρωτοβουλία, η οποία βασίζεται στα δεδομένα, με πρώτη και προγενέστερη αυτής, το νόμο για την διακυβέρνηση των δεδομένων, ο οποίος συμφωνήθηκε το Νοέμβριο του 2021 και αφορά τη διευκόλυνση της χρήσης δεδομένων, από όλους, ενώ αντίθετα η πρόταση Eu Data Act εξειδικεύει και διευκρινίζει τον παραπάνω νόμο, δημιουργώντας αξία από τα δεδομένα.<sup>116</sup>

Και οι δύο πρωτοβουλίες αποτελούν πολύ σημαντικές πράξεις, τόσο για το οικονομικό, όσο και για το κοινωνικό δυναμικό των δεδομένων και θα δημιουργήσουν την ελεύθερη ροή δεδομένων εντός της Ευρωπαϊκής Ένωσης σε ενιαία αγορά, προς όφελος όλων.<sup>117</sup>

### 3.8.2 Τα μέτρα που περιλαμβάνονται στο νόμο περί δεδομένων

Τα μέτρα του νόμου περί δεδομένων, μέσω της πρότασης Eu Data Act, παρουσιάζουν στοιχεία, τα οποία οδηγούν στον ψηφιακό μετασχηματισμό και στην πιο δίκαιη και ανταγωνιστική ψηφιακή οικονομία. Πρόκειται για μέτρα, τα οποία δίνουν τη δυνατότητα σε χρήστες με συνδεδεμένες συσκευές, να έχουν πρόσβαση σε δεδομένα, τα οποία δημιουργούν οι ίδιοι.<sup>118</sup>

Οι συγκεκριμένες πληροφορίες, συχνά αποτελούν αντικείμενο επεξεργασίας και διαμοιρασμού σε τρίτους από τους κατασκευαστές και με αυτό τον τρόπο δίνονται κίνητρα για τους τελευταίους, να συνεχίσουν την επένδυση σε αυτό το τεχνολογικό και καινοτόμο επίτευγμα στην ψηφιακή αγορά.<sup>119</sup>

Επιπλέον, τίθενται μέτρα αναφορικά με την αποτροπή της κατάχρησης των δεδομένων από το μέρος που έχει μεγαλύτερη και ισχυρότερη διαπραγματευτική ισχύ, το οποίο καταπατά τα δικαιώματα του άλλου μέρους που βρίσκεται σε δυσχερέστερη ή ασθενέστερη θέση.

---

<sup>116</sup> [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_1113](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113)

<sup>117</sup> [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_1113](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113)

<sup>118</sup> [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_1113](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113)

<sup>119</sup> [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_1113](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113)



Παράλληλα, οι νέοι κανόνες επιτρέπουν στους καταναλωτές και στους πελάτες να εναλλάσσονται αποτελεσματικά και να νιώθουν πιο ασφαλείς σε ζητήματα που αφορούν την παράνομη μεταφορά δεδομένων εναντίον τους, δημιουργώντας δικλείδες ασφαλείας για εκείνους.

### **3.8.3 Τα αποτελέσματα της πράξης Eu Data Act**

Αυτή η πράξη για τα προσωπικά δεδομένα, έχει θετικά αποτελέσματα τόσο για τους καταναλωτές και τις επιχειρήσεις, οι οποίοι θα μπορούν να έχουν πρόσβαση στις πληροφορίες τους και στα δεδομένα, τα οποία χρησιμοποιούν, θα μπορούν να λάβουν πολύ καλύτερες αποφάσεις από πριν, αναφορικά με την αγορά των προϊόντων και των υπηρεσιών τους στις ψηφιακές αγορές.<sup>120</sup>

Επιπλέον, ως προς τους επιχειρηματίες, αυτή η πρόταση, η οποία εφαρμόζεται, έχει ως αποτέλεσμα να έχουν περισσότερα δεδομένα στη διάθεσή τους και να αποκτούν μεγάλα οικονομικά οφέλη σε μία πολύ μεγάλη ανταγωνιστική αγορά δεδομένων. Οι υπηρεσίες, οι οποίες θα παρέχονται θα είναι πιο εξατομικευμένες και τα νέα δεδομένα θα αποτελέσουν τη βάση για τη δημιουργία νέων και καινοτόμων ψηφιακών υπηρεσιών.<sup>121</sup>

---

<sup>120</sup> [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_1113](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113)

<sup>121</sup> [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_1113](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113)

## ΚΕΦΑΛΑΙΟ 4

### Η Γερμανική Υπόθεση “Facebook” - C-252/21

#### 4.1 Η ανάλυση της υπόθεσης

##### 4.1.1 Εισαγωγή

Στην παρούσα ενότητα γίνεται αναφορά στην απόφαση του Γερμανικού Ομοσπονδιακού Δικαστηρίου, η οποία εξεδόθη στις 6 Φεβρουαρίου 2019, αναφορικά με την απαγόρευση στη συλλογή και επεξεργασία προσωπικών δεδομένων της ψηφιακής πλατφόρμας του Facebook, για την καταπάτηση των δικαιωμάτων της ιδιωτικότητας των χρηστών της πλατφόρμας και την καταχρηστική εκμετάλλευση της δεσπόζουσας θέσης, στην αγορά της ψηφιακής οικονομίας.<sup>122</sup>

Η συγκεκριμένη απόφαση πυροδότησε μία αξιοσημείωτη διαφωνία αναφορικά με την ισχύ των γερμανικών νόμων του Δικαίου του Ανταγωνισμού.<sup>123</sup> Πρόκειται για διαφωνία αναφορικά με τον υπερβολικό όγκο της συλλογής και επεξεργασίας προσωπικών δεδομένων των χρηστών, αλλά και για τη δημιουργία βλάβης (harm), εξαιτίας της εκτεταμένης χρήσης των ψηφιακών πλατφορμών, οι οποίες πολύ συχνά παραβιάζουν τους κανόνες περί ανταγωνισμού.<sup>124</sup>

Η γερμανική Bundeskartellamt εξέδωσε τη συγκεκριμένη απόφαση, η οποία μάλιστα δεν είναι ακόμα διαθέσιμη στο κοινό. Το Bundeskartellamt έχει δημοσιεύσει μέχρι την συγκεκριμένη περίοδο τρία έγγραφα, μεταξύ των οποίων, ένα δελτίο τύπου και μία περίληψη της υπόθεσης.<sup>125</sup> Πρόκειται στην ουσία, για υπόθεση ορόσημο, διότι εκείνη αντιπροσωπεύει ένα σημαντικό γεγονός, αναφορικά με το μέλλον του

---

<sup>122</sup> Anne C., Witt, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law

<sup>123</sup> <https://jeanmonnetprogram.org/paper/excessive-data-collection-as-anticompetitive-conduct-the-german-facebook-case/>

<sup>124</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

<sup>125</sup> Viktoria H.S.E. Robertson (University of Graz), The Theory of Harm in the Bundeskartellamt's Facebook Decision, Edited by Thibault Schrepel, Sam Sadden & Jan Roth (CPI), Competition Policy International, Inc., March 2019

ευρωπαϊκού νόμου στο πεδίο του ανταγωνισμού στα πλαίσια της ψηφιακής οικονομίας.<sup>126</sup>

#### 4.1.2 Η γερμανική υπόθεση Facebook

Στην απόφαση της 6<sup>ης</sup> Φεβρουαρίου 2019, το Bundeskartellamt απαγόρευσε στο Facebook Inc., στο Facebook Ireland, στο Facebook Dublin, και στο Facebook Germany τη χρήση του συγκεκριμένου μέσου κοινωνικής δικτύωσης, σε όσα άτομα κατοικούν στην Γερμανία, τα οποία χρησιμοποιούν παράλληλα και τις εταιρικές υπηρεσίες του WhatsApp, Oculus, Masquerade και Instagram.<sup>127</sup>

Αυτό συνέβη διότι συνέλεξαν και επεξεργάστηκαν τα δεδομένα προσωπικού χαρακτήρα των χρηστών, δίχως την συγκατάθεσή τους. Η συγκεκριμένη απαγόρευση έχει ως βάση της το άρθρο 19 παράγραφος 1 του γερμανικού ACT (GWB).

Όλη αυτή η διαδικασία είχε ως αρχή της τον Μάρτιο του 2016, όπου η πλατφόρμα άρχισε να χρησιμοποιεί τις προσωπικές πληροφορίες και τα δεδομένα των χρηστών από το κοινωνικό δίκτυο, μαζί με άλλες εταιρικές υπηρεσίες και ιστοσελίδες, χωρίς τη συναίνεση των μερών για αυτή την επεξεργασία και τον συγκεκριμένο συνδυασμό, ο οποίος παραβιάζει τα κατοχυρωμένα συνταγματικά δικαιώματα των χρηστών στις ψηφιακές πλατφόρμες.<sup>128</sup>

Η διαδικασία αυτή αφορούσε όλους τους χρήστες, οι οποίοι έχουν εγγραφεί στις ψηφιακές πλατφόρμες στο Facebook και των σχετιζόμενων με αυτό το μέσο εταιρικών υπηρεσιών και όχι για άτομα, τα οποία δεν αποτελούν χρήστες και δεν έχουν εγγραφεί στη συγκεκριμένη διαδικτυακή πλατφόρμα.

Στην πραγματικότητα το Bundeskartellamt δεν εντόπισε κάποιο συγκεκριμένο λόγο, προκειμένου να παρέμβει στο πεδίο της απαγόρευσης της καταχρηστικής

---

<sup>126</sup><https://www.competitionpolicyinternational.com/wp-content/uploads/2019/03/EU-News-Column-March-2019-Full-1.pdf>

<sup>127</sup>[https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v=](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=)

<sup>128</sup>[https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v=](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=)

εκμετάλλευσης και των πρακτικών αυτών, στα πλαίσια του Δικαίου του Ανταγωνισμού.<sup>129</sup>

Η βάση σε αυτή τη θεωρία του υπήρξε το γεγονός ότι προκειμένου να υπάρξουν συγκεκριμένες διαφημίσεις, οι οποίες θα πρέπει να προωθηθούν μέσα στην πλατφόρμα, θα χρειαστεί απαραιτήτως να προωθηθούν και οι αντίστοιχες πληροφορίες, έτσι ώστε να επιτευχθεί ο σκοπός. Αυτό βέβαια, έχει θεωρητική βάση, διότι στην πραγματικότητα ήταν απαραίτητη η εφαρμογή των κανόνων του Ανταγωνισμού, όπως άλλωστε και σε αυτή την περίπτωση.

Όπως κατανοούμε, αυτή η παρέμβαση χρειαζόταν οπωσδήποτε, διότι ξεπερνούσε τα όρια της προστασίας των δεδομένων προσωπικού χαρακτήρα, όπως ορίζονται από το GDPR, αλλά κι υπό το πρίσμα της κυριαρχίας της ψηφιακής πλατφόρμας του Facebook στην ψηφιακή οικονομία μέσω της πρακτικής της καταχρηστικής εκμετάλλευσης της δεσπόζουσας θέσης στην αγορά.<sup>130</sup>

#### 4.1.3 Ιστορικό της υποθέσεως

Το 2019 εκδόθηκε η απόφασή του Facebook, αναφορικά με τα ζητήματα των προσωπικών δεδομένων και των συμπράξεων, ζητήματα μάλιστα, τα οποία, απασχόλησαν ιδιαίτερα τους νομικούς. Το ανώτερο περιφερειακό δικαστήριο του Ντίσελντορφ υπέβαλε αίτηση προδικαστικής απόφασης στο Ευρωπαϊκό Δικαστήριο, διακόπτοντας αιφνιδιαστικά τη διαδικασία.<sup>131</sup>

Η δημοσίευση αυτού του αιτήματος από το Δικαστήριο έγινε στις 23 Απριλίου και περιελάμβανε ιδιαίτερα σημαντικά ζητήματα της νομοθεσίας για τα προσωπικά δεδομένα, αλλά και για τις σχέσεις των κανόνων του Ανταγωνισμού και των κανόνων για την προστασία δεδομένων προσωπικού χαρακτήρα.<sup>132</sup>

---

<sup>129</sup>[https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v=](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=)

<sup>130</sup>[https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v=](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=)

<sup>131</sup><https://www.cms-lawnow.com/ealerts/2021/04/ecj-to-issue-preliminary-ruling-on-german-fco-facebook-case>

<sup>132</sup><https://www.cms-lawnow.com/ealerts/2021/04/ecj-to-issue-preliminary-ruling-on-german-fco-facebook-case>

Κρίθηκε λοιπόν, ότι οι όροι χρήσης του Facebook αντέβαιναν στη γερμανική νομοθεσία των κανονισμών του Ανταγωνισμού και ότι η πλατφόρμα λειτουργούσε καταχρηστικά. Το αποτέλεσμα της αποφάσεως, ουσιαστικά, αφορούσε την επίκριση για τη διαχείριση των προσωπικών δεδομένων και τη συνεργασία με εταιρικές υπηρεσίες τρίτων, αναφορικά με το συνδυασμό τους και διέταξε την πλατφόρμα να προχωρήσει σε προσαρμογή των όρων χρήσης του, να αναπροσαρμόσει, δηλαδή, όλους τους κανόνες. Φυσικά, η πλατφόρμα, αμφισβήτησε αυτή την απόφαση άμεσα.<sup>133</sup>

Το δικαστήριο του Ντίσελντορφ διέταξε να υπάρξει ανασταλτική ισχύς στη διαδικασία και προχώρησε στην εξήγηση ότι δεν ήταν ιδιαίτερα πιθανό αυτή η συμπεριφορά να παραβιάζει τους κανόνες του Ανταγωνισμού. Από την άλλη πλευρά όμως, η γερούσια του Ομοσπονδιακού Δικαστηρίου ανέτρεψε αυτή την απόφαση του Δικαστηρίου του Ντίσελντορφ, προβάλλοντας διαφορετική συλλογιστική.<sup>134</sup>

Στις 24 Μαρτίου, το Δικαστήριο του Ντίσελντορφ, ύστερα από εκ νέου εξέταση του θέματος, εξέφρασε τη δυσαρέσκειά του απέναντι στο Ομοσπονδιακό Δικαστήριο, αναστέλλοντας τη διαδικασία και υποβάλλοντας παραπομπή στο ΔΕΚ.<sup>135</sup>

Το δικαστήριο του Ντίσελντορφ εξηγεί ότι υπήρξε ζημιά στον Ανταγωνισμό, αναφορικά με το θέμα της παραβίασης της ελευθερίας διαθέσεως προσωπικών δεδομένων, η οποία μάλιστα, τελεί υπό το πεδίο προστασίας των κανόνων του GDPR.

Επιπρόσθετα, θεωρεί ότι υπάρχει αιτιώδης σύνδεσμος μεταξύ αυτής της παραβίασης και της πρακτικής της καταχρηστικής εκμετάλλευσης της δεσπίζουσας θέσης της εταιρείας, δηλαδή παράβαση του άρθρου 102 ΣΛΕΕ, διότι η εταιρεία κατά πάσα πιθανότητα, δεν θα μπορούσε να εφαρμόσει όλους αυτούς καταχρηστικούς όρους, εάν λειτουργούσε κανονικά ο Ανταγωνισμός και οι καταναλωτές είχαν όντως, τη δυνατότητα να επιλέξουν κάποιον άλλο προμηθευτή στην αγορά.<sup>136</sup>

---

<sup>133</sup> <https://www.cms-lawnow.com/ealerts/2021/04/ecj-to-issue-preliminary-ruling-on-german-fco-facebook-case>

<sup>134</sup> Ως ανωτέρω, βλ. υπ. 133

<sup>135</sup> <https://www.cms-lawnow.com/ealerts/2021/04/ecj-to-issue-preliminary-ruling-on-german-fco-facebook-case>

<sup>136</sup> <https://www.cms-lawnow.com/ealerts/2021/04/ecj-to-issue-preliminary-ruling-on-german-fco-facebook-case>

Χρησιμοποιούσε δηλαδή, τη δεσπόζουσα θέση στην ψηφιακή οικονομία καταχρηστικά και έτσι λειτουργούσε παραβιάζοντας τα συνταγματικώς κατοχυρωμένα δικαιώματα των χρηστών του διαδικτύου και της συγκεκριμένης πλατφόρμας, αποσπώντας προσωπικές τους πληροφορίες και συνδυάζοντας αυτές, με εκείνες από υπηρεσίες τρίτων.<sup>137</sup>

Βέβαια, το Δικαστήριο του Ντίσελντορφ παρέπεμψε ερωτήσεις στο ΔΕΚ, το οποίο, ήταν αρμόδιο για την ερμηνεία του δικαίου του Ανταγωνισμού και πιο συγκεκριμένα, του κανονισμού GDPR. Μάλιστα, το αίτημα για προδικαστική απόφαση περιελάμβανε επτά ερωτήσεις, δύο εκ των οποίων, αφορούσαν τους κανόνες εφαρμογής του GDPR και 5 εκ των οποίων, το γενικότερο περιεχόμενό του.

Αρχικά, το πρώτο ερώτημα, αφορούσε την εφαρμογή του άρθρου 51 του GDPR, και πιο συγκεκριμένα, εάν μπορεί να αξιολογηθεί η συγκεκριμένη πρακτική της πλατφόρμας, εάν είναι σύμφωνη με αυτό τον Κανονισμό και εάν μπορεί να απευθυνθεί σχετική εντολή στο κατάλληλο γερμανικό υποκατάστημα, σε περίπτωση που τα δεδομένα τίθενται σε επεξεργασία από το ιρλανδικό υποκατάστημα του Facebook, η οποία τίθεται υπό την επίβλεψη της ιρλανδικής εποπτικής αρχής.<sup>138</sup>

Επιπλέον, το δεύτερο ερώτημα αφορούσε στο τι είναι η καταχρηστική εκμετάλλευση της δεσπόζουσας θέσης, και εάν λαμβάνεται υπ' όψιν ως προς την αξιολόγηση, το εάν υπάρχει επεξεργασία προσωπικών δεδομένων αντίθετη από τους κανονισμούς του GDPR.

Τα αλλά πέντε ερωτήματα, αφορούν τους σκοπούς του GDPR, τις προϋποθέσεις εφαρμογής των άρθρων του Κανονισμού για το περιεχόμενό του γενικότερα.

Ειδικότερα, το πρώτο ερώτημα αφορούσε το κατά πόσο μπορεί οποιαδήποτε εταιρεία να βασίζεται σε νομικούς λόγους, άλλους από εκείνους της συναινέσεως στη συλλογή και την επεξεργασία προσωπικών δεδομένων, όπως για παράδειγμα, τα «Δεδομένα Facebook», μέσω του «like button» ή την σύνδεσή του με την ψηφιακή πλατφόρμα του Instagram.<sup>139</sup>

---

<sup>137</sup><https://www.cms-lawnow.com/ealerts/2021/04/ecj-to-issue-preliminary-ruling-on-german-fco-facebook-case>

<sup>138</sup><https://www.cms-lawnow.com/ealerts/2021/04/ecj-to-issue-preliminary-ruling-on-german-fco-facebook-case>

<sup>139</sup><https://www.cms-lawnow.com/ealerts/2021/04/ecj-to-issue-preliminary-ruling-on-german-fco-facebook-case>

Το δεύτερο ερώτημα αφορά το πεδίο εφαρμογής του άρθρου 9 του Γενικού Κανονισμού Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, δηλαδή, κατά πόσο μπορεί το Facebook, να επεξεργάζεται ειδικές κατηγορίες τέτοιων δεδομένων, να αποκτά πρόσβαση σε αυτά ή να τα διαθέτει.

Το τρίτο ερώτημα αφορά το εάν μία εταιρεία έχει το δικαίωμα να βασιστεί στα άρθρο 6 του GDPR, αναφορικά με την συνδυασμό των δεδομένων για σκοπούς προώθησης διαφημίσεων, ενώ στην τέταρτη ερώτηση γίνεται αναφορά σε αυτό το συνδυασμό της πλατφόρμας του Facebook με εταιρικές υπηρεσίες τρίτων.<sup>140</sup>

Στο πέμπτο ερώτημα, το Δικαστήριο του Ντίσελντορφ γίνεται αναφορά στο εάν αυτή η επεξεργασία μπορεί να βασίζεται στο άρθρο 6 παράγραφος 1 γ,δ,ε του GDPR, ενώ με το έκτο ερώτημα γίνεται λόγος στη συναίνεση με βάση τον Κανονισμό και εάν αυτή, μπορεί να αποτελέσει νομική βάση σε περίπτωση που ο DPO είναι εταιρεία, η οποία κατέχει δεσπόζουσα θέση στην αγορά.<sup>141</sup>

Κατανοούμε λοιπόν, ότι εάν αποφασιστεί ότι οι εταιρίες δεν μπορούν να βασιστούν σε αυτή την συναίνεση των χρηστών, αυτό το γεγονός θα δημιουργούσε περαιτέρω προϋποθέσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα, τόσο στις παραδοσιακές αγορές, όσο και σε εκείνες της ψηφιακής οικονομίας των πλατφορμών. Έτσι, το ΔΕΚ και οι απαντήσεις του αναφορικά με αυτή την υπόθεση, αφορά τόσο την εφαρμογή της αντιμονοπωλιακής νομοθεσίας στις ψηφιακές αγορές, αλλά και τις απαντήσεις αναφορικά με την ερμηνεία θεμελιωδών διατάξεων του Γενικού Κανονισμού Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (GDPR).

## **4.2 Τα πραγματικά περιστατικά και το διαδικαστικό υπόβαθρο**

Η πλατφόρμα του Facebook αποτελεί ένα μέσο κοινωνικής δικτύωσης με πολύ μεγάλη ισχύ στην ψηφιακή οικονομία, λόγω της παγκόσμιας απήχυσής του στους χρήστες του διαδικτύου. Στη Γερμανία ειδικότερα, η βάση των χρηστών του

---

<sup>140</sup> <https://www.cms-lawnow.com/ealerts/2021/04/ecj-to-issue-preliminary-ruling-on-german-fco-facebook-case>

<sup>141</sup> <https://www.cms-lawnow.com/ealerts/2021/04/ecj-to-issue-preliminary-ruling-on-german-fco-facebook-case>

αυξήθηκε, μέχρι το 2018, σε 23 εκατομμύρια χρήστες ημερησίως και 32 εκατομμύρια χρήστες ανά μήνα.<sup>142</sup>

Όπως ήδη έχει αναφερθεί, η χρηματοδότηση γίνεται μέσω των διαφημίσεων και των χορηγών, ενώ η παροχή στους ιδιώτες χρήστες δεν έχει κανένα χρηματικό κόστος. Ωστόσο, απαραίτητη προϋπόθεση είναι η εγγραφή και η δημιουργία προφίλ στην πλατφόρμα του Facebook. Παράλληλα, η αποδοχή πολιτικών “cookies”, αλλά και η επιλογή των πλήκτρων αποδοχής των όρων και των προϋποθέσεων της πλατφόρμας, αποτελούσε απαραίτητο «βήμα» προκειμένου να προχωρήσει ο χρήστης στην επόμενη ιστοσελίδα. Αυτό το γεγονός, είχε ως αποτέλεσμα την υπερβολική (excessive) συλλογή δεδομένων από τους κατασκευαστές της πλατφόρμας. Δεδομένα, τα οποία χρησιμοποιούνταν, είτε από την ίδια την πλατφόρμα, ή από άλλη υπηρεσία που ανήκε σε αυτήν, είτε από ιστοτόπους τρίτων, που τη χρησιμοποιούσαν μέσω των επιχειρηματικών εργαλείων (“Facebook Business Tools”).<sup>143</sup>

Εργαλεία, τα οποία, πολλές φορές, οι χρήστες δεν τα γνώριζαν, στην πραγματικότητα, καθώς σύμφωνα με το FCO, εκατομμύρια επιχειρήσεις τα χρησιμοποιούσαν με τους χρήστες να μην μπορούν να αναγνωρίσουν, εάν κάποιος ιστότοπος τα είχε ενσωματώσει ή όχι, πριν την εγγραφή τους σε αυτή.<sup>144</sup>

Αυτό είχε ως αποτέλεσμα, η πλατφόρμα να παρακολουθεί τις κινήσεις των χρηστών, τόσο γεωγραφικά, όσο και διαδικτυακά, να συλλέγει δεδομένα με κάθε λεπτομέρεια για τους χρήστες και να «αλιεύει» ευαίσθητες πληροφορίες, που αφορούσαν το φύλο, την ηλικία, την αγοραστική συμπεριφορά ή τα ενδιαφέροντά τους.<sup>145</sup>

Έτσι, η πλατφόρμα κατάφερε να αποκτήσει 98% των παγκόσμιων κερδών και να αποκομίσει περιουσιακά οφέλη 55 δισεκατομμυρίων δολαρίων από τις διαφημίσεις. Ο FCO κίνησε επίσημες διαδικασίες κατά του Facebook, την 1η Μαρτίου 2016. Στις 6 Φεβρουαρίου του 2019, το πόρισμα της απόφασης ήταν ότι η

---

<sup>142</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

<sup>143</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

<sup>144</sup> Anne C. Witt, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law

<sup>145</sup> Anne C. Witt, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law



πλατφόρμα είχε καταχραστεί τη δεσπόζουσα θέση της, διότι συνέλεξε, συνδύασε και ανέλυσε δεδομένα των χρηστών, μέσω των τριών πηγών που αναφέρθηκαν ανωτέρω και ζήτησε από την πλατφόρμα να προχωρήσει σε ουσιαστικές και εκτεταμένες αλλαγές στο πεδίο της πολιτικής συλλογής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα των χρηστών του διαδικτύου στην πλατφόρμα.<sup>146</sup>

### 4.3 Το νομικό πλαίσιο στη C-252/21

Ένα σημαντικό νομικό ζήτημα που καλούταν να αντιμετωπίσει το FCO ήταν το νομικό πλαίσιο, το οποίο θα έπρεπε να εφαρμόσει. Πιο συγκεκριμένα, έπρεπε να αξιολογήσει, εάν η συμπεριφορά των κατασκευαστών της πλατφόρμας, θα πρέπει να υπαχθεί στη γερμανική ή στην κοινοτική νομοθεσία περί Ανταγωνισμού.<sup>147</sup>

Το συγκεκριμένο θέμα διέπεται από τον κανονισμό ΕΚ αρ. 1/2003. Αυτό που ισχύει, είναι η εφαρμογή των άρθρων 101 και 102 ΣΛΕΕ, μαζί με τους εθνικούς νόμους περί Ανταγωνισμού.<sup>148</sup> Ο FCO έκρινε ότι το άρθρο 102 παράγραφος 2, στοιχείο α της ΣΛΕΕ, θα μπορούσε να προβλέπει την απαγόρευση της εκμετάλλευσης των χρηστών, λόγω της υπερβολικής συλλογής και επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Ωστόσο, λόγω του γεγονότος ότι δεν υπήρχε νομολογία ή παρόμοια πρακτική στηριζόμενη στο άρθρο, σε αντίθεση με το γερμανικό νομικό πλαίσιο, ο FCO, επρόκειτο να στηρίξει τη θεωρία του αναφορικά με τη βλάβη σε παραβίαση του GDPR. Τελικά, όμως, δεν θεώρησε το άρθρο 102 του ΣΛΕΕ, την κατάλληλη βάση και στηρίχθηκε για την απόφασή του αποκλειστικά και μόνο στην απαγόρευση της καταχρηστικής συμπεριφοράς και πιο συγκεκριμένα, στο άρθρο 19 GWB.<sup>149</sup>

---

<sup>146</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

<sup>147</sup> Anne C. Witt, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law

<sup>148</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

<sup>149</sup> Anne C. Witt, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law

### 4.3.1 Το δίκαιο της Ένωσης

Όσον αφορά το δίκαιο της Ένωσης, στη συγκεκριμένη περίπτωση, το νομικό πλαίσιο, είναι ο Κανονισμός GDPR, ο οποίος έχει αναπτυχθεί ήδη, ανωτέρω. Πιο συγκεκριμένα, πρόκειται για το άρθρο 4 του Γενικού Κανονισμού Προστασίας Δεδομένων, στο οποίο, γίνεται αναφορά στην έννοια της συγκατάθεσης του υποκειμένου, δηλαδή ότι το τελευταίο, συμφωνεί ρητά και ελεύθερα στην επεξεργασία των προσωπικών του δεδομένων.<sup>150</sup> Επιπλέον, το άρθρο 6 παρ. 1 του Κανονισμού, αφορά τη νομιμότητα της επεξεργασίας και αναλύει τις επιμέρους προϋποθέσεις για αυτήν την επεξεργασία, η οποία θα πρέπει να είναι σύννομη και να τηρεί τα στοιχεία ά έως στ' του άρθρου 6 του Κανονισμού.

Επιπρόσθετα, το άρθρο 9 παρ. 1 και 2, αφορά στην επεξεργασία των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα και το άρθρο 51, αφορά όλα όσα έχουν αναφερθεί για την εποπτική αρχή και τις ανεξάρτητες εποπτικές αρχές στο GDPR.<sup>151</sup>

### 4.3.2 Το γερμανικό δίκαιο

Από τους νόμους του γερμανικού δικαίου, οι οποίοι εμπίπτουν στη συγκεκριμένη υπόθεση του Facebook, είναι εκείνοι, οι οποίοι αφορούν την καταχρηστική εκμετάλλευση δεσπόζουσας θέσης και πιο συγκεκριμένα, το άρθρο 19 παράγραφος 12 GWB, που έχει ως περιεχόμενο τους νόμους κατά των περιορισμών του Ανταγωνισμού.<sup>152</sup>

Βέβαια, το άρθρο 57 του GWB, αναφέρει όλους τους υπεύθυνους της συλλογής, της επεξεργασίας των προσωπικών δεδομένων των χρηστών και διευκρινίζει ότι όλες αυτές οι πληροφορίες, οι οποίες συλλέγονται θα πρέπει να καλύπτονται από το εμπορικό και το επιχειρηματικό απόρρητο και να

---

<sup>150</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionId=F2B26B34234145C1836F498702E9236F?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&o>

<sup>151</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionId=F2B26B34234145C1836F498702E9236F?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&o>

<sup>152</sup>,<sup>153</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionId=F2B26B34234145C1836F498702E9236F?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&o>

χρησιμοποιούνται μόνο για όσες εργασίες είναι αναγκαίες για την εκτέλεση των αντίστοιχων καθηκόντων και μόνο για όσο χρονικό διάστημα είναι απαραίτητο αυτό.<sup>153</sup>

Όπως αναφέρθηκε ήδη παραπάνω, ο FCO στηρίχθηκε στο άρθρο 19 GWB του γερμανικού δικαίου, αναφορικά με την υπόθεση του Facebook και την απαγόρευση της καταχρηστικής εκμετάλλευσης δεσπόζουσας θέσης της πλατφόρμας στην ψηφιακή οικονομία.

#### **4.4 Αίτηση για την έκδοση προδικαστικής απόφασης από το Oberlandesgericht Düsseldorf (Γερμανία)- Facebook Inc. και άλλοι κατά Bundeskartellamt**

Το δικαστήριο Oberlandesgericht Düsseldorf της Γερμανίας, στις 22 Απριλίου του 2021, έκανε αίτηση προδικαστικής απόφασης. Οι Facebook Inc., Facebook Ireland Ltd, Facebook Deutschland GmbH τίθενται κατά του Bundeskartellamt και παρεμβαίνουν στην υπόθεση της κυρίας δίκης είναι η Verbraucherzentrale Bundesverband e.V.<sup>154</sup>

##### **4.4.1 Προδικαστικά ερωτήματα**

##### **4.4.1 α) Ο ρόλος του Bundeskartellamt**

Το πρώτο προδικαστικό ερώτημα αφορά το πώς υπάρχει η δυνατότητα το Bundeskartellamt, το οποίο είναι εθνική αντιμονοπωλιακή αρχή κράτους-μέλους και δεν είναι εποπτική αρχή, να προβαίνει σε αντιμονοπωλιακό έλεγχο σε εταιρία, η οποία, μάλιστα έχει έδρα εκτός Ευρωπαϊκής Ένωσης και πραγματοποιεί όλες τις απαραίτητες διαδικασίες, ευρισκόμενη η ίδια η αντιμονοπωλιακή εθνική αρχή σε έδαφος Ευρωπαϊκής Ένωσης.<sup>155</sup>

Αυτός ο έλεγχος, ο οποίος αφορά την συλλογή και επεξεργασία προσωπικών δεδομένων της επιχείρησης πραγματοποιείται από την ίδια, ενώ επίσης διατάσσει την

---

<sup>154</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62021CN0252>

<sup>155</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62021CN0252>

παύση της παράβασης τον πολιτικών της επιχείρησης σε παραβάσεις, οι οποίες αφορούν τα προσωπικά δεδομένα.

Ειδικότερα, το ερώτημα αφορά το εάν αυτή η πρακτική συνάδει με το άρθρο 51 επ. του Κανονισμού GDPR, δηλαδή, να μπορεί μία εθνική αρχή κράτους-μέλους να προβαίνει σε αυτές τις ενέργειες, χωρίς να είναι εποπτική αρχή, όπως προβλέπεται από τον Κανονισμό.<sup>156</sup>

Επιπρόσθετα, τίθεται το ερώτημα (στοιχείο β'), το οποίο έχει ως περιεχόμενο, εάν ισχύουν τα παραπάνω και υπάρχει αυτή η δυνατότητα για το Bundeskartellamt, εάν αυτή η διάταξη, συνάδει με εκείνη του άρθρου 4 παράγραφος 3 ΣΕΕ, όταν η εποπτική αρχή, η οποία ορίζεται στο άρθρο 56 παρ. 1 του GDPR, διεξάγει ταυτοχρόνως και εκείνη, έρευνα στο ίδιο περιεχόμενο και στα ίδια πλαίσια με την εθνική αρχή.<sup>157</sup>

#### **4.4.1 β) Η επεξεργασία ευαίσθητων προσωπικών δεδομένων από την ίδια και η συσχέτιση αυτών με πληροφορίες άλλων εταιριών**

Το δεύτερο προδικαστικό ερώτημα αφορά την περίπτωση, κατά την έννοια του άρθρου 9 παρ. 1 του Γενικού Κανονισμού Προστασίας Δεδομένων, κατά την οποία, οι χρήστες χρησιμοποιούν ιστοσελίδες και εφαρμογές, στις οποίες ενσωματώνουν τα «ευαίσθητα» προσωπικά τους δεδομένα, όπως το φύλο, η ηλικία, οι προτιμήσεις.

Αυτές οι εφαρμογές, οι οποίες συλλέγουν και αποθηκεύουν αυτά τα προσωπικά δεδομένα, είτε μέσω των «εργαλείων επιχειρήσεων του Facebook» (“Facebook Business Tools”), είτε μέσω των “cookies”, χρησιμοποιούνται από την ίδια την εταιρεία του Facebook, είτε από κάποια άλλη επιχείρηση.<sup>158</sup>

Το δεύτερο ερώτημα, λοιπόν, αφορά την δημοσιοποίηση αυτών των προσωπικών δεδομένων, κατά την έννοια του άρθρου 9 παρ. 2, στοιχείο ε' του ΓΚΠΔ. Δηλαδή, εάν αυτές οι προτιμήσεις των χρηστών, μέσω της επιλογής του πλήκτρου

---

<sup>156</sup><https://curia.europa.eu/juris/document/document.jsf?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=1527>

<sup>157</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62021CN0252>

<sup>158</sup>,<sup>159</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62021CN0252>

«μου αρέσει», ή μέσω της σύνδεσης στο λογαριασμό, ή με τις κοινοποιήσεις στην πλατφόρμα, αυτά τα προσωπικά στοιχεία δημοσιεύονται σε τρίτους.<sup>159</sup>

#### **4.4.1 γ) Επιχειρήματα και δικαιολογητική βάση της επεξεργασίας και της συσχέτισης, δυνάμει των άρθρων του Κανονισμού GDPR**

Το τρίτο προδικαστικό ερώτημα αφορά την περίπτωση, κατά την οποία το Facebook Ireland Inc., μπορεί να βρει κάποιο δικαιολογητικό λόγο γι' αυτή τη συλλογή και επεξεργασία προσωπικών δεδομένων. Δηλαδή, εάν χρησιμοποιηθεί το επιχειρήμα ότι η επεξεργασία αυτή είναι απαραίτητη, σύμφωνα με το άρθρο 6 παρ. 1, στοιχείο β' του GDPR για την εκτέλεση της σύμβασης ή ότι αποσκοπεί στο άρθρο 6 παρ. 1, στοιχείο του GDPR, για την προστασία των εννόμων συμφερόντων της επιχείρησης.<sup>160</sup>

Εάν δηλαδή, μπορεί να θέσει ως βάση του επιχειρήματος ότι όλες αυτές οι πληροφορίες, που συλλέγονται μέσω των “Facebook Business Tools” ή των “cookies”, είναι απαραίτητες και προβλέπονται από τον Κανονισμό, διότι η πλατφόρμα εκμεταλλεύεται το ψηφιακό μέσο κοινωνικής δικτύωσης και έχει συγκεκριμένους όρους και προϋποθέσεις χρήσης.<sup>161</sup>

#### **4.4.1 δ) Οι σκοποί της επεξεργασίας ως έννομα συμφέροντα κατά το άρθρο 6 παρ. 1, στοιχείο στ' του GDPR**

Το τέταρτο προδικαστικό ερώτημα αναφέρεται στην περίπτωση, κατά την οποία, μπορούν να θεωρηθούν ως έννομα συμφέροντα, κατά την έννοια του άρθρου 6 παρ. 1 στοιχείο στ' του GDPR και άλλα, περαιτέρω στοιχεία.

Αυτά τα περαιτέρω στοιχεία, μπορεί να αφορούν την ανηλικότητα του χρήστη, τη διάθεση των στοιχείων-μετρήσεων, τη δυνατότητα επικοινωνίας για σκοπούς εμπορικούς, την ενίσχυση της έρευνας και της καινοτομίας, την ενημέρωση

---

<sup>160</sup>,<sup>161</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62021CN0252>

διωκτικών και δικαστικών αρχών, σε περίπτωση συλλογής πληροφοριών και περιεχομένου χρήσιμου για εκείνους.<sup>162</sup>

Το ερώτημα που τίθεται είναι εάν αυτή η επιχείρηση, η οποία συλλέγει και επεξεργάζεται προσωπικά δεδομένα, μέσω των εργαλείων που προαναφέρθηκαν, συσχετίζει τα δεδομένα του λογαριασμού της πλατφόρμας και τα εάν τα χρησιμοποιεί.

#### **4.4.1 ε) Δικαιολογητική βάση της επεξεργασίας για νόμιμους σκοπούς**

Το πέμπτο προδικαστικό ερώτημα αναφέρεται στο εάν η συλλογή και η επεξεργασία των προσωπικών δεδομένων, που γίνεται από άλλες εταιρίες του ίδιου ομίλου και στη συνέχεια, που ενσωματώνονται μέσω αυτών των διεπαφών, μέσω των “cookies” και συσχετίζονται με τα δεδομένα που έχει συλλέξει ο λογαριασμός του Facebook, εάν μπορούν, στην πράξη, να εφαρμοστούν και να δικαιολογηθούν από το άρθρο 6 παρ. 1, στοιχεία γ', δ', ε', του GDPR, όταν ο σκοπός είναι να παρασχεθούν πληροφορίες, έπειτα από νόμιμο αίτημα για συγκεκριμένα δεδομένα (στοιχείο γ'), για την καταπολέμηση επιβλαβών συμπεριφορών, για την έρευνα προς όφελος του κοινωνικού συνόλου (στοιχείο δ') και την προστασία της ασφάλειας (στοιχείο ε').<sup>163</sup>

#### **4.4.1 στ) Δήλωση συγκατάθεσης χρήστη προς την επιχείρηση που κατέχει δεσπόζουσα θέση στην αγορά**

Το έκτο προδικαστικό ερώτημα έχει ως περιεχόμενο, εάν μπορεί να είναι έγκυρη, σύμφωνα με το άρθρο 6 παρ.1, στοιχείο α' και 9 παρ. 2, στοιχείο α' του GDPR, η δήλωση συγκατάθεσης χρήστη, η οποία απευθύνεται προς την επιχείρηση που κατέχει δεσπόζουσα θέση, σύμφωνα με το άρθρο 4 παρ. 11 του GDPR.<sup>164</sup>

---

<sup>162</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62021CN0252>

<sup>163</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62021CN0252>

<sup>164</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62021CN0252>

#### **4.4.1 ζ) Ο ρόλος της εποπτικής αρχής κατά τις διατάξεις του ΓΚΠΔ**

Σε περίπτωση αρνητικής απάντησης στο έκτο προδικαστικό ερώτημα, το έβδομο προδικαστικό ερώτημα (στοιχείο α), έχει ως περιεχόμενο, εάν μπορεί το Bundeskartellamt, το οποίο αποτελεί εθνική αντιμονοπωλιακή αρχή κράτους-μέλους, χωρίς να έχει ρόλο εποπτικής αρχής, όπως προβλέπεται από το άρθρο 51 επ. του GDPR, να αποφανθεί σχετικά με το εάν οι όροι χρήσης της επιχείρησης για την συλλογή και επεξεργασία των δεδομένων συνάδουν με το GDPR, παρότι η παραβίαση δεν αφορά παράβαση του ΓΚΠΔ.<sup>165</sup>

Επιπρόσθετα, το έβδομο προδικαστικό ερώτημα (στοιχείο β'), έχει περιεχόμενο το εάν ισχύει, υπό το πρίσμα του άρθρου 4 παρ. 3 ΣΕΕ, το ότι η επιχείρηση, αναφορικά με την επεξεργασία των δεδομένων, ελέγχεται και από το άρθρο 56 παρ.1 του GDPR από την εποπτική αρχή, η οποία είναι επικεφαλής και αρμόδια.<sup>166</sup>

Είναι αξιοσημείωτο να αναφερθεί ότι εάν η απάντηση στο έβδομο προδικαστικό ερώτημα είναι καταφατική, τότε το τρίτο, το τέταρτο και το πέμπτο ερώτημα, πρέπει να έχουν ως απάντηση και για τη συλλογή και την επεξεργασία προσωπικών δεδομένων, κατά την χρήση της υπηρεσίας του Instagram, διότι ανήκουν στον ίδιο όμιλο (Meta Platforms).<sup>167</sup>

### **4.5 Απαντήσεις επί των προδικαστικών ερωτημάτων**

#### **4.5.1 Απάντηση του πρώτου προδικαστικού ερωτήματος**

Επί του πρώτου προδικαστικού ερωτήματος, σχετικά με το εάν μπορεί να έχει την αρμοδιότητα το Bundeskartellamt να λειτουργήσει ελεγκτικά και να μπορεί να αποφανθεί, αναφορικά με την παραβίαση των κανόνων του Γενικού Κανονισμού Προσωπικών Δεδομένων (GDPR) και αν αυτή η τακτική συνάδει με το άρθρο 56 παρ.1 του Κανονισμού, η απάντηση είναι ότι το Bundeskartellamt δεν επέβαλε κυρώσεις, προέβη ωστόσο, προς τον σκοπό και μόνο της εφαρμογής όλων των

---

<sup>165</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62021CN0252>

<sup>166</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62021CN0252>

<sup>167</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62021CN0252>

κανόνων του Ανταγωνισμού που προβλέπονται στον έλεγχο. Δηλαδή, της διάπραξης αυτής της παραβάσεως από την πλευρά της επιχείρησης, η οποία καταχράστηκε την δεσπόζουσα θέση της και λειτούργησε αντανταγωνιστικά και με τρόπο αντίθετο από τις διατάξεις του Γενικού Κανονισμού (GDPR).<sup>168</sup>

Επομένως, το ά στοιχείο του πρώτου προδικαστικού ερωτήματος, θεωρείται αλυσιτελέες, όπως άλλωστε και το β' στοιχείο, του οποίου η καταφατική απάντηση εξαρτάται από το πρώτο μέρος.<sup>169</sup>

#### 4.5.2 Απάντηση του δεύτερου προδικαστικού ερωτήματος

Ως προς το ά στοιχείο του δεύτερου προδικαστικού ερωτήματος, αναφορικά με τις «ευαίσθητες» πληροφορίες, οι οποίες αποκαλύπτονται, η απάντηση που δίνεται είναι ότι οι πληροφορίες αυτές, είναι προσωπικά δεδομένα, χωρίς ωστόσο, να διευκρινίζεται, εάν αποκαλύπτονται στην πραγματικότητα και «ευαίσθητα» προσωπικά δεδομένα, μέσα από την επίσκεψη στην πλατφόρμα ή σε κάποια ιστοσελίδα.<sup>170</sup> Είναι δηλαδή, σημαντικό να τεθεί διάκριση επί του ζητήματος, εάν πρόκειται για αποκάλυψη «ευαίσθητων» προσωπικών δεδομένων ή δεδομένων που δεν έχουν τόσο σκληρό πυρήνα.

Αναφορικά με το στοιχείο β' του δεύτερου προδικαστικού ερωτήματος δίνεται η απάντηση ότι για να μπορεί να γίνει εφαρμογή του νόμου, ο χρήστης θα πρέπει να γνωρίζει πλήρως και να δηλώνει με ρητή πράξη ότι δημοσιοποιεί δεδομένα προσωπικού χαρακτήρα. Θα πρέπει δηλαδή, τα προσωπικά δεδομένα να έχουν «προδήλως» δημοσιοποιηθεί από το ίδιο το υποκείμενο.<sup>171</sup>

---

<sup>168</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionId=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

<sup>169</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionId=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

<sup>170</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionId=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

<sup>171</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionId=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>



Επομένως, στην υπό κρίση περίπτωση, κάτι τέτοιο δεν μπορεί να εξομοιωθεί με συμπεριφορά «πρόδηλης» δημοσιοποίησης.<sup>172</sup> Επιπρόσθετα, ακόμη και σε περίπτωση συγκατάθεσης του χρήστη, δεν αφορά την επεξεργασία των «ευαίσθητων» προσωπικών του δεδομένων και δεν μπορεί να θεωρηθεί ότι έχει συναινέσει σε πρόδηλη δημοσιοποίηση αυτών των δεδομένων, διότι κάθε φορά που θα πρέπει να εγκατασταθεί κάποιο τεχνικό μέσο, αυτές οι πληροφορίες ζητούνται και θεωρούνται απαραίτητες για την είσοδο στην εκάστοτε ιστοσελίδα ή πλατφόρμα.

#### **4.5.3 Απάντηση του τρίτου, τέταρτου και πέμπτου προδικαστικού ερωτήματος**

Με το τρίτο, τέταρτο και πέμπτο προδικαστικό ερώτημα, ουσιαστικά το δικαστήριο, ζητά να υπάρξει διευκρίνιση του περιεχομένου του άρθρου 6 παρ.1 και στοιχεία β' γ' δ' ε' και στ' του GDPR, αναφορικά με το πεδίο εφαρμογής και των δικαιολογητικών λόγων της επεξεργασίας, που προβλέπονται από τις διατάξεις. Σύμφωνα με το άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, υπάρχει δυνατότητα, η επεξεργασία των δεδομένων να είναι σύνομη, εφόσον ισχύει κάποια από τις έξι προϋποθέσεις που προβλέπονται στη διάταξη. Επιπρόσθετα, σύμφωνα με τη νομολογία του δικαστηρίου, προβλέπονται τρεις οριστικές προϋποθέσεις, έτσι ώστε η επεξεργασία προσωπικών δεδομένων να είναι σύνομη.<sup>173</sup>

Αρχικά θα πρέπει να επιδιώκεται το έννομο συμφέρον του υπεύθυνου επεξεργασίας, διότι σε αυτόν γνωστοποιούνται τα προσωπικά δεδομένα. Έπειτα, θα πρέπει να εκτιμηθεί η αναγκαιότητα αυτής της επεξεργασίας, έτσι ώστε να επιτευχθεί ο επιδιωκόμενος κάθε φορά σκοπός, με βάση το νόμο και τρίτον, είναι πολύ

---

<sup>172</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionid=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

<sup>173</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionid=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

σημαντική προϋπόθεση ότι προέχουν τα δικαιώματα και ελευθερίες του υποκειμένου των δεδομένων.<sup>174</sup>

Συμπερασματικά, οι απαντήσεις που μπορούν να δοθούν στο τρίτο, τέταρτο και πέμπτο προδικαστικό ερώτημα, είναι ότι το άρθρο 6 παρ. 1 στοιχείο β' γ' δ' ε' και στ' έχει την έννοια ότι η συγκεκριμένη συμπεριφορά και πρακτική είναι δυνατόν να είναι σύμφωνη με το νόμο και με τις διατάξεις, εφόσον πληρούνται οι προϋποθέσεις, οι οποίες προβάλλονται, από τον υπεύθυνο επεξεργασίας.

Ειδικότερα, εάν αυτή η πρακτική είναι αναγκαία, προκειμένου να παρασχεθούν όλες οι υπηρεσίες, οι οποίες προσφέρονται από το λογαριασμό του Facebook, εφόσον είναι αναγκαία για την επίτευξη του εννόμου συμφέροντος, πρέπει να πληρούνται οι σωρευτικές τρεις προϋποθέσεις, οι οποίες αναπτύχθηκαν ανωτέρω και τέλος, εάν αυτή η επεξεργασία είναι αναγκαία, προκειμένου να ικανοποιηθούν νόμιμα αιτήματα παροχής δεδομένων, έτσι ώστε να καταπολεμηθούν συμπεριφορές και πρακτικές επιζήμιες, ή για την προώθηση της ασφάλειας και την ενίσχυση της ακεραιότητας, τότε μόνο η συμπεριφορά είναι δυνατόν να είναι σύννομη.<sup>175</sup>

#### **4.5.4 Απάντηση του έκτου προδικαστικού ερωτήματος**

Στο έκτο προδικαστικό ερώτημα, αναφορικά με το κύρος της συγκατάθεσης της δήλωσης, θα πρέπει, κάθε φορά, αυτό να εξετάζεται υπό το πρίσμα όλων των παραγόντων της συγκεκριμένης περίπτωσης, καθώς και από το βάρος αποδείξεως ότι το υποκείμενο των δεδομένων ή ο χρήστης, τα έχει παράσχει ρητά και ελεύθερα.

Η απάντηση, λοιπόν, που δίνεται είναι ότι το άρθρο 6 παρ. 1 στοιχείο α' και το άρθρο 9 παρ. 2 στοιχείο α' του Κανονισμού, έχουν την έννοια ότι δε γίνεται η επιχείρηση να καταστήσει άκυρη τη συγκατάθεσή του χρήστη, αναφορικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, κατά το άρθρο 4 στοιχείο 11 του Κανονισμού. Ωστόσο, κατά την εκτίμηση του ελεύθερου χαρακτήρα της

---

<sup>174</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionid=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

<sup>175</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionid=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

συγκατάθεσης, ο υπεύθυνος επεξεργασίας οφείλει να αποδείξει οποιαδήποτε πρακτική του εις βάρος του υποκειμένου των δεδομένων.<sup>176</sup>

#### 4.5.5 Απάντηση του εβδόμου προδικαστικού ερωτήματος

Επί του εβδόμου προδικαστικού ερωτήματος, η απάντηση που προκύπτει από την ανάλυσή του, στηρίζεται στο ότι, παρά το γεγονός ότι η αρχή του Ανταγωνισμού δεν έχει την αρμοδιότητα διαπίστωσης της παράβασης των κανόνων του GDPR, ωστόσο αυτό δεν σημαίνει ότι δεν μπορεί παρεμπιπτόντως να λειτουργήσει ελεγκτικά, με βάση το άρθρο 102 ΣΛΕΕ και το άρθρο 5 πρώτο εδάφιο του Κανονισμού ΕΚ αρ. 1/2003. Είναι ιδιαίτερα σημαντικό να τονιστεί, ότι κάθε φορά θα πρέπει να λαμβάνει χώρα αξιολόγηση, ως προς τη συμπεριφορά της αρχής αλλά και τον σκοπό αυτού του ελέγχου, που στη συγκεκριμένη περίπτωση είναι υγιής ανταγωνισμός και δεν έχει καταχρηστικό χαρακτήρα.<sup>177</sup>

Επομένως, έλεγχος κατάχρησης της δεσπόζουσας θέσης μιας επιχείρησης μπορεί να δικαιολογήσει τη συμπεριφορά της αρχής Ανταγωνισμού, εφόσον λειτουργεί παρεμπιπτόντως, με τη διευκρίνιση όμως, ότι δεν προδικάζει την εφαρμογή του Κανονισμού από τις αρμόδιες αρχές που ασκούν την εποπτική αρμοδιότητα.<sup>178</sup>

Ως προς το β' στοιχείο του εβδόμου προδικαστικού ερωτήματος, θα πρέπει να τονιστεί ότι η εποπτική αρχή και η αρχή Ανταγωνισμού, θα πρέπει να βρίσκονται σε συνεχή συνεργασία και να τηρούν τις αρχές της ισοδυναμίας και της αποτελεσματικότητας.<sup>179</sup>

---

<sup>176</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionId=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

<sup>177</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionId=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

<sup>178</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionId=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

<sup>179</sup>,<sup>180</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionId=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

Στην υπό κρίση περίπτωση το Bundeskartellamt κίνησε τη διαδικασία συνεργασίας με τις αρμόδιες αρχές εποπτείας και επικοινωνήσε με την εποπτική αρχή της Ιρλανδίας και επομένως, η πρώτη εκπλήρωσε τις υποχρεώσεις, τόσο της καλόπιστης συνεργασίας, όσο και της επιμέλειας.

Το συμπέρασμα από αυτό είναι ότι τα άρθρα 51 έως 66 του GDPR, συνάδουν με τη συμπεριφορά αυτή, διότι μία αρχή Ανταγωνισμού μπορεί να εξετάζει παρεμπιπτόντως, εάν οι πρακτικές της επιχείρησης τηρούν τους κανόνες του GDPR, φυσικά, λαμβάνοντας υπόψη αποφάσεις ή έρευνες των αρμοδίων εποπτικών αρχών, όπως ισχύει με βάση τον Κανονισμό και ενημερώνοντας κάθε φορά, την εποπτική αρχή και συνεργαζόμενη με αυτήν.<sup>180</sup>

#### **4.6 Προτάσεις του γενικού εισαγγελέα Α. Ράντου**

Κατά τον γενικό εισαγγελέα Α. Ράντο, μία αρχή Ανταγωνισμού μπορεί να ελέγχει και να λαμβάνει υπ' όψιν, κατά πόσο μία εμπορική πρακτική δεν παραβιάζει τον Γενικό Κανονισμό για την Προστασία των Δεδομένων, αλλά παράλληλα, είναι υποχρεωμένη να λαμβάνει υπ' όψιν, αποφάσεις ή έρευνες της εποπτικής αρχής, όπως ορίζεται από τον Κανονισμό.<sup>181</sup>

Οι προτάσεις αυτές, αφορούν την υπόθεση C-252/21, για την υπόθεση “Meta Platforms” και τους γενικούς όρους χρήσης των κοινωνικών δικτύων. Ειδικότερα, οι προτάσεις του επικεντρώνονται σε τέσσερα βασικά σημεία.<sup>182</sup>

Αρχικά, ο γενικός εισαγγελέας Ράντος, επικεντρώνεται στο γεγονός ότι μία αρχή Ανταγωνισμού, παρότι δεν είναι αρμόδια για να διαπιστώνει παραβάσεις στο Γενικό Κανονισμό Προστασίας Δεδομένων, μπορεί ωστόσο, να λαμβάνει υπ' όψιν, εάν μία εμπορική πρακτική ταιριάζει με τις διατάξεις του.

Επιπλέον, τονίζει το γεγονός ότι εάν μία εμπορική πρακτική δεν συνάδει με τις αρχές GDPR, ίσως να αποτελεί στοιχείο ότι παραβιάζει και τις αρχές του κανόνων του Ανταγωνισμού. Διευκρινίζει λοιπόν, ότι μία αρχή Ανταγωνισμού, μπορεί να

---

<sup>181</sup> <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220158e1.pdf>

<sup>182</sup> <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220158e1.pdf>

ασκεί αυτή την αρμοδιότητα παρεμπιπτόντως<sup>183</sup> και όχι κυρίως, υπό την επιφύλαξη ωστόσο, των εξουσιών της εποπτικής αρχής, όπως ορίζονται από τον Κανονισμό, αλλά και να λαμβάνει υπ' όψιν τις πράξεις της εποπτικής αρχής και να τηρεί τις αρχές της συνεργασίας και της επικοινωνίας με αυτήν.<sup>184</sup>

Η δεύτερη πρόταση αφορά την έννοια της συγκατάθεσης του χρήστη της πλατφόρμας, αναφορικά με την επεξεργασία των προσωπικών του δεδομένων.<sup>185</sup> Ειδικότερα, διευκρινίζει ότι το γεγονός πως μία επιχείρηση έχει δεσπίζουσα θέση στην αγορά, δεν σημαίνει ότι θίγεται το κύρος της συγκατάθεσης της δήλωσης του χρήστη στην επεξεργασία των προσωπικών του δεδομένων, αλλά σε κάθε περίπτωση, οφείλει ο υπεύθυνος επεξεργασίας να αποδείξει αυτή την περίσταση (άρ.6 παρ. 1 στοιχείο α και άρθρο 9 παρ. 2 στοιχεία α του GDPR).<sup>186187</sup>

Τρίτον, ο γενικός εισαγγελέας, αναφερόμενος στις πρακτικές της Meta Platforms, εκτιμά ότι υπάρχουν δικαιολογητικοί λόγοι και βάσεις, οι οποίοι δικαιολογούν την επεξεργασία των προσωπικών δεδομένων των χρηστών, χωρίς τη συγκατάθεσή τους, μόνο εφόσον είναι αναγκαίο για την ασφάλεια του δικτύου ή τη βελτίωση των προϊόντων, εφόσον αυτό είναι προς το όφελος του χρήστη. Ωστόσο, στη συγκεκριμένη περίπτωση κάτι τέτοιο δεν ισχύει. (άρ. 6 παρ.1 στοιχεία β', γ', δ,' ε' και στ')

Τέταρτον, ο γενικός εισαγγελέας διευκρινίζει το θέμα, αναφορικά με τα «ευαίσθητα» προσωπικά δεδομένα των χρηστών, τα οποία συλλέγονται και επεξεργάζονται από την πλατφόρμα.<sup>188</sup>

Τονίζει ότι στην πραγματικότητα, καθίσταται δυνατή η κατάρτιση προφίλ με βάση αυτά τα προσωπικά δεδομένα, τα οποία καλούνται ως «ευαίσθητα», πράγμα το οποίο απαγορεύει το GDPR, με μόνη την εξαίρεση ότι ο χρήστης θα πρέπει να

---

<sup>183</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionid=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

<sup>184</sup> <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220158el.pdf>

<sup>185</sup> <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220158el.pdf>

<sup>186</sup> <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220158el.pdf>

<sup>187</sup><https://curia.europa.eu/juris/document/document.jsf?jsessionid=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

<sup>188</sup> <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220158el.pdf>

γνωρίζει πλήρως και με ρητή του πράξη ότι δημοσιεύει δεδομένα, τα οποία είναι προσωπικά, με την είσοδό του σε πλατφόρμες και την εγγραφή του σε ιστοσελίδες.<sup>189</sup> Σε κάθε περίπτωση, ο γενικός εισαγγελέας εκτιμά ότι η επίσκεψη σε σελίδες δεν συνιστά συμπεριφορά, η οποία μπορεί να εξομοιωθεί με προδήλως δημοσιοποίηση «ευαίσθητων» προσωπικών δεδομένων από το χρήστη ή με ρητή συγκατάθεσή του.<sup>190</sup> (άρ. 9 παρ. 2 στοιχείο ε').<sup>191</sup>

---

<sup>189</sup> <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220158el.pdf>

<sup>190</sup> <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220158el.pdf>

<sup>191</sup> <https://curia.europa.eu/juris/document/document.jsf?jsessionid=F8BD0AEE52A9EE3064962FD8010D3326?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=59126>

## ΚΕΦΑΛΑΙΟ 5

### Η Γερμανική Υπόθεση Facebook- C-252/21 και η ανάλυσή της υπό το πρίσμα του Δικαίου του Ανταγωνισμού

#### 5.1 Η σχετική αγορά στην υπόθεση Facebook

Ο FCO επεξεργάστηκε το θέμα της σχετικής αγοράς μεγάλη λεπτομέρεια. Ο Γερμανός νομοθέτης του 2016, ήδη από τότε, προσπάθησε να αντιμετωπίσει τα νέα ζητήματα που προκύπτουν στην ψηφιακή οικονομία και υποχρεώθηκε να λάβει υπ' όψιν όλους αυτούς, τους πρώτους παράγοντες των πολύπλευρων αγορών δικτύου στην ψηφιακή οικονομία.<sup>192</sup>

Έτσι, τις καθόρισε ως άμεσες και έμμεσες επιδράσεις δικτύου, όσες αγορές έχουν κόστος πολλαπλής έδρας και μεταγωγής, όσες αποτελούν οικονομίες κλίμακας και αφορούν την πρόσβαση της δεσπόζουσας επιχείρησης σε δεδομένα σχετικά με τον Ανταγωνισμό, αλλά και αυτές που έχουν ανταγωνιστική πίεση, με γνώμονα την καινοτομία.<sup>193</sup>

Επιπλέον, ο FCO χρησιμοποίησε τον όρο της υποκατάστασης, από την πλευρά της ζήτησης, χρησιμοποιώντας την ως βάση, για τον ορισμό της αγοράς κάποιου προϊόντος.

Ειδικότερα, αναφορικά με την πλατφόρμα του Facebook, ο FCO προσδιόρισε δύο ομάδες χρηστών της πλατφόρμας. Αρχικά, τους ιδιωτικούς χρήστες και τους επιχειρηματίες. Καθεμία κατηγορία εκ των δύο, χρησιμοποιεί το δίκτυο για διαφορετικό σκοπό. Οι πρώτοι, με σκοπό την επικοινωνία και την ενημέρωση, ενώ οι δεύτεροι, με σκοπό το οικονομικό κέρδος από τις διαφημίσεις.<sup>194</sup>

Κατέληξε στο συμπέρασμα ότι οι και οι δύο πλευρές είχαν διαφορετικά συμφέροντα και ότι η πλατφόρμα απέκτησε μεγαλύτερη ισχύ για τους διαφημιστές,

---

<sup>192</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

<sup>193</sup> Anne C. Witt, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law

<sup>194</sup> Anne C. Witt, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law

αναλογικά με τον αριθμό των ιδιωτικών χρηστών της πλατφόρμας. Εν συνεχεία, ο FCO, εξέτασε το δίκτυο του Facebook να υπόκειται στους κανόνες του Ανταγωνισμού, λόγω του ότι ήταν διαθέσιμο σε πολλούς χρήστες σε όλο τον κόσμο, χωρίς να υπάρχει κανένα χρηματικό κόστος και κατέληξε στο συμπέρασμα ότι όντως, υπόκειται στους κανόνες του Ανταγωνισμού.<sup>195</sup>

Επιπρόσθετα, χρησιμοποιώντας την παραδοσιακή τιμή του SNIPP test, αξιολόγησε τη δυνατότητα υποκατάστασης άλλων υπηρεσιών κοινωνικής δικτύωσης, πέραν του Facebook και κατέληξε στο συμπέρασμα ότι η αγορά για τα κοινωνικά δίκτυα ήταν διαφορετική, από άλλες υπηρεσίες που πρόσφεραν παρόμοιους σκοπούς λειτουργίας και εμπειρίες.<sup>196</sup>

## 5.2 Η καταχρηστική εκμετάλλευση δεσπόζουσας θέσης

### 5.2.1 Νομικό Πλαίσιο

Ο νόμος 703/1977 αφορά τον έλεγχο των μονοπωλίων, αλλά και των ολιγοπωλίων και το περιεχόμενό του, έχει ως κεντρική έννοια την προστασία του ελεύθερου ανταγωνισμού. Ο συγκεκριμένος νόμος αντικατέστησε το άρθρο 1 παρ. 1 του ν. 3959/2011, αναφορικά με τις πρακτικές, οι οποίες είχαν ως σκοπό την παρεμπόδιση, τον περιορισμό ή τη νόθευση του Ανταγωνισμού.<sup>197 198</sup>

Στις παραγράφους 1, 2 και 3 του νόμου 3959/2011, γίνεται εκτενής αναφορά στην καταχρηστική εκμετάλλευση δεσπόζουσας θέσης, ενώ στο άρθρο 101 παρ. 1 ΣΛΕΕ και 102 ΣΛΕΕ, έχουν τέτοιο περιεχόμενο, ωστόσο υπό το πρίσμα των ευρωπαϊκών διατάξεων.<sup>199</sup>

Το άρθρο 2 του νόμου 3959/2011 απαγορεύει την καταχρηστική εκμετάλλευση δεσπόζουσας θέσης, με τις μορφές και τις εκφάνσεις που μπορεί να

---

<sup>195</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

<sup>196</sup> Anne C. Witt, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law

<sup>197</sup> Τζουγανάτος Δ., Δίκαιο του Ελεύθερου Ανταγωνισμού, Νομική Βιβλιοθήκη, Αθήνα, 2020

<sup>198</sup> Τριανταφυλλάκης Γ., Δίκαιο του Ελεύθερου Ανταγωνισμού, Αθήνα, 2019

<sup>199</sup> [https://curia.europa.eu/juris/document/document\\_print.jsf;jsessionid=9ea7d2dc30dd837ad3b01545491499c2cdd5d24daad3.e34KaxiLc3qMb40Rch0SaxuNbxfo?doclang=EL](https://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d2dc30dd837ad3b01545491499c2cdd5d24daad3.e34KaxiLc3qMb40Rch0SaxuNbxfo?doclang=EL)



έχει, είτε μέσω της άμεσης ή έμμεσης επιβολής τιμών στην αγορά, ή τον περιορισμό της παραγωγής, ή την εφαρμογή άνισων όρων για ισοδύναμες παροχές και όλα όσα προβλέπονται στο άρθρο 102 ΣΛΕΕ.<sup>200</sup>

Επιπρόσθετα, τίθενται κυρώσεις, σε περιπτώσεις που παραβιάζεται το δίκαιο του Ελεύθερου Ανταγωνισμού, όπως προβλέπεται από το παρόν νομοθετικό πλαίσιο.<sup>201</sup>

### 5.2.2 Η έννοια της κατάχρησης

Με βάση τη νομική προσέγγιση, μία επιχείρηση με δεσπόζουσα θέση απολαμβάνει μεγάλης οικονομικής δύναμης, που την καθιστά ικανή να λειτουργεί στην αγορά ανεξάρτητα, αλλά και να παρακωλύει τη διατήρηση αποτελεσματικού ανταγωνισμού.<sup>202</sup> Παράλληλα, με βάση την οικονομική προσέγγιση, η δύναμη αυτής της αγοράς αντιστοιχεί σε μονοπωλιακή δύναμη. Το γεγονός ότι μία επιχείρηση, ή μία ένωση επιχειρήσεων έχει τη δυνατότητα για μία μεγάλη χρονική περίοδο να καθορίσει τιμές στην αγορά πάνω από το ανταγωνιστικό επίπεδο, υποδηλώνει κατά την οικονομική προσέγγιση, ύπαρξη δεσπόζουσας θέσης<sup>203</sup>.

Οι παράγοντες για την θεμελίωσή της είναι τα μερίδια αγοράς, τα εμπόδια εισόδου στην αγορά, ο βαθμός της συγκέντρωσης κ.ά. Οι επιχειρήσεις, οι οποίες κατέχουν δεσπόζουσα θέση στην αγορά έχουν ιδιαίτερη ευθύνη (special responsibility) να μη νοθεύουν με πρακτικές τους τον ανταγωνισμό. Αυτό σημαίνει δηλαδή, ότι η δεσπόζουσα θέση καθαυτή, δε σημαίνει απαραίτητα ότι λειτουργεί καταχρηστικά.<sup>204</sup>

Επίσης αυτή η υποχρέωση, όπως κατανοούμε, δεν υφίσταται για τις επιχειρήσεις, οι οποίες δεν κατέχουν δεσπόζουσα θέση στην αγορά. Παράλληλα, μία επιχείρηση με μεγάλο μερίδιο στην αγορά, η οποία κατέχει δεσπόζουσα θέση έχει την υποχρέωση και το δικαίωμα να διαφυλάσσει όλα τα συμφέροντά της όταν τίθενται

---

<sup>200</sup>[https://curia.europa.eu/juris/document/document\\_print.jsf;jsessionid=9ea7d2dc30dd837ad3b01545491499c2cdd5d24daad3.e34KaxiLc3qMb40Rch0SaxuNbxfo?doclang=EL](https://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d2dc30dd837ad3b01545491499c2cdd5d24daad3.e34KaxiLc3qMb40Rch0SaxuNbxfo?doclang=EL)

<sup>201</sup> Τζουγανάτος Δ., Δίκαιο του Ελεύθερου Ανταγωνισμού, Νομική Βιβλιοθήκη, Αθήνα, 2020

200-205 Δρ. Παναγιώτης Αγησιλάου, Καταχρηστική Εκμετάλλευση Δεσπόζουσας θέσης, Επιμορφωτικό Σεμινάριο ΚΕΒΕ, 18 Μαρτίου 2021-Μέρος Β.

υπό απειλή. Δηλαδή, μπορεί να προβαίνει σε πρακτικές που κρίνει κατάλληλες και πρόσφορες, έτσι ώστε να προστατεύσει τα συμφέροντά της, χωρίς όμως αυτές να αποσκοπούν στην ενίσχυση της θέσης της και κατ' επέκταση στην καταχρηστική εκμετάλλευσή της.<sup>205</sup>

Η έννοια της κατάχρησης είναι αντικειμενική και αυτό που ενδιαφέρει την θεωρία είναι τα ενδεχόμενα αποτελέσματά της, δηλαδή, δεν απαιτείται η ύπαρξη προθέσεως, προκειμένου αυτή να αποδειχθεί εμπράκτως. Ωστόσο, τα στοιχεία που δείχνουν ότι υπάρχει δόλος λαμβάνονται υπ' όψιν, ως προς τον υπολογισμό του προστίμου.<sup>206</sup>

Επιπρόσθετα, με βάση την οικονομοκεντρική προσέγγιση<sup>207</sup>, η θεωρία εστιάζει περισσότερο στην ανταγωνιστική ζημιά (competitive harm) και όχι τόσο πολύ στον τύπο παράβασης. Επιπλέον, εστιάζει στις θεωρίες ανταγωνιστικής ζημιάς (theories of harm) και στα σχετικά έγγραφα. Έτσι, με βάση τους τύπους των καταχρηστικών πρακτικών, διακρίνουμε σε τιμολογιακές και μην τιμολογιακές καταχρήσεις. Ενδεικτικά αναφέρουμε τη ληστρική υποτιμολόγηση (predatory pricing), την υπερβολική τιμολόγηση (excessive pricing) και τη διακριτική τιμολόγηση (price discrimination). Ενώ στις μη τιμολογιακές, αναφέρονται η άρνηση/διακοπή προμήθειας (refusal to deal/supply), οι αθέμιτοι όροι συναλλαγής κ.ά. Επιπλέον οι καταχρηστικές πρακτικές, διακρίνονται σε εκμεταλλευτικές πρακτικές, όπως είναι ο άμεσος επηρεασμός των συμφερόντων καταναλωτών ή άλλων επιχειρήσεων.<sup>208</sup>

### **5.2.3 Η πρακτική της καταχρηστικής εκμετάλλευσης στην υπόθεση Facebook**

Σύμφωνα με όσα αναφέρθηκαν στην παραπάνω ενότητα, αναφορικά με την κυριαρχία μιας επιχείρησης στην αγορά και την κατοχή της δεσπόζουσας θέσης, θα

---

<sup>207</sup> Τριανταφυλλάκης Γ., Δίκαιο του Ελεύθερου Ανταγωνισμού, Αθήνα, 2019

<sup>208</sup> Δρ. Παναγιώτης Αγησιλάου, Καταχρηστική Εκμετάλλευση Δεσπόζουσας θέσης, Επιμορφωτικό Σεμινάριο ΚΕΒΕ, 18 Μαρτίου 2021-Μέρος Β.

πρέπει να αναφερθούμε στην πλατφόρμα του Facebook, η οποία στην πραγματικότητα είναι μία κυρίαρχη εταιρεία στην αγορά.<sup>209</sup>

Είναι μία επιχείρηση με δεσπόζουσα θέση στην αγορά κοινωνικών δικτύων για ιδιωτικούς χρήστες. Σύμφωνα με το άρθρο 18 παρ. 1 σε συνδυασμό με τα 3 και 3α GWB και σύμφωνα με όλους τους παράγοντες, οι οποίοι αναλύθηκαν παραπάνω, αναφορικά με τις προϋποθέσεις για την κατοχή δεσπόζουσας θέσης, η εταιρεία έχει πραγματικό πεδίο δράσης στην αγορά και είναι ιδιαίτερα ανταγωνιστική.<sup>210</sup>

Επιπλέον, το Bundeskartellamt προχώρησε σε έλεγχο του μεριδίου αγοράς της επιχείρησης του Facebook στη σχετική αγορά, το οποίο αποδείχθηκε ότι είναι πολύ υψηλό σε ποσοστά αγοράς άνω του 95% των καθημερινών ενεργών χρηστών, το μερίδιο αγοράς μεταξύ των μηνιαίων ενεργών χρηστών είναι άνω του 80% και μεταξύ των εγγεγραμμένων χρηστών άνω του 50%.<sup>211</sup>

Θεωρεί λοιπόν, το Bundeskartellamt ότι η επιχείρηση του Facebook έχει πολύ υψηλά μερίδια στην αγορά και αυτό αποτελεί δείκτη, αναφορικά με την ανταγωνιστική σημασία του και την επιτυχία του κοινωνικού δικτύου, ως μέσου, λόγω της συχνότητας της χρήσης του από τους ιδιώτες.

Η αξιολόγηση αυτού του κριτηρίου έγινε σε συνδυασμό με τον χρόνο που δαπανάται στα μέσα κοινωνικής δικτύωσης από τους χρήστες, οι οποίοι με την δράση τους θεμελιώνουν τη δεσπόζουσα θέση της εταιρείας ως κυρίαρχο ανταγωνιστή στην αγορά. Το Facebook για λόγους ανταγωνισμού αγόρασε στο Instagram, έτσι ώστε να έχει ακόμη μεγαλύτερο μερίδιο στην αγορά, και τα δικά του οικονομικά στοιχεία αυξάνονται συνεχώς, ενώ των υπολοίπων μέσων κοινωνικής δικτύωσης, δεν είναι σε τόσο υψηλό επίπεδο, αλλά φθίνουν συγκριτικά.<sup>212</sup>

Επιπλέον, ένα άλλο σημείο, το οποίο αποτελεί παράγοντα καταχρηστικής εκμετάλλευσης δεσπόζουσας θέσης της πλατφόρμας του Facebook, είναι η χρηματοδότηση από άλλες εταιρίες για τη διαφήμιση, η οποία έχει ως αποτέλεσμα να

---

<sup>209</sup> Bundeskartellamt, Case Summary, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing, 15 February 2019

<sup>210</sup>[https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v=](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=)

<sup>211</sup> Bundeskartellamt, Case Summary, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing, 15 February 2019

<sup>212</sup>[https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v=](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=)

αυξάνονται τα εμπόδια εισόδου στην αγορά. Πιο συγκεκριμένα, οι πλατφόρμες, οι οποίες χρηματοδοτούνται από τη διαφήμιση, δεν επιτρέπουν με αυτό τον τρόπο σε άλλες ανταγωνιστικές επιχειρήσεις να εισέλθουν στην αγορά και να έχουν επιτυχίες για μεγάλο χρονικό διάστημα.<sup>213</sup>

Επιπρόσθετα, ένα ιδιαίτερα σημαντικό γεγονός είναι η ύπαρξη των πηγών δεδομένων, διότι το κοινωνικό δίκτυο χρησιμοποιεί προσωπικά δεδομένα, τα συλλέγει και επεξεργάζεται και τα τελευταία οδηγούν στην ύπαρξη μεγαλύτερου ανταγωνισμού στην αγορά, λόγω του εμποδίου εισόδου των άλλων πλατφορμών σε αυτή.

### **5.3 Η θεωρία της βλάβης (theory of harm) στα πλαίσια της αναλύσεως της γερμανικής υποθέσεως**

Το Bundeskartellamt κρίνει ότι η πρακτική του Facebook, αναφορικά με την παρακολούθηση των χρηστών, μέσω της συλλογής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα από άλλους ιστοτόπους ή εφαρμογές και εταιρικές υπηρεσίες, αποτελεί κατάχρηση της δεσπόζουσας θέσης της εταιρείας, αλλά και συγκέντρωση υπερβολικού όγκου δεδομένων στην πλατφόρμα του.

Η γερμανική αρχή διαπίστωσε ότι υπάρχουν αρκετοί διαφορετικοί τρόποι με τους οποίους τα δεδομένα διατίθενται, όπως για παράδειγμα μέσω της χρήσης ψηφιακών υπηρεσιών που ανήκουν στο Facebook, όπως είναι το Instagram ή το WhatsApp, είτε μέσω της συλλογής των δεδομένων που προκύπτουν από το “Facebook like”, τις κοινοποιήσεις (share), ακόμη και των πλήκτρων που επιλέγει να πατήσει ο χρήστης.<sup>214</sup>

Ειδικότερα, αυτή η παρακολούθηση της συμπεριφοράς συνδυάζει τα δεδομένα από όλες τις πλατφόρμες και δημιουργεί ένα συγκεκριμένο ολοκληρωμένο προφίλ του χρήστη, χωρίς να είναι απαραίτητο να συνδεθεί ο τελευταίος στην πλατφόρμα ή να είναι εγγεγραμμένος, διότι ακόμη και αν δεν είναι εγγεγραμμένος σε

---

<sup>213</sup> Bundeskartellamt, Case Summary, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing, 15 February 2019

<sup>214</sup> Viktoria H.S.E. Robertson (University of Graz), The Theory of Harm in the Bundeskartellamt's Facebook Decision, Edited by Thibault Schrepel, Sam Sadden & Jan Roth (CPI), Competition Policy International, Inc., March 2019

μία από αυτές, ίσως θα είναι σε κάποια από τις υπόλοιπες και επομένως, τα δεδομένα συλλέγονται και επεξεργάζονται κατά τον ίδιο τρόπο.

Βέβαια οι χρήστες δεν συμφωνούν με αυτή την πρόσβαση στα προσωπικά τους δεδομένα και η γερμανική αρχή θεωρεί ότι δεν υπάρχει συγκατάθεση των χρηστών. Το Bundeskartllamt θεωρεί ότι η επιχείρηση έχει ιδιαίτερη ευθύνη, λόγω της κυρίαρχης θέσης της στην αγορά, αναφορικά με αυτή την συμπεριφορά της για τα προσωπικά δεδομένα των χρηστών, αλλά και την αντιανταγωνιστική της πρακτική.

Επιπρόσθετα, η γερμανική αρχή υποστηρίζει την άποψη ότι στην περίπτωση του Facebook τίθεται ζήτημα, αναφορικά με την προστασία δεδομένων που τίθενται από τους κανονισμούς της Ευρωπαϊκής Ένωσης και πιο συγκεκριμένα, από τον κανονισμό του GDPR. Στηρίζει αυτή την άποψη, στο γεγονός ότι αυτή η κατάχρηση της δεσπόζουσας θέσης αφορά τους χρήστες, οι οποίοι δεν γνωρίζουν την τεράστια έκταση της παρακολούθησής τους, της συλλογής των προσωπικών δεδομένων μέσα στο διαδικτυακό ιστό, η οποία χρησιμοποιείται και εκμεταλλεύεται εμπορικά από την πλατφόρμα.<sup>215</sup>

Επιπλέον, υποστηρίζεται ότι στην πραγματικότητα οι χρήστες δεν έχουν συναινέσει για αυτή την εμπορική εκμετάλλευση των προσωπικών τους δεδομένων, με αποτέλεσμα την αύξηση των εσόδων της πλατφόρμας και την εμπορική της επιτυχία, η οποία την καθιερώνει στην αγορά, ενισχύει την κυρίαρχη θέση της και είναι πλέον δεσπόζουσα σε αυτή.

Σε αυτήν την ανισορροπία, η γερμανική αρχή αναφέρεται σε εκμεταλλευτική κατάχρηση, ενώ παράλληλα, κάνει αναφορά στο άρθρο 102 ΣΛΕΕ και στις περιπτώσεις απαγόρευσης. Το δικαστήριο της Ευρωπαϊκής Ένωσης έκρινε ότι όλοι οι όροι θα πρέπει να αναφέρονται στους χρήστες, ενώ η Ευρωπαϊκή Επιτροπή θεωρεί ότι μία εταιρεία με δεσπόζουσα θέση, θα πρέπει να ακολουθεί την αρχή της αναλογικότητας στους όρους της, έτσι ώστε αυτοί να συνάδουν με το άρθρο 102 ΣΛΕΕ.<sup>216</sup>

---

<sup>215</sup> Viktoria H.S.E. Robertson (University of Graz), The Theory of Harm in the Bundeskartellamt's Facebook Decision, Edited by Thibault Schrepel, Sam Sadden & Jan Roth (CPI), Competition Policy International, Inc., March 2019

<sup>216</sup> Viktoria H.S.E. Robertson (University of Graz), The Theory of Harm in the Bundeskartellamt's Facebook Decision, Edited by Thibault Schrepel, Sam Sadden & Jan Roth (CPI), Competition Policy International, Inc., March 2019

#### **5.4 Η σχέση μεταξύ Δικαίου Ανταγωνισμού και του Νόμου για την προστασία των προσωπικών δεδομένων**

Ο FCO έκρινε ότι ο κανονισμός GDPR δεν αντικατέστησε τους κανόνες του Ανταγωνισμού, για τους λόγους που πρόκειται να αναφερθούν παρακάτω.

Αρχικά, ο Κανονισμός GDPR δεν περιέχει κάποια διάταξη, η οποία να κινείται προς τέτοιο αποκλεισμό. Επιπρόσθετα, αρκετές υπηρεσίες προστασίας δεδομένων προσωπικού χαρακτήρα υποστήριξαν με έντονο τρόπο, την εφαρμογή των κανόνων Ανταγωνισμού για σκοπούς της προστασίας, ενώ παράλληλα, η τροποποίηση του 2016 της GWB, έκανε σαφές ότι ο Γερμανός νομοθέτης θεωρούσε την πρόσβαση στα δεδομένα πολύ σημαντικό παράγοντα για την αξιολόγηση του ίδιου του Δικαίου του Ανταγωνισμού.<sup>217</sup>

Επιπλέον, έτσι ώστε να μην υπάρχουν κίνδυνοι σύγκρουσης των ερμηνειών, είχε διαβουλευθεί με τις αντίστοιχες γερμανικές αρχές, σε όλη τη διάρκεια της διαδικασίας, προκειμένου να διευκολυνθεί η επιβολή του νόμου περί Ανταγωνισμού στην ψηφιακή οικονομία.<sup>218</sup>

#### **5.5 Εξέταση πτυχών της προστασίας δεδομένων**

Σύμφωνα με το άρθρο 61 του GDPR, το Facebook, δεν είναι ανάγκη να επεξεργάζεται τα προσωπικά δεδομένα, προκειμένου να εκπληρώσει τη σύμβασή του. Αυτή το γεγονός θα πρέπει να ερμηνεύεται στενά, διότι η επιχείρηση του Facebook, δεν μπορεί να δικαιούται απεριόριστα την επεξεργασία δεδομένων, αποκλειστικά και

---

<sup>217</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

<sup>217</sup> Anne C. Witt, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law

<sup>218</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

<sup>218</sup> Anne C. Witt, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law

μόνο, για τους λόγους του επιχειρηματικού τους μοντέλου, αλλά και των ιδιοτήτων του προϊόντος που παρέχει, ή των υπηρεσιών που παρέχει στην ψηφιακή αγορά.<sup>219</sup>

Κάθε επεξεργασία προσωπικών δεδομένων θα πρέπει να κρίνεται απαραίτητη για την εκπλήρωση της σύμβασης, καθώς κάθε πληροφορία, η οποία αντλείται από την πλατφόρμα, αποτελεί στοιχεία κάθε μεμονωμένου χρήστη και η επεξεργασία από πηγές τρίτων, επίσης θα πρέπει να ερμηνευθεί στενά.<sup>220</sup>

Το ίδιο συμβαίνει και για την επεξεργασία των δεδομένων από υπηρεσίες τρίτων ή μέσω της διαφήμισης. Καμία από τις διατάξεις του άρθρου 61 γ' έως ε' του GDPR, που εφαρμόζεται, δεν μπορεί να δικαιολογήσει την επεξεργασία των δεδομένων για ειδικούς σκοπούς.<sup>221</sup>

## 5.6 Συμβατότητα με τις αξίες του GDPR

Ο FCO αξιολόγησε, εάν η συλλογή και η επεξεργασία δεδομένων προσωπικού χαρακτήρα από το Facebook και η πολιτική αυτής ήταν συμβατή με τις αξίες του GDPR.

Ειδικότερα, ο FCO πραγματοποίησε μία πολύ λεπτομερή νομική ανάλυση, αναφορικά με τα άρθρα 6 και 9 του GDPR και διαπίστωσε ότι το Facebook επεξεργαζόταν και δημιουργούσε προφίλ των χρηστών της πλατφόρμας του, καταπατώντας τα δικαιώματά τους.<sup>222</sup>

Πιο συγκεκριμένα, συνέβη παραβίαση του άρθρου 4 GDPR και το 9 παρ.1 του Κανονισμού. Ωστόσο, το Facebook, χρησιμοποίησε ως δικαιολογητικούς λόγους, αναφορικά με αυτό το γεγονός, την αναγκαιότητα και το αναγκαίο συμφέρον, από τον Κανονισμό. Ο FCO κατέληξε στο συμπέρασμα ότι καμία από αυτές τις αιτιολογίες στην πραγματικότητα δεν υφίσταται.<sup>223</sup>

---

<sup>219</sup>[https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v=](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=)

<sup>220</sup>[https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v=](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=)

<sup>221</sup>[https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v=](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=)

<sup>222</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

<sup>222</sup> Anne C. Witt, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law

<sup>223</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

## 5.7 Η συγκατάθεση των χρηστών της πλατφόρμας

Ο FCO κατέληξε στο συμπέρασμα ότι οι χρήστες της πλατφόρμας Facebook δεν είχαν ουσιαστικά, συναίνεση για την συλλογή και την επεξεργασία των προσωπικών δεδομένων των χρηστών, διότι η συγκεκριμένη συγκατάθεση δεν δόθηκε ελεύθερα, όπως προβλέπεται στο άρθρο 4 παράγραφος 11 του GDPR.<sup>224</sup>

Δηλαδή, βασίστηκε στο γεγονός ότι το υποκείμενο των δεδομένων δεν είχε πραγματική επιλογή, έτσι ώστε να καταφέρει να αρνηθεί τη συγκατάθεσή χωρίς να ζημιωθεί.<sup>225</sup>

### 5.7.1 Η παραβίαση της ιδιωτικότητας ως βλάβη των καταναλωτών- χρηστών της Πλατφόρμας του Facebook

Το δικαστήριο του Ντίσελντορφ και ο FCO, δεν συμφώνησαν, αναφορικά με το κατά πόσο υπήρξε παραβίαση της ιδιωτικής ζωής των καταναλωτών-χρηστών, αναφορικά με την συμπεριφορά του Facebook.<sup>226</sup>

Ούτε ο FCO, ούτε το δικαστήριο του Ντίσελντορφ καθόρισε την έννοια της βλάβης, ωστόσο, το συμπέρασμα είναι ότι οι χρήστες ζημιώθηκαν. Σύμφωνα με το FCO, το Facebook έχει βλάψει τους χρήστες, παραβιάζοντας το δικαίωμα στην ιδιωτικότητα και όλες τις αρχές που εγγυάται το γερμανικό Σύνταγμα, ο GDPR και ο Χάρτης των θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.<sup>227</sup>

Ωστόσο, το δικαστήριο του Ντίσελντορφ διαφώνησε, διότι θεώρησε ότι οι καταναλωτές δεν είχαν υποστεί συγκεκριμένη βλάβη, ούτε οικονομική ζημιά. Επιπρόσθετα, υποστήριξε ότι οι χρήστες δεν είχαν χάσει τον έλεγχο των προσωπικών τους δεδομένων, επειδή πρόθυμα συμφώνησαν με τους όρους και τις προϋποθέσεις

---

<sup>223</sup> Anne C. Witt, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law

<sup>224</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

<sup>225</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

<sup>226</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>

<sup>227</sup> <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>



του Facebook ή ακόμη και για το γεγονός ότι δεν προχώρησαν στην ανάγνωση των συγκεκριμένων όρων πριν την εγγραφή ή τη σύνδεσή τους στην πλατφόρμα.<sup>228</sup>

### **5.8 Συμπεράσματα από την απόφαση**

Το GDPR, έχει απαγορεύσει τη συλλογή και επεξεργασία των προσωπικών δεδομένων από το Facebook προς στους χρήστες, αλλά και την εφαρμογή των όρων, με βάση τους κανονισμούς 19, 1 GWB.<sup>229</sup>

Επιπρόσθετα, διέταξε τον τερματισμό αυτής της συμπεριφοράς, ενώ παράλληλα, αυτή η απαγόρευση αναφέρεται, τόσο στα εργαλεία του Facebook, όσο και στα “cookies”.

Το Δικαστήριο του Ντίσελντορφ απαγόρευσε επίσης, την εφαρμογή των όρων και των προϋποθέσεων και διέταξε την πλατφόρμα να προχωρήσει σε άμεσες αλλαγές, μέσα σε μικρό χρονικό διάστημα. Το Facebook είχε λάβει προθεσμία τεσσάρων μηνών, προκειμένου να υλοποιήσει αυτές τις νέες αλλαγές. Η εταιρία προσέφυγε κατά της απόφασης στο Ανώτερο Περιφερειακό Δικαστήριο του Ντίσελντορφ και ζήτησε η απόφαση να έχει ανασταλτικό αποτέλεσμα.<sup>230</sup>

### **5.9 Σχολιασμός και αξιολόγηση της αποφάσεως**

Έπειτα από την εκτενή ανάλυση στο θέμα της παράβασης των προσωπικών δεδομένων, αλλά και τις πρακτικές καταχρηστικής εκμετάλλευσης δεσπόζουσας θέσης από την πλατφόρμα του Facebook, κατανοούμε ότι υπάρχει ανάγκη για μια ευρύτερη και πιο ολοκληρωμένη πολιτική.

Οι συνέπειες από σχέση μεταξύ των δύο πολιτικών και πιο συγκεκριμένα οι αυστηρή προσέγγιση δεν λειτουργεί σε ψηφιακές αγορές και έχει αρνητικές επιπτώσεις στην ιδιωτική ζωή. Τα αποτελέσματα από αυτή την αλληλεπίδραση, ίσως

---

<sup>228</sup> Anne C. Witt, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law

<sup>229</sup>[https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v=](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=)

<sup>230</sup>[https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v=](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=)

και να απαιτούν την χρήση διορθωτικών μέτρων και στις δύο πολιτικές.<sup>231</sup> Ο καλύτερος συνδυασμός διορθωτικών μέτρων αφορά την περισσότερη συνεργασία μεταξύ των δύο πολιτικών, αλλά και σε επίπεδο μεταρρυθμίσεων στους κανονισμούς προστασίας δεδομένων, αλλαγές στον νόμο περί ανταγωνισμού, δηλαδή η προσέγγιση να είναι πιο ολοκληρωμένη.<sup>232</sup>

Επιπλέον, με εξαίρεση το άρθρο 5 του DMA, οι αρχές της δεν φαίνεται να είναι περισσότερο ενσωματωμένες σε πιο συνεργατική αντίληψη πολιτικής. Από την άλλη πλευρά, η πρόταση CMA του Δεκεμβρίου του 2020, στο Ηνωμένο Βασίλειο, είναι σαφέστερη και συνεργάζεται ευκολότερα με άλλες πολιτικές.<sup>233</sup>

---

<sup>231</sup> Wolfgang Kerber & Karsten K. Zolna, *The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law*, University of Marburg

<sup>232</sup> [https://www.ucl.ac.uk/laws/sites/laws/files/kerber\\_zolna\\_2021\\_facebook\\_case\\_competition\\_law\\_data\\_protection\\_law\\_01.pdf](https://www.ucl.ac.uk/laws/sites/laws/files/kerber_zolna_2021_facebook_case_competition_law_data_protection_law_01.pdf)

<sup>233</sup> Wolfgang Kerber & Karsten K. Zolna, *The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law*, University of Marburg

## ΚΕΦΑΛΑΙΟ 6

### Η παραβίαση των προσωπικών δεδομένων στις πλατφόρμες

#### 6.1 Ψηφιακές πλατφόρμες και Δίκαιο του Ανταγωνισμού

Ήδη στις παραπάνω ενότητες, έχει γίνει πλήρης και εκτενής αναφορά σε όλα τα θέματα των προσωπικών δεδομένων, τόσο της προστασίας τους, όσο και των περιπτώσεων παραβίασής τους από τρίτους. Παράλληλα, έχει αναφερθεί ότι αυτές οι παραβιάσεις δεν αφορούν μόνο τον φυσικό χώρο, αλλά και τον χώρο του διαδικτύου, δηλαδή, τον κυβερνοχώρο.

Οι ψηφιακές πλατφόρμες, δημιουργούν ένα νέο σύστημα, το οποίο θα πρέπει να προστατεύεται σε πολύ μεγάλο βαθμό, διότι τα δεδομένα που υπάρχουν σε αυτές είναι πάρα πολλά και αφορούν εκατομμύρια χρήστες ανά τον κόσμο. Επιπλέον, οι ψηφιακές πληροφορίες, οι οποίες συλλέγονται μέσω των πλατφορμών, έχουν αποτελέσει την κινητήρια δύναμη για την ανάπτυξη της οικονομίας. Πρόκειται για την ψηφιακή οικονομία, η οποία στηρίζεται στην τεχνολογία.<sup>234</sup>

Γενικότερα, το διαδίκτυο ενώνει παγκοσμίως όλους τους χρήστες, ανεξάρτητα από το πραγματικό τόπο διαμονής τους και δημιουργεί μια επικοινωνία άμεση και πολύ αποτελεσματική. Είναι ωστόσο, πολύ σημαντικό να μπορέσουν να εφαρμοστούν όλοι οι κανόνες του Δικαίου του Ανταγωνισμού στο διαδίκτυο. Τίθεται λοιπόν το ερώτημα, εάν υπάρχει δυνατότητα της εφαρμογής των κανόνων του στις αγορές της λεγόμενης «Νέας Οικονομίας» (“New Economy”) ή εάν πρέπει να υπάρξουν τροποποιήσεις.<sup>235</sup>

Κατανοούμε λοιπόν, ότι υπάρχουν ιδιαίτερες δυσκολίες ως προς την εφαρμογή των κανόνων του Δικαίου του Ανταγωνισμού στις ηλεκτρονικές αγορές. Το δίκαιο του Ανταγωνισμού, αφορά ένα μεγάλο περιβάλλον αγοράς, στο οποίο οι χρήστες αλληλεπιδρούν, λειτουργούν αμφίδρομα, αλλά και έρχονται σε επαφή με τα αντικείμενα της οικονομίας, όπως είναι τα προϊόντα, η παροχή υπηρεσιών και γενικότερα όλα τα αγαθά.<sup>236</sup>

<sup>234</sup> Ιγγλεζάκης Ι., Το δίκαιο της ψηφιακής οικονομίας, Εκδόσεις Σάκκουλα, Αθήνα, 2022

<sup>235</sup> Μικρούλεα Α., «Ηλεκτρονικές αγορές μεταξύ επιχειρήσεων (B2B) και Δίκαιο Ανταγωνισμού», ΕΕμπΔ 4/2003

<sup>236</sup> Τριανταφυλλάκης Γ., «Δίκαιο του Ελεύθερου Ανταγωνισμού», Νομική Βιβλιοθήκη, 2014

Όπως ήδη γνωρίζουμε, το Δίκαιο του Ανταγωνισμού αφορά τη σχετική αγορά προϊόντων και υπηρεσιών, δηλαδή μία αγορά που περιλαμβάνει πλήθος αγαθών και υπηρεσιών, τα οποία παρουσιάζουν συγκεκριμένα χαρακτηριστικά, έτσι ώστε ο καταναλωτής να μπορεί να τα θεωρεί εναλλάξιμα, ή δυνάμενα υποκατάστασης.<sup>237</sup>

Στα πλαίσια αυτής της σχετικής αγοράς, γίνεται λόγος και για τη γεωγραφική αγορά, δηλαδή έναν τόπο, στον οποίο όλες οι επιχειρήσεις, οι οποίες ενδιαφέρονται να πουλήσουν τα σχετικά προϊόντα της επιχείρησής τους δρουν, υπό παρόμοιες και ομοιογενείς συνθήκες.

Ωστόσο δεν είναι εύκολο να προσδιοριστεί η ψηφιακή αγορά, δηλαδή μία αγορά προϊόντων και υπηρεσιών, η οποία δρα και λειτουργεί στο διαδίκτυο, δημιουργώντας τη λεγόμενη «Ψηφιακή Οικονομία». Είναι δύσκολο να προσδιοριστεί αυτή η σχετική αγορά, αλλά και να εφαρμοστούν οι κανόνες του Ανταγωνισμού.

Η δυσκολία έγκειται, τόσο στον προσδιορισμό των προϊόντων που ανήκουν στην ίδια αγορά, όσο και στην ύπαρξη λειτουργικής εναλλαξιμότητας μεταξύ των υπηρεσιών και των προϊόντων που παρέχονται μεταξύ της ηλεκτρονικής – ψηφιακής και της παραδοσιακής αγοράς προϊόντων. Όσο πιο μεγάλη είναι η ποικιλία των υπηρεσιών που παρέχονται στον καταναλωτή, τόσο πιο μεγάλες είναι οι πιθανότητες να υπάρχει διακριτή ηλεκτρονική αγορά.<sup>238</sup>

Επιπλέον, θα πρέπει να είναι διακριτή η ύπαρξη της ψηφιακής αγοράς από τις άλλες αγορές, αλλά και των μελών που αλληλεπιδρούν σε αυτές. Δηλαδή, μία ηλεκτρονική αγορά, η οποία εξασφαλίζει προϊόντα και υπηρεσίες σε μία άλλη επιχείρηση, ονομάζεται “Business to Business” (B2B), ενώ αντίθετα, εκείνη η οποία απευθύνεται από την επιχείρηση σε κάποιον καταναλωτή, ονομάζεται “Business to Consumer” (B2C).<sup>239</sup> Έτσι, λόγω αυτής της δυσκολίας, η Αρχή Ανταγωνισμού, λειτουργεί ιδιαίτερα επιφυλακτικά ως προς την εξαγωγή συμπερασμάτων σχετικά με τον ορισμό της.<sup>240</sup>

---

<sup>237</sup> Κασσελούρη Θ., «Η αρχή της ουδετερότητας και της ίσης μεταχείρισης στο Διαδίκτυο: Το Open Internet και η εποχή των Big Data», Διπλωματική Εργασία, Εμπορικού Δικαίου, του Προγράμματος Μεταπτυχιακών Σπουδών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, Αθήνα, 2020.

<sup>238</sup> Μικρουλέα Α., «Η κατάχρηση δεσπόζουσας θέσης του άρθρου 2 ν.703/77, ΧρΙΔ τ. ΣΤ/2006

<sup>239</sup> Ως ανωτέρω, βλ. υπ. 237

<sup>240</sup> Buchhold F., “Business to Business Internet Marktplatze im Blickpunkt des europäischen und deutschen Kartellrechts, TENEA, 2005

Αξιοσημείωτο είναι το γεγονός ότι στις παραδοσιακές αγορές γίνεται αναφορά στην τιμή επιφύλαξης, στην αγοραία αξία, στο κόστος και γενικότερα στις τιμές και στην ποσότητα των αγαθών.

Αντίθετα σε μία διαδικτυακή αγορά, αυτά τα χαρακτηριστικά δεν παίζουν τόσο μεγάλο ρόλο, καθώς πρόκειται για της αποκαλούμενες “zero price markets” ή “attention markets”. Αυτό σημαίνει ότι ο χρήστης των ψηφιακών πλατφορμών δεν θα πρέπει να πληρώσει κάποια τιμή για την υπηρεσία που του προσφέρεται, ωστόσο πληρώνει με την ιδιωτικότητά του, είτε με την προβολή των διαφημίσεων, κατά την χρήση της ηλεκτρονικής πλατφόρμας.<sup>241</sup>

Δηλαδή, η επιχείρηση που λειτουργεί στην ηλεκτρονική πλατφόρμα προσπαθεί με κάθε τρόπο να προβεί στην εμπορευματοποίηση των προσωπικών δεδομένων και την απόσπαση της προσοχής του καταναλωτή μέσω της προβολής των διαφημίσεων που εμφανίζονται στη σελίδα. Έτσι, απομακρύνεται ο τελευταίος από τα πρότυπα που υπάρχουν στην παραδοσιακή αγορά, αυτά, της τιμής του κόστους, της προσφοράς και της ζήτησης.

Επιπλέον, οι δημιουργοί των πλατφορμών έχουν μηδενικό οριακό κόστος, ενώ το κόστος διανομής και της αποθήκευσης είναι επίσης μηδενικό, καθώς όλα βρίσκονται εικονικά μέσα στο διαδίκτυο.<sup>242</sup>

Επιπλέον, αποτελεί θεμελιώδη έννοια για το Δίκαιο Ανταγωνισμού, η δεσπόζουσα θέση μιας επιχείρησης και το ερώτημα κατά πόσο μία επιχείρηση με φυσική παρουσία στο χώρο, είτε με ηλεκτρονική παρουσία μέσω των ψηφιακών πλατφορμών καταχράζεται τη θέση της, προκειμένου να αποκομίσει ίδιον όφελος. Κατά πόσο δηλαδή, πρόκειται για αντιανταγωνιστικές πρακτικές, οι οποίες εφαρμόζονται προκειμένου να εξαφανιστούν οι ανταγωνιστές και να μονοπωλήσει την αγορά.

Στις ψηφιακές αγορές και στις διαδικτυακές πλατφόρμες, τις περισσότερες φορές τα μερίδια των τεχνολογικών επιχειρήσεων είναι πολύ υψηλά, διότι εισάγονται

---

<sup>241</sup> Κασσελούρη Θ., «Η αρχή της ουδετερότητας και της ίσης μεταχείρισης στο Διαδίκτυο: Το Open Internet και η εποχή των Big Data», Διπλωματική Εργασία, Εμπορικού Δικαίου, του Προγράμματος Μεταπτυχιακών Σπουδών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, Αθήνα, 2020.

<sup>242</sup> Overby H., J.A. Audestad, Standards, Regulations and Net Neutrality in the Digital Economy, 2020.

είτε καινοτομίες, είτε νέα τεχνολογικά μέσα, τα οποία καταλαμβάνουν την αγορά, σε πολύ μεγάλο βαθμό.<sup>243</sup>

Προκειμένου, βέβαια, να διευκρινιστεί κάτι τέτοιο, θα πρέπει να ληφθεί υπ' όψιν η δομή της ψηφιακής αγοράς, αλλά και να γίνεται ενδελεχής έρευνα για κάθε συγκεκριμένη συμπεριφορά, η οποία εμφανίζεται στο διαδίκτυο. Φυσικά, μία λύση, αναφορικά με αυτό το ζήτημα αυτό, είναι η αλλαγή των κανόνων Ανταγωνισμού, ο οποίος είναι επικεντρωμένος περισσότερο στο παραδοσιακό μοντέλο ορισμού της αγοράς, αλλά και η περαιτέρω εφαρμογή, τόσο τεχνολογικών όσο και οικονομικών κριτηρίων από τις Αρχές Ανταγωνισμού.<sup>244</sup>

Επιπρόσθετα, είναι σημαντικό να αναφερθεί ότι με τις τελευταίες εξελίξεις, ένας πολύ βασικός κανόνας του ευρωπαϊκού δικαίου του ελεύθερου ανταγωνισμού είναι η θεωρία του “more economic technological approach”, η οποία έχει ως βάση την εξασφάλιση της κατανομητικής αποτελεσματικότητας για τον καταναλωτή και όχι τόσο την ανάλυση ορισμένων τύπων συμπεριφοράς (“form based approach”).<sup>245</sup>

Αυτό σημαίνει, ότι όλες αυτές οι προκλήσεις, οι οποίες εμφανίζονται λόγω της νέας ψηφιακής οικονομίας απαιτούν, δίχως αμφιβολία, την προσαρμογή όλων των κανόνων που ήδη υφίστανται στον ανταγωνισμό, στην στροφή σε μία νέα πραγματικότητα, η οποία πλησιάζει περισσότερο αυτή του “more technological approach”.<sup>246</sup>

Επομένως, είναι κατανοητό ότι και το Δίκαιο Ανταγωνισμού, θα πρέπει να προσαρμόζεται στις νέες συνθήκες και οι κανόνες του να αφορούν και τις νέες ψηφιακές αγορές, οι οποίες έχουν κατακλύσει την σύγχρονη εποχή και να λειτουργήσουν σε μία πραγματικότητα διαφορετική, από εκείνη των παραδοσιακών αγορών που υπήρχαν στο παρελθόν και εξακολουθούν να υπάρχουν, αλλά σε μικρότερη έκταση.

Μέσα σε αυτά τα πλαίσια, δεν πρέπει να ξεχνάμε ότι κατά την λειτουργία των ηλεκτρονικών πλατφορμών, χρησιμοποιούνται και εμπορευματοποιούνται τα προσωπικά δεδομένα των ατόμων – χρηστών του διαδικτύου, οι οποίοι καταγράφουν

---

<sup>243</sup> Βέττας Ν./ Κατσουλάκος Γ., «Πολιτική Ανταγωνισμού και Ρυθμιστική Πολιτική», Εκδόσεις Τυπωθήτω- Γιώργος Δαρδανός, 2004

<sup>244</sup> Έκθεση OECD, Abuse of Dominance in Digital Markets, 2020

<sup>245</sup> Τζουγανάτος Δ., «Δίκαιο του Ελεύθερου Ανταγωνισμού, Νομική Βιβλιοθήκη, Αθήνα, 2013

<sup>246</sup> Cremer J. / Y-A de Montjoye/ Schweitzer, “Competition Policy for the Digital era, Report for the European Commission, 2019

τα προσωπικά τους στοιχεία, προκειμένου να επικοινωνήσουν με τις εκάστοτε επιχειρήσεις, να εκτελέσουν χρηματικές συναλλαγές μέσω διαδικτύου, προκειμένου να αποπληρώσουν την επιχείρηση, λόγω της αγοράς κάποιου ή της παροχής κάποιας υπηρεσίας προς αυτούς.

Επίσης, είναι πολύ σημαντικό το γεγονός ότι αυτά τα δεδομένα, που χρησιμοποιούνται από τους δημιουργούς των πλατφορμών, θα πρέπει να χρησιμοποιούνται για ορισμένο χρονικό διάστημα μέχρι να εκπληρωθεί ο σκοπός της καταγραφής αυτών των δεδομένων και στη συνέχεια, να διαγράφονται.

Βέβαια σε πολλές περιπτώσεις οι ίδιοι οι καταναλωτές – χρήστες των ψηφιακών αγορών, εντάσσουν τα προσωπικά τους στοιχεία, πατούν σε υπερσυνδέσμους (links) και αποδέχονται “cookies” με τα οποία δίνουν την συναίνεσή τους, σχετικά με την ιδιωτικότητά τους και πολλές φορές, κάποιιο από αυτούς δεν γνωρίζουν, αναφορικά την επεξεργασία των δεδομένων τους από τρίτους.<sup>247</sup>

### **6.1.1 Τα δεδομένα προσωπικής και μη προσωπικής ταυτοποίησης των χρηστών του διαδικτύου**

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), ορίζει τα προσωπικά δεδομένα του διαδικτύου, ως την οποιαδήποτε πληροφορία, η οποία σχετίζεται με την ταυτοποίηση ενός ατόμου. Αυτό το πρόσωπο, είναι το υποκείμενο των δεδομένων και εν προκειμένω, ο χρήστης της ψηφιακής πλατφόρμας.<sup>248</sup>

Οι τύποι αυτών των προσωπικών δεδομένων του διαδικτύου αφορούν κάθε περιεχόμενο (content) που υπάρχει στις προσωπικές ιστοσελίδες (blogs), οποιαδήποτε δραστηριότητα συμπεριλαμβάνει αναζήτηση στον ιστό και τις διαδικτυακές αγορές, αλλά και τη δραστηριότητα των χρηστών στα μέσα κοινωνικής δικτύωσης, τα αποκαλούμενα και ως «κοινωνικά δεδομένα». Ακόμη,

---

<sup>247</sup>Κασσελούρη Θ., «Η αρχή της ουδετερότητας και της ίσης μεταχείρισης στο Διαδίκτυο: Το Open Internet και η εποχή των Big Data», Διπλωματική Εργασία, Εμπορικού Δικαίου, του Προγράμματος Μεταπτυχιακών Σπουδών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, Αθήνα, 2020.

<sup>248</sup> OECD, “Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value”, OECD Digital Economy Papers, No 220, OECD Publishing, 2013

περιλαμβάνονται οι κατηγορίες των δεδομένων τοποθεσίας, αναφορικά με την χρήση της τεχνολογίας GPS ή μέσω του κινητού τηλεφώνου και των διευθύνσεων IP (IP Address), ενώ παράλληλα, αναγνωρίζονται και τα δεδομένα «επίσημης φύσης», όπως είναι για παράδειγμα, το όνομα, ο αριθμός μητρώου (ΑΜ) και γενικότερα οι οικονομικές πληροφορίες.<sup>249</sup>

Βέβαια, βιβλιογραφικά εντοπίζεται και άλλη κατηγοριοποίηση των προσωπικών δεδομένων, βασιζόμενη κυρίως στη δραστηριότητα των κοινωνικών δικτύων.<sup>250</sup> Έτσι, η πρώτη κατηγορία αφορά τα δεδομένα εξυπηρέτησης (service data), τα εμπιστευτικά δεδομένα (entrusted data), τα δεδομένα γνωστοποίησης (disclosed data), τα δεδομένα συμπεριφοράς (behavioral data), τα συναγόμενα δεδομένα (inferred data) και τα συμπτωματικά δεδομένα (incidental data).<sup>251</sup>

Επιπροσθέτως, τα προσωπικά δεδομένα στο διαδίκτυο, μπορεί να κατηγοριοποιηθούν και σε άλλες ταξινομήσεις, με βάση αρχικά, τη συλλογή από έναν ορισμένο φορέα, είτε την αποθήκευση για χρήση και πώληση σε τρίτους.<sup>252</sup>

Οι πληροφορίες και τα προσωπικά δεδομένα, τα οποία συλλέγονται και αποθηκεύονται για χρήση ή πώληση σε τρίτους, μπορούν να διαχωριστούν και σε επιμέρους κατηγορίες.

Αρχικά, η μία κατηγορία αφορά τα «στατικά» προσωπικά δεδομένα (static private information), δηλαδή, όλες εκείνες οι πληροφορίες, οι οποίες δεν αλλάζουν δραματικά με την πάροδο του χρόνου, όπως για παράδειγμα, το ιατρικό ιστορικό και οι προσωπικές πληροφορίες.

Η άλλη κατηγορία αφορά τις πληροφορίες, οι οποίες υπάρχουν στο διαδίκτυο και μπορούν να αλλάξουν με την πάροδο του χρόνου. Πρόκειται δηλαδή, για πληροφορίες «δυναμικές», όπως άλλωστε, ονομάζονται. Αυτές οι πληροφορίες μπορούν να αφορούν το ιστορικό, τη δραστηριότητα στο διαδίκτυο ή το περιεχόμενο που παρακολουθεί ο χρήστης, το οποίο μπορεί να αλλάζει ανά περιόδους. Βέβαια,

---

<sup>249</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

<sup>250</sup> Ως ανωτέρω, βλ. υπ. 249

<sup>251</sup> Schneier, “Schneier on Security: A blog covering security and security technology, 2010

<sup>252</sup> FTC, “Self-Regulatory Principles for Online Behavioral Advertising”, FTC, Washington DC, 2009



αυτό δε σημαίνει ότι οι πληροφορίες αυτές δεν είναι χρήσιμες, αναφορικά με την συλλογή και την ανάλυσή τους.<sup>253</sup>

Μία ακόμη διάκριση που αφορά τα προσωπικά δεδομένα των χρηστών του διαδικτύου, είναι εκείνη των δεδομένων της προσωπικής ταυτοποίησης (Personally Identifiable Information) και των δεδομένων μη προσωπικής ταυτοποίησης ( Non - PII).<sup>254</sup>

Η πρώτη κατηγορία των δεδομένων, αφορά όλες εκείνες τις πληροφορίες, οι οποίες δύνανται να οδηγήσουν στην ταυτοποίηση του χρήστη. Πρόκειται δηλαδή, για πληροφορίες, όπως είναι η ατομικοί αριθμοί ΑΜΚΑ, ΑΦΜ, αριθμοί κινητού τηλεφώνου, αριθμοί διεύθυνσεως και ονοματεπώνυμο.<sup>255</sup> Πληροφορίες δηλαδή, οι οποίες είναι εξατομικευμένες και ξεχωριστές για κάθε χρήστη, με αποτέλεσμα να επέρχεται η άμεση ταυτοποίησή του, σε περίπτωση που κάποιος λάβει γνώση αυτών των πληροφοριών – ατομικών στοιχείων. Αυτά τα δεδομένα είναι προσωπικά, δεν θα πρέπει να διαρρέουν, αλλά αντίθετα θα πρέπει να προστατεύονται σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ).

Η δεύτερη κατηγορία αφορά τις πληροφορίες μη προσωπικής ταυτοποίησης, δηλαδή πληροφορίες, οι οποίες δεν ταυτοποιούν άμεσα τον χρήστη του διαδικτύου ή της ψηφιακής πλατφόρμας, αλλά δείχνουν στοιχεία της διαδικτυακής του συμπεριφοράς ή των διαδικτυακών αποτυπωμάτων του στον κυβερνοχώρο. Τέτοιες πληροφορίες αφορούν το ιστορικό περιήγησης, το περιεχόμενο παρακολούθησης, τη χρησιμοποίηση των διαδικτυακών εργαλείων, αλλά και τις αγορές ή πληρωμές, οι οποίες έχουν λάβει χώρα στο διαδικτυακό τόπο. Αυτές οι πληροφορίες δεν οδηγούν άμεσα σε κάποιο συγκεκριμένο πρόσωπο, έτσι ώστε να οδηγηθούμε στην ταυτοποίησή του κατευθείαν και οριστικά, διότι υπάρχει πλήθος χρηστών, οι οποίοι χρησιμοποιούν ίδια- ή σχεδόν ίδια- πορεία πλοήγησης με συγκεκριμένη προτίμηση, την επιλογή του περιεχομένου, πράγμα που κάνει δυσδιάκριτο για κάποιον να ταυτοποιήσει το χρήστη με τις συγκεκριμένες πληροφορίες.<sup>256</sup>

---

<sup>253</sup> Wang H., M.K.O. Lee, and C. Wang, “Consumer Privacy Concerns about Internet Marketing”, 1998

<sup>254</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

<sup>255</sup> Ως ανωτέρω, βλ. υπ. 254

<sup>256</sup> Ως ανωτέρω, βλ. υπ. 254

Επίσης λόγω του ότι δεν πρόκειται για πληροφορίες άμεσης, προσωπικής ταυτοποίησης ή για μοναδικούς αριθμούς, ονοματεπώνυμο ή διευθύνσεις, δεν προσωποποιείται το άτομο σε αυτή την περίπτωση, διότι οι πληροφορίες αυτές δεν είναι εξατομικευμένες. Βέβαια, οφείλουμε να παρατηρήσουμε ότι κάθε πληροφορία στο διαδίκτυο δείχνει τις προτιμήσεις που μπορεί να έχουμε στην παρακολούθηση των θεαμάτων, ή στην επιλογή του περιεχομένου που παρακολουθούμε, οι οποίες «προδίδουν» στοιχεία της προσωπικότητας, όπως το φύλο, ο σεξουαλικός προσανατολισμός, η θρησκεία, ή η καταγωγή.<sup>257</sup>

Θα πρέπει να αναφερθεί βέβαια, σε αυτό το σημείο, ότι παρά το γεγονός πως οι πληροφορίες μη προσωπικής ταυτοποίησης δεν οδηγούν άμεσα στην ταυτοποίηση του ατόμου που χρησιμοποιεί τη διαδικτυακή πλατφόρμα, υπάρχει πιθανότητα ύστερα από συνδυασμό των ατομικών πληροφοριών, που παρέχονται στο διαδίκτυο να υπάρξει ταυτοποίηση του χρήστη. Δηλαδή, όλες οι υπηρεσίες που αφορούν τη γεωγραφική θέση ή τη διεύθυνση IP ενός χρήστη, όταν συνδυαστούν με πληροφορίες όπως το φύλο, το περιεχόμενο ή τη δραστηριότητα στο διαδίκτυο, μπορεί να οδηγήσει σε ταυτοποίηση του χρήστη.<sup>258</sup>

## 6.2 Παραβάσεις των πλατφορμών

Οι διαδικτυακές πλατφόρμες έχουν αποτελέσει έναν λόγο ριζικής αλλαγής της ψηφιακής οικονομίας και έχουν παράσχει μέχρι σήμερα πάρα πολλά οφέλη στην αποτελεσματική, γρήγορη και εύκολη επικοινωνία και διεκπεραίωση συναλλαγών. Διεκδικούν τις παραδοσιακές αγορές και δημιουργούν καινοτομίες και νέες επιχειρηματικές δραστηριότητες.

Τα τελευταία χρόνια, παρατηρούνται όλο και περισσότερες παραβάσεις, οι οποίες αφορούν τις πλατφόρμες που μάλιστα, πολλές φορές χρησιμοποιούν τη δεσπόζουσα θέση τους καταχρηστικά. Τέτοιες περιπτώσεις, συχνά αφορούν καθετοποιημένες επιχειρήσεις, οι οποίες λαμβάνουν την δεσπόζουσα θέση τους

---

<sup>257</sup> OECD, “Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value”, OECD Digital Economy Papers, No 220, OECD Publishing, 2013

<sup>258</sup> Narayanan A. and V. Shmatikov, Privacy and Security Myths and fallacies of Personally identifiable information”, Communications of the ACM, vol.53, 2010

καταχρηστικά, έναντι των άλλων επιχειρήσεων. Υποστηρίζεται ότι οι ψηφιακές πλατφόρμες λόγω του γεγονότος ότι ασχολούνται με την ιεράρχηση των αποτελεσμάτων (search and matching), λόγω της χρήσης των αλγορίθμων, δεν μπορούν, ουσιαστικά, να είναι αμερόληπτες και ουδέτερες. Μην ξεχνάμε ότι δεν πρόκειται για υποκείμενα, αλλά για αλγόριθμους, δηλαδή για τεχνολογικά εργαλεία διευκόλυνσης των χρηστών και παροχής των υπηρεσιών του διαδικτυακού τόπου.<sup>259</sup>

Έτσι, κατανοούμε ότι στις διαδικτυακές πλατφόρμες παρατηρείται πλήθος παραβάσεων, που αφορούν είτε την παραβίαση των προσωπικών δεδομένων των χρηστών, είτε άλλου είδους παραβάσεις, που αφορούν και σχετίζονται με το Δίκαιο του Ανταγωνισμού, όπως για παράδειγμα, την κατάχρηση της δεσπόζουσας θέσης ή την άνιση μεταχείριση μεταξύ των χρηστών.

Στις διαδικτυακές πλατφόρμες, θα πρέπει να αντιμετωπίζονται οι καταναλωτές με δίκαιο τρόπο και χωρίς διακρίσεις, ως προς την ιεράρχηση των αποτελεσμάτων, όπως εμφανίζονται κατά τη σειρά τους στις μηχανές αναζήτησης. Παραδείγματα εκ της νομολογίας, έχουν δείξει ότι υπάρχουν πολλές εξελίξεις, οι οποίες αφορούν παραβάσεις από τις πιο δημοφιλείς καθετοποιημένες ηλεκτρονικές πλατφόρμες, όπως για παράδειγμα, την Google, την Amazon και το Facebook.<sup>260</sup>

### 6.2.1 α) Google

Η Google αποτελεί μία πολύ μεγάλη επιχείρηση, η οποία είναι συνώνυμη με την αντίστοιχη μηχανή αναζήτησής της και αποτελεί την πλατφόρμα, στην οποία συνδέονται εκατομμύρια άτομα, παγκοσμίως. Η εταιρεία Google σίγουρα κατέχει δεσπόζουσα θέση στην αγορά, καθώς χρησιμοποιείται ευρέως, τόσο σε κινητά τηλέφωνα, όσο και σε ηλεκτρονικούς υπολογιστές, για προβολή ειδήσεων στον παγκόσμιο ιστό, για προβολή εικόνων για μηχανή αναζήτησης πληροφοριών, για την επεξεργασία κειμένων και για την ενημέρωσή τους.

---

<sup>259</sup> Κασσελούρη Θ., «Η αρχή της ουδετερότητας και της ίσης μεταχείρισης στο Διαδίκτυο: Το Open Internet και η εποχή των Big Data», Διπλωματική Εργασία, Εμπορικού Δικαίου, του Προγράμματος Μεταπτυχιακών Σπουδών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, Αθήνα, 2020

<sup>260</sup> Bostoen F., “Online Platforms and Vertical Integration: The Return of Margin Squeeze? Journal of Antitrust Enforcement, 2018, Faculty of Law, Stockholm University Research Paper No 42, Vol 6(3), 2017

Η εταιρεία αυτή, αποτελεί τη βάση, στην οποία ερείζονται και άλλες επιχειρήσεις, προκειμένου να επιβιώσουν στο διαδίκτυο. Στη μηχανή αναζήτησης της Google τα αποτελέσματα που βγαίνουν, με τη σειρά που εμφανίζονται στην οθόνη, αποτελούν διαφημίσεις για άλλες εταιρείες, οι οποίες προσπαθούν να προωθήσουν τα προϊόντα και τις υπηρεσίες τους στους καταναλωτές, μέσα από αυτή την εφαρμογή. Με αυτό τον τρόπο, θα αυξήσουν τα έσοδά τους και η επιχείρηση θα αποκτήσει πολύ μεγάλη οικονομική αξία. Αυτή η αξία πολλαπλασιάζεται, διότι εάν υπολογιστεί πόσες επιχειρήσεις στηρίζονται στην Google, μπορούμε να αθροίσουμε τα οικονομικά της οφέλη συνολικά.

Αποκτώντας πρόσβαση σε αυτή την πλατφόρμα, οι χρήστες δεν υποχρεούνται να πληρώσουν κάποιο αντίτιμο προκειμένου να εκπληρώσουν κάποια συναλλαγή, αλλά αντίθετα, η πρόσβασή τους είναι πάρα πολύ εύκολη, γρήγορη και άμεση, πληκτρολογώντας στη μηχανή αναζήτησης το περιεχόμενο που επιθυμούν να παρακολουθήσουν.

Βέβαια, μπορεί να είναι μια δωρεάν υπηρεσία, που παρέχεται σε όλους, ωστόσο, δεν πρέπει να ξεχνάμε, ότι ο κάθε χρήστης προσφέρει στην εφαρμογή πολύτιμα δεδομένα, τα οποία στη συνέχεια, η επιχείρηση τα χρησιμοποιεί προκειμένου να βελτιστοποιήσει την συνάφεια της αναζήτησης, αλλά ταυτόχρονα και ως δέλεαρ για τους διαφημιστές, από τους οποίους θα αποκομίσει και τελικά τα έσοδα της.<sup>261</sup>

Αυτό είναι πολύ σπουδαίο, διότι κατανοούμε ότι εμπορευματοποιούνται τα προσωπικά δεδομένα των χρηστών, προκειμένου να αυξηθεί η οικονομική αξία των εταιρειών και στην πράξη χρησιμοποιούνται ως το αντίτιμο ή το αντάλλαγμα της δωρεάν υπηρεσίας, η οποία θεωρείται οικονομική και παρέχεται εύκολα και γρήγορα στον καταναλωτή.

Ο τρόπος δηλαδή με τον οποίο λειτουργεί η Google, αλλά και κάθε μηχανή αναζήτησης είναι ο εξής: οι χρήστες – καταναλωτές επιδιώκουν να αποκτήσουν την πληροφορία, ενώ οι επιχειρήσεις επιδιώκουν να βρουν το καταναλωτικό κοινό και τους κατάλληλους διαφημιστές, οι οποίοι χρειάζονται πελάτες για να προωθήσουν τις

---

<sup>261</sup> Κασσελούρη Θ., «Η αρχή της ουδετερότητας και της ίσης μεταχείρισης στο Διαδίκτυο: Το Open Internet και η εποχή των Big Data», Διπλωματική Εργασία, Εμπορικού Δικαίου, του Προγράμματος Μεταπτυχιακών Σπουδών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, Αθήνα, 2020

υπηρεσίες και τα προϊόντα τους. Τα αποτελέσματα της μηχανής αναζήτησης που εμφανίζονται στην οθόνη επηρεάζουν όλες τις πλευρές.

Κατανοούμε λοιπόν, ότι όσο μεγαλύτερο ποσοστό καταναλωτών και χρηστών χρησιμοποιούν κάποια μηχανή αναζήτησης, τόσα περισσότερα δεδομένα λαμβάνονται και τόσο μεγαλύτερη είναι η συνάφεια των αποτελεσμάτων. Αυτό σημαίνει ότι, όσο πιο συναφή είναι τα αποτελέσματα, τόσο περισσότερο θα το χρησιμοποιούν οι χρήστες και κατ' επέκταση, θα γίνεται ακόμη πιο ελκυστική για τους διαφημιστές. Έπειτα, όσο πιο ελκυστική γίνεται για τους διαφημιστές, τόσες περισσότερες προσφορές θα λαμβάνει η μηχανή αναζήτησης και η επιχείρηση, αλλά και τόσο μεγαλύτερα έσοδα συνολικά.

Επιπροσθέτως, αναφορικά με το ζήτημα της παράβασης των πλατφορμών, θα πρέπει να σημειώσουμε ότι η Google, ως εταιρεία δεν έχει μόνο τη μηχανή αναζήτησης, αλλά και δικά της, ατομικά προϊόντα και υπηρεσίες, τις οποίες παρέχει ευρέως στους καταναλωτές της.<sup>262</sup>

Το ζήτημα είναι ότι υπήρχε πιθανότητα να συμβαίνει παράβαση με την εξαγωγή των αποτελεσμάτων στην ιστοσελίδα. Δηλαδή, η Google λόγω της δεσπόζουσας θέσης της, να καταχράζεται αυτή και να λειτουργεί με τρόπο, που αντιβαίνει τους Κανόνες του Δικαίου του Ανταγωνισμού. Να λειτουργεί δηλαδή άνισα, σχετικά με τις δικές της υπηρεσίες. Αυτή ήταν και η έρευνα της Ευρωπαϊκής Επιτροπής για την Google. Εξέτασε αν υπάρχει τοποθέτηση πιο ψηλά, στα αποτελέσματα της αναζήτησης, σε σχέση με τις άλλες σε επιχειρήσεις. Εάν δηλαδή, πέραν από κατάχρηση της δεσπόζουσας θέσης της, εάν υπήρχε και ζήτημα προτιμησιακής μεταχείρισης (preferential treatment).

Η Ευρωπαϊκή Επιτροπή κατέληξε στο συμπέρασμα ότι πράγματι η Google μεταχειριζόταν προτιμησιακά τη δική της αναζήτηση, σε σχέση με τις υπόλοιπες ανταγωνιστικές υπηρεσίες (Google Shopping Case).<sup>263</sup>

Η συγκεκριμένη παράβαση αφορούσε την προτιμησιακή μεταχείριση και την καταχρηστική εκμετάλλευση της δεσπόζουσας θέσης της, έναντι των άλλων επιχειρήσεων. Λειτουργούσε δηλαδή, αντίθετα από τους κανόνες του Δικαίου Ανταγωνισμού.

---

<sup>262</sup> <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31987D0500&from=EL>

<sup>263</sup> <https://eurlex.europa.eu/legalcontent/EL/TXT/PDF/?uri=CELEX:31987D0500&from=EL>

### 6.2.1 β) Facebook

Στην υπόθεση Facebook, ωστόσο η παράβαση ήταν διαφορετική, τόσο ως προς το είδος, όσο και ως προς τη φύση της διαφοράς. Γνωρίζουμε ότι το Facebook, το οποίο ονομάζεται πλέον “Meta”, αποτελεί ένα πολύ δημοφιλές μέσο κοινωνικής δικτύωσης, χωρίς βέβαια, να θεωρείται καθετοποιημένη επιχείρηση. Ωστόσο, έχει αγοράσει άλλες επιχειρήσεις, οι οποίες ασχολούνται εν γένει με τον τομέα είτε της επικοινωνίας, είτε της κοινωνικής δικτύωσης.

Παράλληλα, το Facebook χρησιμοποίησε μία ιδιαίτερη πρακτική, αναφορικά με την αναγνώριση μιας ανταγωνιστικής απειλής σε μία άλλη πλατφόρμα, την οποία επέλεξε να αγοράσει, έτσι ώστε να μειώσει την επερχόμενη επιτυχία της και να την αποκτήσει, έτσι ώστε να έχει αυτή πλέον δεσπόζουσα θέση στην αγορά και όχι έναν πολύ ισχυρό ανταγωνιστή με δισεκατομμύρια χρήστες να τη χρησιμοποιούν. Πρόλαβε δηλαδή, να το αγοράσει, πριν εκείνο αποκτήσει ακόμα μεγαλύτερη δύναμη, μέσω της επιτυχίας του στα μέσα κοινωνικής δικτύωσης. Αυτή η συμπεριφορά φαίνεται και με την αγορά της πλατφόρμας του Instagram, το οποία αγόρασε, το 2012.<sup>264</sup>

Μία άλλη παράβαση της πλατφόρμας του Facebook, αφορά το θέμα της συλλογής και της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Το Facebook έχει αποκτήσει και επιμέρους πλατφόρμες κοινωνικής δικτύωσης και τίθεται ζήτημα σχετικά με το διαμοιρισμό των προσωπικών στοιχείων των χρηστών στις επιμέρους πλατφόρμες.<sup>265</sup>

Η Γερμανική Αρχή Ανταγωνισμού Bundeskartellamt, έκανε έρευνα και δεν προχώρησε πρώτα, στις Αρχές του Ανταγωνισμού, αλλά έλεγξε τον τρόπο, με τον οποίο λειτουργεί, αναφορικά με την συλλογή και την επεξεργασία των προσωπικών δεδομένων και εάν υπάρχει πράγματι συναίνεση των χρηστών του για αυτή την επεξεργασία.

Η Γερμανική Αρχή Ανταγωνισμού διαπίστωσε ότι η εφαρμογή συγχώνευε τα δεδομένα προσωπικού χαρακτήρα, αλλά και όλες τις προτιμήσεις του καταναλωτή σε

---

<sup>264</sup> Κασσελούρη Θ., «Η αρχή της ουδετερότητας και της ίσης μεταχείρισης στο Διαδίκτυο: Το Open Internet και η εποχή των Big Data», Διπλωματική Εργασία, Εμπορικού Δικαίου, του Προγράμματος Μεταπτυχιακών Σπουδών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, Αθήνα, 2020

<sup>265</sup>[https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07\\_02\\_2019\\_Facebook.html](https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html)

κάθε χωριστό μέσο κοινωνικής δικτύωσης και δημιουργούσε ένα ξεχωριστό προφίλ. Αυτή, ωστόσο, η πρακτική δεν αναφερόταν πουθενά στους όρους και τις προϋποθέσεις και επομένως αποτελεί εκμεταλλευτική κατάχρηση δεσπόζουσας θέσης της κατά το άρθρο 102 ΣΛΕΕ. Με σκοπό την απόκτηση περιουσιακού οφέλους.<sup>266</sup>

Ένα ακόμη στοιχείο, το οποίο αποτελεί παράβαση των κανόνων του Δικαίου του Ανταγωνισμού, αποτελεί η παραπληροφόρηση και η ύπαρξη “fake news”, ψευδών ειδήσεων και πληροφοριών, στην πλατφόρμα της, πράγμα που σημαίνει ότι οι χρήστες, δεν προστατεύονται και υπάρχει ένας ακόμα μεγαλύτερος λόγος για ρύθμιση του τρόπου συλλογής των προσωπικών δεδομένων των χρηστών. Αυτό δε σημαίνει ότι πρέπει να σταματήσει το Facebook να λειτουργεί ως μονοπώλιο, ή να έχει δεσπόζουσα θέση, αλλά θα πρέπει να περιοριστεί και να ρυθμιστεί το γεγονός της παράβασης της παραπληροφόρησης, της συλλογής και της επεξεργασίας των προσωπικών δεδομένων των χρηστών και της προστασίας τους από τα “fake news” και την παραπληροφόρηση.<sup>267</sup>

### **6.2.2 Ζητήματα ιδιωτικότητας στο διαδίκτυο (Internet Privacy Issues)**

Ήδη από την αρχή της χρήσης του διαδικτύου και των ηλεκτρονικών πλατφορμών, υπήρχε το ζήτημα και η ανησυχία σχετικά με την πιθανότητα παραβάσεως των προσωπικών δεδομένων και των ιδιωτικών πληροφοριών, μέσω της χρήσης των υπολογιστικών συστημάτων.<sup>268</sup>

Αυτό συμβαίνει, διότι η προστασία της ιδιωτικότητας των προσωπικών δεδομένων και των πληροφοριών, παίζει πρωταρχικό ρόλο σε κάθε δημοκρατία. Κάθε χρήστης, θα πρέπει να έχει δηλαδή, τη δυνατότητα να ελέγχει τον τρόπο, τον χρόνο και τη διαδικασία επεξεργασίας των προσωπικών του πληροφοριών, αλλά και

---

<sup>266</sup> Μικρούλεα Α., «Η κατάχρηση δεσπόζουσας θέσης του άρθρου 2 ν.703/77, ΧρΙΔ τ. ΣΤ/2006

<sup>267</sup> Satariano A., “Big Tech ‘knows you better than your wife’, He plans to Rein it in, 2019

<sup>268</sup> E.E. David and R.M. Fano, “Some thoughts about the Social Implications of Accessible Computing”, Proceedings 1965 Fall Joint Computer Conference, 1965

την κοινοποίησή τους σε άλλους, <sup>269</sup>διότι αυτό είναι πολύ συχνό φαινόμενο στην εποχή της πληροφορίας.<sup>270, 271</sup>

Εμφανίζονται συνεχόμενες, νέες προκλήσεις, τόσο για τις επιχειρήσεις, όσο και για τους χρήστες των πλατφορμών, αναφορικά με το ζήτημα της ιδιωτικότητας, της προστασίας της ιδιωτικής σφαίρας, της προστασίας της προσωπικότητας και των προσωπικών δεδομένων τους, στο διαδίκτυο.<sup>272, 273, 274</sup>

Ειδικότερα στη σύγχρονη εποχή, όπου τα ηλεκτρονικά συστήματα και το διαδίκτυο έχουν αποκτήσει άλλη ισχύ κι άλλη δυναμική αποτελεσματικότητα, υπάρχουν χιλιάδες πλατφόρμες και εφαρμογές, όπου οι χρήστες μπορούν να καταγράψουν τα προσωπικά τους δεδομένα.<sup>275</sup>

Επιπρόσθετα, οι χρήστες εξακολουθούν να προμηθεύουν τις σελίδες του διαδικτύου με προσωπικές τους πληροφορίες, που αφορούν την ιδιωτική του ζωή, το ζήτημα των προσωπικών δεδομένων σε όλο και μεγαλύτερο βαθμό στις μέρες μας

. Ο συνδυασμός των δύο παραγόντων οδηγεί στην εύκολη πρόσβαση οποιουδήποτε τρίτου στα προσωπικά δεδομένα των χρηστών και σύμφωνα με την βούλησή του μπορεί να τα επεξεργαστεί και να τα αποθηκεύσει με κακόβουλο τρόπο.

Οι καταναλωτές- χρήστες του διαδικτύου, που χρησιμοποιούν τις πλατφόρμες, προκειμένου να αγοράσουν προϊόντα ή να τους παρασχεθούν υπηρεσίες, δίνουν πολύ μεγάλη έμφαση στη χρήση των δεδομένων τους, αλλά και στον τρόπο με τον οποίο

---

<sup>269</sup> Westin A., “Privacy and Freedom”, 25 Wash and Lee L. Rev. 166, 1968

<sup>270</sup> Milberg S. J., Smith H. J., and Burke, S. J., “Information Privacy: Corporate management and National Regulation”, *Organization Science*, 2000, p.35-37

<sup>271</sup> Culcan, M.J., Bies R.J., “ Consumer Privacy: Balancing Economic and Justice Considerations”, *Journal of Social Issues*, 2003, p.323-342

<sup>272</sup> Angst, C.M. and Agarwal, R., “Adoption of Electronic Health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion”, *MIS Quarterly*, 2009, p. 339-370

<sup>273</sup> Malhotra N. K., Kim S. S., and Agarwal J., “Internet users’ information privacy concerns (IUIPC): The construct, the scale and a casual model”, *Information Systems Research*, 2004, p.336-355

<sup>274</sup> Ward S., Bridges K., and Chitty B., “Do Ncentives matter? An examination of on-line privacy concerns nd willingness to provide personal and financial information”, *Journal of Marketing Communications*, 2005, p. 21-40

<sup>275</sup> Li, X. B. and Sharkar S., “Privacy Protection in data mining: A perturbation approach for categorical data”, *Information Systems Research*, 2006, 254-270



θα μπορούσαν να έχουν έλεγχο της συλλογής, της αποθήκευσης και της επεξεργασίας τους.<sup>276</sup>

Εξαιτίας του γεγονότος ότι οι χρήστες δεν δύνανται να έχουν μεγάλο έλεγχο στις πρακτικές που χρησιμοποιεί η κάθε επιχείρηση στη διαχείριση των δεδομένων τους, επιδιώκουν κάθε φορά που χρειάζεται να καταγράψουν τα προσωπικά τους δεδομένα στο διαδίκτυο, να έρχονται σε επικοινωνία με επιχειρήσεις ή οργανισμούς, οι οποίοι αποτελούν επίσημα δίκτυα και οι οποίοι, μπορούν να εμπιστευτούν τις πληροφορίες που επιλέγουν να καταχωρήσουν τα ατομικά τους στοιχεία σε αυτές.<sup>277</sup>

Οι περισσότεροι από τους χρήστες που ανησυχούν για την διαρροή των προσωπικών δεδομένων ή την λανθασμένη διαχείρισή τους από τρίτους, αισθάνονται ότι οι πρακτικές που ακολουθούν οι επιχειρήσεις αναφορικά με την συλλογή, τη, μη εξουσιοδοτημένη δευτερεύουσα χρήση των πληροφοριών τους, μπορεί να τους προκαλέσει βλάβη και να τους εκθέσει εν γένει.<sup>278</sup>

Οι περισσότεροι είναι επιφυλακτικοί, καθώς θεωρούν ότι οι επιχειρήσεις μπορούν να κάνουν λάθη στις ατομικές τους πληροφορίες, είτε να έχουν πρόσβαση σε αυτές δίχως τη συναίνεσή τους.<sup>279</sup>

Επιδιώκουν τη γνώση, σχετικά με την διαχείριση των πληροφοριών τους, τόσο σε ό,τι αφορά τις επιχειρήσεις του διαδικτύου, όσο και στο φυσικό τόπο, στις χρηματικές και εμπορικές συναλλαγές τους με τρίτους και στην επικοινωνία μεταξύ τους.

---

<sup>276</sup> Malhotra N. K., Kim S. S., and Agarwal J., “Internet users’ information privacy concerns (IUIPC): The construct, the scale and a casual model”, Information Systems Research, 2004, p.336-355

<sup>277</sup> Tsai et al., “The Effect of Online Private Information on Purchasing Behavior”, Information Systems Research 22, 2011, p. 254-268

<sup>278</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

<sup>279</sup> Malhotra N. K., Kim S. S., and Agarwal J., “Internet users’ information privacy concerns (IUIPC): The construct, the scale and a casual model”, Information Systems Research, 2004, p.336-355

### 6.2.3 Η παραβίαση των προσωπικών δεδομένων των υποκειμένων, μέσω των “cookies”

Κατά την περιήγηση των χρηστών στο διαδίκτυο και την επίσκεψή τους σε διάφορες ιστοσελίδες του κυβερνοχώρου, παρατηρείται, πολλές φορές, η ύπαρξη ενός «διαδικτυακού παραθύρου», το οποίο ονομάζεται «cookies». Στο περιεχόμενο του κειμένου, που εμφανίζεται στην οθόνη, αναγράφονται οι όροι και οι πολιτικές της ιστοσελίδας και η έγκριση, δηλαδή η αποδοχή ή η απόρριψη των λεγομένων «cookies», ενώ συχνά, δίνεται εκεί και η επιλογή: «περισσότερες πληροφορίες».

Κάθε χρήστης κατανοεί ότι, αυτό, αφορά σημείο απορρήτου, όρων και πολιτικών της σελίδας και συχνά προκειμένου να επισκεφθεί την ιστοσελίδα, συναινεί, επιλέγοντας το πλήκτρο της αποδοχής.

Τα «cookies» αποτελούν μικρά αρχεία, τα οποία περιέχουν πληροφορίες και πολλές φορές είναι κρυπτογραφημένα και τοποθετούνται σε μία συγκεκριμένη ιστοσελίδα, την οποία πρόκειται να επισκεφτεί κάποιος χρήστης. Οι πληροφορίες, οι οποίες περιέχονται στο κείμενο των «cookies» και οι οποίες, μάλιστα, είναι αποθηκευμένες μέσα σε αυτά τα μικρά αρχεία, αφορούν όλες τις προτιμήσεις του χρήστη.<sup>280</sup>

Αυτές οι προτιμήσεις, μπορεί να προέκυψαν είτε από αναζητήσεις που έκανε στις μηχανές αναζήτησης, είτε από την επιλογή πλήκτρων που οδηγούσαν σε διαφημίσεις, είτε διευθύνσεις IP και κωδικούς του χρήστη. Διακρίνονται σε δύο κατηγορίες, αυτής των πρώτων μερών (first party cookies) και στον τρίτων μερών (third party cookies) και διαφέρουν ως προς την εγκατάσταση από τα άτομα. Τα πρώτα, αφορούν την εγκατάσταση από τον ίδιο τον πάροχο, ενώ τα δεύτερα, από τρίτους παρόχους.<sup>281</sup>

Οι δημιουργοί των «cookies» έχουν σκοπό τη βελτίωση της εμπειρίας των χρηστών στο διαδίκτυο και στις σελίδες τους, αλλά και στην αποκάλυψη των επιλογών, των προτιμήσεων, ή των αγαπημένων ιστοσελίδων, που επισκέπτονται, προκειμένου να δημιουργούν περιεχόμενο πιο κοντά στις προτιμήσεις τους και να βελτιώνουν κάθε μέρα τις εφαρμογές τους.

---

<sup>280</sup> Παπαδοπούλου Β., «Η παραβίαση των προσωπικών δεδομένων στο Διαδίκτυο με σκοπό τη διαφήμιση», Διπλωματική Εργασία Προγράμματος Μεταπτυχιακών Σπουδών, Τομέα Ιστορίας, Φιλοσοφίας και Κοινωνιολογίας του Δικαίου, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2018

<sup>281</sup> [www.allaboutcookies.org](http://www.allaboutcookies.org)

Ωστόσο, είναι πολύ σημαντικό να τηρούνται οι όροι, προκειμένου να μην υπάρξει παραβίαση των προσωπικών δεδομένων των χρηστών, μέσω της συλλογής της αποθήκευσης, ή της επεξεργασίας των πληροφοριών του, με παράνομο τρόπο.<sup>282</sup>

Προκειμένου, βέβαια, να χρησιμοποιηθούν και να εγκατασταθούν τα «cookies», στην ιστοσελίδα, απαιτείται η πρότερη συναίνεση του χρήστη (πρόκειται για σύστημα opt-in), κατά τα οριζόμενα στο νόμο 3471/2006, με την τροποποίηση του νόμου 4070/2012. Το παλαιότερο σύστημα, που ήταν opt-out, ίσχυε πριν την τροποποίηση της Οδηγίας 2002/58/EK, η οποία αφορούσε την εγκατάσταση και χρήση, δίχως οποιαδήποτε συναίνεση του χρήστη.<sup>283</sup>

Πολλές φορές, βέβαια, τα «cookies», χρησιμοποιούνται και για διαφημιστικούς σκοπούς στο διαδίκτυο, ωστόσο θα πρέπει να αναφέρεται ρητά αυτός ο σκοπός και να ενημερώνεται ο χρήστης αναφορικά με αυτόν.

Ωστόσο, το πρόβλημα είναι ότι στην πράξη, οι κανόνες και οι προϋποθέσεις της χρήσης ιστοσελίδων, που περιέχουν τα «cookies» και ζητούν την αποδοχή ή την απόρριψή τους, δεν παρέχουν σαφή ενημέρωση στους χρήστες, είτε λαμβάνουν την συγκατάθεση των χρηστών με παράνομο τρόπο, είτε εγκαθιστούν «cookies» παρακολούθησης («tracking cookies») των χρηστών, έτσι ώστε να τους προωθούν προϊόντα υπηρεσίες μέσω της διαφήμισης.<sup>284</sup>

Παρόλο που στην πράξη, δεν μπορούν τα ίδια να λειτουργήσουν ως «αίτιο», στις ιστοσελίδες, υπάρχει περίπτωση, μέσα από όλη αυτή τη διαδικασία, να υπάρξει υποκλοπή δεδομένων προσωπικού χαρακτήρα, ειδικότερα όταν το δίκτυο χρήσης, δεν είναι ατομικό ή ασφαλισμένο.<sup>285</sup>

---

<sup>282</sup> βλ. «Πολιτική Χρήσης «cookies» στην ιστοσελίδα του Εργαστηρίου Επενδυτικών Εφαρμογών του Τμήματος Οικονομικών Επιστημών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών στη σελίδα: [www.epefa.econ.uoa.gr](http://www.epefa.econ.uoa.gr), και [allaboutcookies.org](http://allaboutcookies.org)

<sup>283</sup> Παπαδοπούλου Β., «Η παραβίαση των προσωπικών δεδομένων στο Διαδίκτυο με σκοπό τη διαφήμιση», Διπλωματική Εργασία Προγράμματος Μεταπτυχιακών Σπουδών, Τομέα Ιστορίας, Φιλοσοφίας και Κοινωνιολογίας του Δικαίου, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2018

<sup>284</sup> Ως ανωτέρω, βλ. υπ. 283

<sup>285</sup> «Υπηρεσίες Διαδικτύου- η χρήση cookies στο διαδίκτυο», στην ιστοσελίδα της ΑΠΔΠΧ: [www.dpa.gr](http://www.dpa.gr)

#### 6.2.4 Συνέπειες από την παραβίαση των δεδομένων στις πλατφόρμες

Υπάρχουν αρκετές δημοφιλείς ιστοσελίδες, όπως είναι για παράδειγμα, το Google και το Amazon, οι οποίες έχουν διαπράξει παραβάσεις της διαδικτυακής ιδιωτικότητας και έχουν υποστεί μηνύσεις, αλλά και ελέγχους από την Αρχή Ανταγωνισμού. Πάνω σε αυτόν τον τομέα της προστασίας των προσωπικών δεδομένων τίθεται και περισσότερο το ζήτημα της σύστασης για επανεξέταση όλων αυτών των θεμάτων ενδελεχώς.<sup>286, 287</sup>

Είναι ανάγκη να υπάρχει και να προετοιμάζεται, ένα ευοίωνο μέλλον για το internet, τόσο στα ζητήματα των προσωπικών δεδομένων,<sup>288</sup> όσο και των παραβάσεων που αφορούν τους κανόνες του Δικαίου του Ανταγωνισμού.

Χρήστες του διαδικτύου, εμπιστεύονται τα προσωπικά τους δεδομένα στις ψηφιακές πλατφόρμες, τις οποίες χρησιμοποιούν, με αποτέλεσμα πολλές φορές να εμφανίζονται ανεπιθύμητες συνέπειες, μετά από την καταχώριση των προσωπικών τους δεδομένων τους στο διαδίκτυο.

Υπάρχουν λοιπόν, περιπτώσεις, όπου οι επιχειρήσεις ή οι οργανισμοί συλλέγουν και επεξεργάζονται προσωπικά δεδομένα των χρηστών, με τρόπο, όπου αντίκειται στα χρηστά ήθη ή πολλές φορές, ακόμα και οι ίδιες οι επιχειρήσεις πέφτουν θύματα “hacking”, δηλαδή της παράνομης δράσεως των χρηστών-επαγγελματιών, οι οποίοι έχουν πλήρη γνώση για την κακόβουλη εκμετάλλευση του λογισμικού των πλατφορμών, παρεμβαίνουν στα προσωπικά δεδομένα και βλάπτουν τους χρήστες, πολλές φορές ζητώντας και αντίτιμο ή εκβιάζοντας τα θύματά τους.

Το ζήτημα της εμπιστευτικότητας είναι πολύ σπουδαίο, θα πρέπει ωστόσο, να κατανοήσουμε ότι οι συνέπειες, οι οποίες προκύπτουν από αυτή τη διαδικασία,

---

<sup>286</sup> Chen H. G., Chen C. C., Lo, L and Yang S. C., “Online Privacy control via anonymity and pseudonym: Cross-cultural implications”, Behaviour and Information Technology, 2008, p.229-242

<sup>287</sup> Malhotra N. K., Kim S. S., and Agarwal J., “Internet users’ information privacy concerns (IUIPC): The construct, the scale and a casual model”, Information Systems Research, 2004, p.336-355

<sup>288</sup> Weiyin Hong and James Y. L. Thong, “Internet Privacy Concerns: An integrated conceptualization and four empirical studies”, MIS Quarterly, Vol 37, No 1, March 2013, p. 275-298

μπορεί να είναι ιδιαίτερα αρνητικές, να είναι εις βάρος των καταναλωτών αλλά και να λειτουργούν ιδιαίτερα επικίνδυνα.<sup>289</sup>

Αρχικά, υπάρχει πιθανότητα, οι χρήστες να βιώσουν οικονομικές απώλειες, ύστερα από διαρροή των προσωπικών τους δεδομένων. Ατομικά στοιχεία, όπως, ο αριθμός της ταυτότητάς τους, τα στοιχεία της τραπεζής τους ή γενικότερα ατομικές πληροφορίες, οι οποίες μπορούν να οδηγήσουν σε πολύ μεγάλη βλάβη οικονομική για τον χρήστη.

Μία άλλη συνέπεια αφορά την κοινωνική ζωή του ατόμου. Οι χρήστες, οι οποίοι χρησιμοποιούν κυρίως, τα μέσα κοινωνικής δικτύωσης (social media) και προμηθεύουν υλικό στις ηλεκτρονικές πλατφόρμες, δηλαδή, στοιχεία από την ιδιωτική τους ζωή, μπορεί με τη διαρροή των παραπάνω πληροφοριών σε τρίτους, να προσβληθεί η τιμή, η υπόληψη και η αξιοπρέπειά τους, αλλά και να συμβεί η πλήρης έκθεσή τους στο δημόσιο βίο, χωρίς την άδεια, τη συναίνεση και την συγκατάθεσή τους.

Άλλη μία συνέπεια, είναι η πρόκληση ψυχολογικών ζητημάτων, λόγω του άγχους, της αναστάτωσης και του ενδεχόμενου επερχόμενου κινδύνου, τον οποίο αισθάνεται ο χρήστης, ακόμη και εάν στην πράξη, κάτι τέτοιο δε συμβαίνει.

Τέτοιο παράδειγμα, αποτελεί η περίπτωση, κατά την οποία ένας χρήστης, μπορεί να χάσει στοιχεία της τραπεζής του στην ηλεκτρονική πλατφόρμα και να θεωρήσει ότι έχει χάσει μεγάλο μέρος των χρημάτων του και να μπει στην διαδικασία να αλλάξει κωδικούς πρόσβασης ή να είναι ακόμη πιο ενεργητικός και καχύποπτος για οποιαδήποτε πιθανή, ύποπτη ενέργεια στο λογαριασμό του.<sup>290</sup>

Σ' αυτή την περίπτωση, υπάρχει ψυχολογικό άγχος, αγωνία και φόβος. Επομένως, αυτή η πρόκληση των αρνητικών συναισθημάτων, δρα αρνητικά στο άτομο και το οδηγεί στην ανάγκη ελέγχου των προσωπικών δεδομένων, αλλά και στη μεγάλη επιφυλακτικότητά του, ως προς την εμπιστοσύνη που θα πρέπει να παράσχει στις ηλεκτρονικές πλατφόρμες ή γενικότερα στο διαδίκτυο.<sup>291</sup>

---

<sup>289</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

<sup>290</sup> Ως ανωτέρω, βλ. 289

<sup>291</sup> NIST, National Institute of Standards and Technology Special Publication, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)- Recommendations of the National Institute of Standards and Technology”, 2010

## ΚΕΦΑΛΑΙΟ 7

### Πλατφόρμες κοινωνικής δικτύωσης και Facebook Cases

#### 7.1 Οι ιστοσελίδες κοινωνικής δικτύωσης (social media) και τα δεδομένα προσωπικού χαρακτήρα

Σύμφωνα με τον T. Funk (2010), τα social media, ή αλλιώς, τα μέσα κοινωνικής δικτύωσης, αποτελούν πλατφόρμες ή εφαρμογές, οι οποίες δίνουν τη δυνατότητα στους χρήστες, να φτιάξουν ένα δικό τους, εξατομικευμένο, προσωπικό και επαγγελματικό δίκτυο.

Τα πιο γνωστά μέσα κοινωνικής δικτύωσης είναι το Facebook (Meta), το Instagram, το Twitter και το LinkedIn. Σ' αυτές τις ψηφιακές πλατφόρμες, πλήθος ατόμων, αναρτά προσωπικές στιγμές του, από τον ιδιωτικό βίο, δημοσιεύσεις που αφορούν την καθημερινότητά του, απόψεις, σχόλια, γνώμες, προσωπικές εκτιμήσεις και εμπειρίες για θέματα της καθημερινότητας.<sup>292</sup>

Ακόμη, υπάρχουν πολλοί, οι οποίοι διαφημίζουν τη δουλειά τους, μέσω των κοινωνικών δικτύων, καθώς πλήθος κόσμου ακολουθούν τις σελίδες του προσωπικού προφίλ και εκείνοι, μέσα από την πλατφόρμα, παρουσιάζουν καθημερινά τη δουλειά τους, η οποία γίνεται ευρέως γνωστή, διαφημίζεται και αυτό, έχει ως αποτέλεσμα, την απόκτηση περιουσιακού οφέλους, στους χρήστες του προφίλ.

Επιπλέον όσο μεγαλύτερος είναι ο αριθμός των ατόμων που παρακολουθούν τη σελίδα του προσωπικού προφίλ, τόσο μεγαλύτερη είναι και η προσέλκυση από διαφημιστικές εταιρείες, οι οποίες έναντι αντιτίμου, επικοινωνούν με τους χρήστες, προκειμένου να προωθήσουν προϊόντα της επιχείρησής τους στο καταναλωτικό κοινό και τους υποψήφιους πελάτες που παρακολουθούν το προφίλ του χρήστη.

Η δύναμη του διαδικτύου και των μέσων κοινωνικής δικτύωσης είναι ιδιαίτερα μεγάλη, διότι έχουν πρόσβαση σ' αυτό, εκατομμύρια χρήστες ανά τον κόσμο, οι οποίοι έχουν άποψη, γνώση και εκθέτουν γνώμες και αντιλήψεις, οι οποίες επηρεάζουν σε μεγάλο βαθμό την κοινωνική ζωή.

---

<sup>292</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

Κάθε προσωπικό στοιχείο ή κομμάτι της καθημερινότητάς τους, το οποίο δημοσιεύεται στο διαδίκτυο, δε διαγράφεται από τον κυβερνοχώρο, αλλά παραμένει μέσα σε αυτόν και παντοτινά. Η διασύνδεση των ανθρώπων είναι τόσο μεγάλη, που επιτρέπει στους χρήστες να επικοινωνούν από τεράστιες αποστάσεις .

Φυσικά, πολλά από τα στοιχεία που αναρτώνται και δημοσιεύονται στο διαδίκτυο, λειτουργούν εις βάρος των χρηστών, διότι πρόκειται για δεδομένα, τα οποία είναι ιδιαίτερα προσωπικά και επιτρέπουν την εισβολή στην ιδιωτικότητά τους από τα άτομα που παρακολουθούν το προσωπικό προφίλ που έχουν δημιουργήσει.

## **7.2 Η εφαρμογή του “Facebook” και τα προσωπικά δεδομένα**

Η εφαρμογή του Facebook, η οποία αποκαλείται σήμερα ως “Meta”, αποτελεί μία από τις πιο δημοφιλείς πλατφόρμες μέσω κοινωνικής δικτύωσης παγκοσμίως. Η πλατφόρμα αυτή, το 2012 αγόρασε μία επίσης δημοφιλή εφαρμογή, εκείνη του Instagram, η οποία άρχισε, τα τελευταία χρόνια, να αποκτά τεράστια έκταση και δημοφιλία στους χρήστες του διαδικτύου και κυρίως, των social media.

Στην συγκεκριμένη πλατφόρμα, οι χρήστες δημιουργούν διαδικτυακό προφίλ, στο οποίο δημοσιεύουν στιγμές από την ιδιωτική τους ζωή, αλλά και γενικότερα, δεδομένα προσωπικού χαρακτήρα.

Ήδη από την αρχή της δημιουργίας του συγκεκριμένου προφίλ, απαιτούνται κάποια στοιχεία εξατομικευμένα, προκειμένου να μπορούν να ταυτοποιηθούν οι χρήστες, όπως είναι το ονοματεπώνυμο, ο λογαριασμός το ηλεκτρονικού ταχυδρομείου (e-mail) ή και κάποιος κωδικός πρόσβασης στην πλατφόρμα.

Κάθε προφίλ λειτουργεί με συγκεκριμένο τρόπο μέσα στην πλατφόρμα, ενώ ο κάθε χρήστης έχει το δικαίωμα να αναρτά, να δημοσιεύει οτιδήποτε εκείνος επιθυμεί στο περιεχόμενο της πλατφόρμας του, χωρίς ωστόσο, τα στοιχεία ή το περιεχόμενο που αναρτά, να αντιβαίνει τους κανονισμούς και τους όρους της πλατφόρμας.

Οι κανονισμοί αυτοί, αναφέρονται στον τρόπο με τον οποίο, θα πρέπει να λειτουργούν μέσα στην εφαρμογή, ενώ παράλληλα, αναφέρονται αναλυτικά οι όροι και οι απαγορεύσεις. Πρακτικές οι οποίες απαγορεύονται, για παράδειγμα, είναι η ώθηση σε βία, οι ψευδείς πληροφορίες, η ανάρτηση περιεχομένου που εκφράζει σύμβολα μισούς, ή οι ρατσιστικές εκφράσεις έναντι τρίτων. Πρόκειται για όρους, οι

οποίοι, είναι πρέπει να απαραίτητο να τηρούνται από όλους, έτσι ώστε να λειτουργεί ομαλά η πλατφόρμα και να μην αποτελεί εκείνη μέσο παράνομων πρακτικών.<sup>293</sup>

Η πλατφόρμα αυτή λειτουργεί με σκοπό την αλληλεπίδραση και την επικοινωνία των χρηστών, γι' αυτό άλλωστε και τους παρέχει πάρα πολλά εργαλεία, που μπορούν να χρησιμοποιήσουν για τη διευκόλυνση της επικοινωνίας μεταξύ τους.<sup>294</sup>

Όπως ήδη αναφέρθηκε, προκειμένου ένας χρήστης να δημιουργήσει προφίλ στο Facebook, αναρτά ατομικά στοιχεία και δεδομένα προσωπικού χαρακτήρα, τα οποία πολλές φορές, είτε κατά την δημιουργία του προφίλ, είτε κατά τη λειτουργία του, αποκαλύπτονται. Πολύ συχνά, αυτή η αποκάλυψη αφορά και «ευαίσθητα» προσωπικά δεδομένα, μέσω των αναρτήσεων και δημοσιεύσεων των χρηστών, στιγμών, από την ιδιωτική ζωή των ατόμων.<sup>295</sup>

Επιπροσθέτως, είναι πολύ εύκολη η παρακολούθησή τους από τρίτους, διότι κάθε δημιουργία τέτοιου αρχείου, που αφορά τα δεδομένα προσωπικού χαρακτήρα των χρηστών, είναι πολύ εύκολη στο διαδίκτυο και δύσκολα αποτελεί αντικείμενο διαγραφής από αυτό.<sup>296</sup>

Η εφαρμογή του Facebook, προκειμένου να προστατεύσει τους χρήστες της από κάθε κακόβουλη χρήση των προσωπικών τους δεδομένων, έχει δημιουργήσει εργαλεία και μηχανισμούς, προκειμένου να στραφεί προς αυτό το σκοπό, αλλά και στην προστασία της ιδιωτικής ζωής των χρηστών. Ένας τέτοιος μηχανισμός, αποτελεί το εργαλείο με όνομα «ρυθμίσεις ιδιωτικότητας» ή αλλιώς «private settings», όπου ο κάθε χρήστης έχει τη δυνατότητα να περιορίζει τη δυνατότητα άλλων χρηστών να

---

<sup>293</sup> Μαθιουδάκη Μ., «Ευρωπαϊκή Πολιτική και Θεσμοί για την Προστασία των προσωπικών δεδομένων στο Διαδίκτυο», Διπλωματική Εργασία Προγράμματος Μεταπτυχιακών Σπουδών στις Διεθνείς και Ευρωπαϊκές Σπουδές, Τμήμα Διεθνών και Ευρωπαϊκών Σπουδών, Πανεπιστήμιο Πειραιώς, 2014

<sup>294</sup> Καρύδα Μ. /Σ. Κοκολάκη, «Ψηφιακά κοινωνικά δίκτυα: Ζητήματα ιδιωτικότητας και η τεχνολογική αντιμετώπισή τους», σε Λ. Μήτρου/Α.Πισκοπάνη/Σ. Τάσση/Μ. Καρύδα/Σ.Κοκολάκη, «Facebook, blogs και δικαιώματα», Εκδόσεις Σάκκουλας, 2013.

<sup>295</sup> Παναγοπούλου-Κουτνατζή Φ., «Οι ιστότοποι Κοινωνικής Δικτύωσης ως Εθνική, Ευρωπαϊκή και Διεθνής Πρόκληση της Προστασίας της Ιδιωτικότητας», Σάκκουλας 2010.

<sup>296</sup> Καρακώστας Ι, Προστασία της ιδιωτικότητας στην Κοινωνία της Πληροφορίας, ΔιΜΕΕ 1/2004



παρακολουθούν το περιεχόμενο που δημοσιεύει, μέσω του αποκλεισμού τους από αυτό.<sup>297</sup>

Φυσικά, είναι απαραίτητο να υπάρχει γνώση, τόσο στη χρήση του διαδικτύου, όσο και ως προς την χρήση των μέσων κοινωνικής δικτύωσης, τον έλεγχο των ρυθμίσεων και την πλήρη ενημέρωση τους, έτσι ώστε οι ίδιοι να είναι εξοικειωμένοι και να μπορούν να χρησιμοποιούν κάθε εργαλείο που τους παρέχεται από την πλατφόρμα και να προστατεύονται.<sup>298</sup>

Κατανοούμε λοιπόν, ότι με αυτό τον τρόπο, το υποκείμενο των προσωπικών δεδομένων και παράλληλα, χρήστης του Facebook, δεν επιτρέπει σε όλους τους χρήστες να παρακολουθήσουν τις δημοσιεύσεις του, ή το υλικό που εκείνος επιθυμεί να αναρτήσει στην προσωπική του σελίδα, αλλά δημιουργεί ένα κύκλο προσώπων. Ένα πιο περιορισμένο, δηλαδή, σύνολο ανθρώπων οι οποίοι, μπορούμε να πούμε ότι αποτελούν τα άτομα της ιδιωτικής του σφαίρας.

Έχει επιλέξει τα άτομα, με τα οποία βρίσκεται πιο κοντά και με τα οποία επιθυμεί να επικοινωνεί περισσότερο και τα εντάσσει σε ένα προσωπικό του χώρο, χωρίς να έχει κάποιο θέμα ως προς την παρακολούθηση του υλικού του από εκείνους, τους οποίους ο ίδιος επέλεξε, σε σύγκριση με τους υπόλοιπους χρήστες.<sup>299</sup> Δηλαδή, για την μερίδα των φίλων του, την οποία επιλέγει για να ακολουθήσει κάθε δημοσίευσή του, αλλά δεν επιθυμεί να είναι όλες οι πληροφορίες του δημόσιες προς όλους. Βέβαια, ακόμα και σ' αυτή την περίπτωση, βλέπουμε στην πραγματικότητα κάτι τέτοιο να μην ισχύει, εφόσον όλες οι πληροφορίες, οι οποίες σε καταγράφονται στο διαδίκτυο, στην πραγματικότητα δύσκολα αφαιρούνται από αυτό, ενώ πολλές φορές, διαρρέουν δεδομένα προσωπικού χαρακτήρα, πράγμα το οποίο σίγουρα το υποκείμενο των δεδομένων δεν θα επιθυμούσε.<sup>300</sup>

---

<sup>297</sup> Μαθιουδάκη Μ., «Ευρωπαϊκή Πολιτική και Θεσμοί για την Προστασία των προσωπικών δεδομένων στο Διαδίκτυο», Διπλωματική Εργασία Προγράμματος Μεταπτυχιακών Σπουδών στις Διεθνείς και Ευρωπαϊκές Σπουδές, Τμήμα Διεθνών και Ευρωπαϊκών Σπουδών, Πανεπιστήμιο Πειραιώς, 2014

<sup>298</sup> Πάντζιου Γ., *Ιδιωτική ζωή και Τεχνολογίες Επικοινωνιών και Πληροφορικής*, Βήμα Ιδεών, 2008.

<sup>299</sup> Γεωργαλής Φ.-Ε. , *Η ιδιωτικότητα στο Facebook μετά τον Γενικό Κανονισμό για την Προστασία Δεδομένων*, ΔΙΤΕ 2020, 395

<sup>300</sup> Πισκοπάνη Α-Μ, *Η προστασία της ιδιωτικότητας των χρηστών του Facebook*, ΔΙΜΕΕ, 2009

Επιπρόσθετα κατά τον Ιγγλεζάκη, η προσωπική – οικιακή χρήση υπάρχει μόνο εάν το άτομο έχει πολύ στενό κύκλο προσώπων ως φίλους και πιο συγκεκριμένα, την οικογένεια, τους συγγενείς, ενώ στην πραγματικότητα δε συμβαίνει κάτι τέτοιο κατά πάσα πιθανότητα. Αντίθετα, όλα όσα δημοσιεύονται αφορούν πολύ περισσότερους φίλους.<sup>301</sup>

Κατανοούμε λοιπόν, ότι η συγκεκριμένη πλατφόρμα έχει ως στόχο την επικοινωνία και την αλληλεπίδραση των χρηστών του διαδικτύου μεταξύ τους. Είναι πολύ ευρείας κλίμακας εφαρμογή και αφορά εκατομμύρια χρήστες παγκοσμίως, οι οποίοι συνδέονται στον κυβερνοχώρο άμεσα, γρήγορα και εύκολα.

Η πλατφόρμα του Facebook έχει πολλές φορές, ενημερώσει τους χρήστες της, προκειμένου να είναι προσεκτικοί, με τις πληροφορίες που αναρτούν, ενώ επίσης, ενημερώνει για τους όρους, που διέπουν την εφαρμογή και τονίζει την προσοχή, που θα πρέπει να έχουν οι χρήστες, ως προς το περιεχόμενο που ανεβάζουν και κοινοποιούν σε τρίτους, προκειμένου να είναι ενήμεροι και να προσέχουν για τα προσωπικά τους δεδομένα. Αυτές οι προειδοποιήσεις, βέβαια, αφορούν όλους τους χρήστες, οι οποίοι κατά πάσα πιθανότητα, θεωρούν ότι βρίσκονται σε ένα ασφαλές πλαίσιο και δημοσιοποιούν τα στοιχεία της προσωπικής του ζωής σε όλους.<sup>302</sup>

### **7.2.1 Οι υποχρεώσεις των παρόχων**

Σύμφωνα με τις διατάξεις του νόμου 2472/1997, τίθενται συγκεκριμένες υποχρεώσεις από τους παρόχους των υπηρεσιών των «social media», οι οποίες αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα από κάθε παραβίαση.

Στο άρθρο 6 του ίδιου νόμου, αναφέρεται υποχρέωση του παρόχου για γνωστοποίηση, δηλαδή την ενημέρωση της αρμόδιας Αρχής, αναφορικά με την τήρηση ενός αρχείου δεδομένων. Παράλληλα, με βάση το άρθρο 11 του ίδιου νόμου,

---

<sup>301</sup> Ιγγλεζάκης Ι, Προστασία προσωπικών δεδομένων στις υπηρεσίες κοινωνικής δικτύωσης, Συνήγορος 86/2011

<sup>302</sup> Μαθιουδάκη Μ., «Ευρωπαϊκή Πολιτική και Θεσμοί για την Προστασία των προσωπικών δεδομένων στο Διαδίκτυο», Διπλωματική Εργασία Προγράμματος Μεταπτυχιακών Σπουδών στις Διεθνείς και Ευρωπαϊκές Σπουδές, Τμήμα Διεθνών και Ευρωπαϊκών Σπουδών, Πανεπιστήμιο Πειραιώς, 2014

υπάρχει υποχρέωση ενημέρωσης του υποκειμένου των δεδομένων, όπως αναφέρθηκε ήδη, σε προηγούμενες ενότητες.

Σύμφωνα με το άρθρο 4 του νόμου αυτού, οι πάροχοι, υποχρεούνται να τηρούν τα νόμιμα χαρακτηριστικά της επεξεργασίας των προσωπικών δεδομένων των χρηστών, δηλαδή να χρησιμοποιούνται, να συλλέγονται και να αποθηκεύονται από τους παρόχους, μόνο τα απαραίτητα δεδομένα, τα οποία χρειάζονται για τον εκάστοτε σκοπό και έπειτα από ένα χρονικό διάστημα, να διαγράφονται, έτσι ώστε να μην παραμένουν στην πλατφόρμα.<sup>303</sup> Ύστερα από την υλοποίηση του σκοπού τους, θα πρέπει να υπάρχει συναίνεση των χρηστών, αναφορικά με τα προσωπικά τους δεδομένα, να μην επεξεργάζονται δίχως την συγκατάθεση τους για μεγαλύτερο χρονικό διάστημα από αυτό που έχει οριστεί και να μην υπάρχει καμία παραβίαση.

Με βάση το άρθρο 12 του ίδιου νόμου, ο πάροχος οφείλει να ικανοποιήσει τα αιτήματα των υποκειμένων των προσωπικών δεδομένων, χωρίς αδικαιολόγητη καθυστέρηση, σε άμεσο χρόνο, διότι όπως επιβάλλεται από το νόμο, τα υποκείμενα έχουν το δικαίωμα της διαγραφής, τις αντιρρήσεως και της πρόσβασης στα αρχεία που αφορούν τα προσωπικά τους δεδομένα.

Παράλληλα, σύμφωνα με το άρθρο 10, υπάρχει υποχρέωση από τον πάροχο του απορρήτου, αναφορικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, των υποκειμένων. Δηλαδή, ο πάροχος θα πρέπει να διασφαλίζει με κάθε τρόπο, το απόρρητο της επεξεργασίας των δεδομένων, αλλά ταυτοχρόνως και να λαμβάνει κάθε μέτρο τεχνικού ή οργανωτικού χαρακτήρα, για την ασφάλεια των ατομικών στοιχείων των χρηστών.<sup>304</sup>

Τα συγκεκριμένα μέτρα αφορούν την ασφάλεια της καταγραφής και της επεξεργασίας των προσωπικών δεδομένων, αλλά και ειδικότερα, της επιλογής του προσωπικού-αρμοδίων της επεξεργασίας, όπως και του υπεύθυνου των προσωπικών δεδομένων, ο οποίος τα διαχειρίζεται. Κάθε πρόσωπο αυτής της θέσης, θα πρέπει να ενημερώνεται συχνά και να διαπνέεται από τις αρχές της ακεραιότητας και της εμπιστευτικότητας.

Επίσης, αναφορικά με την πλατφόρμα του Facebook, για την οποία έχει γίνει λόγος ήδη παραπάνω, είναι σημαντικό να αναφερθεί, ότι δεν επιτρέπεται η επεξεργασία «ευαίσθητων» δεδομένων των χρηστών, χωρίς να υπάρχει συναίνεση για

---

<sup>303</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

<sup>304</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

την συλλογή και την επεξεργασία των προσωπικών τους δεδομένων. Ακόμη, σε περίπτωση που χρειαστεί να συμπληρώσουν κάποια φόρμα με ερωτήσεις και απαντήσεις, θα πρέπει να είναι ξεκάθαρο ότι πρόκειται για προαιρετική συμπλήρωση της φόρμας (άρθρο 3 παρ. 4, Γνώμης 5/2009 του Art.29. WP).<sup>305</sup>

### **7.2.2 Ευθύνη μεσαζόντων στην παροχή των υπηρεσιών του διαδικτύου**

Η Οδηγία 2000/31, η οποία αφορά το ηλεκτρονικό εμπόριο, δίνει κατευθυντήριες γραμμές αναφορικά με την ύπαρξη και την ευθύνη των μεσαζόντων και γίνεται λόγος για μεσάζοντες στις υπηρεσίες διαδικτύου, στους παρόχους των υπηρεσιών και στους παρόχους περιεχομένου και στα social media, δηλαδή στα μέσα κοινωνικής δικτύωσης.

Η πάροχοι των υπηρεσιών του διαδικτύου (Internet Service Providers) είναι εκείνοι, οι οποίοι παρέχουν την πρόσβαση στο τελευταίο βήμα της διανομής των δεδομένων. Εκείνοι, δεν έχουν το δικαίωμα της παρέμβασης στο περιεχόμενο (content), αλλά απλώς της διανομής, στην τελευταία φάση, στον τελικό χρήστη.

Γίνεται κατανοητό ότι δεν υφίσταται ευθύνη του φορέα (ISP), σχετικά με τις μεταδιδόμενες πληροφορίες, καθώς εκείνος δεν είναι υπεύθυνος για τα όσα μεταφέρονται, για το περιεχόμενο, δηλαδή, της πληροφορίας, έτσι ώστε να προβεί στον έλεγχο της, πριν την διανεμίει.<sup>306</sup>

Από την άλλη πλευρά, υπάρχουν οι πάροχοι υπηρεσιών διαδικτύου, οι οποίοι ονομάζονται ως πάροχοι περιεχομένου και είναι υπεύθυνοι για το περιεχόμενο, που δημοσιεύουν στις ιστοσελίδες, αλλά και στις πλατφόρμες, στις οποίες δραστηριοποιούνται.

Κάθε πάροχος μεταφέρει την πληροφορία και το περιεχόμενο, το οποίο εκείνος δημιουργεί και τα διανέμει στο διαδίκτυο. Η πάροχοι αυτοί, ονομάζονται “Content Applications and Services Providers” (CAPs) και συμμετέχουν με ενεργό

---

<sup>305</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

<sup>306</sup> Κασσελούρη Θ., «Η αρχή της ουδετερότητας και της ίσης μεταχείρισης στο Διαδίκτυο: Το Open Internet και η εποχή των Big Data», Διπλωματική Εργασία, Εμπορικού Δικαίου, του Προγράμματος Μεταπτυχιακών Σπουδών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, Αθήνα, 2020.

τρόπο στη δημιουργία περιεχομένου, μέσω των πληροφοριών, αλλά και στη διακίνηση αυτών, στους διαδικτυακούς τόπους.<sup>307</sup>

Τίθεται η διχογνωμία, αναφορικά με την ευθύνη του, διότι υποστηρίζεται ότι δεν υπάρχει λόγος υπαιτιότητας του παρόχου περιεχομένου, σε περίπτωση που δεν μπορεί να παρακολουθεί γενικευμένα, το σύνολο των εκατομμυρίων δεδομένων και πληροφοριών, που θα αναρτηθεί στην πλατφόρμα του, δεν μπορεί να έχει πλήρη γνώση, έτσι ώστε να έχει πλήρη ευθύνη για το περιεχόμενο που παρέχει.

Ωστόσο, είναι πολύ σημαντικό να σκεφτούμε ότι υπάρχουν περιπτώσεις, όπως αυτές που εξετάζουμε, αναφορικά με την προσβολή της προσωπικότητάς, την προσβολή πνευματικής ιδιοκτησίας, ή των προσωπικών δεδομένων, ή ακόμη και του απορρήτου των επικοινωνιών.<sup>308</sup>

Βέβαια, νομολογιακά έχει κριθεί, ότι οι πάροχοι του περιεχομένου, είναι υπεύθυνοι να ενημερώνουν τις αρχές του κράτους, σε περίπτωση που υποπτεύονται ή έχουν λάβει γνώση, κάποιας παραβάσεως στο διαδίκτυο ή της απόπειρας αναρτήσεως περιεχομένου, που αντίκειται στους κανόνες του δικαίου και τις διατάξεις του νόμου, αναφορικά με τα προσωπικά δεδομένα, το απόρρητο των επικοινωνιών, η παράνομων γενικότερα, αναρτήσεων, οι οποίες εκφεύγουν από τις διατάξεις του νόμου.

Έτσι κατανοούμε, ότι οι φορείς περιεχομένου ευθύνονται για την παράβαση, εάν και εφόσον γνώριζαν την προσβολή και δεν προέβησαν σε ενημέρωση των κρατικών αρχών, άμεσα και χωρίς καθυστέρηση, ή αγνόησαν τις συστάσεις των αρχών για την άμεση αφαίρεση της παράνομης δημοσίευσης ή στην περίπτωση αδράνειάς τους, εν γένει.

Φυσικά, δεν θα πρέπει να ξεχνάμε και την περίπτωση των μέσων κοινωνικής δικτύωσης (social media), για τα οποία γίνεται λόγος και σε αυτή την ενότητα. Έχουμε παρατηρήσει πολλές μορφές παραβάσεων, σε όλες σχεδόν, τις εφαρμογές που δραστηριοποιείται στο διαδίκτυο και χρησιμοποιούνται από δισεκατομμύρια χρήστες παγκοσμίως.

Επιπρόσθετα, αυτές αφορούν παράνομες δραστηριότητες των χρηστών, που αναρτούν περιεχόμενο στις προσωπικές σελίδες τους, στο διαδίκτυο, οι οποίες ξεπερνούν τα όρια του δικαίου και του νόμου και στις οποίες, θα πρέπει να υπάρχει

---

<sup>307</sup> Ως ανωτέρω, βλ. υπ. 306

<sup>308</sup> Τασίκας Α., Άρση από Τρίτο της Προσβολής Προσωπικότητας (σε Ευθύνη από Προσβλητικό Περιεχόμενο Αναρτήσεων στο Διαδίκτυο), ΔΙΜΕΕ 3/2019

ευθύνη για αφαίρεση από τον κυβερνοχώρο, αλλά και για την προάσπιση των ελευθεριών και των δικαιωμάτων των ατόμων.

Τα social media, δηλαδή, τα μέσα κοινωνικής δικτύωσης, έχουν εδραιωθεί στην καθημερινότητα των χρηστών και χρησιμοποιούνται για πλήθος λόγων, όπως η επικοινωνία, η ενημέρωση, η έκθεση απόψεων, αλλά και ο διάλογος ή ο σχολιασμός με άλλους χρήστες, σε όλα τα θέματα της καθημερινής οικονομικής, κοινωνικής ή πολιτικής ζωής.

Ωστόσο, όπως γνωρίζουμε, δεν υπάρχει η πιθανότητα να λειτουργούν ανεξέλεγκτα όλες αυτές οι εφαρμογές, από τόσα εκατομμύρια χρήστες, χωρίς να υπάρχει έστω και ο παραμικρός έλεγχος, προκειμένου να διασφαλιστούν τα δικαιώματα των χρηστών, αλλά και οι αρχές που διέπουν το δίκαιο.

Ένα παράδειγμα ανεξέλεγκτης χρήσης πληροφοριών στο διαδίκτυο και συγκεκριμένα, στις εφαρμογές αυτές, όπως είναι το Facebook, το οποίο ονομάζεται πλέον “Meta”, είναι η ύπαρξη των ψευδών πληροφοριών, δηλαδή των «fake news», οι οποίες κατέκλυσαν το διαδίκτυο, ειδικότερα τα τελευταία χρόνια και παρέσυραν εκατομμύρια χρήστες, μέσω αυτών των ψευδών πληροφοριών, αυτών των μη αξιόπιστων και αβάσιμων στοιχείων, στην παραπληροφόρηση ή ακόμα και στην προπαγάνδα.<sup>309</sup>

Ακόμη και αν υπάρξει αφαίρεση από τις σελίδες του διαδικτύου, κάποιας ανάρτησης που δημιουργεί παραπληροφόρηση, ήδη η πληροφορία έχει μεταφερθεί σε πλήθος κόσμου και η πρόκληση της βλάβης πλέον δεν αντιστρέφεται.<sup>310</sup>

Σύμφωνα με τον Κουκιάδη, η πιο σωστή λύση θα ήταν να υπάρχει μία εξισορρόπηση, η οποία θα είναι δίκαιη και θα σταθμίζει τα δικαιώματα της

---

<sup>309</sup> Κασσελούρη Θ., «Η αρχή της ουδετερότητας και της ίσης μεταχείρισης στο Διαδίκτυο: Το Open Internet και η εποχή των Big Data», Διπλωματική Εργασία, Εμπορικού Δικαίου, του Προγράμματος Μεταπτυχιακών Σπουδών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, Αθήνα, 2020.

<sup>310</sup> Καραγκούνης Δ., «Η επιβολή περιορισμών στα μέσα κοινωνικής δικτύωσης μετά τον νέο γερμανικό Νόμο περί Βελτίωσης της Επιβολής της Νομοθεσίας στα Κοινωνικά Δίκτυα» (Netzwerkdurchsetzungsgesetz) -Επίθεση στην ελευθερία έκφρασης ή αναγκαίο μέσο καταπολέμησης της διαδικτυακής εγκληματικότητας;, ΔΙΜΕΕ 3/2018

ελευθερίας της έκφρασης και της προστασίας της προσωπικότητας του ατόμου, χωρίς ωστόσο, το ένα δικαίωμα να είναι υπέρτερο η κατώτερο του άλλου.<sup>311</sup>

Δυστυχώς, πολλές φορές στις πλατφόρμες κοινωνικής δικτύωσης, δημιουργούνται και αξιόποινες πράξεις, μέσω της δημοσίευσης παράνομου περιεχομένου, αλλά και προσβολής της προσωπικότητας των ατόμων, μέσω της ανάρτησης ρατσιστικών σχολίων, απέναντι σε ομάδες ατόμων ή ακόμη και σε ώθηση σε πρόκληση βίας ή σε εγκλήματα μίσους, τα αποκαλούμενα κα ως “hate crimes”.<sup>312</sup>

Σε κάθε περίπτωση, είναι αναγκαία η αυξημένη ευθύνη των μεσαζόντων των παρόχων υπηρεσιών περιεχομένου και στα μέσα κοινωνικής δικτύωσης, διότι υπάρχει πολύ μεγάλη και ανεξέλεγκτη πηγή πληροφοριών και η οποία, στην πραγματικότητα βλάπτει τους χρήστες και θα έπρεπε να υπάρχει μία δυνατότητα ελέγχου, αλλά και επιβολή προστίμων, σε περίπτωση που η δημοσίευση των παράνομων και ψευδών δημοσιεύσεων, δεν αποσύρεται από το περιεχόμενο των εφαρμογών, ή στην περίπτωση της σκοπούμενης παραπληροφόρησης ή δημιουργίας προπαγάνδας, ακόμη και οποιασδήποτε άλλης αξιόποινης συμπεριφοράς από τους χρήστες.

### 7.2.3 Facebook και Διαφήμιση στην πλατφόρμα

Η πλατφόρμα της κοινωνικής δικτύωσης του Facebook εμπορευματοποιεί τα προσωπικά δεδομένα σε τρίτους και αντλεί τα κέρδη της από αυτή την επεξεργασία, έτσι ώστε να επιτευχθούν οι σκοποί της διαφήμισης.

Σύμφωνα με την Οδηγία 26/2004 της ΑΠΔΠΧ, η διαφήμιση αποτελεί νόμιμη δραστηριότητα. Απορρέει από το δικαίωμα της ελεύθερης ανάπτυξης της προσωπικότητας, αλλά και το δικαίωμα της ελεύθερης ανάπτυξης οικονομικών δραστηριοτήτων.<sup>313</sup>

Σύμφωνα με το άρθρο 4 παρ.1 του νόμου 2472/1997, ο τρόπος συλλογής και επεξεργασίας των προσωπικών δεδομένων, πρέπει να γίνεται με νόμιμο τρόπο και

---

<sup>311</sup> Κουκιάδης Δ., “Fake News and Post-Truth Politics”: Μια προσέγγιση της διαδικτυακής επικοινωνίας από την οπτική της Θεωρίας του Δικαίου και του Συγκριτικού Δικαίου, Pro Justitia, τόμος 1/2018

<sup>312</sup> Κασσελούρη Θ., «Η αρχή της ουδετερότητας και της ίσης μεταχείρισης στο Διαδίκτυο: Το Open Internet και η εποχή των Big Data», Διπλωματική Εργασία, Εμπορικού Δικαίου, του Προγράμματος Μεταπτυχιακών Σπουδών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, Αθήνα, 2020.

<sup>313</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

στα πλαίσια της πλατφόρμας του Facebook, έτσι ώστε να επιτυγχάνονται οι σκοποί της διαφήμισης.

Δεν θα πρέπει βέβαια να ξεχνάμε ότι απαιτείται η συγκατάθεση του χρήστη, σύμφωνα με το άρθρο 5 παρ.1 του νόμου 2472/1997, η οποία, θα πρέπει να πραγματοποιείται με οποιοδήποτε πρόσφορο μέσο, στην οθόνη της πλατφόρμας, έτσι ώστε να μπορέσει το άτομο να δει το κείμενο της συγκατάθεσης και να δηλώσει ρητά τη συναίνεσή του (υπ' αριθμόν 2/2011 Οδηγία ΑΠΔΠΧ).

Αξιοσημείωτο είναι βέβαια, ότι αυτή η διαδικασία μπορεί να γίνει και να είναι επιτρεπτή και χωρίς την συγκατάθεση του χρήστη σε περίπτωση, κατά την οποία, είναι απαραίτητη για την εκτέλεση της σύμβασης παροχής όλων των υπηρεσιών των κοινωνικών δικτύων. Οι περιπτώσεις κατά τις οποίες επιτρέπεται και χωρίς τη συγκατάθεσή του χρήστη, η επεξεργασία των προσωπικών του δεδομένων, ορίζονται με βάση την ΑΠΔΠΧ και αφορά τους δημόσιους καταλόγους, την περίπτωση, κατά την οποία, το ίδιο το άτομο δημοσιοποίησε τα συγκεκριμένα στοιχεία, για ορισμένους μένους σκοπούς ή αν ορίζεται με βάση της εναλλακτικές σχέσεις.<sup>314</sup>

Η πλατφόρμα του Facebook έχει ως νομικό επιχειρήμα της το γεγονός ότι κατά την εγγραφή τους, οι χρήστες γνωρίζουν τους όρους και τις πολιτικές της κάθε πλατφόρμας, επομένως συγκατατίθενται με την εγγραφή τους. Ωστόσο, δεν θα πρέπει να μην ξεχνάμε, ότι πολλές φορές, αυτοί οι όροι δεν γίνονται αντιληπτοί από το σύνολο της κοινότητας, είτε συχνά, τροποποιούνται, δίχως να γίνει συγκεκριμένη ενημέρωση των χρηστών και κατά πάσα πιθανότητα δεν γνωρίζουν ότι οι όροι ή οι πολιτικές της πλατφόρμας του Facebook έχουν τροποποιηθεί και ισχύουν νέα πράγματα, πλέον.<sup>315</sup>

Είναι επομένως, σημαντικό να υπάρχει βεβαιότητα, αναφορικά με την συγκατάθεση, τη ρητή και άμεση συναίνεση των χρηστών, έτσι ώστε να είναι ασφαλή τα προσωπικά τους δεδομένα και να μην υπάρξει οποιαδήποτε παραβίαση.

---

<sup>314</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

<sup>315</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>



#### 7.2.4 Το δικαίωμα της ελευθερίας της έκφρασης στην πλατφόρμα με τη χρήση ψευδωνύμου

Τόσο στο κείμενο του ελληνικού Συντάγματος, όσο και στην Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ), προστατεύεται θεμελιωδώς, το δικαίωμα στην ελευθερία της έκφρασης.

Αυτό σημαίνει ότι κάθε άτομο έχει δικαίωμα να εκφράζει την άποψή του, αναφορικά με οποιοδήποτε ζήτημα εκείνο επιθυμεί. Παράλληλα, υπάρχει και το δικαίωμα της μετάδοσης των πληροφοριών, αλλά και η ελευθερία της συμμετοχής σε οποιαδήποτε μέσο κοινωνικής δικτύωσης επιθυμεί ο κάθε χρήστης και η οποία, μάλιστα, προστατεύεται με το δικαίωμα της πρόσβασης στην κοινωνία της πληροφορίας με βάση το άρθρο 5Α παρ. 2 του Συντάγματος.

Μέσω της χρήσης των “social media”, έχουν τη δυνατότητα να εκφράζουν την άποψή τους, είτε χρησιμοποιώντας το ονοματεπώνυμό τους, είτε ανώνυμα ή ακόμη και με τη χρήση ψευδωνύμου. Όλες αυτές οι περιπτώσεις κρίνονται ως άξιες προστασίας, προκειμένου να υπάρχει ελεύθερη πληροφόρηση, η οποία δεν περιορίζεται από κάποια επώνυμη υποχρεωτικά τοποθέτηση, αλλά μπορεί να γίνεται και εκτός επίσημης ονομασίας με τη χρήση ψευδωνύμου ή και δίχως αυτό.<sup>316</sup>

Οι χρήστες του διαδικτύου έχουν δικαίωμα, είτε στην ανώνυμη, είτε στην ψευδώνυμη επικοινωνία στην πλατφόρμα, η οποία μάλιστα μπορεί να ασκείται και χωρίς να υπάρξει καμία παρεμπόδιση ή έννομη συνέπεια εις βάρος τους, είτε από το κράτος, είτε από τους παρόχους των υπηρεσιών της πλατφόρμας.<sup>317</sup>

Παράλληλα στο κοινοτικό δίκαιο, το δικαίωμα αυτό κατοχυρώνεται επίσης, καθώς οι πάροχοι των μέσων κοινωνικής δικτύωσης οφείλουν να σέβονται την ψευδώνυμη επικοινωνία των χρηστών στο διαδίκτυο και σε περίπτωση κάποιας παραβίασης αυτού του δικαιώματος, τίθεται η γνωμοδότηση της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (άρθρο 5 παρ. 5 ν. 3471/2006 σε ενσωμάτωση της Οδηγίας 2002/58/EK).

Το ίδιο λοιπόν συμβαίνει και στην πλατφόρμα του Facebook, αλλά και σε κάθε μέσο κοινωνικής δικτύωσης, όπου η πάροχοι των συγκεκριμένων υπηρεσιών,

---

<sup>316</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

<sup>317</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

οφείλουν να σεβαστούν το δικαίωμα των χρηστών στην ψευδώνυμη επικοινωνία προκειμένου να σχολιάσουν κάποια δημοσίευση της πλατφόρμας, ή στην επιλογή της ανωνυμίας, χωρίς να τους υποχρεώνει να εκφράζονται δημόσια, εφόσον εκείνοι δεν το επιθυμούν (άρθρο 5 παρ 18, Γνώμης 5/2009 του Art.29 WP).

### **7.2.5 Η διαρροή των προσωπικών δεδομένων από την πλατφόρμα κοινωνικής δικτύωσης του “Facebook”**

Τα δεδομένα προσωπικού χαρακτήρα εκατομμυρίων χρηστών του Facebook διέρρευσαν από την ηλεκτρονική πλατφόρμα του, το 2018. Ένας ομοσπονδιακός δικαστής, λοιπόν, ενέκρινε προσωρινά, σε αυτή την περίπτωση, ότι η εφαρμογή θα πρέπει να υποβληθεί σε ελέγχους των μέτρων ασφαλείας της, για τα επόμενα πέντε χρόνια.

Η συμφωνία αυτή, θα έπρεπε να λειτουργήσει με συγκεκριμένο τρόπο, έτσι ώστε να επιλυθεί μία κατηγορία παράνομων συμπεριφορών, σχετικά με τη διείσδυση των hackers στους λογαριασμούς των χρηστών. Οι εκπρόσωποι της εφαρμογής Facebook, δήλωσαν στην αρχή, ότι αυτή η παραβίαση των προσωπικών δεδομένων, είχε ως αποτέλεσμα τη βλάβη 50 εκατομμυρίων χρηστών.<sup>318</sup>

Στη συνέχεια, ωστόσο, εκτίμησε ξανά τους χρήστες, υπολογίζοντας τους, σε 29 εκατομμύρια, εκ των οποίων τα τέσσερα ήταν γεωγραφικά τοποθετημένα στις ΗΠΑ. Ο William Alsup, ο οποίος ήταν περιφερειακός δικαστής των ΗΠΑ, ανέφερε ότι ο σκοπός ήταν να εξαλειφθεί η εύκολη πρόσβαση των hackers, οι οποίοι προσέβαλαν τα προσωπικά δεδομένα εκατομμυρίων χρηστών ανά τον κόσμο, αλλά και να υπάρξει δέσμευση, αναφορικά με τα μέτρα προστασίας, τα οποία πρέπει να ληφθούν από την ομάδα του Facebook.<sup>319</sup>

Η συμφωνία αυτή είχε ως βάση της, την ανάγκη υποβολής ελέγχου στην ασφάλεια των δεδομένων, για τα επόμενα πέντε χρόνια, ενώ παράλληλα, απαιτούσε από την πλατφόρμα, να βελτιώσει την ασφάλεια των προσωπικών δεδομένων των χρηστών της. Έπειτα, στις 5 Μαρτίου, η εταιρεία ζήτησε περαιτέρω λεπτομέρειες, αναφορικά με την επερχόμενη συμφωνία για τον έλεγχο ασφαλείας της.

---

<sup>318</sup> <https://www.courthousenews.com/judge-advances-settlement-over-2018-facebook-data-breach/>

<sup>319</sup> <https://www.courthousenews.com/judge-advances-settlement-over-2018-facebook-data-breach/>

Όλες αυτές οι δεσμεύσεις, οι οποίες περιγράφονται στη συμφωνία, αφορούν αρχικά, την αύξηση των ελέγχων ασφαλείας, την ενεργοποίηση αυτόματων ειδοποιήσεων, την ασφάλεια σε περίπτωση εντοπισμού υπόπτων μοτίβων συμπεριφοράς, τα οποία ενδέχεται να είναι παράνομα στην πλατφόρμα, αλλά και την απαίτηση από τους χρήστες λιγότερων προσωπικών στοιχείων, προκειμένου να δημιουργήσουν προφίλ ή να έχουν πρόσβαση στην πλατφόρμα τους.

Η διαρροή των προσωπικών δεδομένων του 2018 από τους hackers, ήταν ιδιαίτερα μεγάλη, διότι επηρέασε 2,7 εκατομμύρια χρήστες στις Ηνωμένες Πολιτείες Αμερικής και εξετέθησαν εκατομμύρια δεδομένα των χρηστών, αναφορικά με το ονοματεπώνυμο, την πατρίδα, την καταγωγή, την γέννηση, ή τους χώρους εργασίας τους.<sup>320</sup>

Ο Steven Adkins, υπέβαλε μήνυση στο Facebook, στις 28 Σεπτεμβρίου του 2018, όταν έλαβε γνώση της παραβίασης, αλλά και ύστερα από τη δημοσιοποίηση αυτής. Ο Alsup, αρνήθηκε το αίτημα των εναγόντων να ζητήσουν αποζημίωση, λόγω του γεγονότος ότι έχασαν τον έλεγχο, αναφορικά με τα στοιχεία των χρηστών

Η ομάδα του Facebook αντιπροσωπεύεται από την Elizabeth Deeley, τη Latham and Watkins στο Σαν Φρανσίσκο. Ο De Bartolomeo και ο Andrew Friedman της Cohen Milstein Sellers and Toll, στη Νέα Υόρκη, αντιπροσωπεύει τον ενάγοντα.  
321

## **7.2.6 Η ανάλυση της υπόθεσης “Facebook”**

### **α) Υπόθεση Cambell v. Facebook Inc**

Το 2013 στην περιοχή της California, οι Mathew Campbell και Michael Harley, σε ομαδική αγωγή, την οποία κατέθεσαν κατά της εταιρείας Facebook, υποστήριξαν ότι η εταιρεία παρακολουθούσε συστηματικά τα μηνύματα των χρηστών της, αλλά και τις διευθύνσεις που αντάλλασσαν, διαχειριζόταν τους υπερσυνδέσμους (links) και άνοιγε αυτές τις διευθύνσεις, χωρίς να έχει καμία ενημέρωση ή συναίνεση από τους χρήστες.

---

<sup>320</sup> <https://www.courthousenews.com/judge-advances-settlement-over-2018-facebook-data-breach/>

<sup>321</sup> <https://www.courthousenews.com/judge-advances-settlement-over-2018-facebook-data-breach/>

Συγκέντρωνε αυτά τα δεδομένα και στη συνέχεια, τα προωθούσε σε τρίτους, συνήθως διαφημιστές, οι οποίοι στην πορεία, απέστειλαν στοχευμένες διαφημίσεις στους χρήστες. Αυτή η πρακτική, όπως κατανοούμε, ξεπερνά τους όρους της πλατφόρμας, αλλά και παραβιάζει ταυτόχρονα, τόσο την ιδιωτικότητα των χρηστών, όσο και τα δεδομένα προσωπικού χαρακτήρα.<sup>322</sup>

Ο σκοπός αντιβαίνει στα χρηστά ήθη, διότι δεν υπήρχε καμία συναίνεση των χρηστών σε κάτι τέτοιο, ενώ επίσης, το γεγονός ότι εμφανιζόταν σε εκείνους διαφημίσεις από εμπόρους, οι οποίες ήταν στοχευμένες μάλιστα, με βάση τις προτιμήσεις τους, δείχνει ότι η διαχείριση των προσωπικών δεδομένων από τρίτους εξέφυγε τα όρια.<sup>323</sup>

Σε απάντησή της, η εταιρεία Facebook υποστήριξε ότι ο τρόπος με τον οποίο διαχειριζόταν τα δεδομένα, ήταν ανώνυμος δηλαδή ότι δεν επενέβαινε στην αλληλογραφία των χρηστών, αλλά δημιουργούσε αρχεία, τα οποία ήταν ανώνυμα. Ωστόσο, ύστερα από έρευνα, αποδείχτηκε ότι αυτός ισχυρισμός δεν ευσταθούσε, διότι κατά την προσωπική αλληλογραφία των χρηστών στο Facebook, αναγράφεται τόσο η ώρα αποστολής του μηνύματος, όσο και η ημερομηνία, ο αποστολέας και παραλήπτης του κάθε μηνύματος.<sup>324</sup>

Αυτά τα στοιχεία δεν διαγράφονται, παραμένουν στη μνήμη των πλατφορμών, ενώ οι διαχειριστές τους, τα συλλέγουν, τα αποθηκεύουν και τα επεξεργάζονται, έχοντας ως σκοπό την προώθηση τους σε τρίτους, ικανοποιώντας οικονομικούς σκοπούς και αποστέλλοντας διαφημιστικά μηνύματα, με βάση τις επιλογές, τις προτιμήσεις και τις ανάγκες του κάθε χρήστη.

Πληροφορίες, οι οποίες αποσπάστηκαν από τα προφίλ τους, από τις προσωπικές τους συνομιλίες, οι οποίες κατεγράφησαν και από τις σελίδες, τις οποίες παρακολουθούσαν ή στις οποίες δήλωσαν ότι τους αρέσουν.

Στο πρωτοβάθμιο δικαστήριο συμφωνήθηκε ως αποζημίωση το ποσό των 3, 9 εκατομμυρίων δολαρίων, ενώ οι ενάγοντες έλαβαν μόνο προσωπική, ηθική ικανοποίηση, μέσω ενός ανηρτημένου κειμένου στο Facebook..<sup>325</sup> Η συγκεκριμένη

---

<sup>322</sup> Παπαδοπούλου Β., «Η παραβίαση των προσωπικών δεδομένων στο Διαδίκτυο με σκοπό τη διαφήμιση», Διπλωματική Εργασία Προγράμματος Μεταπτυχιακών Σπουδών, Τομέα Ιστορίας, Φιλοσοφίας και Κοινωνιολογίας του Δικαίου, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2018

<sup>323</sup> Case number: 5:2013cv05996, California Northern District Court

<sup>324</sup> Ως ανωτέρω, βλ. υπ. 322

<sup>325</sup> <https://dockets.justia.com>

υπόθεση βρίσκεται στο στάδιο της έφεσης και αναμένεται η δικαστική έκβασή της.<sup>326, 327</sup>

### **β) Υπόθεση παραβίασης δεδομένων προσωπικού χαρακτήρα μέσω Facebook fanpage**

Η παρούσα υπόθεση αφορά την αίτηση για έκδοση προδικαστικής αποφάσεως, με βάση την ερμηνεία της Οδηγίας 95/46/EK, αναφορικά με την προστασία των φυσικών προσώπων, σχετικά με την επεξεργασία των προσωπικών τους δεδομένων, αλλά και την ελευθερία στην κυκλοφορία τους.<sup>328</sup>

Η συγκεκριμένη υπόθεση αφορά την Γερμανία και πιο συγκεκριμένα, ένα αίτημα το οποίο υποβλήθηκε από το Κέντρο Προστασίας Δεδομένων της Γερμανίας, έναντι μίας γερμανικής εταιρείας, η οποία ασχολείται με τον τομέα της εκπαίδευσης και είχε ως βάση την έρευνα, σχετικά με το εάν πρόκειται για νόμιμη εντολή της απενεργοποίησης της σελίδας θαυμαστών (fanpage) στην ιστοσελίδα του Facebook.

Υστερα από επεξεργασία των άρθρων της Οδηγίας, κατέληξαν στην απόφαση, αναφορικά με τις υποχρεώσεις και τις ευθύνες του υπεύθυνου επεξεργασίας των δεδομένων των χρηστών του Facebook.<sup>329</sup>

Ειδικότερα, πρόκειται για διαφορά της ιδιωτικής εταιρείας Wirtschaftsakademie, η οποία χρησιμοποιεί σελίδα θαυμαστών, μέσω της εφαρμογής κοινωνικής δικτύωσης του Facebook, προκειμένου να προσφέρει στους χρήστες, εκπαιδευτικές υπηρεσίες.<sup>330</sup>

Δηλαδή, μέσω αυτής της πλατφόρμας προωθεί τις υπηρεσίες που θέλει να παράσχει στους καταναλωτές, έτσι ώστε να επιτύχει, τόσο τη διαφήμιση όσο και την αποκόμιση πελατείας και κατ' επέκταση της αύξησης του οικονομικού οφέλους της.

---

<sup>326</sup> Frank Bednarz “Seven Reasons to object in Campbell v Facebook στον ιστότοπο: <https://cei.org/>

<sup>327</sup> Παπαδοπούλου Β., «Η παραβίαση των προσωπικών δεδομένων στο Διαδίκτυο με σκοπό τη διαφήμιση», Διπλωματική Εργασία Προγράμματος Μεταπτυχιακών Σπουδών, Τομέα Ιστορίας, Φιλοσοφίας και Κοινωνιολογίας του Δικαίου, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2018

<sup>328</sup> Ως ανωτέρω βλ. υπ. 327

<sup>329</sup> C-210/2016, <https://curia.europa.eu/juris/document>

<sup>330</sup> Ως ανωτέρω βλ. υπ. 327

Οι συγκεκριμένες σελίδες, οι οποίες βρίσκονται στο Facebook, μπορούν να δημιουργηθούν και να χρησιμοποιούνται, τόσο από επιχειρήσεις, όσο και από ιδιώτες, ύστερα από εγγραφή των δημιουργών στη σελίδα και την ταυτόχρονη ενημέρωση των χρηστών, αναφορικά με το σκοπό δημιουργίας της και τις υπηρεσίες της.<sup>331</sup>

Ωστόσο, το ζήτημα έγκειται στο γεγονός ότι εκείνοι, οι οποίοι διαχειρίζονται τη σελίδα fanpage, τη σελίδα, δηλαδή θαυμαστών, έχουν τη δυνατότητα να λάβουν στατιστικές πληροφορίες, αναφορικά με τους επισκέπτες, οι οποίες βέβαια, είναι ανώνυμες, αλλά συλλέγονται μέσω των μικρών αρχείων αποθήκευσης (“cookies”), τα οποία, όπως αναφέρθηκε και παραπάνω, εμπεριέχουν έναν εξατομικευμένο, αποκλειστικό κωδικό password και τα οποία αποθηκεύουν στοιχεία των χρηστών, για ένα συγκεκριμένο χρονικό διάστημα δύο ετών.

Η εταιρεία βέβαια, ισχυρίζεται ότι ουδέποτε υπήρξε κοινοποίηση, αποθήκευση και στη συνέχεια επεξεργασία των προσωπικών δεδομένων των χρηστών της σελίδας ή του μέσου κοινωνικής δικτύωσης. Στη συνέχεια, η εποπτική αρχή διέταξε να απενεργοποιηθεί η συγκεκριμένη σελίδα και σε περίπτωση μη συμμόρφωσης, να υπάρξει χρηματική ποινή, διότι ούτε η πλατφόρμα του Facebook, αλλά ούτε το fanpage Facebook, ενημέρωσαν τους χρήστες, αναφορικά με την συλλογή και την επεξεργασία των δεδομένων τους μέσω των “cookies”, ενώ ιδιωτική εταιρεία κατήγγειλε τη συγκεκριμένη απόφαση, ότι δεν ήταν εκείνη υπεύθυνη, βάσει της νομοθεσίας για την προστασία των προσωπικών δεδομένων μέσω της χρήσης των “cookies”.<sup>332</sup>

Με απόφαση της εποπτικής αρχής, απορρίφθηκε η καταγγελία, καθώς θεώρησε ότι η ιδιωτική επιχείρηση σκοπίμως συνέβαλε σε αυτή την συλλογή και την επεξεργασία των προσωπικών δεδομένων από το Facebook, και μάλιστα, ότι επωφελήθηκε μέσω της παροχής όλων αυτών των πληροφοριών και των στατιστικών, που παρέχονται από την πλατφόρμα.<sup>333</sup>

Ύστερα από δικαστική διαμάχη και υποβολή προδικαστικών ερωτημάτων, αναφέρθηκε το γεγονός ότι το φαινόμενο ονομάζεται «webtracking», δηλαδή η απόσπαση πληροφοριών μέσω στατιστικών, για την ικανοποίηση εμπορικών σκοπών,

---

<sup>331</sup> C-210/2016, <https://curia.europa.eu/juris/document>

<sup>332</sup> C-210/2016, <https://curia.europa.eu/juris/document>

<sup>333</sup> C-210/2016, <https://curia.europa.eu/juris/document>

οι οποίοι οδηγούν σε οικονομικά οφέλη των εταιρειών, μέσω της συλλογής και της αποθήκευσης προσωπικών δεδομένων των χρηστών.<sup>334</sup>

Κατανοούμε λοιπόν, ότι οι εταιρείες, οι οποίες προωθούν είτε προϊόντα είτε υπηρεσίες μέσω οποιαδήποτε πλατφόρμας, είναι υπεύθυνες εξίσου με αυτές, γεγονός που είναι πολύ σημαντικό προκειμένου να γίνει αντιληπτό ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να προστατεύονται άμεσα και αποτελεσματικά.<sup>335</sup>

### **γ) Υπόθεση Max Schrems κατά Facebook**

Το αντικείμενο της παρούσας υπόθεσης, αφορά την αίτηση της προδικαστικής αποφάσεως για την ερμηνεία του άρθρου 15 και 16 του κανονισμού 44/2001/ ΕΚ, αναφορικά με τη διεθνή δικαιοδοσία, αλλά και την αναγνώριση και την εκτέλεση αποφάσεων σε αστικές αλλά και εμπορικές υποθέσεις.

Συγκεκριμένα, η κύρια διαφορά, βρίσκεται ανάμεσα στον Maximilian Schrems κατά της Facebook Ireland Limited. Πρόκειται για διάφορα η οποία αφορά την συλλογή και την επεξεργασία των προσωπικών δεδομένων των χρηστών και την προσβολή συγκεκριμένα, του χρήστη Schrems, αναφορικά με τη μεταφορά πληροφοριών και λογιστικών στοιχείων μέσω του λογαριασμού κοινωνικής δικτύωσης του Facebook.

Ο Schrems, χρησιμοποιούσε το Facebook, ήδη από το 2008, αρχικά με ψευδώνυμο και στη συνέχεια από το 2010 και έπειτα με το πραγματικό του όνομα, χρησιμοποιώντας το για την αλληλεπίδραση με άλλους χρήστες, για επικοινωνία, αλλά και γενικότερη χρήση, με δημοσίευση φωτογραφιών και προσωπικών του στοιχείων.<sup>336</sup>

Ο Schrems υποστηρίζει ότι ο σκοπός προσφυγής δεν αφορά το οικονομικό κέρδος, αλλά την επιδίωξη του σεβασμού κάθε θεμελιώδους δικαιώματος, της προστασίας της προσωπικότητας, της ιδιωτικής ζωής και των προσωπικών δεδομένων, αλλά και την ανάγκη για παροχή σχετικής ενημέρωσης σε όλους τους χρήστες, αναφορικά με την πολιτική και τις πρακτικές της χρήσης του Facebook.

---

<sup>334</sup> Παπαδοπούλου Β., «Η παραβίαση των προσωπικών δεδομένων στο Διαδίκτυο με σκοπό τη διαφήμιση», Διπλωματική Εργασία Προγράμματος Μεταπτυχιακών Σπουδών, Τομέα Ιστορίας, Φιλοσοφίας και Κοινωνιολογίας του Δικαίου, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2018

<sup>335</sup> C-210/2016, <https://curia.europa.eu/juris/document>

<sup>336</sup> C-498/16, <https://curia.europa.eu/juris/document/document>.

Ο ενάγων υποστηρίζει ότι το Facebook προέβη σε πολλές παραβιάσεις προσωπικών δεδομένων και προσέφυγε στο Δικαστήριο της Ιρλανδίας, όπου έχει την έδρα της, το Facebook.<sup>337</sup>

Η αρχική προσφυγή του, δεν έγινε δεκτή, απορρίφθηκε, από το ιρλανδικό δικαστήριο, ωστόσο δικαιώθηκε από το δικαστήριο της Ευρωπαϊκής Ένωσης, όπου κατέφυγε σε μεταγενέστερο χρόνο.<sup>338</sup>

Παράλληλα, αξιοσημείωτο είναι να αναφερθεί ότι στην πράξη και γίνεται διανομή των προσωπικών δεδομένων των χρηστών μέσω των σελίδων του κυβερνοχώρου σε διαφημιστές, αλλά και στην ανταλλαγή πληροφοριών και δεδομένων μεταξύ εταιρειών και παροχών.<sup>339</sup>

Επιπλέον ως Schrems συμμετείχε και σε μία υπόθεση, τη λεγόμενη «Ευρώπη κατά Facebook», όπου μαζί με 25.000 χρήστες του Facebook, προσέφυγαν στο δικαστήριο και αξιώνουν από την εταιρεία 500 € ο καθένας για την παραβίαση της ευρωπαϊκής νομοθεσίας.<sup>340</sup>

#### δ) Sponsored Stories

Το Facebook είχε εγκαταστήσει ένα πρόγραμμα διαφημίσεων, το οποίο ονομάζεται «Sponsored Stories». Το συγκεκριμένο πρόγραμμα αποτελούσε κλασική περίπτωση παραβίασης προσωπικών δεδομένων των χρηστών στο διαδίκτυο, διότι εμφάνιζε στους χρήστες πληροφορίες άλλων χρηστών, στο Facebook, αναφορικά με την προτίμηση που εξέφραζαν, μέσω της επιλογής του πλήκτρου «Like».<sup>341</sup>

Πιο συγκεκριμένα, χρήστες, οι οποίοι ήταν φίλοι στο Facebook ειδοποιούνταν ο ένας από τον άλλον, αναφορικά με το αν πάτησε ή όχι, το πλήκτρο «μου αρέσει» σε κάποια σελίδα ή σύνδεσμο, χωρίς να δοθεί συγκατάθεση από τους χρήστες, αλλά και χωρίς να υπάρχει η δυνατότητα να ρυθμίσουν οι ίδιοι, μέσω του

---

<sup>337</sup> C-498/16, <https://curia.europa.eu/juris/document/document>

<sup>338</sup> Παπαδοπούλου Β., «Η παραβίαση των προσωπικών δεδομένων στο Διαδίκτυο με σκοπό τη διαφήμιση», Διπλωματική Εργασία Προγράμματος Μεταπτυχιακών Σπουδών, Τομέα Ιστορίας, Φιλοσοφίας και Κοινωνιολογίας του Δικαίου, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2018

<sup>339</sup> C-498/16, <https://curia.europa.eu/juris/document/document>

<sup>340</sup> Ως ανωτέρω, βλ. υπ. 338

<sup>341</sup> Ως ανωτέρω, βλ. υπ. 338



απορρήτου την μη εμφάνιση αυτών των πληροφοριών, οι οποίες είναι προσωπικές και αποτελούν δεδομένα των χρηστών.<sup>342</sup>

Αυτή η δυνατότητα, δεν δινόταν σε κανέναν από τους χρήστες, ούτε σε εκείνον, ο οποίος επέλεγε μέσω του « fb like» να δηλώσει την προτίμηση του, αλλά ούτε και στο χρήστη, ο οποίος λαμβάνει την ειδοποίηση, προκειμένου να μην του εμφανίζονται αυτές οι προσωπικές πληροφορίες.

Ύστερα από την εκδίκαση της υπόθεσης, το αμερικανικό δικαστήριο έκρινε ότι το Facebook όφειλε να αποζημιώσει τους χρήστες, τους οποίους έβλαψε, διότι αποκόμισε 73 εκατομμύρια από το διαφημιστικό πρόγραμμα «sponsored stories» παρουσιάζοντας τα προσωπικά δεδομένα 150 εκατομμυρίων χρηστών.<sup>343</sup>

Αυτή η παραβίαση, αφορά μεγάλο αριθμό χρηστών, στους οποίους όφειλε να καταβάλει αποζημίωση ύψους 20 εκατομμυρίων δολαρίων, ενώ παράλληλα ακολούθησε διακανονισμός, ο οποίος αφορούσε μέτρα, τα οποία θα έπρεπε να λάβει το Facebook, αναφορικά με τα δικαιώματα των χρηστών και τη χρήση των προσωπικών δεδομένων τους, αλλά να τους δώσει τη δυνατότητα να ελέγχουν τις προσωπικές τους πληροφορίες στην πλατφόρμα.<sup>344</sup>

---

<sup>342</sup> Drew Hendricks, άρθρο σε [www.forbes.com](http://www.forbes.com) και [www.newmoney.gr](http://www.newmoney.gr), 2014

<sup>343</sup> Παπαδοπούλου Β., «Η παραβίαση των προσωπικών δεδομένων στο Διαδίκτυο με σκοπό τη διαφήμιση», Διπλωματική Εργασία Προγράμματος Μεταπτυχιακών Σπουδών, Τομέα Ιστορίας, Φιλοσοφίας και Κοινωνιολογίας του Δικαίου, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2018

<sup>344</sup> Ως ανωτέρω, βλ. υπ. 343

## ΚΕΦΑΛΑΙΟ 8

### Τρόποι προστασίας, Δικαιώματα και Κυρώσεις

#### 8.1 Νέες Τεχνολογίες και τρόποι προστασίας των προσωπικών δεδομένων στον κυβερνοχώρο

Οι χρήστες του διαδικτύου και των μέσων κοινωνικής δικτύωσης επιθυμούν πάντοτε να χρησιμοποιούν εφαρμογές, οι οποίες θα προστατεύουν τα προσωπικά τους δεδομένα, από τη διαχείρισή τους από κακόβουλους τρίτους, οι οποίοι μπορούν να τους βλάψουν.

Το κομμάτι της ιδιωτικότητας, της προστασίας της προσωπικότητας, αλλά και της εμπιστευτικότητας, έχει αναλυθεί παραπάνω και έχει ως βασική προϋπόθεση, την εφαρμογή στην πράξη, όλων αυτών των αρχών, προκειμένου να αποφευχθεί οποιαδήποτε αρνητική συνέπεια, όπως περιγράφηκε αναλυτικά στις προηγούμενες ενότητες.

Τα υποκείμενα των προσωπικών δεδομένων, τα οποία προωθούν τα ατομικά τους στοιχεία στις εφαρμογές, επιθυμούν να τις χρησιμοποιούν με ασφάλεια, να αισθάνονται ότι μπορούν να εμπιστευτούν τα άτομα που τις διαχειρίζονται και να ικανοποιήσουν τους σκοπούς της παροχής των προσωπικών δεδομένων σε τρίτους.

Αυτοί οι σκοποί ικανοποιούνται μέσω της εκπλήρωσης των επιθυμιών τους, των αναγκών τους και την κάλυψη οποιοδήποτε αγοράς, η συναλλαγής, με κάποια επιχείρηση, η οποία λειτουργεί στο διαδίκτυο. Παράλληλα, η αναζήτηση στις μηχανές αναζήτησης, θα πρέπει να είναι ασφαλής για όλους τους χρήστες και να είναι σίγουροι ότι μπορούν να ελέγξουν, ανά πάσα στιγμή, τον τρόπο επεξεργασίας των δεδομένων τους, αλλά και τον χρόνο παραμονής τους στην πλατφόρμα.

Υπάρχουν χρήστες, οι οποίοι έχουν ως σκοπό τους, την ελεγχόμενη γνωστοποίηση των ατομικών τους στοιχείων. Αυτό σημαίνει ότι δεν αποδέχονται να αποκαλύψουν τις διευθύνσεις προσωπικής ταυτοποίησης (IP), αλλά αποδέχονται την αποκάλυψη των διευθύνσεων μη προσωπικής ταυτοποίησης, έτσι ώστε να μπορέσουν

να έχουν πρόσβαση στο διαδίκτυο, στις εφαρμογές και σε ηλεκτρονικές πλατφόρμες, τις οποίες θέλουν να επισκεφθούν.<sup>345</sup>

Βέβαια, θα πρέπει να αναφέρουμε ότι αυτή η δυνατότητα δεν παρέχεται σε όλους και είναι ιδιαίτερα δύσκολο να γίνει αυτή η διάκριση από τους χρήστες. Σε περίπτωση βέβαια, που οι χρήστες επιθυμούν, μία πολύ μεγάλη προστασία της ιδιωτικής σφαίρας της προσωπικής του ζωής, των ατομικών των στοιχείων, στις πλατφόρμες, μπορούν να επιτύχουν τη λεγόμενη «διαδικτυακή ανωνυμία» (internet anonymity), έτσι ώστε να μην έχουν τρίτοι, τα ατομικά στοιχεία προσωπικής ταυτοποίησης των χρηστών, να μην μπορούν να τα διαχειριστούν και να συλλέξουν ή να συνδεθούν με τις συγκεκριμένες πληροφορίες σε ηλεκτρονικές σελίδες και ιστοτόπους.<sup>346</sup>

Προς αυτή την κατεύθυνση κινούνται και περισσότερες νέες τεχνολογίες και εφαρμογές, προκειμένου να εξασφαλίζεται η πλήρης προστασία των χρηστών, να διαπνέεται από κλίμα εμπιστοσύνης και σεβασμού των προσωπικών δεδομένων των καταναλωτών – χρηστών. Βασιζόμενη σε όλες τις αρχές που αναφέρθηκαν παραπάνω, αυτές οι νέες τεχνολογίες, οδηγούν σε τρόπους προστασίας, που ενισχύουν στην πράξη την ασφάλεια των χρηστών.

Η Privacy Rights Clearing House, κινούμενη προς αυτό το στόχο, ενημέρωσε τους χρήστες, ήδη παρέχοντάς τους ιδιαίτερες οδηγίες, αναφορικά με την προστασία τους στο διαδίκτυο, την προστασία των προσωπικών τους δεδομένων και της ιδιωτικότητάς τους.<sup>347</sup>

Αρχικά, μία οδηγία, η οποία κατευθύνεται προς αυτό το σκοπό, είναι η χρήση πολύ καινοτόμων και εξειδικευμένων νέων λογισμικών, τα οποία δίνουν τη δυνατότητα στους χρήστες να αποκρύπτουν τη διεύθυνση IP τους, ή να μην επιτρέπουν την αποκάλυψη της διεύθυνσης προσωπικής ταυτοποίησης, αλλά αντίθετα να παρέχονται στην εφαρμογή, μόνο οι πληροφορίες μη προσωπικής ταυτοποίησης

---

<sup>345</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

<sup>346</sup> Tucker C., “The Economic Value of Online Customer Data”, OECD, Paris, 2010

<sup>347</sup> Πόπη Κ. Ευγενία, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015

των χρηστών, οι οποίες, άλλωστε δεν οδηγούν σε άμεση ταυτοποίησή του και αναγνώρισή του από το περιβάλλον του ή τρίτους.<sup>348</sup>

Δίνεται η δυνατότητα της χρήσης παράλληλα, του προγράμματος περιήγησης “Web Browser” και πιο συγκεκριμένα, η επιλογή της ιδιωτικής περιήγησης, δηλαδή “Private Browsing”, έτσι ώστε να μην επιτρέπεται η χρήση των “cookies” και να προστατεύεται περισσότερο η ιδιωτικότητα των χρηστών. Βέβαια, υπάρχει και η πιθανότητα να μην σβήνονται στην πραγματικότητα όλα τα ίχνη περιήγησης, αλλά σε κάθε περίπτωση, αυτή είναι μία επιλογή και ένας τρόπος προστασίας, μέσω της χρήσης των νέων τεχνολογιών.<sup>349</sup>

Μέσω του “Browser” υπάρχει επίσης, η δυνατότητα της επιλογής από τον χρήστη της εντολής «Do not track», που σημαίνει ότι δεν επιθυμεί το άτομο τη συνέχιση της παρακολούθησής του. Ωστόσο, υπάρχουν εταιρείες, οι οποίες δεν επιδέχονται αυτή την εντολή στο λογισμικό τους και εξακολουθούν να λειτουργούν στο διαδίκτυο, χωρίς αυτό.<sup>350</sup>

Επιπρόσθετα, κάθε φορά που οι χρήστες, θέλουν να επιλέξουν μία μηχανή αναζήτησης, θα πρέπει να παρατηρήσουν συγκεκριμένα χαρακτηριστικά και τους όρους ή τις πολιτικές της καθεμίας από αυτές. Υπάρχουν μηχανές αναζήτησης, οι οποίες δεν καταγράφουν την διεύθυνση IP των χρηστών τους.

Παράλληλα, έχουν τις δικές τους κατευθυντήριες γραμμές, από την Ομοσπονδιακή Επιτροπή Εμπορίου των ΗΠΑ, αναφορικά με τον τρόπο χρήσης των πλατφορμών και την καταχώριση των προσωπικών στοιχείων των χρηστών.<sup>351</sup> Πιο συγκεκριμένα, υπάρχουν συστάσεις, οι οποίες αναφέρονται στον τρόπο πλοήγησης, την προσεκτική χρήση ιστοσελίδων, που δημιουργούν καχυποψία ή παρουσιάζουν χαρακτηριστικά, τα οποία μπορεί να περιλαμβάνουν ανεπιθύμητο περιεχόμενο, «ιούς», υποκλοπή προσωπικών στοιχείων μέσω του ηλεκτρονικού ταχυδρομείου (e-mail), αλλά και την πολύ προσεκτική δημιουργία κωδικών (password και username), τα οποία θα πρέπει να χρησιμοποιούν οι χρήστες ατομικά, αποκλειστικά, χωρίς να

---

<sup>348</sup> Ως ανωτέρω, βλ. υπ. 347

<sup>349</sup> Angst, C.M. and Agarwal, R., “Adoption of Electronic Health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion”, MIS Quarterly, 2009, p. 339-370

<sup>350</sup> Ως ανωτέρω, βλ. υπ. 347

<sup>351</sup> Ως ανωτέρω, βλ. υπ. 347

δίνουν σε τρίτους αυτές τις πληροφορίες, προκειμένου να συνδέονται στο λογαριασμό τους.<sup>352</sup>

Με αυτούς τους τρόπους και τις συστάσεις, οι οποίες δίνουν τις κατευθυντήριες γραμμές από την Επιτροπή των ΗΠΑ, δημιουργούν περισσότερο το αίσθημα ασφάλειας στην περιήγηση του διαδικτύου, αλλά και το αίσθημα εμπιστευτικότητας, ως προς τη χρήση των ιστοτόπων, μέσα από αυτούς τους όρους και τις προϋποθέσεις που τίθενται, έτσι ώστε να διαφυλαχθούν τα προσωπικά τους δεδομένα από κάθε κακόβουλη διαχείριση.<sup>353</sup>

## **8.2 Δικαίωμα άσκησης μέσω έννομης προστασίας**

Σε περιπτώσεις κατά τις οποίες παραβιάζονται τα προσωπικά δεδομένα των χρηστών του διαδικτύου και πιο συγκεκριμένα, των χρηστών των μέσω κοινωνικής δικτύωσης, όπως είναι το Facebook, οι χρήστες θα πρέπει να γνωρίζουν ότι έχουν δικαίωμα για την άσκηση μέσω έννομης προστασίας, προκειμένου να προστατευτούν αποτελεσματικά και να αποτρέψουν οποιαδήποτε προσβολή των δικαιωμάτων τους στο μέλλον.

Αρχικά, τα υποκείμενα, έχουν το δικαίωμα της υποβολής αίτησης, αναφορικά με την παροχή από τα “social media”, όλων εκείνων των πληροφοριών που αφορούν τα προσωπικά τους δεδομένα. Πρόκειται για το δικαίωμα της ενημέρωσης, το δικαίωμα της πρόσβασης, αλλά και τις αντιρρήσεως, όπως έχει αναφερθεί στα προηγούμενα κεφάλαια της παρούσας μελέτης.<sup>354</sup>

Επιπρόσθετα, έχουν το δικαίωμα να καταγγείλουν κάθε παράβαση και να αιτηθούν την επιβολή προστίμου, έτσι ώστε να υπάρξει συμμόρφωση από τους παρόχους ενώπιον της ΑΠΔΠΧ. Επιπλέον, οι χρήστες έχουν τη δυνατότητα να ζητήσουν αποζημίωση, κατά το ελάχιστο 5900 ευρώ (άρθρο 23 ν. 2472/1997), την παύση της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και τη διαγραφή τους.<sup>355</sup>

---

<sup>352</sup> FTC (Nicole Vincent), “Preventing Identity Theft and other Cyber-Crimes”, 2011

<sup>353</sup> Ως ανωτέρω, βλ. υπ. 347

<sup>354</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

<sup>355</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

Τέλος, μπορούν να καταθέσουν έγκληση, σε περίπτωση τέλεσης ποινικού αδικήματος κατά οποιουδήποτε υπευθύνου των υπηρεσιών των «social media». Όλες αυτές οι δυνατότητες, παρέχονται στους χρήστες, προκειμένου να αισθάνονται ασφάλεια σε περίπτωση που βρεθούν στη θέση εκείνη, κατά την οποία έχουν παραβιαστεί τα προσωπικά τους δεδομένα και χρειάζονται οπωσδήποτε άμεση λύση στο ζήτημα αυτό, ενώ πολλές φορές, το ζήτημα της αποζημίωσης, δεν καλύπτει τους χρήστες, διότι έχουν διαρρεύσει τα στοιχεία της ιδιωτικής τους ζωής, χωρίς τη συναίνεση και τη θέλησή τους. Έχουν εμπορευματοποιηθεί τα ατομικά τους στοιχεία, ενώ συχνά, αυτή η κατάσταση είναι μη αναστρέψιμη, διότι στο διαδίκτυο οι πληροφορίες διανέμονται σε ταχύτατο ρυθμό και πολλές φορές, είναι δύσκολη η διαγραφή τους από τον κυβερνοχώρο, διότι έχει γίνει ήδη η κυκλοφορία της πληροφορίας σε τρίτους.<sup>356</sup>

### **8.3 Οι κυρώσεις σε περιπτώσεις παραβάσεων**

#### **α) Διοικητικές κυρώσεις**

Σύμφωνα με το άρθρο 21 του νόμου 2472/1997, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μπορεί να επιβάλει πρόστιμο σε παρόχους των υπηρεσιών των «social media», σε κάθε περίπτωση κατά την οποία παραβαίνουν τους όρους και τις πολιτικές τους και το νόμο. Οι διοικητικές κυρώσεις, σε περίπτωση της παραβίασης αφορούν την ενημέρωση, προκειμένου να αρθεί η παράβαση με αποκλειστική προθεσμία.<sup>357</sup>

Η Αρχή μπορεί να τους επιβάλει χρηματικό πρόστιμο, να προβεί σε ανάκληση άδειας προσωρινού η οριστικού χαρακτήρα, αλλά και να επιβάλει την καταστροφή του αρχείου, που αφορά τα προσωπικά δεδομένα. Όλες αυτές οι κυρώσεις, αφορούν διοικητικές κυρώσεις, οι οποίες επιβάλλονται από την ΑΠΔΠΧ, προκειμένου να υπάρχει μια ασφάλεια, προστασία και έλεγχος, οι πάροχοι να μη δρουν ανεξέλεγκτα και να υπάρχει επιβολή κυρώσεων σε περίπτωση παραβίασης.<sup>358</sup>

---

<sup>356</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

<sup>357</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

<sup>358</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

## β) Ποινικές κυρώσεις

Σύμφωνα με το άρθρο 22 του νόμου 2472/1997, προβλέπονται ποινικές κυρώσεις σε κάθε φυσικό ή νομικό πρόσωπο, το οποίο δρα αντίθετα με τις διατάξεις του παρόντος νόμου, αναφορικά με την προστασία των προσωπικών δεδομένων.

Αυτές οι κυρώσεις επιβάλλονται σε κάθε άτομο, το οποίο διατηρεί αρχείο με προσωπικά δεδομένα χρηστών του διαδικτύου ή γενικότερα δεδομένα προσωπικού χαρακτήρα τρίτων, κατά παράβαση τόσο του νόμου του κράτους, όσο και των όρων της άδειας της Αρχής Προστασίας Δεδομένων Προσωπικού χαρακτήρα.<sup>359</sup>

Αυτό το αρχείο με τα ατομικά στοιχεία, αποτελεί παράνομο αρχείο, διότι κανένας δεν έχει δικαίωμα να βλάπτει, να επεξεργάζεται, να κοινοποιεί, ή να αλλοιώνει ατομικά στοιχεία τρίτων, δίχως τη συναίνεση και την άδειά τους.

Σ' αυτή την περίπτωση, τίθεται φυλάκιση ενός έτους και χρηματική ποινή. Σε περίπτωση κατά την οποία, ήθελε να αποκομίσει παράνομο περιουσιακό όφελος, ή να προβεί σε βλάβη τρίτου, επιβάλλεται κάθειρξη χρονικού διαστήματος έως και 10 ετών και χρηματική ποινή, ενώ εάν οι παραπάνω πράξεις τελέστηκαν από αμέλεια, προβλέπεται φυλάκιση έως τριών ετών και χρηματική ποινή.<sup>360</sup>

Παράλληλα, εάν το πρόσωπο, το οποίο επεξεργάστηκε τα προσωπικά δεδομένα είναι υπεύθυνος για αυτά, αλλά αποτελεί νομικό πρόσωπο, τότε την ευθύνη την έχει ο εκπρόσωπός του ή η διεύθυνση αυτού.<sup>361</sup>

---

<sup>359</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

<sup>360</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

<sup>361</sup> <https://lawandtech.eu/2015/02/02/facebook-data-protection/>

## Συμπεράσματα

Στην παρούσα μελέτη έγινε εκτενής αναφορά στο ζήτημα των προσωπικών δεδομένων, της παραβίασής τους, αλλά και για τη σχέση τους με το δίκαιο του Ανταγωνισμού. Το γεγονός της παράνομης συγκέντρωσης, αλλά και της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα άρχισε να απασχολεί από πολύ νωρίς τους νομικούς, διότι αποτελούσε έναν μεγάλο κίνδυνο για την εισβολή στην ιδιωτικότητα των καταναλωτών, των πολιτών αλλά και των χρηστών του διαδικτύου σε περίπτωση που εκείνοι χρησιμοποιούσαν τις διαδικτυακές πλατφόρμες για την επικοινωνία τους με άλλους χρήστες ή για την διεκπεραίωση ηλεκτρονικών συναλλαγών και εμπορικών δραστηριοτήτων στον κυβερνοχώρο.

Η προστασία των χρηστών του διαδικτύου αλλά και η εν γένει προστασία των ατόμων, αποτέλεσε καθοριστικό λόγω σύνταξης νομοθεσιών, οι οποίες θα απαγορεύουν ρητά την οποιαδήποτε κατάχρηση εις βάρος των πολιτών από τρίτους, οι οποίοι με κακόβουλο τρόπο εκμεταλλεύονται, καταχρώνται και παραβιάζουν τα δεδομένα προσωπικού χαρακτήρα άλλων.

Η ανθρώπινη αξιοπρέπεια και η προστασία της, αποτέλεσαν δηλαδή πρωταρχικούς παράγοντες, έτσι ώστε να θεσπιστούν νόμοι, προκειμένου να σταματήσει η συλλογή, η χρήση, η επεξεργασία των πληροφοριών ή η διαρροή τους τόσο στον κυβερνοχώρο όσο και εκτός τούτου.

Το ζήτημα αυτό απασχόλησε, αλλά εξακολουθεί να απασχολεί πλήθος ατόμων τόσο νομοθετών όσο και καταναλωτών, διότι είναι όντως, υψίστης σημασίας το γεγονός εάν οι πολίτες θα μπορούν να εμπιστεύονται τις ατομικές τους πληροφορίες σε τρίτους, δίχως τα στοιχεία τους να εκτίθενται σε κακόβουλους χρήστες, οι οποίοι έχουν σκοπό την κερδοσκοπική χρήση αποκομίζοντας ίδιον όφελος και βλάπτοντας τους πρώτους.

Τόσο η γέννηση, όσο και η εξέλιξη του διαδικτύου, αλλά την ραγδαία ανάπτυξη του στο σύγχρονο κόσμο μέσω της παγκόσμιας χρήσης του σε καθημερινή βάση, αποτέλεσαν το έρεισμα για την επεξεργασία εκατομμυρίων δεδομένων καταναλωτών ανά τον πλανήτη. Δηλαδή, το συγκεκριμένο δίκτυο αποτελεί παγκόσμιο δίκτυο υπολογιστών το οποίο έχει τη δυνατότητα να παρέχει σε κάθε άτομο πρόσβαση στην πληροφορία, αλλά και στα δεδομένα τρίτων ατόμων.



Επιπρόσθετα, στην παρούσα μελέτη, έγινε λόγος για το δικαίωμα στην ιδιωτικότητα, αναφορικά με τη συλλογή, επεξεργασία, αποθήκευση και επίδειξη πληροφοριών σε τρίτους τόσο διαδικτυακά όσο και εκτός του συστήματος των ηλεκτρονικών πλατφορμών.

Επιπλέον, όπως ήδη έχει αναφερθεί, το θέμα της παράβασης των προσωπικών δεδομένων έχει λάβει μεγάλες διαστάσεις σε παγκόσμιο επίπεδο, διότι οι καταναλωτές δεν έχουν μεγάλη δυνατότητα ελέγχου των πρακτικών που ακολουθούν οι επιχειρήσεις αναφορικά με τα ατομικά τους στοιχεία.

Τα αποτελέσματα αυτής της κατάχρησης και της εκμετάλλευσης είναι ποικίλα, όπως για παράδειγμα, η κλοπή στοιχείων της ταυτότητας, οικονομικές απώλειες, ή ακόμα και απώλεια της ζωής και της υγείας του ατόμου, εξαιτίας διαρροής δεδομένων προσωπικού χαρακτήρα από κακόβουλους τρίτους με σκοπό την βλάβη των πρώτων.

Κατανοούμε λοιπόν, ότι είτε πρόκειται για διαδικτυακές πλατφόρμες, είτε για φυσική επικοινωνία στην σχετική αγορά, σε κάθε περίπτωση, τα προσωπικά δεδομένα θα πρέπει να προστατεύονται από εκείνους οι οποίοι τα συλλέγουν, αλλά και να ελέγχονται από τους καταναλωτές έτσι ώστε να εφαρμόζονται οι νομοθεσίες που έχουν θεσπιστεί για την προστασία της αξιοπρέπειας, της τιμής και της προσωπικότητας του κάθε πολίτη.

## Βιβλιογραφία και Ηλεκτρονικές Πηγές

### Ελληνική Βιβλιογραφία

- *Αγρησιλάου Π.*, «Καταχρηστική Εκμετάλλευση Δεσπόζουσας θέσης», Επιμορφωτικό Σεμινάριο ΚΕΒΕ, 18 Μαρτίου 2021-Μέρος Β.
- *Αλεξανδροπούλου-Αιγυπτιάδου Ευγενία*, « Προσωπικά δεδομένα: Η νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους», Εκδ. Αντ. Ν. Σάκκουλας, 2007
- *Βέττας Ν./ Κατσουλάκος Γ.*, «Πολιτική Ανταγωνισμού και Ρυθμιστική Πολιτική», Εκδόσεις Τυπωθήτω- Γιώργος Δαρδανός, 2004
- *Γεωργαλής Φ.-Ε.* , Η ιδιωτικότητα στο Facebook μετά τον Γενικό Κανονισμό για την Προστασία Δεδομένων, ΔΙΤΕ 2020, 395
- *Γιαννοπούλου Σ.*, «Προστασία Προσωπικών Δεδομένων στον Εργασιακό Χώρο», Διπλωματική Εργασία Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών (Δ.Π.Μ.Σ.) «Δίκαιο και Οικονομία», Πανεπιστήμιο Πειραιώς, 2017
- *Ξανθούλης Ν.*, «Το δικαίωμα στη λήθη υπό το φως των ανθρωπίνων δικαιωμάτων», ΔΙΜΕΕ 2/2013, σελ. 178
- *Σιδηρόπουλος Θ.*, «Το Δίκαιο του Διαδικτύου, Εκδόσεις Αντ. Σάκκουλα, Αθήνα, 2008
- *Ιγγλεζάκης Ι.*, Το δίκαιο της ψηφιακής οικονομίας, Εκδόσεις Σάκκουλα, Αθήνα, 2022

- **Ιγγλεζάκης Ι**, Προστασία προσωπικών δεδομένων στις υπηρεσίες κοινωνικής δικτύωσης, Συνήγορος 86/2011
- **Καραγκούνης Δ.**, «Η επιβολή περιορισμών στα μέσα κοινωνικής δικτύωσης μετά τον νέο γερμανικό Νόμο περί Βελτίωσης της Επιβολής της Νομοθεσίας στα Κοινωνικά Δίκτυα» (Netzwerkdurchsetzungsgesetz) -Επίθεση στην ελευθερία έκφρασης ή αναγκαίο μέσο καταπολέμησης της διαδικτυακής εγκληματικότητας;, ΔΙΜΕΕ 3/2018
- **Καράκωστας Ι**, Προστασία της ιδιωτικότητας στην Κοινωνία της Πληροφορίας, ΔιΜΕΕ 1/2004
- **Κασσελούρη Θ.**, «Η αρχή της ουδετερότητας και της ίσης μεταχείρισης στο Διαδίκτυο: Το Open Internet και η εποχή των Big Data», Διπλωματική Εργασία, Εμπορικού Δικαίου, του Προγράμματος Μεταπτυχιακών Σπουδών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, Αθήνα, 2020.
- **Καρύδα Μ. /Σ. Κοκολάκη**, «Ψηφιακά κοινωνικά δίκτυα: Ζητήματα ιδιωτικότητας και η τεχνολογική αντιμετώπισή τους», σε Λ. Μήτρου/Α.Πισκοπάνη/Σ. Τάσση/Μ. Καρύδα/Σ.Κοκολάκη, «Facebook, blogs και δικαιώματα», Εκδόσεις Σάκκουλας, 2013.
- **Κουκιάδης Δ.**, “Fake News and Post-Truth Politics”: Μια προσέγγιση της διαδικτυακής επικοινωνίας από την οπτική της Θεωρίας του Δικαίου και του Συγκριτικού Δικαίου, Pro Justitia, τόμος 1/2018
- **Μαθιουδάκη Μ.**, «Ευρωπαϊκή Πολιτική και Θεσμοί για την Προστασία των προσωπικών δεδομένων στο Διαδίκτυο», Διπλωματική Εργασία Προγράμματος Μεταπτυχιακών Σπουδών στις Διεθνείς και Ευρωπαϊκές Σπουδές, Τμήμα Διεθνών και Ευρωπαϊκών Σπουδών, Πανεπιστήμιο Πειραιώς, 2014

- **Μικρουλέα Α.**, «Ηλεκτρονικές αγορές μεταξύ επιχειρήσεων (B2B) και Δίκαιο Ανταγωνισμού», ΕΕμπΔ 4/2003
- **Μικρουλέα Α.**, «Η κατάχρηση δεσπόζουσας θέσης του άρθρου 2 ν.703/77, ΧρΙΔ τ. ΣΤ/2006
- **Παναγοπούλου - Κουτνατζή Φ.**, «Ο Γενικός Κανονισμός για την προστασία Δεδομένων, 790/2016/ΕΕ, Εισαγωγή και Προστασία Δεδομένων», Σάκκουλας 2017
- **Παναγοπούλου-Κουτνατζή Φ.**, «Οι ιστότοποι Κοινωνικής Δικτύωσης ως Εθνική, Ευρωπαϊκή και Διεθνής Πρόκληση της Προστασίας της Ιδιωτικότητας», Σάκκουλας 2010.
- **Πάντζιου Γ.**, Ιδιωτική ζωή και Τεχνολογίες Επικοινωνιών και Πληροφορικής, Βήμα Ιδεών, 2008.
- **Παπαδοπούλου Β.**, «Η παραβίαση των προσωπικών δεδομένων στο Διαδίκτυο με σκοπό τη διαφήμιση», Διπλωματική Εργασία Προγράμματος Μεταπτυχιακών Σπουδών, Τομέα Ιστορίας, Φιλοσοφίας και Κοινωνιολογίας του Δικαίου, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2018
- **Πισκοπάνη Α-Μ**, Η προστασία της ιδιωτικότητας των χρηστών του Facebook, ΔΙΜΕΕ, 2009
- **Πόπη Κ. Ευγενία**, « Η Διαχείριση των προσωπικών δεδομένων στην εποχή του Διαδικτύου», Διπλωματική Εργασία Διατμηματικού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα, Φεβρουάριος, 2015
- **Τασίκας Α.**, Άρση από Τρίτο της Προσβολής Προσωπικότητας (σε Ευθύνη από Προσβλητικό Περιεχόμενο Αναρτήσεων στο Διαδίκτυο), ΔΙΜΕΕ 3/2019
- **Τάσσης Σ.**, ΔΕΕ – δύο θεμελιώδεις αποφάσεις για τα προσωπικά μας δεδομένα και τα ηλεκτρονικά δίκτυα: Απόφαση C-131/12 (Google) και

συνεκδικαζόμενες C-293/12 και C-594/12 (νομιμότητα υποχρεωτικής διατήρησης τηλεπικοινωνιακών δεδομένων), ΔΙΜΕΕ 1/2014

- *Τζουγανάτος Δ.*, «Δίκαιο του Ελεύθερου Ανταγωνισμού, Νομική Βιβλιοθήκη, Αθήνα, 2020
- *Τζουγανάτος Δ.*, «Δίκαιο του Ελεύθερου Ανταγωνισμού», Νομική Βιβλιοθήκη, Αθήνα, 2013
- *Τριανταφυλλάκης Γ.*, «Δίκαιο του Ελεύθερου Ανταγωνισμού», Αθήνα, 2019
- *Τριανταφυλλάκης Γ.*, «Δίκαιο του Ελεύθερου Ανταγωνισμού», Νομική Βιβλιοθήκη, 2014
- *Χατζόπουλος Β.*, Η οικονομία των πλατφορμών (“platform economy”) και η εσωτερική αγορά της ΕΕ, ΕυΔικ 4/2019

#### **Ξενόγλωσση Βιβλιογραφία**

- *Adkinson, W.F., Eisenach, J.A., and Lenard, T.M.*, “Privacy online: A report on the information practices and policies of commercial websites, The Progress and Freedom Foundation, 2002
- *Angst, C.M. and Agarwal, R.*, “Adoption of Electronic Health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion”, MIS Quarterly, 2009, p. 339-370
- *Anne C. Witt*, Excessive Data Collection as Anticompetitive Conduct – The German Facebook Case, Jean Monnet Working Paper 8/19, THE JEAN MONNET PROGRAM J.H.H. Weiler, Director Gráinne de Burca, Director, New York, NY 10011, NYU School of Law

- **Bostoan F.**, “Online Platforms and Vertical Integration: The Return of Margin Squeeze? Journal of Antitrust Enforcement, 2018, Faculty of Law, Stockholm University Research Paper No 42, Vol 6(3), 2017
- **Buchhold F.**, “Business to Business Internet Marktplatze im Blickpunkt des europäischen und deutschen Kartellrechts, TENEA, 2005
- **Boyd M. and N.B. Ellison**, “Social network Sites: Definition, History and Scholarship”, Journal of Computer-Mediated Communication, 2007).
- **Cavoukian A. and Hamilton T.**, “Privacy Pay-off”, Mc Graw -Hill, 2002
- **Chen H. G., Chen C. C., Lo, L and Yang S. C.**, “Online Privacy control via anonymity and pseudonym: Cross-cultural implications”, Behaviour and Information Technology, 2008, p.229-242
- **Clarke Roger**, “Information privacy on the Internet”, 1998
- **Cremer J. / Y-A de Montjoye/ Schweitzer**, “Competition Policy for the Digital era, Report for the European Commission, 2019
- **Culcan, M.J., Bies R.J.**, “ Consumer Privacy: Balancing Economic and Justice Considerations”, Journal of Social Issues, 2003, p.323-342
- **E.E. David and R.M. Fano**, “Some thoughts about the Social Implications of Accessible Computing”, Proceedings 1965 Fall Joint Computer Conference, 1965
- **Elinor Mills**, “Obama unveils Consumer Privacy Bill of Rights”, 2012
- **Federal Trade Commision**, 2000

- **FTC**, “Self-Regulatory Principles for Online Behavioral Advertising”, FTC, Washington DC, 2009
- **FTC (Nicole Vincent)**, “Preventing Identity Theft and other Cyber-Crimes”, 2011
- **Funk T.**, “Social Media Playbook for Business: Reaching your online community with Twitter, Facebook, LinkedIn and more 8”, Praeger Publishers, London, 2010
- **Kirkpatrick D.**, “The Facebook effect: The inside story of the company that is connecting the world, Simon and Schuster/ Virgin Books, New York, 2010
- **Kosinski et al.**, “Private traits and attributes are predictable from digital networks of human behavior”,5802-5805 PNAS, 2013
- **Longman Dictionary of Contemporary English**, “Privacy-Definition”, Pearson, 2014
- **Malhotra N. K., Kim S. S., and Agarwal J.**, “Internet users’ information privacy concerns (IUIPC): The construct, the scale and a casual model”, Information Systems Research, 2004, p.336-355
- **Milberg S. J., Smith H. J., and Burke, S. J.**, “Information Privacy: Corporate management and National Regulation”, Organization Science, 2000, p.35-37
- **OECD**, “Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value”, OECD Digital Economy Papers, No 220, OECD Publishing, 2013
- **OECD**, “The OECD Privacy Framework”, 2013
- **Overby H., J.A. Audestad**, Standards, Regulations and Net Neutrality in the Digital Economy, 2020.

- **Li, X. B. and Sharkar S.**, “Privacy Protection in data mining: A perturbation approach for categorical data”, Information Systems Research, 2006, 254-270.
- **Narayanan A. and V. Shmatikov**, Privacy and Security Myths and fallacies of Personally identifiable information”, Communications of the ACM, vol.53, 2010
- **NIST, National Institute of Standards and Technology** Special Publication, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)- Recommendations of the National Institute of Standards and Technology”, 2010
- **Privacy** Leadership Initiative, 2001
- **Satariano A.**, “Big Tech ‘knows you better than your wife’, He plans to Rein it in, 2019
- **S. Scheindlin and D. Carpa**, “The Sedona Conference, Electronic Discovery and Digital Evidence, Thomson Reuters,2009, p.204
- **Schneier**, “Schneier on Security: A blog covering security and security technology, 2010
- **Tsai et al.**, “The Effect of Online Private Information on Purchasing Behavior”, Information Systems Research 22, 2011, p. 254-268
- **Tucker C.**, “The Economic Value of Online Customer Data”, OECD, Paris, 2010
- **Viktoria H.S.E. Robertson** (University of Graz), The Theory of Harm in the Bundeskartellamt's Facebook Decision, Edited by Thibault Schrepel, Sam Sadden & Jan Roth (CPI), Competition Policy International, Inc., March 2019



- **Wang H., M.K.O. Lee, and C. Wang**, “Consumer Privacy Concerns about Internet Marketing”, 1998
- **Ward S., Bridges K., and Chitty B.**, “Do Ncentives matter? An examination of on-line privacy concerns nd willingness to provide personal and financial information”, Journal of Marketing Communications, 2005, p. 21-40
- **Weiyin Hong and James Y. L. Thong**, “Internet Privacy Concerns: An integrated conceptualization and four empirical studies”, MIS Quarterly, Vol 37, No 1, March 2013, p. 275-298
- **Westin A.**, “Privacy and Freedom”, 25 Wash and Lee L. Rev. 166, 1968
- **Wolfgang Kerber & Karsten K. Zolna**, The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law, University of Marburg
- **Yeager J.B. and R.K Sisson**, “USER BEWARE: Maximizing the Possibilities, Minimizing the Risks of using Social Media, 33-OCT, Pa. Law.26., 2011

### **Ηλεκτρονικές Πηγές**

- [www. allaboutcookies.org](http://www.allaboutcookies.org)
- [http://www.areiospagos.gr/nomologia/apofaseis\\_result.asp?s=2&code=113](http://www.areiospagos.gr/nomologia/apofaseis_result.asp?s=2&code=113)
- [https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungn/2019/07\\_02\\_2019\\_Facebook.html](https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungn/2019/07_02_2019_Facebook.html)
- <https://www.courthousenews.com/judge-advances-settlement-over-2018-facebook-data-breach/>
- <https://cei.org/>

- <https://curia.europa.eu/juris/document/document.jsf;jsessionid=A6F40023008B4D2EEB441EF38608AC83?text=&docid=261210&pageIndex=0&doclang=DA&mode=re>
- <https://curia.europa.eu/juris/document/document.jsf;jsessionid=9232C5497F1F10E644FEDFBFF0576DAB?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&d>
- <https://curia.europa.eu/juris/document/document.jsf?mode=DOC&pageIndex=0&docid=198764&part=1&doclang=EN&text=&dir=&occ=first&cid=1870476>
- <https://dockets.justia.com>
- <https://www.dsanet.gr/Epikairothta/Nomologia/MPrAth%2011358.19.htm>
- Έκθεση OECD, Abuse of Dominance in Digital Markets, 2020
- «Πολιτική Χρήσης «cookies» στην ιστοσελίδα του Εργαστηρίου Επενδυτικών Εφαρμογών του Τμήματος Οικονομικών Επιστημών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, στη σελίδα: [www.epefa.econ.uoa.gr](http://www.epefa.econ.uoa.gr) και [allaboutcookies.org](http://allaboutcookies.org))
- («Υπηρεσίες Διαδικτύου- η χρήση cookies στο διαδίκτυο», στην ιστοσελίδα της ΑΠΔΠΧ: [www.dpa.gr](http://www.dpa.gr))
- [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach\\_el](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_el)
- [https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_el.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm)
- <https://eur-lex.europa.eu/legal-content>

- [https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31987D0500&from=EL\)](https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31987D0500&from=EL)
- <https://www.ethemis.gr/information-law-prosopika-dedomena/2022/07/29/gdpr-anaklhsh-apofasis.html>
- <https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-phek-137a-29-8-2019.html>
- Drew Hendricks, «Facebook To Drop Sponsored Stories: What Does This Mean For Advertisers?» στο διαδικτυακό περιοδικό [www.forbes.com](http://www.forbes.com), 16/1/2014, καθώς και το άρθρο «Facebook:αποζημιώνει χιλιάδες χρήστες για παραβίαση προσωπικών δεδομένων», στην ηλεκτρονική εφημερίδα [www.newmoney.gr](http://www.newmoney.gr), 27/8/2013
- <https://lawandtech.eu/2015/02/02/facebook-data-protection/>
- <https://jeanmonnetprogram.org/wp-content/uploads/JMWP-08-Anne-Witt.pdf>
- <https://jeanmonnetprogram.org/paper/excessive-data-collection-as-anticompetitive-conduct-the-german-facebook-case/>
- [https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v)
- <https://www.cms-lawnow.com/ealerts/2021/04/ecj-to-issue-preliminary-ruling-on-german-fco-facebook-case>
- Bundeskartellamt, Case Summary, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing, 15 February 2019
- [https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v)

- [https://www.ucl.ac.uk/laws/sites/laws/files/kerber\\_zolna\\_2021\\_facebook\\_case\\_competition\\_law\\_data\\_protection\\_law\\_01.pdf](https://www.ucl.ac.uk/laws/sites/laws/files/kerber_zolna_2021_facebook_case_competition_law_data_protection_law_01.pdf)
- <https://www.consilium.europa.eu/el/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/#>
- <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52020PC0842&from=en>
- <https://marketingweek.gr/dma-i-archi-mias-epochis>
- <https://www.consilium.europa.eu/media/56086/st08722-xx22.pdf>
- [https://cerre.eu/wp-content/uploads/2020/11/CERRE\\_DMA\\_Making-economic-regulation-of-platforms-fit-for-the-digital-age\\_Full-report\\_December2020.pdf](https://cerre.eu/wp-content/uploads/2020/11/CERRE_DMA_Making-economic-regulation-of-platforms-fit-for-the-digital-age_Full-report_December2020.pdf)
- [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_1113](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113)
- [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4109299](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4109299)
- <https://curia.europa.eu/juris/document/document.jsf;jsessionid=F2B26B34234145C1836F498702E9236F?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&o>
- <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62021CN0252>
- <https://curia.europa.eu/juris/document/document.jsf?text=&docid=265901&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=1527>

- <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220158e1.pdf>
- [https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?\\_\\_blob=publicationFile&v=](https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=)
- [https://curia.europa.eu/juris/document/document\\_print.jsf;jsessionid=9ea7d2dc30dd837ad3b01545491499c2cdd5d24daad3.e34KaxiLc3qMb40Rch0SaxuNbxfo?doclang=EL](https://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d2dc30dd837ad3b01545491499c2cdd5d24daad3.e34KaxiLc3qMb40Rch0SaxuNbxfo?doclang=EL)

# ΠΑΡΑΡΤΗΜΑ Ι

## Νομοθεσία

**ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4624/2019**

**ΦΕΚ 137/Α/29-8-2019**

**(άρθρα: 1, 9, 22, 23, 80, 81, 82)**

*Στο παρόν κείμενο του Παραρτήματος ΙΙ, παρατίθενται αυτούσια, άρθρα από τη νομοθεσία, όπως ανακτώνται από την ηλεκτρονική πηγή:<https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-phem-137a-29-8-2019.html>*

*«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.*

### **Άρθρο 1**

#### **Σκοπός του νόμου**

Σκοπός του παρόντος νόμου είναι:

α) η αντικατάσταση του νομοθετικού πλαισίου που ρυθμίζει τη συγκρότηση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,

β) η λήψη μέτρων 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 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, εφεξής: ΓΚΠΔ),

γ) η ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και

για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης - πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου

## **Άρθρο 9**

### **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**

Η εποπτεία της εφαρμογής των διατάξεων του ΓΚΠΔ, του παρόντος και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στην Ελληνική Επικράτεια ασκείται από την Αρχή που έχει συσταθεί με τον ν. 2472/1997 (Α' 50). Η Αρχή αποτελεί ανεξάρτητη δημόσια αρχή κατά το άρθρο 9Α του Συντάγματος και εδρεύει στην Αθήνα.

## **Άρθρο 22**

### **Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα**

1. Κατά παρέκκλιση από το άρθρο 9 παράγραφος 1 του ΓΚΠΔ η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα με την έννοια του άρθρου 9 παράγραφος 1 του ΓΚΠΔ από δημόσιους και ιδιωτικούς φορείς επιτρέπεται, εφόσον είναι απαραίτητη:

α) για την άσκηση δικαιωμάτων που απορρέουν από το δικαίωμα κοινωνικής ασφάλισης και κοινωνικής προστασίας και για την εκπλήρωση των συναφών υποχρεώσεων·

β) για λόγους προληπτικής ιατρικής, για την εκτίμηση της ικανότητας προς εργασία του εργαζομένου, για ιατρική διάγνωση, για την παροχή υγείας ή κοινωνικής περίθαλψης ή για τη διαχείριση των συστημάτων και υπηρεσιών υγείας ή κοινωνικής περίθαλψης ή δυνάμει σύμβασης με επαγγελματία του τομέα υγείας ή άλλου προσώπου που δεσμεύεται από το επαγγελματικό απόρρητο ή είναι υπό την εποπτεία του·ή

γ) για λόγους δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας, όπως σοβαρών διασυννοριακών απειλών κατά της υγείας ή για την εξασφάλιση υψηλών προδιαγραφών ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων, επιπλέον των μέτρων που αναφέρονται στο δεύτερο εδάφιο της παραγράφου 3, πρέπει να τηρούνται ιδίως οι διατάξεις που εξασφαλίζουν το επαγγελματικό απόρρητο που προβλέπει νόμος ή κώδικας δεοντολογίας.

2. Κατά παρέκκλιση από το άρθρο 9 παράγραφος 1 του ΓΚΠΔ η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα με την έννοια του άρθρου 9 παράγραφος 1 του ΓΚΠΔ από δημόσιους φορείς επιτρέπεται, εφόσον είναι:

- α) απολύτως απαραίτητη για λόγους ουσιώδους δημοσίου συμφέροντος·
- β) απαραίτητη για την αποτροπή σημαντικής απειλής για την εθνική ασφάλεια ή τη δημόσια ασφάλεια· ή
- γ) είναι απαραίτητη για τη λήψη ανθρωπιστικών μέτρων, και στις περιπτώσεις αυτές το συμφέρον για την επεξεργασία είναι υπέρτερο του συμφέροντος του υποκειμένου των δεδομένων.

3. Στις περιπτώσεις των προηγούμενων παραγράφων, λαμβάνονται όλα τα κατάλληλα και ειδικά μέτρα για τη διαφύλαξη των συμφερόντων του υποκειμένου των δεδομένων προσωπικού χαρακτήρα. Λαμβάνοντας υπόψη την κατάσταση της τεχνολογίας, το κόστος εφαρμογής και τη φύση, την έκταση, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους που θέτει, ανάλογα με τη σοβαρότητά τους στα δικαιώματα και στις ελευθερίες των φυσικών προσώπων η επεξεργασία αυτή, στα μέτρα αυτά μπορούν να περιλαμβάνονται ιδίως:

- α) τεχνικά και οργανωτικά μέτρα που διασφαλίζουν ότι η επεξεργασία είναι σύμφωνη με τον ΓΚΠΔ·
- β) μέτρα για να διασφαλιστεί ότι είναι δυνατή η εκ των υστέρων επαλήθευση και ο προσδιορισμός του εάν και από ποιον έχουν εισαχθεί, τροποποιηθεί ή αφαιρεθεί τα προσωπικά δεδομένα·
- γ) μέτρα για την ενδυνάμωση της ευαισθητοποίησης του προσωπικού που ασχολείται με την επεξεργασία·
- δ) περιορισμοί πρόσβασης από τους υπεύθυνους επεξεργασίας και εκτελούντες την επεξεργασία·
- ε) η ψευδωνυμοποίηση των δεδομένων προσωπικού χαρακτήρα·
- στ) η κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα·
- ζ) μέτρα για τη διασφάλιση της ικανότητας, της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της ανθεκτικότητας των συστημάτων και υπηρεσιών επεξεργασίας που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένης της δυνατότητας ταχείας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε περίπτωση φυσικού ή τεχνικού συμβάντος·
- η) διαδικασίες για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας·



θ) ειδικοί κανόνες διασφάλισης της συμμόρφωσης με τον παρόντα νόμο και τον ΓΚΠΔ σε περίπτωση διαβίβασης ή επεξεργασίας για άλλους σκοπούς·ι) ο ορισμός ΥΠΔ.

### **Άρθρο 23**

#### **Επεξεργασία γενετικών δεδομένων**

Κατ' εφαρμογή της παραγράφου 4 του άρθρου 9 του ΓΚΠΔ απαγορεύεται η επεξεργασία γενετικών δεδομένων για σκοπούς ασφάλισης υγείας και ζωής.

### **Άρθρο 80**

#### **Αστική ευθύνη του υπεύθυνου επεξεργασίας**

##### **(άρθρα 54 και 56 της Οδηγίας)**

Δημόσια αρχή, με την ιδιότητα του υπεύθυνου επεξεργασίας δεδομένων προσωπικού χαρακτήρα, που έχει προκαλέσει παρανόμως ζημία στο υποκείμενο των δεδομένων προσωπικού χαρακτήρα, κατά παράβαση των διατάξεων των άρθρων 6 έως και 8 ή των διατάξεων του παρόντος Κεφαλαίου υποχρεούται, σύμφωνα με τις διατάξεις των άρθρων 105 και 106 του ΕισΝΑΚ, σε αποζημίωση ή σε χρηματική ικανοποίηση λόγω ηθικής βλάβης στο υποκείμενο των δεδομένων.

### **Άρθρο 81**

#### **Ποινικές κυρώσεις**

##### **(άρθρα 54 και 57 της Οδηγίας)**

Το άρθρο 38 εφαρμόζεται και στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς του άρθρου 43.

### **Άρθρο 82**

#### **Διοικητικές κυρώσεις**

##### **(άρθρα 54 και 57 της Οδηγίας)**

1. Με την επιφύλαξη των εξουσιών ελέγχου της Αρχής σύμφωνα με το άρθρο 15 του παρόντος, η Αρχή με ειδικά αιτιολογημένη απόφασή της και κατόπιν προηγούμενης κλήσης για παροχή εξηγήσεων των ενδιαφερομένων μπορεί να επιβάλει σε αρμόδιες Αρχές για παραβάσεις των υποχρεώσεών τους ως υπεύθυνων επεξεργασίας δεδομένων προσωπικού χαρακτήρα τα παρακάτω διοικητικά πρόστιμα:

α) για παραβάσεις των άρθρων 6 έως 8 και των άρθρων 60 έως 78 διοικητικό πρόστιμο έως ένα εκατομμύριο (1.000.000) ευρώ,

β) για παραβάσεις των άρθρων 45 έως 57, διοικητικό πρόστιμο έως δύο εκατομμύρια (2.000.000) ευρώ και

γ) για μη συμμόρφωση προς εντολή της Αρχής σύμφωνα με το άρθρο 15 παράγραφος 4 διοικητικό πρόστιμο έως δύο εκατομμύρια (2.000.000) ευρώ.

2. Κατά τη λήψη απόφασης σχετικά με την επιβολή διοικητικού προστίμου, καθώς και για το ύψος αυτού, για κάθε εξατομικευμένη περίπτωση λαμβάνονται υπόψη τα ακόλουθα:

α) η φύση, η βαρύτητα, η διάρκεια της παράβασης, η έκταση ή ο σκοπός της σχετικής επεξεργασίας, καθώς και ο αριθμός των υποκειμένων των δεδομένων που έθιξε η παράβαση και το μέγεθος της ζημίας που αυτά υπέστησαν,

β) οποιεσδήποτε ενέργειες στις οποίες προέβη η αρμόδια Αρχή για να μετριάσει τη ζημία που υπέστησαν τα υποκείμενα των δεδομένων προσωπικού χαρακτήρα,

γ) τυχόν σχετικές προηγούμενες παραβάσεις της αρμόδιας Αρχής,

δ) οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που θίγει η παράβαση,

ε) ο τρόπος με τον οποίο η Αρχή πληροφορήθηκε την παράβαση, ειδικότερα αν και κατά πόσον η αρμόδια Αρχή κοινοποίησε την παράβαση και

στ) εάν έχουν ήδη διαταχθεί σε βάρος της αρμόδιας αρχής για την ίδια παράβαση, τα μέτρα που αναφέρονται στο άρθρο 15 παράγραφος 4, ο βαθμός συμμόρφωσής της με αυτά.»

## ΠΑΡΑΡΤΗΜΑ ΙΙ

### Νομολογία

Στο παρόν κείμενο του Παραρτήματος ΙΙ, παρατίθενται αυτούσια, κάποιες αποφάσεις από τη νομολογία, αναφορικά με το ζήτημα της παραβίασης δεδομένων προσωπικού χαρακτήρα, όπως ανακτώνται από την ηλεκτρονική σελίδα-πηγή:  
[http://www.areiospagos.gr/nomologia/apofaseis\\_result.asp?s=2&code=113](http://www.areiospagos.gr/nomologia/apofaseis_result.asp?s=2&code=113)

#### «Δεδομένα Προσωπικού Χαρακτήρα

---

- 1) **1238/2013** Απορρίπτει αίτηση αναίρεσης κατηγορουμένου ως αβάσιμη. Αβάσιμοι οι από το άρθρο 510 παρ. 1 στοιχ. Δ και Ε ΚΠΔ λόγοι αναίρεσεως, για έλλειψη ειδικής αιτιολογίας και για εσφαλμένη εφαρμογή και ερμηνεία ουσιαστικής ποινικής διάταξης, διότι: 1. Η με τη βιντεοσκόπηση δια κινητού τηλεφώνου δημιουργία οπτικοακουστικού υλικού της ερωτικής πράξης του κατ/νου και της εγκαλούσας, δε χρειάζεται καμία ομαδοποίηση ή ταξινόμηση και είναι απλή η επεξεργασία και η ηλεκτρονική μετάδοση αυτού ανά πάσα στιγμή σε τρίτους.
- 2) **1370/2010** Παραβίαση προσωπικών δεδομένων. Αίτηση αναίρεσεως κατά της καταδικαστικής αποφάσεως του δικάζοντος σε δεύτερο βαθμό Τριμελούς Πλημμελειοδικείου. Απορρίπτεται ο λόγος από το άρθρ. 510 § 1 στοιχ. Γ' ΚΠΔ για παράβαση των διατάξεων για δημοσιότητα της διαδικασίας, διότι η απαγγελία της αποφάσεως έγινε δημόσια στο ακροατήριο του Τριμελούς Πλημμελειοδικείου μετά το πέρας της συζητήσεως και δεν απαιτείτο να αναφέρονται στα πρακτικά της δίκης και άλλα στοιχεία ως προς τη βεβαίωση τηρήσεως των διατάξεων.
- 3) **1857/2010** Καταδικαστική απόφαση για συκοφαντική δυσφήμιση και παραβίαση του νόμου δεδομένων προσωπικού χαρακτήρα (άρθρο 22 Ν. 2472/1997). Απόρριψη λόγου αναίρεσεως για

έλλειψη αιτιολογίας εν σχέσει με την πράξη της συκοφαντικής δυσφημίσεως. Παραδοχή λόγου αναιρέσεως για εσφαλμένη ερμηνεία του νόμου δεδομένων προσωπικού χαρακτήρα. Ειδικότερα ως προς την έννοια του "Αρχείου". Κήρυξη αθώου του κατηγορουμένου - αναιρεσεύοντος για την πράξη της παραβίαση δεδομένων προσωπικού χαρακτήρα.

- 4) **2054/2010** Ορθή και αιτιολογημένη καταδίκη για παράβαση του Ν. 2472/1997. Έννοια αρχείου. Παράδοση αντιγράφου μηνύσεως, της οποίας είχε προηγηθεί ανάκληση και θέση στο Αρχείο της Εισαγγελίας, με συνημμένα αντίγραφα υπομνημάτων, τα οποία περιείχαν προσωπικά δεδομένα φυσικών προσώπων και στη συνέχεια, πρωτοκόλληση αυτής στο γενικό Πρωτόκολλο του Πανεπιστημίου, όπου υπήρχε ελεύθερη πρόσβαση από τρίτους, στοιχειοθετεί την αξιόποινη αυτή πράξη. Ορθά το δικαστήριο δεν απάντησε επί αυτοτελών ισχυρισμών.
- 5) **1187/2009** Προστασία δεδομένων προσωπικού χαρακτήρα. Έννοια αρχείου. Ποινικά αδικήματα. Επέμβαση κλπ. σε αρχείο χωρίς δικαίωμα. Στοιχεία του εγκλήματος του άρθρου 22 ν. 2472/1997. Έννοια δεδομένων προσωπικού χαρακτήρα. Δεν θεωρούνται δεδομένα οι πληροφορίες των οποίων κάνει κάποιος χρήση και οι οποίες περιήλθαν σε γνώση του χωρίς να ερευνήσει αυτός κάποιο αρχείο ή χωρίς να του τις έχει μεταδώσει τρίτος που επενέβη σε αρχείο, γιατί εκλείπει η προϋπόθεση του αρχείου ως στοιχείου της αντικειμενικής υπόστασης....
- 6) **1381/2009** Δίχως δικαίωμα η επεξεργασία προσωπικών δεδομένων, με τη γνώση καταδικαστικών αποφάσεων σε βάρος του μηνυτή και την ανακοίνωση του περιεχομένου των σε αρχές που δεν είναι δικαστικές. Ορθή και αιτιολογημένη καταδίκη του κατηγορουμένου. Αόριστος ο λόγος για συγγνωστή νομική πλάνη και μη νόμιμος ο ισχυρισμός ότι προέβη στην επεξεργασία προκειμένου να υπερασπίσει τον εαυτό του αφού δεν ανακοίνωσε τα προσωπικά δεδομένα στις δικαστικές αρχές,

αλλά σε τρίτους που δεν είχαν δικαίωμα να λάβουν γνώση αυτών.

- 7) **1744/2009** Ηθική αυτουργία κατ' εξακολούθηση σε παράβαση του άρθρου 22 § 4 του Ν. 2472/1997 (δεδομένα προσωπικού χαρακτήρα). Στοιχεία ηθικής αυτουργίας. Για το δόλο του ηθικού αυτουργού δεν απαιτείται ιδιαίτερη αιτιολογία γιατί αυτός ενυπάρχει στη θέληση παραγωγής των πραγματικών περιστατικών που συγκροτούν την αντικειμενική υπόσταση του εγκλήματος, στο οποίο παρακινεί ο ηθικός αυτουργός το φυσικό αυτουργό και εξυπακούεται ότι υπάρχει στην πραγμάτωση των περιστατικών αυτών.
- 8) **2515/2009** Καταδικαστική απόφαση για παράβαση του άρθρου 22 § 4 Ν. 2472/1997 "προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα" και συκοφαντική δυσφήμιση δια του τύπου κατ' εξακολούθηση. Στοιχεία εγκλημάτων. Έννοια "αρχείου". Απόρριψη λόγου αναιρέσεως για απόλυτη ακυρότητα επειδή δεν προσδιορίζεται η ταυτότητα εγγράφων που αναγνώστηκαν, αφού τα έγγραφα αυτά προσδιορίστηκαν επαρκώς και, με την ανάγνωση του κειμένου τους, κατέστησαν γνωστά κατά το περιεχόμενό τους στον αναιρεσείοντα.
- 9) **2638/2008** Αναίρεση Εισαγγελία Α.Π. Για την αντικειμενική και υποκειμενική υπόσταση του εκ του άρθρ. 22 παρ. 4 Ν.2472/97 εγκλήματος, αρκεί και ο ενδεχόμενος δόλος. Αναιρείται η προσβαλλόμενη αθωωτική απόφαση για έλλειψη αιτιολογίας, καθόσον, εκτός του άμεσου δόλου, που δέχθηκε ότι δεν συνέτρεχε, δεν ερεύνησε την ύπαρξη των άλλων μορφών δόλου. Επίσης γίνεται δεκτός ο λόγος της αρνητικής υπέρβασης εξουσίας, διότι δεν ερευνήθηκε αν στη συγκεκριμένη περίπτωση συνέτρεχε αμέλεια στο πρόσωπο της κατηγορούμενης, ...
- 10) **2079/2007** Ο νόμος 2472/1997 (δεδομένα προσωπικού χαρακτήρα)

εφαρμόζεται όταν υπάρχουν προσωπικά δεδομένα σε Αρχείο και τυγχάνουν επεξεργασίας και δι' αυτής ανακοινώσεις προσωπικών δεδομένων, ενώ ελλείπει Αρχείου, η ανακοίνωση πληροφορίας στο τηλεοπτικό κοινό που αναφέρεται στην προσωπική ζωή του θιγομένου, δια προβολής συνομιλίας του δημοσιογράφου με παριστάμενο στην εκπομπή, εκφεύγει του πεδίου εφαρμογής του νόμου τούτου και οι οποίες προσβολές στην προσωπικότητα εμπίπτουν σε άλλες διατάξεις του ποινικού δικαίου»

**«11) ΜΠρΑθ 11358/2019** Σύμφωνα με την ηλεκτρονική πηγή παρατίθεται αυτούσια:

<https://www.dsnet.gr/Epikairothta/Nomologia/MPrAth%2011358.19.htm>

### **Ηθική βλάβη για διαβίβαση δεδομένων από τράπεζα σε εταιρεία ενημέρωσης οφειλετών χωρίς προγενέστερη ενημέρωση του υποκειμένου**

Απαιτείται εξατομικευμένη ενημέρωση του υποκειμένου σύμφωνα και με την υπ' αριθμ. 98/2017 απόφαση της ΑΠΔΠΧ. Νόθος αντικειμενική ευθύνη. Η τράπεζα ως μεγάλος οργανισμός με οργανωμένο νομικό τμήμα όφειλε να γνωρίζει την πιθανότητα επέλευσης ηθικής βλάβης. Η ηθική βλάβη του 2472/1997 διαφέρει από την αντίστοιχη του άρθρου 932 ΑΚ που απαιτεί πλήρη αιτιολόγηση, συνεπώς στην αγωγή που ζητείται ηθική βλάβη για παραβίαση των διατάξεων του ν. 2472/1997 αρκεί να αναφέρεται η συγκεκριμένη παράβαση, που ως αποτέλεσμα, σε απλή τυπική διαδικασία απόδειξης της παράβασης, οδηγεί στην ηθική βλάβη του υποκειμένου των δεδομένων και δεν υπάρχει ανάγκη αναφοράς των επιμέρους στοιχείων της ηθικής βλάβης που

θεωρείται δεδομένη. Το ελάχιστο όριο που επιδικάζεται από τον Ν. 2472/1997 δεν προσβάλλει την αρχή της αναλογικότητας.»

### **Υπόθεση C-319/20**

*Στο παρόν κείμενο του Παραρτήματος II, παρουσιάζεται αυτούσια, μέρος από την απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης, σε υπόθεση κατά της Meta (πρώην Facebook): Οι ενώσεις προστασίας καταναλωτών μπορούν να προσφύγουν στη δικαιοσύνη για παραβιάσεις της προστασίας προσωπικών δεδομένων, όπως ανακτάται από την ηλεκτρονική σελίδα-πηγή: <https://curia.europa.eu/juris/document/document.jsf?jsessionid=A6F40023008B4D2EEB441EF38608AC83?text=&docid=261210&pageIndex=0&doclang=DA&mode=req>*

---

### **«Απόφαση Δικαστηρίου**

#### **Υπόθεση C-319/20**

Απόφαση του Δικαστηρίου (τρίτο τμήμα) της 28ης Απριλίου 2022 - Meta Platforms Ireland Limited, Facebook Ireland Limited κατά Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband (αίτηση για την έκδοση προδικαστικής αποφάσεως - Germanyofsrict)

(Αίτηση για την έκδοση προδικαστικής αποφάσεως — Προστασία φυσικών προσώπων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα — Κανονισμός (ΕΕ) 2016/679 — Άρθρο 80 — Εκπροσώπηση των υποκειμένων των δεδομένων από μη κερδοσκοπική ένωση — ομαδική αγωγή από ένωση αρμόδια για προστασία των συμφερόντων των καταναλωτών, χωρίς εξουσιοδότηση και ανεξάρτητα από το εάν έχουν παραβιαστεί τα συγκεκριμένα δικαιώματα του υποκειμένου των δεδομένων – δράση που βασίζεται στην απαγόρευση αθέμιτων εμπορικών πρακτικών,

παραβίαση νόμου για την προστασία των καταναλωτών ή απαγόρευση χρήσης μη έγκυρων γενικών επιχειρηματικών όρων)

### **Οι διάδικοι της κύριας δίκης**

Ενάγων: Meta Platforms Ireland Limited, πρώην Facebook Ireland Limited

Κατηγορούμενος: Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV

### **Συμπέρασμα Απόφασης από το Δικαστήριο της ΕΕ**

*Άρθρο 80 εδάφιο 2, του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ελεύθερη ανταλλαγή τέτοιων δεδομένων και για την κατάργηση της Οδηγίας 95/46/ΕΚ (γενικός κανονισμός για την προστασία δεδομένων) πρέπει να ερμηνεύεται έτσι ώστε να μην εμποδίζει μια εθνική νομοθεσία που επιτρέπει σε μια ένωση που φροντίζει για την προστασία των συμφερόντων των καταναλωτών - χωρίς άδεια που της έχει δοθεί για το σκοπό αυτό και ανεξάρτητα από παραβίαση των συγκεκριμένων δικαιωμάτων του υποκειμένου των δεδομένων – να ασκήσει αγωγή κατά του ατόμου που τεκμαίρεται ότι παραβίασε την προστασία των προσωπικών δεδομένων ισχυριζόμενος ότι υπάρχει παραβίαση της απαγόρευσης κατά των αθέμιτων εμπορικών πρακτικών»*

---

Αυτούσια και συνοπτικά, αναφέρεται η πρόσφατη απόφαση 13/2021 της ΑΠΔΠΧ, όπως παρουσιάζεται από την ηλεκτρονική σελίδα-πηγή: <https://www.ethemis.gr/information-law-prosopika-dedomena/2022/07/29/gdpr-anaklhsh-apofasis.html>



«Ανάκληση εν μέρει της απόφασης 13/2021 της ΑΠΔΠΧ και επιβολή  
προστίμου

Η Αρχή εξέτασε αίτηση θεραπείας κατά της απόφασης 13/2021, με την οποία επιβλήθηκε στην αιτούσα, εμπορική εταιρεία που διαθέτει ηλεκτρονικό και φυσικά καταστήματα, πρόστιμο ύψους είκοσι χιλιάδων (20.000,00 €) ευρώ για παράβαση των άρθρων 17, 21 παρ. 1, 12 παρ. 3 και 25 παρ. 1 ΓΚΠΔ. Κατόπιν εκτίμησης των νέων στοιχείων που προσκόμισε η αιτούσα, η Αρχή αξιολόγησε ως ελαφρυντικές περιστάσεις κατά το άρθρο 83 παρ. 2 ΓΚΠΔ το γεγονός ότι α) η παράβαση οφείλεται σε αμέλεια και όχι σε δόλο της αιτούσας, και β) η αιτούσα φαίνεται ότι κατά κανόνα ακολουθεί τις κατάλληλες διαδικασίες που εξασφαλίζουν την ικανοποίηση των δικαιωμάτων εναντίωσης και διαγραφής των υποκειμένων των δεδομένων, ανακάλεσε εν μέρει την απόφαση 13/2021 και επέβαλε στην αιτούσα πρόστιμο ύψους πέντε χιλιάδων (5.000,00) ευρώ για τις διαπιστωθείσες παραβάσεις του άρθρου 17 σε συνδυασμό με τα άρθρα 21 παρ. 1 και 12 παρ. 3 ΓΚΠΔ»

---

*Παρακάτω, παρουσιάζονται, αυτούσια και με συνοπτικό τρόπο, τα πιο ουσιώδη στοιχεία της υπόθεσης υπ' αριθμόν C-210/16, αναφορικά με την υπόθεση παραβίασης δεδομένων προσωπικού χαρακτήρα των χρηστών μέσω **Facebook fanpage**. Η υπόθεση που παρουσιάζεται αυτούσια, βρίσκεται στην ηλεκτρονική σελίδα: <https://curia.europa.eu/juris/document/document.jsf;jsessionid=9232C5497F1F10E644FEDFBFF0576DAB?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&>*

## **«C-210/16-Facebook Fanpage**

### **Wirtschaftsakademie offers educational services by means of a fan page hosted on Facebook.**

Fan pages are user accounts that can be set up on Facebook by individuals or businesses. To do so, the author of the fan page, after registering with Facebook, can use the platform designed by Facebook to introduce himself to the users of that social network and to persons visiting the fan page, and to post any kind of communication in the media and opinion market. Administrators of fan pages can obtain anonymous statistical information on visitors to the fan pages via a function called 'Facebook Insights' which Facebook makes available to them free of charge under non-negotiable conditions of use. That information is collected by means of evidence files ('cookies'), each containing a unique user code, which are active for two years and are stored by Facebook on the hard disk of the computer or on other media of visitors to fan pages. The user code, which can be matched with the connection data of users registered on Facebook, is collected and processed when the fan pages are opened. According to the order for reference, neither Wirtschaftsakademie nor Facebook Ireland Ltd notified the storage and functioning of the cookie or the subsequent processing of the data, at least during the material period for the main proceedings.

By decision of 3 November 2011 ('the contested decision'), the ULD, as supervisory authority within the meaning of Article 28 of Directive 95/46, with the task of supervising the application in the Land of Schleswig-Holstein (Germany) of the provisions adopted by the Federal Republic of Germany pursuant to that directive, ordered Wirtschaftsakademie, in accordance with the first sentence of Paragraph 38(5) of the BDSG, to deactivate the fan page it had set up on Facebook at the address [www.facebook.com/wirtschaftsakademie](http://www.facebook.com/wirtschaftsakademie), on pain of a penalty payment if it failed to comply within the

prescribed period, on the ground that neither Wirtschaftsakademie nor Facebook informed visitors to the fan page that Facebook, by means of cookies, collected personal data concerning them and then processed the data. Wirtschaftsakademie brought a complaint against that decision, arguing essentially that it was not responsible under data protection law for the processing of the data by Facebook or the cookies which Facebook installed.

By decision of 16 December 2011, the ULD dismissed the complaint, finding that Wirtschaftsakademie as a service provider was liable under Paragraph 3(3)(4) and Paragraph 12(1) of the TMG in conjunction with Paragraph 3(7) of the BDSG. The ULD stated that, by setting up its fan page, Wirtschaftsakademie had made an active and deliberate contribution to the collection by Facebook of personal data relating to visitors to the fan page, from which it profited by means of the statistics provided to it by Facebook.

Wirtschaftsakademie brought an action against that decision in the Verwaltungsgericht (Administrative Court, Germany), submitting that the processing of personal data by Facebook could not be attributed to it and that it had not commissioned Facebook within the meaning of Paragraph 11 of the BDSG to process data that it controlled or was able to influence. Wirtschaftsakademie concluded that the ULD should have acted directly against Facebook instead of adopting the contested decision against it.

By judgment of 9 October 2013, the Verwaltungsgericht (Administrative Court) annulled the contested decision, essentially on the ground that, since the administrator of a fan page on Facebook is not a responsible entity within the meaning of Paragraph 3(7) of the BDSG, Wirtschaftsakademie could not be the addressee of a measure taken under Paragraph 38(5) of the BDSG.

The Oberverwaltungsgericht (Higher Administrative Court, Germany) dismissed the ULD's appeal against that judgment as unfounded. It found essentially that the prohibition of the processing of data in the contested decision was unlawful, in that the second sentence of Paragraph 38(5) of the BDSG lays down a step-by-step procedure whose first step allows only the adoption of measures for the elimination of infringements that have been ascertained in the processing of data. An immediate prohibition of the processing of data comes into consideration only if a data processing procedure is unlawful in its entirety and the only possible remedy is to terminate it. According to the Oberverwaltungsgericht (Higher Administrative Court), that was not the case here, since it would have been possible for Facebook to put an end to the infringements alleged by the ULD.

The Oberverwaltungsgericht (Higher Administrative Court) further stated that the contested decision was also unlawful on the ground that an order under Paragraph 38(5) of the BDSG may only be made against the responsible entity within the meaning of Paragraph 3(7) of the BDSG, and that Wirtschaftsakademie was not such an entity in relation to the data collected by Facebook. Facebook alone decided on the purpose and means of collecting and processing personal data used for the Facebook Insights function, Wirtschaftsakademie receiving only anonymised statistical information.

The ULD appealed on a point of law to the Bundesverwaltungsgericht (Federal Administrative Court, Germany), relying inter alia on an infringement of Paragraph 38(5) of the BDSG and on a number of procedural errors vitiating the appellate court's decision. It considers that the infringement committed by Wirtschaftsakademie consisted in commissioning an inappropriate supplier — inappropriate because it did not comply with the applicable data protection law — namely Facebook Ireland, to create, host and maintain a website. The order to Wirtschaftsakademie to deactivate its fan page, imposed by the contested decision, was thus

intended to remedy that breach, since it prohibited it from continuing to make use of Facebook infrastructure as the technical basis of its website.

Like the Oberverwaltungsgericht (Higher Administrative Court), the Bundesverwaltungsgericht (Federal Administrative Court) takes the view that Wirtschaftsakademie cannot itself be regarded as responsible for the data processing within the meaning Paragraph 3(7) of the BDSG or Article 2(d) of Directive 95/46. It considers nevertheless that the concept of controller should in principle be interpreted broadly, in the interests of effective protection of the right of privacy, as the Court has held in its recent case-law on the point. It further entertains doubts as to the powers of the ULD with respect to Facebook Germany in the present case, given that it is Facebook Ireland that is responsible, at EU level, for the collection and processing of personal data within the Facebook group. Finally, it is uncertain as to the effect, for the purpose of the exercise of the ULD's powers of intervention, of the assessments made by the supervisory authority to which Facebook Ireland is subject concerning the lawfulness of the processing of personal data at issue.

### **Costs**

Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

### **On those grounds, the Court (Grand Chamber) hereby rules:**

1. Article 2(d) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that the concept of

‘controller’ within the meaning of that provision encompasses the administrator of a fan page hosted on a social network.

2. Articles 4 and 28 of Directive 95/46 must be interpreted as meaning that, where an undertaking established outside the European Union has several establishments in different Member States, the supervisory authority of a Member State is entitled to exercise the powers conferred on it by Article 28(3) of that directive with respect to an establishment of that undertaking situated in the territory of that Member State even if, as a result of the division of tasks within the group, first, that establishment is responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State and, second, exclusive responsibility for collecting and processing personal data belongs, for the entire territory of the European Union, to an establishment situated in another Member State.
3. Article 4(1)(a) and Article 28(3) and (6) of Directive 95/46 must be interpreted as meaning that, where the supervisory authority of a Member State intends to exercise with respect to an entity established in the territory of that Member State the powers of intervention referred to in Article 28(3) of that directive, on the ground of infringements of the rules on the protection of personal data committed by a third party responsible for the processing of that data whose seat is in another Member State, that supervisory authority is competent to assess, independently of the supervisory authority of the other Member State, the lawfulness of such data processing and may exercise its powers of intervention with respect to the entity established in its territory without first calling on the supervisory authority of the other Member State to intervene».

Παρακάτω, παρουσιάζονται, αυτούσια και με συνοπτικό τρόπο τα πιο ουσιώδη στοιχεία της υπόθεσης υπ' αριθμόν **C-498/16**, αναφορικά με την υπόθεση παραβίασης δεδομένων προσωπικού χαρακτήρα των χρηστών μέσω **Facebook** και πιο συγκεκριμένα, τις υποθέσεις του **Max Schrems** κατά **Facebook**. Η υπόθεση που παρουσιάζεται αυτούσια, βρίσκεται στην ηλεκτρονική σελίδα: <https://curia.europa.eu/juris/document/document.jsf?mode=DOC&pageIndex=0&docid=198764&part=1&doclang=EN&text=&dir=&occ=first&cid=1870476>

### **« The dispute in the main proceedings and the questions referred for a preliminary ruling**

Mr Schrems has been a user of the social network Facebook since 2008. Initially, he used that social network only for personal purposes under a false name. Since 2010, he has been using a Facebook account solely for his private activities such as exchanging photos, chatting, and posting with approximately 250 Friends. In that account he writes his name using the Cyrillic alphabet in order to prevent any searches under his name. In addition, since 2011, he has opened a Facebook page registered and established by him, in order to report to internet users on his legal proceedings against Facebook Ireland, his lectures, his participation in panel debates and his media appearances, as well as to call for the donation of funds and to publicise his books.

From August 2011, Mr Schrems lodged before the Irish Data Protection Commissioner 23 complaints against Facebook Ireland, one of which gave rise to a reference for a preliminary ruling before the Court (judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650).

Mr Schrems has published two books on his legal proceedings against alleged infringements of data protection, has given lectures, some of which were remunerated, in particular with professionals, has registered a number of internet websites such as blogs, online petitions as well as crowdfunding sites to finance legal proceedings against the defendant in the main proceedings. Furthermore, he has founded an association which seeks to uphold the fundamental right to data protection, has received

various prizes and has had assigned to him, by more than 25 000 people worldwide, claims to be brought in the present case.

The association founded by Mr Schrems and seeking to enforce data protection is a non-profit organisation, the purpose of which is to seek to uphold the fundamental right to data protection, to provide the required associated work on communication and the media and on policy clarification. Its objective is to provide financial support for test cases of public interest brought against undertakings which potentially endanger that fundamental right. The necessary costs are also funded and the corresponding donations gathered, administered and distributed.

Mr Schrems claims, in essence, that the defendant has committed numerous infringements of data protection provisions, inter alia provisions of the Datenschutzgesetz 2000 (Austrian Law of 2000 on data protection), of the Irish Data Protection Act 1988, or of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

Mr Schrems brought an action before the Landesgericht für Zivilrechtssachen Wien (Regional Civil Court, Vienna, Austria), seeking, first, comprehensive declarations of the status of the defendant in the main proceedings as a mere service provider and of its duty to comply with instructions or of its status as an employer, where the processing of data is carried out for its own purposes, the invalidity of contract terms relating to conditions of use, second, an injunction prohibiting the use of his data for its own purposes or for those of third parties, third, disclosure concerning the use of his data and, fourth, the production of accounts and damages in respect of the variation of contract terms, harm suffered and unjustified enrichment.

Mr Schrems claims to have *locus standi* on the basis of both his own rights and similar rights which seven other contractual partners of the defendant in the main proceedings, who are, according to the applicant, also consumers and residing in Austria, Germany or in India, have



assigned to the applicant for the purposes of his action against Facebook Ireland.

According to Mr Schrems, the Landesgericht für Zivilrechtssachen Wien (Regional Civil Court, Vienna) has international jurisdiction as the forum of a consumer under Article 16(1) of Regulation No 44/2001.

Facebook Ireland raises, inter alia, an objection that the action is inadmissible because international jurisdiction is lacking.

The Landesgericht für Zivilrechtssachen Wien (Regional Civil Court, Vienna) dismissed the action brought by Mr Schrems on the ground that, since he is also using Facebook for professional purposes, he could not rely on jurisdiction over consumer contracts. According to that court, the jurisdiction *ratione personae* of the assignors of claims is not transferable to the assignee.

Mr Schrems brought an appeal against the order at first instance before the Oberlandesgericht Wien (Higher Regional Court, Vienna, Austria). That court amended that order in part. It upheld the claims related to the contract concluded between the applicant in the main proceedings in his own name and the defendant in the main proceedings. By contrast, it dismissed the appeal in so far as it concerned the assigned claims on the ground that the forum of a consumer can be invoked only by an applicant relying on his own claims. Consequently, it ruled, Mr Schrems could not successfully rely on the second part of Article 16(1) of Regulation No 44/2001 when seeking to enforce assigned claims. However, as to the remainder, that court rejected Facebook Ireland's procedural objections.

Both parties brought an appeal on a point of law ('Revision') against that judgment before the Oberster Gerichtshof (Supreme Court, Austria).

That court states that, if the applicant in the main proceedings were a 'consumer', the action should be brought in Vienna. The same would apply to any proceedings brought in relation to the rights of a consumer resident in Vienna. According to the referring court, there is no significant additional burden on the defendant in the main proceedings if it were to be required in the course of these proceedings also to defend itself against additional assigned claims.

The referring court nevertheless takes the view that, having regard to the case-law of the Court of Justice, the question of interpretation, namely the extent to which a consumer to whom other consumers assign their claims for joint enforcement can rely on the jurisdiction over consumer contracts relevant to him, cannot be answered with the requisite degree of certainty.

### **Costs**

Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Third Chamber) hereby rules:

1. Article 15 of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as meaning that the activities of publishing books, lecturing, operating websites, fundraising and being assigned the claims of numerous consumers for the purpose of their enforcement do not entail the loss of a private Facebook account user's status as a 'consumer' within the meaning of that article.
2. Article 16(1) of Regulation No 44/2001 must be interpreted as meaning that it does not apply to the proceedings brought by a consumer for the purpose of asserting, in the courts of the place where he is domiciled, not only his own claims, but also claims assigned by other consumers domiciled in the same Member State, in other Member States or in non-member countries».

