



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ  
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ  
Πρόγραμμα Μεταπτυχιακών Σπουδών  
«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»  
Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ  
της Μαρίνας Κοσμίδου (Α.Μ.: ΜΔΙ2019) και της Έλενας Λουκάκη (Α.Μ.: ΜΔΙ2026)

**ΨΗΦΙΑΚΗ ΔΙΑΦΗΜΙΣΗ ΚΑΙ ΖΗΤΗΜΑΤΑ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ  
ΔΕΔΟΜΕΝΩΝ**

Επιβλέπουσα:

Λίλιαν Μήτρου

Πειραιάς, Μάρτιος, 2022

## **ΠΕΡΙΛΗΨΗ**

Αντικείμενο της παρούσας μεταπτυχιακής μελέτης συνιστά η εξέταση του digital advertising, σε συνάρτηση με τα ζητήματα παραβίασης προσωπικών δεδομένων των χρηστών του διαδικτύου. Πιο συγκεκριμένα, στο πλαίσιο της εν λόγω μεταπτυχιακής μελέτης θα επιχειρηθεί θεωρητική προσέγγιση του digital advertising, μέσω της παρουσίασης των θεμελιωδών εννοιών, της λειτουργίας, των βασικών τύπων και μέσων, καθώς επίσης των τεχνικών και των ειδικών διαφημιστικών εργαλείων που χρησιμοποιούνται στο πλαίσιο του digital advertising, ενώ η εργασία θα επικεντρωθεί στην προστασία δεδομένων προσωπικού χαρακτήρα στο περιβάλλον του digital advertising, καθώς και στην εξέταση ειδικότερων ζητημάτων του, όπως λόγου χάριν τα Cookies ως εργαλεία στόχευσης και παρακολούθησης στη Συμπεριφορική Διαφήμιση, το Social Media Advertising και το Real Time Bidding (RTB).

Λέξεις κλειδιά: Ψηφιακή Διαφήμιση, Προσωπικά Δεδομένα, Προστασία Προσωπικών Δεδομένων, AdTech, Cookies, Social Media Advertising, Real Time Bidding (RTB)

## **ABSTRACT**

The subject of this postgraduate study is the examination of digital advertising, in relation to the issues of violation of Internet users' personal data. More specifically, in the framework of this postgraduate study, a theoretical approach to digital advertising will be attempted through the presentation of basic concepts, function, basic types and media, as well as the techniques and special advertising tools used in the context of digital advertising, while the master thesis will focus on the protection of personal data in digital advertising, as well as the examination of specific issues of digital advertising, such as Cookies as Behavioral Advertising targeting and tracking tools, Social Media Advertising and Real Time Bidding (RTB).

Key words: Digital Advertising, Personal Data, Personal Data Protection, AdTech, Cookies, Social Media Advertising, Real Time Bidding (RTB)

## Περιεχόμενα

ΠΕΡΙΛΗΨΗ.....	2
ABSTRACT.....	3
ΕΙΣΑΓΩΓΗ.....	6
1. DIGITAL ADVERTISING.....	8
1.1 Έννοια.....	8
1.2 Λειτουργία.....	9
1.2.1 Βασικοί Τύποι Digital Advertising.....	9
1.2.2 Μέσα στο Digital Advertising.....	13
1.2.3 Τα Εμπλεκόμενα Μέρη.....	14
1.2.4 Τεχνολογίες Διαφήμισης (AdTech) – Η επανάσταση της Προγραμματικής Διαφήμισης (Programmatic Advertising).....	16
1.3 Η στόχευση στο Digital Advertising.....	21
1.4 Παρακολούθηση στο Digital Advertising.....	23
1.4.1 Ο τεχνικός ορισμός της Παρακολούθησης και τα κίνητρα.....	23
1.4.2 Κατηγορίες Δεδομένων στη Προγραμματική Διαφήμιση.....	25
1.4.3 Βασικές τεχνικές OnLine παρακολούθησης.....	26
2. ΤΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ DIGITAL ADVERTISING.....	28
2.1. Η πολυπλοκότητα του νομικού πλαισίου γενικά.....	28
2. 2. Γενικός Κανονισμός Προστασίας Δεδομένων.....	30
2.2.1. Ιστορική Αναδρομή.....	30
2.2.2. Οι στόχοι του Κανονισμού.....	32
2.2.2. Το πεδίο εφαρμογής.....	33
2.3. Οδηγία 2002/58/EK.....	34
2.3.1. Ν.3471/2006.....	35
2.4. Σχέδιο Κανονισμού E-Privacy.....	37
2.4.1. Περί ePrivacy Regulation.....	37
2.4.2. Το χρονικό των διαπραγματεύσεων.....	38
2.4.3. Επισκόπηση ορισμένων εκ των βασικών διατάξεων που εισήχθησαν στο σχέδιο ePrivacy Regulation.....	39

2.5. Digital Services Act .....	43
2.5.1. Φύση και πεδίο εφαρμογής .....	44
2.5.2. Ουσιαστικά μέτρα σχετικά με τη στοχευμένη διαφήμιση.....	44
2.5.3. Αντιδράσεις για τον επερχόμενο νόμο για τις ψηφιακές υπηρεσίες.....	46
3. Η ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ DIGITAL ADVERTISING.....	47
3.1. Η αρχή της διαφάνειας της επεξεργασίας/Το δικαίωμα ενημέρωσης .....	47
3.2. Νομιμότητα επεξεργασίας για διαφημιστικούς σκοπούς .....	49
3.2.1. Γενικότερο κανονιστικό πλαίσιο.....	49
3.3. Ειδικές Κατηγορίες Δεδομένων.....	55
3.4. Προστασία προσωπικών δεδομένων ανηλίκων .....	57
3.4.1. Πρόσβαση ανηλίκων σε ψηφιακές υπηρεσίες .....	57
3.4.2. Το ζήτημα της συγκατάθεσης.....	59
3.4.3. Το δικαίωμα ενημέρωσης .....	63
3.4.4. Προβληματισμοί σχετικά με τη προστασία των ανηλίκων στο ψηφιακό οικοσύστημα .....	63
4. ΕΙΔΙΚΟΤΕΡΑ ΖΗΤΗΜΑΤΑ.....	64
4.1. Cookies και Συμπεριφορική Διαφήμιση ( <i>Behavioral Advertising</i> ).....	64
4.1.1. Η Συμπεριφορική Διαφήμιση και οι κίνδυνοι της <i>Online</i> παρακολούθησης .....	64
4.1.2. Τα cookies ως βασικό εργαλείο της <i>OnLine</i> παρακολούθησης .....	67
4.1.3. Η ρύθμιση των cookies .....	68
4.2. Social Media Advertising .....	76
4.2.1. Τα μέσα κοινωνικής δικτύωσης (« <i>social media</i> ») .....	76
4.2.2. Οι κίνδυνοι.....	77
4.2.3. Οι μηχανισμοί στόχευσης .....	80
4.3. Real Time Bidding (« <i>RTB</i> »).....	81
4.3.1 Τι είναι <i>RTB</i> ;.....	81
4.3.2 Οι κίνδυνοι.....	81
4.3.3 Βασικά ζητήματα που εγείρονται σχετικά με την επεξεργασία προσωπικών δεδομένων .....	82
ΣΥΜΠΕΡΑΣΜΑΤΑ .....	84
ΠΑΡΑΡΤΗΜΑ ΒΙΒΛΙΟΓΡΑΦΙΚΩΝ ΑΝΑΦΟΡΩΝ.....	86

## ΕΙΣΑΓΩΓΗ

Ο τομέας της ψηφιακής διαφήμισης, ή άλλως digital advertising, συνιστά έναν εκ των θεμελιωδών πυλώνων της οικονομίας του διαδικτύου, δεδομένου ότι η συντριπτική πλειοψηφία των υπηρεσιών που προσφέρονται διαδικτυακά, ιδίως δε διαδικτυακοί ιστότοποι ενημέρωσης, μηχανές αναζήτησης και μέσα κοινωνικής δικτύωσης, βασίζονται το επιχειρηματικό τους μοντέλο στην προσέλκυση υψηλού αριθμού χρηστών, προκειμένου να πραγματοποιηθεί ο σκοπός της προσέλκυσης επιχειρήσεων που επιθυμούν να διαφημιστούν μέσω της πλατφόρμας τους. Ο τομέας του digital advertising συνιστά μία παγκόσμια αγορά μεγάλου βεληνεκού, στο πλαίσιο της οποίας παρέχονται χωρίς οικονομικό αντάλλαγμα ποικίλες υπηρεσίες, ενώ το αντιστάθμισμα της δωρεάν παροχής των υπηρεσιών συνίσταται στα δεδομένα, τα οποία παράγονται από έκαστο χρήστη και τα οποία αξιοποιούνται με στόχο τη δημιουργία προφίλ του χρήστη και τη συνακόλουθη προώθηση εξατομικευμένων και προσαρμοσμένων σε κάθε χρήστη προϊόντων και υπηρεσιών.

Εντός του πλέγματος των σύνθετων σχέσεων της ψηφιακής εποχής και της ψηφιακής διαφήμισης αναδύονται νέες πηγές διακινδύνευσης των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικότητας του ατόμου. Πιο συγκεκριμένα, στο πλαίσιο της ψηφιακής διαφήμισης χρησιμοποιούνται πλέον νέες τεχνικές, όπως επί παραδείγματι η συμπεριφορική διαφήμιση μέσω της online παρακολούθησης της διαδικτυακής συμπεριφοράς ενός χρήστη, διά της οποίας τα εμπλεκόμενα μέρη στη ψηφιακή διαφήμιση συγκεντρώνουν προσωπικά δεδομένα και πληροφορίες των χρηστών μιας ιστοσελίδας ή εφαρμογής, προκειμένου να σκιαγραφήσουν εν τέλει συγκεκριμένο προφίλ του κάθε χρήστη βάσει των συλλεχθέντων στοιχείων και να προωθήσουν στοχευμένη διαφήμιση προσαρμοσμένη και ανταποκρινόμενη στις προτιμήσεις και στα ενδιαφέροντα τους.

Τούτων δοθέντων, οι εν λόγω τεχνικές της ψηφιακής διαφήμισης εγείρουν σημαντικά ζητήματα παραβίασης των προσωπικών δεδομένων των χρηστών και της ιδιωτικότητας των τελευταίων, με αποτέλεσμα να κρίνεται αδήριτη η ανάγκη διαμόρφωσης ενός κανονιστικού πλαισίου, που να ρυθμίζει νομοθετικά τον διαρκώς εξελισσόμενο και πολλά υποσχόμενο τομέα του digital

advertising, ο οποίος συνδέεται άρρηκτα με την αξιοποίηση σύγχρονων τεχνολογικών και λογισμικών εργαλείων που εγκυμονούν πολυάριθμους κινδύνους για το δικαίωμα προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας του ατόμου.

Στο πλαίσιο αυτό, αντικείμενο της παρούσας μεταπτυχιακής μελέτης αποτελεί η εξέταση του digital advertising σε συνάρτηση με θέματα προστασίας προσωπικών δεδομένων. Ειδικότερα, στο πρώτο κεφάλαιο θα επιχειρηθεί, μεταξύ άλλων, εννοιολογική προσέγγιση της ψηφιακής διαφήμισης (digital advertising) και επεξήγηση ορισμένων θεμελιωδών εννοιών και παρουσίαση ορισμένων βασικών τύπων της. Ακολούθως, θα παρουσιαστούν τα μέσα που αξιοποιούνται στο πλαίσιο της ψηφιακής διαφήμισης, τα εμπλεκόμενα μέρη και οι τεχνολογίες διαφήμισης (AdTech) και θα δοθεί έμφαση στην online παρακολούθηση και στόχευση των χρηστών. Εν συνεχεία, το δεύτερο κεφάλαιο θα επικεντρωθεί στο ρυθμιστικό πλαίσιο που διέπει την ψηφιακή διαφήμιση. Πιο συγκεκριμένα, γίνεται συνοπτική αναφορά του θεσμικού πλαισίου που διέπει το digital advertising ενώ παρουσιάζονται τα βασικότερα νομοθετικά εργαλεία, που ήδη έχουν τεθεί σε εφαρμογή ή αναμένεται η δημοσίευσή τους και επηρεάζουν τη ρύθμιση της επεξεργασίας προσωπικών δεδομένων στο digital advertising. Στο τρίτο κεφάλαιο παρουσιάζονται οι κίνδυνοι που ελλοχεύουν για την προστασία δεδομένων προσωπικού χαρακτήρα στην ψηφιακή διαφήμιση, όπως επί παραδείγματι η έλλειψη διαφάνειας, το ζήτημα της συγκατάθεσης του υποκειμένου των δεδομένων, η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και η ανάγκη προστασίας των προσωπικών δεδομένων ανηλίκων. Στο τέταρτο και τελευταίο κεφάλαιο της παρούσας μεταπτυχιακής μελέτης θα αναλυθούν ειδικότερα ζητήματα του digital advertising και ειδικότερα τα Cookies, το Social Media Advertising, καθώς και το Real Time Bidding (RTB). Η εργασία ολοκληρώνεται με την παράθεση συμπερασματικών παρατηρήσεων και των σχετικών βιβλιογραφικών πηγών.

# 1. DIGITAL ADVERTISING

## 1.1 Έννοια

Σε μία προσπάθεια εννοιολογικής προσέγγισης της έννοιας του digital advertising, η οποία αποδίδεται στην ελληνική γλώσσα ως ψηφιακή διαφήμιση (στη παρούσα εργασία χρησιμοποιούνται και οι δύο όροι), αρχικά διαπιστώνει κανείς ότι ο όρος digital advertising σχετίζεται με τη διαφήμιση που διενεργείται στο διαδίκτυο. Σύμφωνα, δε, με ακριβέστερο ορισμό του IAB Europe<sup>1</sup> ως ψηφιακή διαφήμιση νοείται οποιαδήποτε μονομερής μετάδοση πληροφοριών και προωθητικών μηνυμάτων αναφορικά με ιδέες, αγαθά ή υπηρεσίες που διενεργείται μέσω του διαδικτύου και πιο συγκεκριμένα μέσω ηλεκτρονικών μηνυμάτων (email), μέσων κοινωνικής δικτύωσης (social media), ιστοσελίδων, μηχανών αναζήτησης, banner ή ακόμη και μέσω κινητού τηλεφώνου τύπου smartphone που υποστηρίζει υπηρεσίες διαδικτύου και καθιστά εφικτή τη σύνδεσή του με το διαδίκτυο σε οποιοδήποτε χρόνο και τόπο (IAB Europe, χ.χ.).

Ο όρος digital advertising δεν είναι ο μοναδικός που απαντάται στην παγκόσμια αρθρογραφία και βιβλιογραφία και πολλές φορές αντί αυτού ενδέχεται να συναντήσει κανείς τους συνώνυμους όρους online advertising, online marketing, internet advertising, web advertising. Το digital advertising αποτελεί μέρος μιας στρατηγικής διαφήμισης που χρησιμοποιεί το διαδίκτυο για τη διάδοση διαφημιστικών μηνυμάτων σε καταναλωτές με σκοπό την προώθηση προϊόντων ή υπηρεσιών (Gurudutta P Japee, 2019).

Το digital advertising δεν έννοια ταυτόσημη με το digital marketing. Το digital advertising είναι το εργαλείο, ενώ το digital marketing αποτελεί τη διαδικασία που διέπει ολόκληρη τη στρατηγική μιας επιχείρησης από τη σύλληψη μιας ιδέας για ένα προϊόν ή μία υπηρεσία μέχρι την υλοποίησή της. Το digital advertising αποτελεί μέρος του μείγματος μάρκετινγκ 4P<sup>2</sup>, και συγκεκριμένα της Προώθησης (Promotion), δηλαδή της προώθησης της ψηφιακής ταυτότητας

---

1 Ο IAB Europe (Interactive Advertising Bureau – Οργανισμός Διαδραστικής Επικοινωνίας) αποτελεί ευρωπαϊκή οργάνωση για το digital marketing και το οικοσύστημα της διαφήμισης, με στόχο την πολιτική εκπροσώπηση και προώθηση της συνεργασίας του κλάδου για την παροχή πλαισίων, προτύπων και κλαδικών προγραμμάτων που επιτρέπουν στις επιχειρήσεις να ευδοκμήσουν στην ευρωπαϊκή αγορά.

2 Product (Προϊόν), Price (Τιμή), Promotion (Προώθηση) και Place (Τοποθεσία).



μιας επιχείρησης (blog, ιστότοπου, εφαρμογής, προϊόντος κ.λ.π.) μέσω διαφήμισης σε σχετικό κοινό (Chibuzor, χ.χ.).

## 1.2 Λειτουργία

Σύμφωνα με τον IAB Hellas<sup>3</sup> (χ.χ.) “...το Internet συγκαταλέγεται μέσα στις 3 κορυφαίες πηγές που συμβουλεύεται ο καταναλωτής κατά τη διάρκεια της διαδικασίας αγοράς (purchase process)”. Ο νέος τύπος καταναλωτή χρησιμοποιεί τα διάφορα μέσα συγχρόνως και συνδυαστικά, οπότε το συνδυαστικό και πολυκαναλικό digital advertising διαδραματίζει πρωτεύοντα ρόλο στη ολοένα αναπτυσσόμενη ψηφιακή οικονομία. Η διαδραστικότητα, συνεπώς, εισάγει νέους κανόνες στο σχεδιασμό, την υλοποίηση και τη μέτρηση μιας διαφημιστικής ενέργειας, η οποία δίνει τη δυνατότητα δημιουργίας πιο στενής και προσωπικής σχέσης με τον καταναλωτή, εμπάθυνσης σε αυτά που τον γοητεύουν και εμπνέουν. Πως λειτουργεί όμως το digital advertising, τόσο από θεμελιώδη, όσο και από τεχνική άποψη;

### 1.2.1 Βασικοί Τύποι Digital Advertising

Μόλις τον Ιούνιο του 2021 δημοσιεύθηκε μελέτη με τίτλο «Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice» που εκπονήθηκε κατόπιν παραγγελίας της Επιτροπής Εσωτερικής Αγοράς και Προστασίας των Καταναλωτών<sup>4</sup> του Ευρωπαϊκού Κοινοβουλίου, σε μία προσπάθεια εντοπισμού των προβλημάτων που προκύπτουν από την ανάπτυξη της αγοράς της ψηφιακής διαφήμισης, ενόψει και της πανδημίας του Covid-19. Η σχετική μελέτη παρέχει επισκόπηση των σχετικών αγορών, εξετάζει σε ποιο βαθμό η υπάρχουσα νομοθεσία αντιμετωπίζει τα προβλήματα που εντοπίζονται και προτείνει πιθανές λύσεις. Σύμφωνα με αυτή την επίκαιρη μελέτη οι τρεις βασικοί τύποι digital advertising είναι οι εξής (Fourberg κ.ά., 2021):

1) Το **Search Advertising** συνδέει τις μηχανές αναζήτησης με τους ιστότοπους των επιχειρήσεων που επιθυμούν να διαφημιστούν με αυτό τον τρόπο, ώστε στη συνέχεια οι ιστότοποι τους να

---

<sup>3</sup> Ο IAB Hellas αποτελεί τον κλαδικό φορέα των εταιρειών που ασχολούνται με όλες τις μορφές του digital και interactive marketing και είναι μέλος του IAB Europe.

<sup>4</sup> Internal Market and Consumer Protection - IMCO

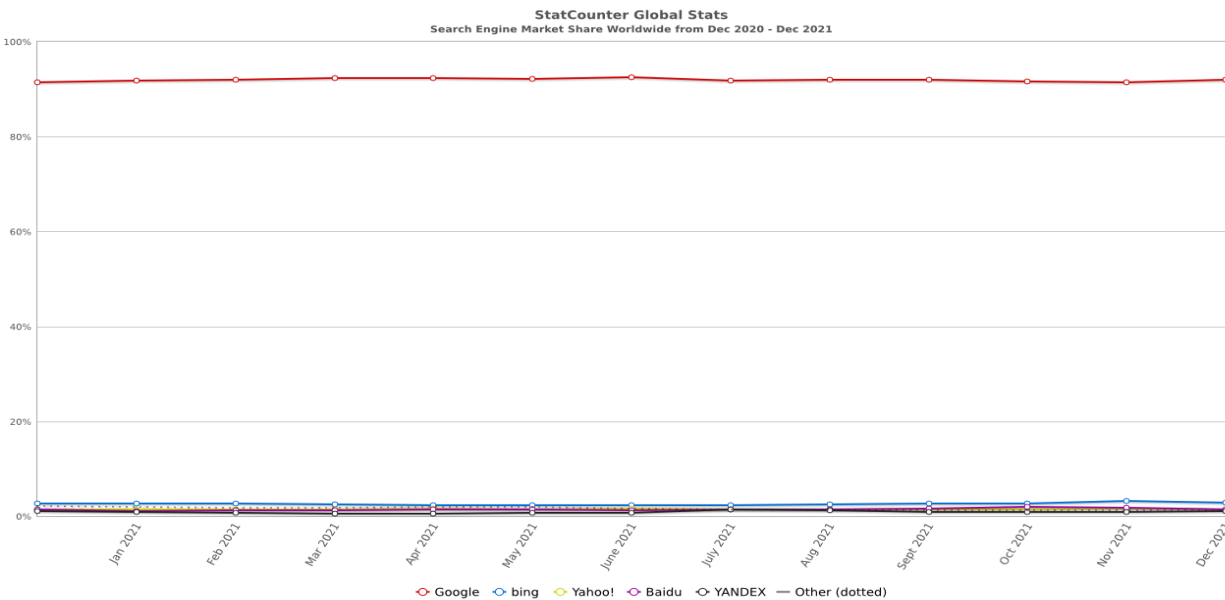
εμφανιστούν όταν οι χρήστες αναζητούν προϊόντα ή υπηρεσίες, μπλέκοντας τις διαφημίσεις με τα οργανικά αποτελέσματα της αναζήτησης (ωστόσο συνήθως οι διαφημιζόμενοι ιστότοποι επισημαίνονται ως διαφημίσεις με την προσθήκη ενός σύντομου αναγνωριστικού κειμένου). Τέτοιες διαφημίσεις εμφανίζονται σε καθορισμένες για τις διαφημίσεις θέσεις στις μηχανές αναζήτησης, στην περίπτωση που κάποιος χρήστης εισάγει λέξεις κλειδιά που ταιριάζουν σε προϊόντα και υπηρεσίες της διαφημιζόμενης επιχείρησης. Η μηχανή αναζήτησης συνήθως καθορίζει ποια διαφήμιση εμφανίζεται σε έναν μεμονωμένο χρήστη και οι διαφημιζόμενες επιχειρήσεις ανταγωνίζονται για να λάβουν προτεραιότητα για προβολή, καθορίζοντας συγκεκριμένες λέξεις-κλειδιά και ομάδες χρηστών. Το Search Advertising κατά κανόνα δεν εξαρτάται από τα δεδομένα των χρηστών καθώς η επιλογή για την εμφάνιση των διαφημίσεων καθορίζεται κυρίως από το συγκεκριμένο ερώτημα αναζήτησης που θέτει ο χρήστης. Ωστόσο, σε ορισμένες περιπτώσεις, τα δεδομένα χρήστη μπορεί να χρησιμοποιηθούν για την προβολή αποτελεσμάτων κατόπιν αντιστοίχισης τους με συγκεκριμένους διαφημιζόμενες επιχειρήσεις<sup>5</sup>. Ο τύπος αυτός της διαφήμισης θεωρείται πετυχημένος, καθώς βασίζεται στην πρόθεση που έχει εκδηλώσει ο ίδιος ο χρήστης και εμφανίζεται σε μορφή native ad<sup>6</sup>. Ενδεικτικό είναι ότι ο σχετικός τύπος διαφήμισης αποτελεί τον δεύτερο μεγαλύτερο από άποψη εσόδων τρόπο ψηφιακής διαφήμισης παγκοσμίως με ποσοστό 43,3% κατά το έτος 2019. Κυρίαρχος στη σχετική αγορά είναι η Google με μερίδιο αγοράς υπολογιζόμενο τον Δεκέμβριο του 2021 παγκοσμίως περί το ποσοστό 90%<sup>7</sup>, όπως προκύπτει από το κατωτέρω γράφημα.

---

<sup>5</sup> Για παράδειγμα η υπηρεσία της Google Customer Match επιτρέπει στους Διαφημιστές να χρησιμοποιούν τις δικές τους βάσεις δεδομένων για την προώθηση των προϊόντων/υπηρεσιών τους μέσω της μηχανής αναζήτησης Google και άλλων υπηρεσιών της, όπως Gmail και YouTube. Για να λάβουν τη σχετική υπηρεσία οι Διαφημιστές ανεβάζουν στη πλατφόρμα της Google τα δεδομένα των πελατών τους, τα οποία στη συνέχεια συσχετίζονται με τα δεδομένα της Google, ώστε να προβάλλει στοχευμένες διαφημίσεις στους πελάτες τους και σε άλλους χρήστες με αντίστοιχα χαρακτηριστικά. Περισσότερα στον ακόλουθο σύνδεσμο <https://support.google.com/google-ads/answer/6379332?hl=en>.

<sup>6</sup> Οι native διαφημίσεις ταιριάζουν με τον οπτικό σχεδιασμό και το look and feel του ιστότοπου στο οποίο φυλοξενούνται και συμπεριφέρονται με συνέπεια στην εμπειρία των χρηστών καθώς λειτουργούν ακριβώς όπως το φυσικό περιεχόμενο του (IAB Hellas, χ.χ.).

<sup>7</sup> Στην Ελλάδα δε το σχετικό ποσοστό την ίδια περίοδο ανέρχεται στο ποσοστό 97%, όπως προκύπτει από τα στατιστικά στοιχεία που δημοσιεύει η ιστοσελίδα Statcounter. Οράτε σχετικά <https://gs.statcounter.com/search-engine-market-share/all/greece>.



Γράφημα 1: <https://gs.statcounter.com/search-engine-market-share>

2) Το **Display Advertising** αποτελεί έναν από τους πιο διαδεδομένους τύπους ψηφιακής διαφήμισης και καταλαμβάνει το μεγαλύτερο τμήμα της σχετικής αγοράς μετά από το Search Advertising και αντιπροσωπεύει το 51,8% των συνολικών εσόδων της. Το Display Advertising εκμεταλλεύεται τους διαθέσιμους και προκαθορισμένους σε διαστάσεις διαφημιστικούς χώρους σε ιστότοπους ή εφαρμογές, όπου προβάλλονται διαφημίσεις σε διάφορες μορφές. Το Display Advertising είναι ευρύτερη έννοια και περιλαμβάνει το Social Media Advertising, Video Advertisements και Banner-Advertisements.

- Το **Social Media Advertising** περιλαμβάνει τις διαφημίσεις που προβάλλονται στους χρήστες των μέσων κοινωνικής δικτύωσης, όπως Facebook, Instagram, TikTok και πλέον των επιχειρηματικών δικτύων, όπως LinkedIn, ανεξάρτητα με τη μορφή της εμφάνισής τους (π.χ. εικόνα, βίντεο). Οι τέτοιες διαφημίσεις εμφανίζονται ως μέρος του οργανικού περιεχομένου του μέσου (Native Ads). Η διαφήμιση social media αντιπροσωπεύει το μεγαλύτερο μερίδιο των εσόδων του Display Advertising. Τα προσωπικά προφίλ των χρηστών του εκάστοτε μέσου, οι αλληλεπιδράσεις τους με την πλατφόρμα (π.χ. likes, κοινή χρήση περιεχομένου) και η συμπεριφορά του χρήστη κατά τη διάρκεια της περιήγησης αποτελούν ανεξάντλητη πηγή δεδομένων καταναλωτών, που στη συνέχεια χρησιμοποιούνται για την ανάπτυξη βαθύτερων μεθόδων στόχευσης για τη διανομή διαφημίσεων. Η κορυφαία εταιρεία σε αυτό το είδος της

ψηφιακής διαφήμισης είναι το Facebook με μερίδιο αγοράς μεταξύ 75-80% στις ΗΠΑ και την Ευρώπη ενώ το περίπου 95% των εσόδων του Facebook προέχεται από τις διαφημίσεις.

- Το **Video Advertising** περιλαμβάνει τις διαφημίσεις που προβάλλονται σε προγράμματα αναπαραγωγής βίντεο, είτε στο διαδίκτυο είτε σε εφαρμογές. Η διαφήμιση μπορεί να προβάλλεται είτε σε μορφή βίντεο πριν από το βίντεο που επιθυμεί να προβάλει ο χρήστης είτε σε μορφή κειμένου ή εικόνας που καλύπτει την οθόνη. Η αυξανόμενη δημοτικότητα του περιεχομένου βίντεο αναμένεται να επεκταθεί περαιτέρω ενόψει των δυνατοτήτων που προσφέρει το 5G σε κινητές συσκευές, που αποτελούν αναπόσπαστο μέρος της ανθρώπινης δραστηριότητας. Κυρίαρχος στην αγορά αυτή είναι το YouTube της Google, όμως είναι σχεδόν σίγουρο ότι και άλλες υπηρεσίες βίντεο που λειτουργούσαν με συνδρομές θα προσαρμόσουν το επιχειρηματικό τους μοντέλο, προσφέροντας δωρεάν περιεχόμενο έναντι προβολής διαφημίσεων.

- Τα **Banner-Advertisements** αποτελούν την πιο παλιά και διαδεδομένη μορφή ψηφιακής διαφήμισης και περιλαμβάνει την εμφάνιση διαφημιστικού περιεχομένου σε προκαθορισμένες θέσεις στις σελίδες ενός ιστότοπου ή σε μια εφαρμογή μαζί με το αρχικό περιεχόμενο τους (IAB HELLAS, χ.χ.). Ο διαφημιστικός χώρος πωλείται τακτικά μέσω μιας πολύπλοκης αλυσίδας ενδιάμεσων που καθορίζουν την τοποθέτηση μιας συγκεκριμένης διαφήμισης banner, όπως θα αναλύσουμε κατωτέρω. Ο τρόπος αυτός διαφήμισης αποτέλεσε την αφορμή για την ανάπτυξη αυτού που ονομάζουμε Programmatic Advertising, που είναι μία αυτοματοποιημένη μέθοδος αγοράς, προβολής και βελτιστοποίησης του διαφημιστικού χώρου μέσω της επεξεργασίας δεδομένων χρηστών για τη στοχευμένη προώθηση προϊόντων και υπηρεσιών σε δυνητικούς πελάτες.

3) Τέλος, το **Classified Advertising** αποτελεί τύπο ψηφιακής διαφήμισης με τον οποίο οι διαφημιζόμενες επιχειρήσεις αγοράζουν διαφημιστικό χώρο από τους ιστότοπους με απευθείας συμφωνίες. Ο τύπος αυτός της διαφήμισης είναι ο πιο απλός και προσομοιάζει με αυτόν της αγοράς διαφημιστικού χώρου εκτός διαδικτύου.

### 1.2.2 Μέσα στο Digital Advertising

Κατά την Clearcode<sup>8</sup> (χ.χ.) η ψηφιακή διαφήμιση χρησιμοποιεί ποικιλία μέσων και καναλιών. Ως Μέσα ορίζει τις λεκτικές ή μη επικοινωνίες, όπως για παράδειγμα text ads, video ads και radio ads. Ως Κανάλια ορίζει τους τρόπους μετάδοσης ή διανομής της διαφήμισης, όπως Social Media, Mobile και Search Engines.

Τα κυριότερα Μέσα στη Ψηφιακή Διαφήμιση είναι τα παρακάτω εν συντομία αναφερόμενα:

1. **Text & Image Ads:** Η διαφήμιση κειμένου και εικόνας χρησιμοποιείται για την προβολή μιας διαφήμισης στο διαδίκτυο όταν ένα ερώτημα ταιριάζει με τη λέξη-κλειδί του Διαφημιστή και ονομάζεται επίσης διαφήμιση Pay-Per-Click (PPC). Οι Διαφημιστές πληρώνουν τον Εκδότη όταν ο χρήστης κάνει κλικ στη διαφήμιση (Mahalakshmi και Rajasekaran, 2018).
2. **Native Ads:** Τα Native Ads είναι μορφή διαφήμισης που χρησιμοποιείται από όλες τις πλατφόρμες κοινωνικής δικτύωσης, όπως Facebook, Twitter κλπ., αλλά και από τους ιστότοπους έντυπου τύπου, όπως η Time Inc και Forbes (IAB HELLAS, χ.χ.). Παρά το γεγονός ότι ο σκοπός της native διαφήμισης είναι να ταιριάζει με το υπόλοιπο περιεχόμενο παραμένει διαφήμιση οπότε θα πρέπει να δηλώνεται εμφανώς ότι πρόκειται για πληρωμένες διαφημίσεις (Clearcode, χ.χ)<sup>9</sup>.
3. **Video Ads:** Η διαφήμιση βίντεο αναφέρεται σε διαφημίσεις που προβάλλονται με τη μορφή βίντεο. Ανάλογα με το Κανάλι, η προβολή μιας διαφήμισης βίντεο είναι παρόμοια με την προβολή μιας διαφήμισης εικόνας, με τη διαφορά ότι το διαφημιστικό κείμενο (δηλαδή το βίντεο) αποστέλλεται και εμφανίζεται σε ένα πρόγραμμα αναπαραγωγής βίντεο<sup>10</sup> και όχι ως μέρος της ίδιας της ιστοσελίδας (Clearcode, χ.χ).

---

8 Η ομάδα Clearcode - μια εταιρεία που σχεδιάζει, αναπτύσσει, κυκλοφορεί και συντηρεί λογισμικό AdTech και MarTech - δημιούργησε το βιβλίο AdTech με σκοπό, όπως δηλώνουν, να μπορεί να καταλάβει ο καθένας την τεχνολογία της ψηφιακής διαφήμισης.

9 Αναγνωρίζοντας τη σημασία της native διαφήμισης ο IAB Europe εξέδωσε το Native Advertising Playbook 2.0 προτείνοντας κάποια βασικά πρότυπα Native Ads. Οράτε σχετικά [https://www.iab.com/wp-content/uploads/2019/05/IAB-Native-Advertising-Playbook-2\\_0\\_Final.pdf](https://www.iab.com/wp-content/uploads/2019/05/IAB-Native-Advertising-Playbook-2_0_Final.pdf)

10 Οι περισσότερες διαφημίσεις βίντεο προβάλλονται μέσω πρωτοκόλλων που έχουν αναπτυχθεί από το IAB Tech Lab, όπως τα VAST, VPAID και VMAP. Οράτε σχετικά <https://iabtechlab.com/audio-video/>

4. **Audio Ads:** Οι διαφημίσεις ήχου κερδίζουν χώρο λόγο της αύξησης της δημοτικότητας των podcast, των υπηρεσιών ροής μουσικής και του ψηφιακού ραδιοφώνου και χρησιμοποιούν παρόμοια πρωτόκολλα αναπαραγωγής με τις διαφημίσεις βίντεο (Clearcode, χ.χ).

5. **Rich Media Ads:** Τα Rich Media Ads (Clearcode, χ.χ) είναι μια διαδραστική μορφή διαφήμισης και μπορεί να περιλαμβάνει κινούμενες εικόνες (π.χ. gif), αρχεία ήχου και βίντεο<sup>11</sup>.

### 1.2.3 Τα Εμπλεκόμενα Μέρη

Το οικοσύστημα του digital advertising αποτελείται από επιχειρήσεις, τεχνολογικά συστήματα και πολύπλοκες τεχνικές διαδικασίες που συνεργάζονται για την προβολή διαφημίσεων σε χρήστες του διαδικτύου. Μέχρι να εμφανιστεί ένα διαφημιστικό μήνυμα σε ένα χρήστη διαδικτύου μεσολαβεί μια σειρά από πλατφόρμες και μεσάζοντες που εμπλέκονται στην αγορά και πώληση διαφημίσεων και δεδομένων. Βασικοί παίχτες στο οικοσύστημα της Ψηφιακής Διαφήμισης είναι τρεις, ο Διαφημιστής (Advertiser) και ο Εκδότης (Publisher) και ο Χρήστης (User) (Clearcode, χ.χ.).

Ο **Διαφημιστής** (Advertiser) είναι η επιχείρηση που έχει στόχο να προωθήσει τα προϊόντα ή τις υπηρεσίες της σε στοχευμένο κοινό για να αυξήσει αναγνωρισιμότητα και καταναλωτική πίστη ώστε τελικά να αυξήσει τις πωλήσεις. Κατά κανόνα, λόγω της θεμελιώδους σημασίας της διαφήμισης για την προώθηση των προϊόντων και υπηρεσιών, οι επιχειρήσεις διαθέτουν συντεταγμένο τμήμα (που ονομάζεται Advertising Operations - AdOps) που παρακολουθεί και βελτιώνει τις διαφημιστικές καμπάνιες. Τις περισσότερες φορές ο Διαφημιστής για τη δημιουργία, προγραμματισμό, οργάνωση και παρακολούθηση των διαφημιστικών του ενεργειών χρησιμοποιεί επίσης τρίτες επιχειρήσεις, τα γνωστά **Διαφημιστικά Πρακτορεία**. Με την εξέλιξη της τεχνολογίας, ο Διαφημιστής και το Διαφημιστικό Πρακτορείο για τον έλεγχο και την παρακολούθηση των διαφημίσεων χρησιμοποιούν τις υπηρεσίες που παρέχονται από τρίτους παρόχους Ad Server, για την λειτουργία των οποίων θα αναφερθούμε αναλυτικότερα στο κεφάλαιο 1.3. Τεχνολογίες Διαφήμισης (AdTech). Περαιτέρω, ο Διαφημιστής και το

---

<sup>11</sup> Το Rich Media Showcase της Google στη σχετική σελίδα της στο <http://www.richmediagallery.com> παρέχει ποικιλία παραδειγμάτων Rich Media Ads.

Διαφημιστικό Πρακτορείο για την αγορά διαφημιστικού χώρου μπορεί να χρησιμοποιεί τα **Agency Trading Desks (ATD)** που εκτελούν τις σχετικές διαδικασίες για λογαριασμό τους.

Ο **Εκδότης (Publisher)** είναι η επιχείρηση που δημιουργεί περιεχόμενο με σκοπό να προσελκύσει κοινό, όπως για παράδειγμα μία εφημερίδα, ένας ιστότοπος, μία εφαρμογή για κινητά τηλέφωνα ή πλατφόρμες, όπως Facebook, Twitch κλπ. Συνηθισμένη πηγή εσόδων για έναν Εκδότη είναι το digital advertising, όπου ο Εκδότης πουλάει διαφημιστικό χώρο της ιστοσελίδας ή πλατφόρμας του είτε απευθείας σε Διαφημιστές είτε εμμέσως μέσω τεχνικών αυτοματοποιημένης αγοραπωλησίας ψηφιακού διαφημιστικού χώρου, μεταχειριζόμενος τα δεδομένα των χρηστών τους ως εμπορεύσιμο αγαθό<sup>12</sup>. Σύμφωνα με την Βρετανική Επιτροπή Ανταγωνισμού<sup>13</sup> (Geradin και Katsifis, 2020), η Google και το Facebook, οι οποίες αποτελούν τις μεγαλύτερες διαδικτυακές πλατφόρμες, χρηματοδοτούνται από την ψηφιακή διαφήμιση, όπου το επιχειρηματικό τους μοντέλο βασίζεται στην προσέλκυση της προσοχής των καταναλωτών και στη συλλογή δεδομένων για αυτούς, τα οποία στη συνέχεια χρησιμοποιούν για την πώληση στοχευμένων διαφημίσεων. Λόγω συνεπώς της θεμελιώδους σημασίας της διαφήμισης ως πηγή εσόδων για τους Εκδότες, αυτοί επίσης διαθέτουν συντεταγμένο τμήμα Advertising Operations (AdOps) υπεύθυνο για τη ρύθμιση και παρακολούθηση των διαφημιστικών καμπανιών και την πραγματοποίηση αλλαγών όποτε απαιτείται. Ο Εκδότης, επίσης, χρησιμοποιεί Ad Servers για τη διαχείριση του διαφημιστικού του χώρου.

Οι **Χρήστες (Users)**, δηλαδή καταναλωτές και οι επιχειρησιακοί χρήστες, είναι οι αποδέκτες των διαφημίσεων κατά τη διάρκεια της περιήγησης τους στο διαδίκτυο. Οι διαφημίσεις που βλέπουν εμφανίζονται μεμονωμένα σε έκαστο Χρήστη με βάση τις διαθέσιμες μεθόδους στόχευσης (Fourberg κ.ά., 2021).

Μεταξύ αυτών των βασικών πυλώνων του οικοσυστήματος της διαφήμισης παρεμβάλλονται ενδιάμεσοι, που δεν είναι τίποτα άλλο παρά οι **Τεχνολογίες Διαφήμισης** (που θα αναλύσουμε στο κεφάλαιο 1.3 της παρούσας μας), όπως Ad Network, Ad Exchange, Demand-Side Platform (DSP), Supply-Side Platform (SSP).

---

12 Οι μεγάλοι Εκδότες με πρόσβαση σε χιλιάδες σύνολα δεδομένων και προφίλ χρηστών μπορούν να εμπορεύονται τα σχετικά δεδομένα σε data brokers (ελληνικά: μεσίτες δεδομένων) ή απευθείας σε Διαφημιστές.

13 Competition and Markets Authority

Στο οικοσύστημα της Ψηφιακής Διαφήμισης συμμετέχουν επίσης πάροχοι και διαχειριστές δεδομένων και ανάλυσης διαφημίσεων (Geradin και Katsifis, 2020). Ειδικότερα, τέτοιοι φορείς είναι οι **Data Brokers** και οι πάροχοι μετρήσεων και επαλήθευσης (**Measurement and Verification Providers**). Οι **Data Brokers** αγοράζουν δεδομένα καταναλωτών από διάφορες πηγές (όπως Εκδότες), τα οποία στη συνέχεια επεξεργάζονται (ώστε να δημιουργήσουν κατηγορίες με κριτήρια όπως δημογραφικά ή οικονομικά) και πωλούν σε τρίτους, όπως Διαφημιστές, που με τη σειρά τους μπορεί να τα χρησιμοποιούν για τη διενέργεια προσωποποιημένων διαφημιστικών καμπανιών. Η πώληση τέτοιων δεδομένων δεν αφορά μόνο τον χώρο της διαφήμισης, αλλά μπορεί να αφορά διάφορες χρήσεις ανάλογα με τη δραστηριότητα του αγοραστή, όπως ασφαλιστικές επιχειρήσεις, παρόχους ιατρικών υπηρεσιών και ούτω καθεξής, με όλες τις αρνητικές συνέπειες που μπορεί να συνεπάγεται μία τέτοια δραστηριότητα για τα δικαιώματα των καταναλωτών στη προστασία των προσωπικών τους δεδομένων και όχι μόνο (Μπούκη, 2019). Οι πάροχοι μετρήσεων και επαλήθευσης (**Measurement and Verification Providers**) παρέχουν εξειδικευμένες υπηρεσίες προς τους Διαφημιστές για τη μέτρηση της απόδοσης και του αντικτύπου των διαφημιστικών καμπανιών (Geradin και Katsifis, 2020).

#### ***1.2.4 Τεχνολογίες Διαφήμισης (AdTech) – Η επανάσταση της Προγραμματικής Διαφήμισης (Programmatic Advertising)***

Με την επέκταση της χρήσης του Διαδικτύου (και την μετάβαση στο συμμετοχικό WEB 2.0) και τη χρήση περισσότερων συσκευών για την πρόσβαση στο Διαδίκτυο, οι ανάγκες για αμεσότερες, ταχύτερες και αυτοματοποιημένες διαδικασίες αυξήθηκαν. Η ανθρώπινη παρέμβαση σχεδόν εξαφανίστηκε και τη θέση της πήραν εργαλεία, πλατφόρμες και λογισμικά προγράμματα γνωστά ως AdTech (Καρκατζούνης και Μήτρου, 2020). Αυτό σηματοδότησε τη μετάβαση στην εποχή της Προγραμματικής Διαφήμισης, η οποία συνίσταται στην αυτοματοποιημένη λήψη αποφάσεων, μέσω ειδικού λογισμικού και αλγόριθμων που τροφοδοτούνται με δεδομένα χρήστη (συμπεριφορικά, δημογραφικά κ.λπ.) και χρησιμοποιούνται για την αγοραπωλησία



αποθεματικού διαφημίσεων<sup>14</sup> σε δευτερόλεπτα, αποφεύγοντας την απαίτηση της ανθρώπινης μεσολάβησης για τις διαπραγματεύσεις Εκδοτών και Διαφημιστών (Geradin και Katsifis, 2019). Τα AdTech επομένως δεν είναι τίποτα άλλο από όλες τις τεχνολογίες, λογισμικά και υπηρεσίες που χρησιμοποιούνται για την αυτοματοποιημένη προβολή διαφημιστικών καμπανιών και συναλλαγών (Worledge και Bamford, 2019). Ο όρος AdTech περιγράφει εργαλεία που αναλύουν και διαχειρίζονται πληροφορίες (περιλαμβανομένων των προσωπικών δεδομένων) για τις διαδικτυακές διαφημιστικές καμπάνιες και αυτοματοποιούν την επεξεργασία των σχετικών συναλλαγών. Διατρέχουν όλη τη διαδικασία που απαιτείται για την προβολή μιας διαφήμισης, με την εμπλοκή τρίτων μερών για την παροχή των σχετικών υπηρεσιών, αν και ορισμένες διαφημίσεις ακόμη προβάλλονται ύστερα από απευθείας συμφωνίες του Διαφημιστή και του Εκδότη (Information Commissioner's Office, 2019). Για τη λειτουργία της η Προγραμματική Διαφήμιση απαιτεί πολλές πληροφορίες σχετικά με τους χρήστες. Όπως θα αναπτυχθεί αργότερα, ο στόχος της προγραμματικής λογικής είναι να μάθει περισσότερα για την άποψη και τα κίνητρα του ατόμου που κάνει κλικ στη διαφήμιση (McStay, 2017). Επομένως τα δεδομένα των χρηστών αποτελούν το καύσιμό της Προγραμματικής Διαφήμισης. Βασικά εργαλεία AdTech είναι οι Ad Servers, Supply-Side Platforms (SSP), Demand-Side Platforms (DSP), Data-Management Platform (DMP), Ad Networks και Ad Exchanges. Ειδικότερα:

**1. Ad Server** αποτελεί εργαλείο AdTech που με αυτοματοποιημένα μέσα διαχειρίζεται τις διαφημίσεις και ειδικότερα αποφασίζει ποιες διαφημίσεις θα προβάλει, αναλαμβάνει την προβολή τους και συγκεντρώνει μετρικά δεδομένα της απόδοσης τους, όπως πόσες φορές εμφανίστηκαν σε χρήστη και πόσα κλικ συγκέντρωσαν. Ο Ad Server επομένως είναι το μέσο στο οποίο αποθηκεύονται οι διαφημίσεις και η τεχνολογία που με βάση συγκεκριμένες διεργασίες και αναλύσεις αποφασίζει ποιες διαφημίσεις θα προβληθούν, που αυτές θα προβληθούν και σε ποια χρονική στιγμή. Για τον λόγο αυτό παίζουν σημαντικό ρόλο στη διαχείριση και μέτρηση των διαφημιστικών καμπανιών (Amazon Europe, χ.χ.). Οι Ad Servers συνδέονται με άλλες πλατφόρμες AdTech, όπως SSP και DSP (Clearcode, χ.χ.). Οι Ad Servers

---

<sup>14</sup> Inventory ή αλλιώς OnLine Media ή Αποθεματικό είναι η συνολική ποσότητα διαφημιστικού χώρου που ένας Εκδότης έχει διαθέσιμη για διαφημίσεις στον ιστότοπο ή στην εφαρμογή του (Clearcode, χ.χ.).

χρησιμοποιούν τόσο οι Διαφημιστές όσο και οι Εκδότες. Οι Ad Servers των Διαφημιστών λέγονται Third-Party Ad Servers και των Εκδοτών First-Party (Publisher's) Ad Server. Ο Third-Party Ad Server για λογαριασμό του Διαφημιστή παρακολουθεί την απόδοση μιας διαφημιστικής καμπάνιας σε όλους τους ιστότοπους που αυτή προβλήθηκε, συγκεντρώνει στοιχεία βάσει των οποίων αποφασίζει για μελλοντικές αγορές διαφημιστικών χώρων, με βάση την απόδοσή τους (Geradin και Katsifis, 2020), λειτουργία που βοηθάει τους Διαφημιστές να ελέγχουν τις χρεώσεις των Εκδοτών. Ο First-Party (Publisher's) Ad Server διευκολύνει τον Εκδότη να διαχειρίζεται το Αποθεματικό (Inventory) των ad spaces<sup>15</sup> που διαθέτει, είναι υπεύθυνος για την τελική επιλογή των διαφημίσεων που θα προβληθούν, με βάση τις προσφορές που λαμβάνει μέσω SSPs και τις απευθείας συμφωνίες με τους Διαφημιστές (Geradin και Katsifis, 2020). Παράλληλα, συγκεντρώνει μετρικά στοιχεία για τις διαφημίσεις, προβλέπει τα ποσοστά διάθεσης των ad spaces και παρακολουθεί τα κέρδη τους (Clearcode, χ.χ.).

**2. Supply-Side Platforms (SSP)** είναι το εργαλείο που χρησιμοποιούν οι Εκδότες για την πώληση διαφημιστικού χώρου. Συγκεκριμένα, χρησιμοποιούνται από τους Εκδότες ώστε αυτοματοποιημένα να πωλούν διαφημιστικό χώρο σε μια μεγαλύτερη ομάδα δυνητικών αγοραστών και επιτρέπουν στους Εκδότες να ορίζουν το εύρος τιμών για να μεγιστοποιήσουν τα έσοδά τους (Amazon Europe, χ.χ.). Τα SSP συνδέονται με Ad Exchanges, Ad Networks και ορισμένες φορές απευθείας με DSPs για τη διενέργεια της πώλησης (Clearcode, χ.χ.).

**3. Demand-Side Platforms (DSP)** είναι το εργαλείο που χρησιμοποιούν οι Διαφημιστές για την αγορά διαφημιστικού χώρου με βάση τους στόχους, το κοινό και το μπάτζετ που έχει θέσει ο εκάστοτε Διαφημιστής (Geradin και Katsifis, 2020). Οι πλατφόρμες DSP είναι μια ενιαία, οργανωμένη αγορά όπου οι Διαφημιστές έχουν πρόσβαση στο απόθεμα των Εκδοτών μέσω της διασύνδεσης τους με τα Ad Exchanges, Ad Network και ενίοτε με SSP (Amazon Europe, χ.χ.). Τα DSPs είναι βασικά συστατικά του Real-Time Bidding, το οποίο θα αναλύσουμε σε ξεχωριστό κεφάλαιο της παρούσας. Για τη βελτίωση των αγορών με σκοπό την καλύτερη δυνατή στόχευση

---

<sup>15</sup> Ad Space ή Ad Slot ή Διαφημιστικός Χώρος είναι η περιοχή εντός ενός website ή μιας εφαρμογής που είναι προορισμένη για την προβολή διαφημίσεων (Chen, G. et al., pp. 2124–2148).

δυνητικών πελατών, τα DSPs συχνά χρησιμοποιούν δεδομένα από τα Data-Management Platforms (DMPs) και τους Data Brokers (Clearcode, χ.χ).

**5. Ad Networks** είναι η τεχνολογία που χρησιμοποιείται ως μεσίτης μεταξύ των Εκδοτών και των Διαφημιστών. Η λειτουργία της συνίσταται στη συγκέντρωση του διαφημιστικού χώρου από τους Εκδότες και τη συσχέτιση του με τις απαιτήσεις που θέτουν οι Διαφημιστές (Geradin και Katsifis, 2020). Ως ενδιάμεσος μεταξύ του Εκδότη και του Διαφημιστή έχει στόχο να εξυπηρετήσει και τα δύο μέρη. Για την εκτέλεση της υπηρεσίας του συνδέεται με το SSP και τις πλατφόρμες Ad-Exchange.

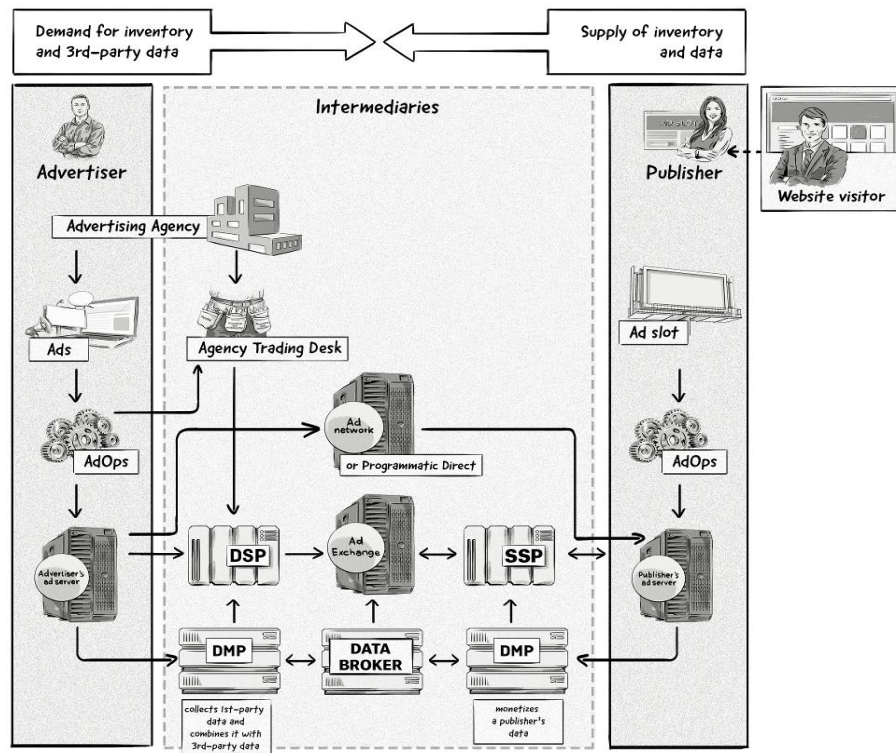
**6. Ad Exchange** είναι η τεχνολογία που παρέχει την αγορά όπου όλοι οι παράγοντες της ψηφιακής διαφήμισης αλληλοεπιδρούν για την αγοραπωλησία των διαθέσιμων impressions<sup>16</sup>. Οι πλατφόρμες Ad Exchange συγκρίνουν την αξία και την ποιότητα των εμφανίσεων και προφέρουν τον τόπο όπου πραγματοποιούνται οι δημοπρασίες μέσω DSPs και SSPs είτε απευθείας μέσω του Ad Exchange (Information Commissioner's Office, 2019). Η επιτυχία μιας προσφοράς Διαφημιστή καθορίζεται από δεδομένα για τον τύπο του χρήστη και τα ενδιαφέροντά του (McStay, 2017). Οι πλατφόρμες Ad Exchange συχνά παρομοιάζονται με το Χρηματιστήριο (Clearcode, χ.χ).

**7. Το Data-Management Platform (DMP)** συλλέγει τεράστιου όγκου δεδομένα από διάφορες πηγές, όπως τους Data Brokers, τα οποία στη συνέχεια αποθηκεύει και κατηγοριοποιεί για λογαριασμό των Διαφημιστών ανά ομάδες με τη χρήση διάφορων κριτηρίων, παρέχοντας τις απαραίτητες πληροφορίες ώστε οι διαφημίσεις να προβληθούν στους κατάλληλους διαφημιστικούς χώρους και επομένως στο κατάλληλο κοινό. Τα δεδομένα αυτά στη συνέχεια διαβιβάζονται σε πλατφόρμες, όπως το DSP, για τη διενέργεια στοχοποιημένων διαφημιστικών камπανιών (Clearcode, χ.χ).

Η περίπλοκη διαδικασία της αγοραπωλησίας διαφημιστικού χώρου εμφανίζεται στην παρακάτω περιγραφική εικόνα:

---

<sup>16</sup> Impression ή Εμφάνιση είναι η κάθε περίπτωση που ένας χρήστης εκτίθεται σε μια διαφήμιση (Chen, G. et al., pp. 2124–2148).



Εικόνα 1: <https://adtechbook.clearcode.cc/adtech-platforms-and-intermediaries/>

Συνεπώς έχουμε την πλευρά του αγοραστή που είναι ο Διαφημιστής και το Διαφημιστικό Πρακτορείο, που με τη σειρά τους χρησιμοποιούν κάποιον Ad Server για τους σκοπούς τους και τις υπηρεσίες μιας επιχείρησης Agency Trading Desks (ATD) για τη διαχείριση των αγοραπωλησιών. Από την άλλη πλευρά είναι ο πωλητής διαφημιστικού χώρου που είναι ο Εκδότης που επίσης χρησιμοποιεί κάποιον Ad Server που εξυπηρετεί τους σκοπούς του. Ενδιάμεσα είναι οι Τεχνολογίες Διαφήμισης που για τον Διαφημιστή είναι το DSP και για τον Εκδότη το SSP. Στο κέντρο της συναλλαγής είναι το Ad Network ή/και το Ad Exchange. Παράλληλα στη διαδικασία της αγοραπωλησίας υπάρχουν τα DMP που χρησιμοποιούνται από το Διαφημιστή για την αγορά δεδομένων με στόχο την καλύτερη στόχευση δυνητικών πελατών και από τον Εκδότη για πώληση των δεδομένων των χρηστών του έναντι αντιτίμου. Ανεξάρτητος παίχτης είναι ο Data Broker που έχει ως αποκλειστικό σκοπό την αγορά και μεταπώληση δεδομένων.

### 1.3 Η στόχευση στο Digital Advertising

Στο πλαίσιο της ψηφιακής διαφήμισης, η στόχευση σχετίζεται με την προβολή διαφημίσεων σε χρήστες που πληρούν μια σειρά κριτηρίων (Clearcode, χ.χ.). Η δυνατότητα στόχευσης στην ψηφιακή διαφήμιση έχει οριστεί από αρκετούς θεωρητικούς ως κύρια διαφορά μεταξύ της ψηφιακής διαφήμισης και της παραδοσιακής διαφήμισης (π.χ. μέσω τηλεόρασης). Η επικοινωνία στο διαδίκτυο μέσω άμεσης αμφίδρομης επικοινωνίας μεταξύ αναγνωρίσιμων υπολογιστών καταγράφεται εύκολα μέσω διαφόρων τεχνολογιών (Goldfarb, 2014). Η δε μετάβαση στο Web 2.0 άλλαξε το προφίλ του διαδικτύου με πρωτόγνωρη εισροή δεδομένων χρηστών μέσω της πολυδιάστατης αλληλεπίδρασης των χρηστών με τις ιστοσελίδες (Καρκατζούνης και Μήτρου, 2020). Συνεπώς, η ψηφιακή διαφήμιση παρέχει πολλές γρήγορες και φθηνές ευκαιρίες στόχευσης, διότι μπορεί να συνδεθεί με τη τρέχουσα δραστηριότητα του χρήστη (π.χ. ανάγνωση άρθρου κ.λπ.) και επιτρέπει την κατηγοριοποίηση των καταναλωτών με βάση πληθώρα δεδομένων που υπάρχουν διαθέσιμα στο διαδίκτυο. Ακόμη, παρέχει τη δυνατότητα μέτρησης και ανάλυσης των αποτελεσμάτων μιας διαφημιστικής καμπάνιας και την αποτελεσματικότερη χρήση των οικονομικών πόρων μιας επιχείρησης, ώστε οι διαφημιστικές καμπάνιες να προβάλλονται σε κοινό το οποίο μπορεί να αποτελέσει δυνητικό πελάτη ενός προϊόντος (Fourberg κ.ά., 2021). Η δυνατότητα της στόχευσης αποτελεί βασικό κίνητρο και επιχειρηματική δραστηριότητα πολλαπλών ενδιάμεσων που εμπλέκονται στην αλυσίδα αγοραπωλησίας της ψηφιακής διαφήμισης παρέχοντας υπηρεσίες συλλογής, ανάλυσης και κατηγοριοποίησης δεδομένων των Χρηστών του διαδικτύου για την καλύτερη στόχευση των διαφημίσεων (European Commission, 2018). Βασικοί μέθοδοι στόχευσης είναι το Contextual Targeting, Behavioral Targeting και Segmented Targeting (Fourberg κ.ά., 2021). Με βάση τη μέθοδο στόχευσης, η ψηφιακή διαφήμιση διακρίνεται στις πιο κάτω κατηγορίες:

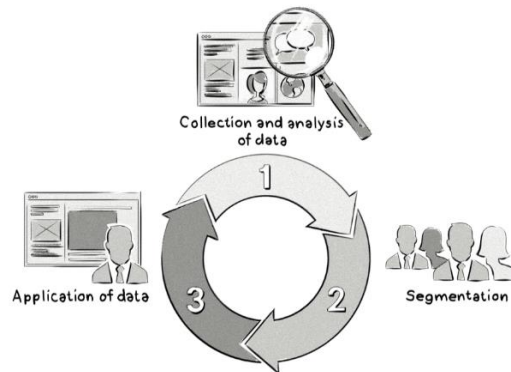
1. Σύμφωνα με την Article 29 Data Protection Working Party (εφεξής «WP 29») στην υπ' αριθμ. 2/2010 γνώμη της σχετικά με την Επιγραμμική Συμπεριφορική Διαφήμιση (2010), το **Contextual Advertising** είναι «..η διαφήμιση που επιλέγεται με βάση το περιεχόμενο που βλέπει ανά πάσα στιγμή ο χρήστης. Σε περίπτωση μηχανής αναζήτησης, το περιεχόμενο μπορεί να προέρχεται από τις λέξεις-κλειδιά της αναζήτησης, την προηγούμενη αναζήτηση ή τη διεύθυνση IP του χρήστη, εάν μέσω αυτής δηλώνεται η πιθανή γεωγραφική του θέση.». Συνεπώς, η στόχευση στο Contextual

Advertising απαιτεί καθόλου ή περιορισμένα δεδομένα για τον καταναλωτή, όπως πληροφορίες συσκευής, τοποθεσίας και γλώσσα (Geradin και Katsifis, 2020). Η σχετική μέθοδος είναι πιο διαδεδομένη στο Classified Advertising και σε μικρότερο βαθμό στο Search και Display Advertising (Fourberg κ.ά., 2021).

2. Σύμφωνα με την ίδια ως άνω αναφερόμενη γνώμη της WP 29 (2010) το **Segmented Advertising** είναι «η διαφήμιση που επιλέγεται με βάση γνωστά χαρακτηριστικά του χρήστη (ηλικία, φύλο, γεωγραφική θέση κλπ.), τα οποία ο χρήστης έχει παράσχει κατά τη φάση της εγγραφής ή καταχώρισης.». Σε αντίθεση με το Contextual και το Behavioral Advertising (που θα αναλύσουμε αμέσως παρακάτω) που βασίζονται σε δεδομένα που συγκεντρώνονται για τους Χρήστες κατά τη διάρκεια της περιήγησης τους στο διαδίκτυο, το Segmented Advertising βασίζεται σε πληροφορίες που ο Χρήστης έχει παράσχει οικειοθελώς. Αυτός ο τρόπος διαφήμισης χρησιμοποιείται από ιστότοπους και πλατφόρμες που απαιτούν από έναν χρήστη να εγγραφεί και να δημιουργήσει προφίλ χρήστη, συμπληρώνοντας το όνομά του, την ηλικία, το φύλο και άλλα στοιχεία. Αν και αυτές οι πληροφορίες επιτρέπουν την τέλεια αναγνώριση του χρήστη, πρέπει να συνδυαστούν με άλλα δεδομένα για να σχηματιστεί προφίλ με τα ενδιαφέροντα του χρήστη (Fourberg κ.ά., 2021) και να επιτευχθεί η αποτελεσματική στόχευσή του.

3. Σύμφωνα με την ίδια ως άνω αναφερόμενη γνώμη της WP 29 (2010), το **Behavioral Advertising** είναι «η διαφήμιση που βασίζεται στην παρατήρηση της συμπεριφοράς των χρηστών σε βάθος χρόνου. Η συμπεριφορική διαφήμιση μελετά τα χαρακτηριστικά της συμπεριφοράς αυτής μέσω των ενεργειών των χρηστών (επαναλαμβανόμενες επισκέψεις σε δικτυακούς τόπους, διαδραστικές ενέργειες, λέξεις -κλειδιά, επιγραμμική παραγωγή περιεχομένου κλπ.) με σκοπό τη δημιουργία συγκεκριμένου προφίλ και την επακόλουθη προώθηση στοχοθετημένης διαφήμισης που να ανταποκρίνεται στα ενδιαφέροντα των προσώπων στα οποία αναφέρονται τα δεδομένα». Με απλά λόγια, οι πληροφορίες που οι Χρήστες έχουν μοιραστεί με μία πλατφόρμα (όπως αναρτήσεις, likes, γραπτές κριτικές, ιστορικό αγορών, ιστορικό περιήγησης και πληροφορίες συσκευής, η διεύθυνση IP και ούτω καθεξής) χρησιμοποιούνται για να συσχετίσουν έναν Χρήστη με μια ομάδα καταναλωτών και τα ενδιαφέροντα και τις ανάγκες τους. Ως εκ τούτου οι απαιτήσεις για συλλογή και επεξεργασία δεδομένων είναι υψηλές σε σύγκριση με άλλους τύπους διαφήμισης (Fourberg κ.ά., 2021). Οι κύριοι τύποι Behavioral Advertising είναι το Audience

Segmentation (δηλαδή η ομαδοποίηση των προφίλ των καταναλωτών σε μια ομάδα – ονομάζεται συνήθως Audience – με κοινούς στόχους, δημογραφικά στοιχεία και ενδιαφέροντα) και το Retargeting (η προβολή στοχευμένων διαφημίσεων σε συγκεκριμένα άτομα τα οποία έχουν αλληλοεπιδράσει με μία επιχείρηση, είτε ως πελάτες είτε ως δυνητικοί πελάτες) (Geradin και Katsifis, 2020). Τα τρία βασικά βήματα στο Behavioral Advertising εμφανίζονται στην παρακάτω εικόνα:



Εικόνα 2: <https://adtechbook.clearcode.cc/targeting-and-budget-control/>

Και είναι (α) η συλλογή δεδομένων, (β) δημιουργία κοινού και (γ) η χρήση των δεδομένων στις διαφημιστικές καμπάνιες του Διαφημιστή για στοχευμένη προώθηση των προϊόντων και υπηρεσιών του (Clearcode, χ.χ.).

## 1.4 Παρακολούθηση στο Digital Advertising

### 1.4.1 Ο τεχνικός ορισμός της Παρακολούθησης και τα κίνητρα

Λαμβάνοντας υπόψη το πλαίσιο της Ευρωπαϊκής Νομοθεσίας για την ιδιωτικότητα, ο ENISA<sup>17</sup> (2017) ορίζει την on line παρακολούθηση ως: «...συλλογή ή περαιτέρω επεξεργασία δεδομένων που φυλάσσονται ή μεταδίδονται από τον τερματικό εξοπλισμό ενός ατόμου ή προέρχονται από τη

---

<sup>17</sup> Ο European Union Agency for Cybersecurity είναι ευρωπαϊκό κέντρο εμπειρογνώσας για την ασφάλεια στον κυβερνοχώρο. Οράτε σχετικά [https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/enisa\\_el](https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/enisa_el)

διαδικτυακή του δραστηριότητα, πέρα από εκείνα που απαιτούνται αποκλειστικά για την υποστήριξη του υποκείμενου καναλιού επικοινωνίας, αυστηρά απαραίτητα για την εκπλήρωση ενός σκοπού που το άτομο έχει ζητήσει συγκεκριμένα. ή για άλλους ειδικούς νομικά εξαιρούμενους σκοπούς που διαθέτουν τις απαιτούμενες διασφαλίσεις.» Η διαδικτυακή παρακολούθηση είναι το απαραίτητο συστατικό του digital advertising για διάφορους σκοπούς μεταξύ των οποίων βασικοί είναι **η δημιουργία προφίλ χρηστών για την αποτελεσματική στόχευσή τους και η μέτρηση και ανάλυση δεδομένων**. Ειδικότερα, ο σκοπός του Behavioral Advertising είναι η παρακολούθηση των χρηστών ώστε με τον καιρό να δημιουργηθεί προφίλ των χρηστών με βάση τα χαρακτηριστικά και ενδιαφέροντα τους. Ο όρος Behavioral Advertising γίνεται καλύτερα κατανοητός με αναφορά στα Third-Party Tracking Cookies που χρησιμοποιούνται από τα Ad Networks για την μέτρηση των ενδιαφερόντων των χρηστών. Τα Ad Networks τοποθετούν Cookies παρακολούθησης στις συσκευές των χρηστών, ώστε να μπορούν να γνωρίζουν ποιους ιστότοπους ο συγκεκριμένος χρήστης επισκέπτεται, ώστε να μπορούν να του εμφανίσουν την κατάλληλη διαφήμιση. Η επιτυχία ενός Ad Networks καθορίζεται από το πόσο πετυχημένα μπορεί να αντιστοιχεί τις κατάλληλες διαφημίσεις με το κατάλληλο κοινό για την καλύτερη προώθηση των προϊόντων και υπηρεσιών των Διαφημιστών (McStay, 2017). Συνεπώς, η δημιουργία ακριβούς προφίλ αποτελεί ισχυρό κίνητρο για τα Ad Networks, ώστε να αποκομίσουν μεγαλύτερα κέρδη. Ακόμη, οι ιστότοποι E-commerce, με τη τοποθέτηση First-Party Tracking Cookies, επίσης εφαρμόζουν τεχνικές συμπεριφορικής παρακολούθησης και δημιουργίας προφίλ χρηστών για την πρόταση προϊόντων και υπηρεσιών κατάλληλων για τους χρήστες τους (ENISA EU, 2012). Άλλη μία Τεχνολογία Διαφήμισης που βασίζεται σε δεδομένα είναι το Ad Exchange, στο οποίο αναφερθήκαμε ανωτέρω. Η επιτυχία μιας προσφοράς Διαφημιστή καθορίζεται από δεδομένα για τον τύπο του Χρήστη και τα ενδιαφέροντά του. Στη Προγραμματική Διαφήμιση ο όρος προγραμματική σημαίνει την μέθοδο βάσει της οποίας καθορίζεται αν ένας συγκεκριμένος διαφημιστικός χώρος είναι κατάλληλος για το Διαφημιστή. Αυτό όμως απαιτεί ιδιαίτερα αυξημένη δυνατότητα κατανόησης του καταναλωτικού κοινού. Η Προγραμματική Διαφήμιση αντλεί δεδομένα από πολλαπλές πηγές μεταξύ των οποίων οι τεχνολογίες cookies αλλά και από διάφορες άλλες πηγές όπως για παράδειγμα οι εφαρμογές που έχουμε στα κινητά μας μέσω ID συσκευών (McStay, 2017).



Η δε παρακολούθηση για λόγους μέτρησης και ανάλυσης δεδομένων στο digital advertising πραγματοποιείται για παράδειγμα για τη συγκέντρωση στατιστικών δεδομένων επισκεψιμότητας σε μία σελίδα ή της αποτελεσματικότητας μίας διαφημιστικής καμπάνιας. Τις περισσότερες φορές για τις μετρήσεις αυτές έχουν αναπτυχθεί και χρησιμοποιούνται τεχνικά εργαλεία τρίτου μέρους, με χαρακτηριστικό παράδειγμα το εργαλείο Google Analytics. Τα εργαλεία αυτά παρακολουθούν τους χρήστες του ιστότοπου για να καταγράψουν τη δραστηριότητά τους εντός ενός ιστότοπου για την παροχή στατιστικών στοιχείων, για την μέτρηση της αποτελεσματικότητας μιας διαφήμισης ή για την βελτίωση του περιεχομένου του (ENISA EU, 2012).

#### **1.4.2 Κατηγορίες Δεδομένων στη Προγραμματική Διαφήμιση**

Όμως αναφέραμε νωρίτερα, τα δεδομένα αποτελούν καύσιμο για τα AdTech της Προγραμματικής Διαφήμισης. Χρησιμοποιούνται σε όλο το εύρος του οικοσυστήματος της ψηφιακής διαφήμισης, όπως στη παροχή στοχευμένης και προσωποποιημένης διαφήμισης, για την ταυτοποίηση χρηστών και την μέτρηση απόδοσης και βελτίωση μιας διαφημιστικής καμπάνιας. Υπάρχουν τρεις κατηγορίες δεδομένων που χρησιμοποιούνται στη Προγραμματική Διαφήμιση. Πρώτη είναι τα **first-party data**, που θεωρούνται και τα πιο πολύτιμα καθώς συλλέγονται απευθείας από τον Εκδότη και περιλαμβάνουν συναλλακτική συμπεριφορά και συμπεριφορά του χρήστη στο συγκεκριμένο ιστότοπο. Δεύτερη κατηγορία δεδομένων είναι τα **second-party data** που προέρχονται από εμπορική συμφωνία μεταξύ δύο επιχειρηματικών συνεργατών που μοιράζονται τα δεδομένα της πελατείας τους. Τρίτη κατηγορία είναι τα **third-party data** που είναι δεδομένα που αγοράζονται από τρίτους, όπως τις πλατφόρμες DMPs ή τους Data Brokers και μπορεί να προέρχονται από διάφορες πηγές, όπως η online παρακολούθηση, τις εγγραφές σε ιστότοπους, δημόσια αρχεία και συναλλαγές εκτός Διαδικτύου. Οι τρεις αυτές κατηγορίες μπορεί να χρησιμοποιούνται συνδυαστικά με στόχο τη μεγαλύτερη ακρίβεια (McStay, 2017). Βασικότερο εργαλείο συλλογής δεδομένων αποτελούν οι τεχνολογίες και τεχνικές online παρακολούθησης.

### 1.4.3 Βασικές τεχνικές *OnLine* παρακολούθησης

Οι browsers υπάρχουν από την αρχή του Διαδικτύου και επιτρέπουν στους χρήστες να έχουν πρόσβαση σε ιστότοπους από υπολογιστές, laptop και άλλες φορητές συσκευές (Clearcode, χ.χ.). Ως κυριότερο μέσω πρόσβασης στο Διαδίκτυο στο παρόν κεφάλαιο θα αναλύσουμε τις τεχνικές παρακολούθησης στο browser. Όλες οι διαδικτυακές τεχνικές παρακολούθησης έχουν ένα κοινό στοιχείο: την απόδοση ενός μοναδικού αναγνωριστικού σε κάθε συνδεδεμένη συσκευή ή/και εφαρμογή, το οποίο χρησιμοποιείται ως βάση για την παρακολούθηση των χρηστών. Κατά τον ENISA (2017), η παρακολούθηση στο Διαδίκτυο διακρίνεται κατά βάση σε παρακολούθηση για ή από "first-party" δηλαδή «οντότητα που ελέγχει το domain που έχει επισκεφτεί συγκεκριμένα ένας χρήστης» ή σε παρακολούθηση για ή από "third-party" δηλαδή «κάθε άλλη οντότητα που ελέγχει τις υπόλοιπες λειτουργίες στις οποίες έχει πρόσβαση ο χρήστης κατά την περιήγηση στην ιστοσελίδα, όπως τυχόν περιεχόμενο που είναι ενσωματωμένο στη σελίδα ή εξωτερικό περιεχόμενο στο οποίο έχει πρόσβαση με σενάριο που εκτελείται στην ιστοσελίδα.». Οι βασικές τεχνικές *OnLine* παρακολούθησης είναι οι παρακάτω:

1. **Cookies:** Τα cookies είναι μικρά αρχεία κειμένου τα οποία αποθηκεύονται στον browser μας κατά την πλοήγησή Διαδίκτυο (Clearcode, χ.χ). Εγκαθίσταται από τον διακομιστή ενός ιστότοπου που επισκέπτεται ο χρήστης και αποτελείται από ένα σύντομο αλφαριθμητικό κείμενο που μπορεί να χρησιμοποιείται για σκοπούς όπως η απομνημόνευση προτιμήσεων, η αποθήκευση πληροφοριών σχετικών με τη σύνοδο περιήγησης ή αναγνώριση ενός χρήστη μέσω μοναδικού αναγνωριστικού στοιχείου (WP 29, 2010). Υπάρχουν δύο είδη cookies: Session που αποθηκεύονται προσωρινά και Persistent που παραμένουν αποθηκευμένα στον browser μέχρι να λήξουν ή να διαγραφούν (ENISA EU, 2012). Τα Session cookies συνήθως χρησιμοποιούνται για αποθήκευση επιλογών χρήση κατά την περιήγηση του στον ιστότοπο. Τα Persistent cookies χρησιμοποιούνται για να αποθηκεύουν πληροφορίες ταυτοποίησης, τις προτιμήσεις του χρήστη ή τα στοιχεία σύνδεσης που έχει προηγουμένως καταχωρήσει ο χρήστης. Επειδή παραμένουν στον browser και αποστέλλονται πίσω στον ιστότοπο που τα εγκατέστησε κάθε φορά που ο χρήστης τον επισκέπτεται ξανά, για αυτό τον λόγο μπορεί να χρησιμοποιούνται για παρακολούθηση. Ανάλογα αν τα cookies αποθηκεύονται από τον ιστότοπο που επισκέφθηκε ο χρήστης ή από τρίτο μέρος, όταν κάποια λειτουργία ή περιεχόμενο ενός ιστότοπου έχει

διαφορετική προέλευση, ονομάζονται "first-party" ή "third-party" cookies, αντίστοιχα (ENISA EU, 2017). Διαφημιστές χρησιμοποιούν τα "third-party" cookies για να παρακολουθούν τους χρήστες κατά την περιήγηση τους σε διάφορες ιστοσελίδες. Τα δεδομένα που συγκεντρώνονται χρησιμοποιούνται για τη στόχευση των χρηστών με βάση τις φερόμενες προτιμήσεις τους (ENISA EU, 2012).

2. **Fingerprinting:** Το Fingerprinting αποτελεί τεχνική παρακολούθησης ενός χρήστη με την εξαγωγή ενός αναγνωριστικού από πληροφορίες αποθηκευμένες ή που σχετίζονται με τον τεμαχικό εξοπλισμό ή το browser. Το αναγνωριστικό μπορεί να αναθεωρείται σε κάθε νέα αλληλεπίδραση του χρήστη με μια ιστοσελίδα και επιτρέπει την ταυτοποίηση του browser του χρήστη σε επόμενες επισκέψεις (ENISA EU, 2017). Η αναγνώριση ενός browser είναι ένα ισχυρό εργαλείο για την παρακολούθηση των χρηστών, όπως οι διευθύνσεις IP και τα cookies. Αυτός ο τρόπος παρακολούθησης είναι ιδιαίτερα προβληματικός καθότι είναι δύσκολο να εντοπιστεί (ENISA EU, 2012).

3. **Web Storage:** Η γλώσσα προγραμματισμού για εφαρμογές σε ιστοσελίδες, γνωστή ως JavaScript, μπορεί να αποθηκεύσει πληροφορίες για τον χρήστη σε συγκεκριμένο τομέα ενός ιστότοπου. Τέτοια αποθήκευση μπορεί να είναι δύο ειδών, είτε "sessionStorage", όπου, όπως τα session cookies, αποθηκεύει πληροφορίες μόνο κατά τη διάρκεια της περιήγησης του χρήστη στην ιστοσελίδα, είτε "localStorage" όπου τα δεδομένα που συγκεντρώνονται αποθηκεύονται μόνιμα (ENISA EU, 2017). Παρά το γεγονός ότι αυτή η μέθοδος παρακολούθησης παρέχει αρκετές δυνατότητες (όπως μεγαλύτερος χώρος αποθήκευσης δεδομένων, οι περισσότεροι browser δεν διαγράφουν τα δεδομένα που αποθηκεύονται τοπικά) θεωρείται πιο ασφαλής από άποψη ιδιωτικότητας καθώς δεν παρέχει δυνατότητα παρακολούθησης του χρήστη σε διάφορες ιστοσελίδες (Clearcode, χ.χ). Ο μεγαλύτερος κίνδυνος για την ιδιωτικότητα δημιουργείται από τη δυνατότητα που παρέχει για αποθήκευση αντιγράφων cookies, ώστε σε περίπτωση που διαγραφούν από το χρήστη να δημιουργηθούν ξανά χωρίς ο χρήστης να το αντιληφθεί (ENISA EU, 2017).

4. **Cache storage:** Με τη σχετική μέθοδο το περιεχόμενο της σελίδας και άλλες πληροφορίες αποθηκεύονται εντός του browser. Αν και η διάρκεια της αποθήκευσης είναι προσωρινή, το Cache storage μπορεί να χρησιμοποιηθεί για τη διατήρηση ενός αναγνωριστικού για

τουλάχιστον κάποιο χρονικό διάστημα. Όμως επειδή η προσωρινή μνήμη εκκαθαρίζεται τακτικά η μέθοδος αυτή ταυτοποίησης δεν θεωρείται αποτελεσματική (ENISA EU, 2017).

**5. Flash cookies και local shared objects:** Τα Flash Cookies επιτελούν ίδια λειτουργία με τα cookies, με τη διαφορά ότι εγκαθίστανται από ιστότοπους που χρησιμοποιούν επεκτάσεις browser, όπως το Flash Player για τη προβολή βίντεο, και δεν ελέγχονται από τον browser. Το περιεχόμενό τους είναι εύκολα προσβάσιμο και δεν διαγράφεται με την εκκαθάριση των cookies μέσω των browsers. Για το λόγο αυτό χρησιμοποιείται συχνά για την αποθήκευση αντιγράφων cookies, όπως το Web Storage (ENISA EU, 2017). Τα Flash cookies συγκαταλέγονται στα Supercookies, δηλαδή cookies που δημιουργήθηκαν ως αντίδραση της τεχνολογίας παρακολούθησης στις τεχνικές μπλοκαρίσματος των απλών cookies. Εγκαθίστανται χωρίς συγκατάθεση του χρήστη και δεν έχουν ημερομηνία λήξης, οπότε μπορούν να επαναδημιουργήσουν αυτόματα τα απλά cookies, εάν αυτά διαγραφούν. Η ανθεκτικότητα των Supercookies βελτιώνεται περαιτέρω με τα Evercookie<sup>18</sup>, που είναι ένας συνδυασμός διάφορων μηχανισμών παρακολούθησης, που ο ένας βοηθάει τον άλλον και είναι σε θέση να αναγνωρίσει έναν Χρήστη ακόμα και όταν τα απλά cookies και τα Flash cookies έχουν αφαιρεθεί (ENISA EU, 2012).

## **2. ΤΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ DIGITAL ADVERTISING**

### **2.1. Η πολυπλοκότητα του νομικού πλαισίου γενικά**

Μολονότι δεν υφίσταται ενιαίο νομοθετικό πλαίσιο που να καλύπτει το Digital Advertising σε επίπεδο ΕΕ, ισχύουν ποικίλα νομοθετικά μέτρα για τη διαφήμιση, τα οποία παρέχουν ορισμένα δικαιώματα στους αποδέκτες. Το ισχύον νομικό πλαίσιο είναι περίπλοκο και αντιμετωπίζει μόνο ορισμένες πτυχές της Ψηφιακής Διαφήμισης, χρησιμοποιώντας συχνά έμμεσο τρόπο. Τα μέτρα αυτά δεν εμπεριέχουν ορισμό για παράδειγμα της «στοχευμένης διαφήμισης» ή της

---

<sup>18</sup> «Το Evercookie είναι μια διεπαφή προγραμματισμού εφαρμογών JavaScript που αναγνωρίζει και αναπαράγει σκόπιμα διαγραμμένα cookie στον χώρο αποθήκευσης του προγράμματος περιήγησης των χρηστών», Wikipedia (2022), διαθέσιμο σε <https://en.wikipedia.org/wiki/Evercookie>, ανακτήθηκε 30.4.2022.

«συμπεριφορικής διαφήμισης», αλλά συνήθως αναφέρονται στις γενικότερες έννοιες της «εμπορικής επικοινωνίας», της «εμπορικής πρακτικής» ή της «διαφήμισης». Κάποια νομοθετήματα που αφορούν τη Ψηφιακή Διαφήμιση στο βαθμό που το πεδίο εφαρμογής τους αναφέρεται σε ψηφιακό περιβάλλον ή τη διαφήμιση είναι τα κατωτέρω (Fourberg et al., 2021) :

- Οδηγία για το ηλεκτρονικό εμπόριο (eCommerce Directive),
- Κανονισμός 2019/1150 για την προώθηση της δίκαιης μεταχείρισης και της διαφάνειας για τους επιχειρηματικούς χρήστες επιγραμμικών υπηρεσιών διαμεσολάβησης (P2B Regulation),
- Οδηγία 2010/13/ΕΕ για τις υπηρεσίες οπτικοακουστικών μέσων (AVMS), όπως τροποποιήθηκε το 2018.
- Οδηγία 2005/29/ΕΚ για τις αθέμιτες εμπορικές πρακτικές (UCPD),
- Οδηγία 2006/114/ΕΚ για την παραπλανητική και συγκριτική διαφήμιση,
- Το Δίκαιο του Ανταγωνισμού εφαρμόζεται σε όλες τις ψηφιακές πλατφόρμες και ενδέχεται να προκαλέσει εκτεταμένες συνέπειες στην παροχή Ψηφιακής Διαφήμισης.
- Οδηγία 2002/58/ΕΚ ή αλλιώς ePrivacy Directive, εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών, περιέχοντας επίσης κανόνες σχετικά με τη χρήση των cookies,
- Κανονισμός (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και εφαρμόζεται στις διαφημιστικές πρακτικές, εφόσον συνεπάγονται χρήση δεδομένων προσωπικού χαρακτήρα.

Οι δυσχέρειες του νομικού πλαισίου που εφαρμόζεται στη διαφήμιση, και κατεξοχήν στην Ψηφιακή Διαφήμιση, έγκειται στα εμπλεκόμενα μέρη (καταναλωτές, εμπόρους, ανηλίκους κ.λπ.), στο περιεχόμενο της διαφήμισης ή στα μέσα που χρησιμοποιούνται για την προβολή του διαφημιστικού μηνύματος, καθώς οι παράγοντες αυτοί οδηγούν στην εκάστοτε εφαρμογή ή όχι των νομοθετικών μέτρων. Το νομικό πλαίσιο είναι επίσης κατακερματισμένο εντός των 27 κρατών μελών, δεδομένου ότι οι παλαιότερες οδηγίες, όπως η οδηγία για το ηλεκτρονικό εμπόριο, διαθέτουν ελάχιστα μέσα εναρμόνισης, με αποτέλεσμα ορισμένα κράτη μέλη να

θεσπίζουν πιο εκτεταμένους κανόνες, διακινδυνεύοντας μ' αυτό το τρόπο την επίτευξη μίας ενιαίας ψηφιακής αγοράς (Fourberg et al., 2021).

Καθότι στο πλαίσιο της παρούσας εξετάζονται ζητήματα επεξεργασίας προσωπικών δεδομένων στο πλαίσιο του Digital Advertising, αμέσως παρακάτω θα παρουσιάσουμε τα βασικότερα νομοθετικά εργαλεία, που ήδη έχουν τεθεί σε εφαρμογή είτε αναμένεται η δημοσίευσή τους και επηρεάζουν τη ρύθμιση της επεξεργασίας προσωπικών δεδομένων στο Digital Advertising, όπως ζητήματα διαφάνειας, συγκατάθεσης, χρήσης cookies και ούτω καθεξής.

## **2. 2. Γενικός Κανονισμός Προστασίας Δεδομένων**

### **2.2.1. Ιστορική Αναδρομή**

Ο Κανονισμός (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» ή «Κανονισμός»)<sup>19</sup> συνιστά αποτέλεσμα πολλαπλών και εντατικών διαβουλεύσεων, οι οποίες ξεκίνησαν ήδη κατά το έτος 2012. Κατόπιν μιας διετούς περιόδου προσαρμογής, ο εν λόγω Κανονισμός τέθηκε σε ενιαία και καθολική εφαρμογή σε είκοσι οκτώ (28) κράτη μέλη της Ευρωπαϊκής Ένωσης την 25<sup>η</sup> Μαΐου 2018 (άρθρο 99, ΓΚΠΔ) και μεταβάλλει το τοπίο στο πεδίο της προστασίας προσωπικών δεδομένων με στόχο την διαμόρφωση εναρμονισμένου και ενιαίου νομοθετικού πλαισίου αναφορικά με την προστασία των υποκειμένων των δεδομένων έναντι επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε όλα τα επιμέρους κράτη μέλη της Ένωσης (Μήτρου, 2017, σελ. 11 επ.).

Ο ΓΚΠΔ αντικατέστησε την Οδηγία 95/46/ΕΚ<sup>20</sup> η οποία είχε ενσωματωθεί στην ελληνική έννομη τάξη δυνάμει του Ν. 2472/1997 (Ιγγλεζάκης, 2004, σελ. 61 επ.). Τούτο διότι οι αλματώδεις

---

<sup>19</sup> Το πλήρες κείμενο του Κανονισμού είναι διαθέσιμο στη διεύθυνση <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=HR>, ανακτήθηκε 24.1.2022.

<sup>20</sup> Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για

τεχνολογικές εξελίξεις είχαν ως αποτέλεσμα να καταστούν ανεπίκαιρες οι ρυθμίσεις της Οδηγίας, καθόσον η μετάβαση στο Web 2.0, στο πλαίσιο του οποίου διαμορφώθηκαν οι υπηρεσίες κοινωνικής δικτύωσης, όπως και η επεξεργασία των καλούμενων μεγαδεδομένων (άλλως mega data), η νεφοϋπολογιστική (cloud computing), ο γεωεντοπισμός και άλλες επεμβατικές τεχνολογίες, οδήγησαν στην αύξηση της έντασης της επιτήρησης των χρηστών των ανωτέρω υπηρεσιών και συνακολούθως της παραβίασης της ιδιωτικής τους ζωής και των προσωπικών τους δεδομένων (Mitrou, 2017 σε: Synodinou et al., p. 19 επ.). Περαιτέρω, η ελεύθερη κυκλοφορία αγαθών, κεφαλαίων, υπηρεσιών και προσώπων στην εσωτερική αγορά απαιτούσε την ελεύθερη ροή δεδομένων, η οποία ήταν αδύνατο να πραγματοποιηθεί χωρίς τα κράτη μέλη να βασιστούν σε ένα υψηλότερο επίπεδο προστασίας των δεδομένων.

Η υιοθέτηση του ΓΚΠΔ συνεπώς έφερε ένα ενιαίο σύνολο κανόνων για την προστασία των δεδομένων προσωπικού χαρακτήρα, διαμορφώνοντας ένα περιβάλλον ασφάλειας δικαίου, στο οποίο δύνανται να βασιστούν τόσο τα άτομα ως υποκείμενα των δεδομένων όσο και οι οικονομικοί φορείς (Ιγγλεζάκης, 2021, σελ. 328).

Παρά το γεγονός ότι ο ΓΚΠΔ τυγχάνει άμεσης εφαρμογής, τα κράτη μέλη κλήθηκαν να εξειδικεύουν ορισμένα μέτρα εφαρμογής του και να επικαιροποιήσουν τους υφιστάμενους εθνικούς νόμους που αφορούν στην προστασία των δεδομένων. Την 29<sup>η</sup> Αυγούστου 2019, συνεπώς, δημοσιεύθηκε ο πολυαναμενόμενος νόμος 4624/2019 (ΦΕΚ 137/Α/29-08-2019), ο οποίος καταργεί τον προγενέστερο Ν.2472/1997 (με εξαίρεση κάποιες ειδικότερες διατάξεις) και συμπληρώνει τις διατάξεις του ΓΚΠΔ σε μία σειρά από τομείς. Συνοπτικά στο πρώτο κεφάλαιο του νόμου προσδιορίζονται ο σκοπός και το πεδίο εφαρμογής του, ο ορισμός δημόσιου και ιδιωτικού φορέα και ο υποχρεωτικός διορισμός υπευθύνου προστασίας δεδομένων σε δημόσιους φορείς. Μεγάλο μέρος του περιεχομένου του Ν.4624/2019 καταλαμβάνουν οι διατάξεις για την οργάνωση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, στο τρίτο κεφάλαιο τίθενται συμπληρωματικά μέτρα εφαρμογής του ΓΚΠΔ για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Τέλος, σημείο αναφοράς για τον ελληνικό νόμο αποτελεί το άρθρο 23, το οποίο προβλέπει ότι στις περιπτώσεις υπηρεσιών της κοινωνίας της

---

την ελεύθερη κυκλοφορία των δεδομένων αυτών, το κείμενο της οποίας είναι διαθέσιμο σε <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A31995L0046>, ανακτήθηκε 21.1.2022.

πληροφορίας, η συγκατάθεση του ανηλίκου είναι έγκυρη, μόνο εφόσον ο τελευταίος έχει συμπληρώσει το 15<sup>ο</sup> έτος της ηλικίας του, αντίθετα με τον Κανονισμό, ο οποίος θέτει ως ηλικιακό όριο τα δεκαέξι έτη, αφήνοντας το περιθώριο στα κράτη-μέλη να το μειώσουν με κατώτατο όριο τα 13 έτη. Συνεπώς σύμφωνα με το νόμο είναι άκυρη η λήψη συγκατάθεσης από ανήλικους κάτω των 15 ετών για τη χρήση υπηρεσιών της κοινωνίας της πληροφορίας, εκτός εάν αυτή δοθεί από νόμιμο αντιπρόσωπό τους.

### **2.2.2. Οι στόχοι του Κανονισμού**

Όπως συνάγεται από το Προοίμιο του Κανονισμού, ο τελευταίος επιδιώκει αφενός μεν το επίπεδο προστασίας των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων αναφορικά με την επεξεργασία των δεδομένων να είναι ισοδύναμο σε όλα τα κράτη μέλη της Ένωσης, ώστε να επιτευχθεί αφενός μια υψηλού επιπέδου προστασία, ικανή να ανταπεξέλθει τις προκλήσεις της ψηφιακής εποχής, υπέρ των φυσικών προσώπων, των οποίων τα δεδομένα υπόκεινται σε επεξεργασία, αφετέρου δε να αρθούν τα εμπόδια στις ροές δεδομένων προσωπικού χαρακτήρα εντός της ΕΕ (Ιγγλεζάκης, 2020, σελ. 26). Επιπροσθέτως, με την υιοθέτηση του Κανονισμού επιχειρείται να διασφαλιστεί η δημιουργία όμοιων οικονομικών προϋποθέσεων στην Ένωση για την ενδυνάμωση της εσωτερικής αγοράς και την ελεύθερη κυκλοφορία προσωπικών δεδομένων (άρθρο 1 παρ. 1, ΓΚΠΔ), η οποία συνιστά έκφανση της ψηφιακής ενιαίας αγοράς και ταυτοχρόνως εξειδίκευση της αρχής της ελεύθερης κυκλοφορίας εμπορευμάτων, υπηρεσιών και κεφαλαίων εντός της εσωτερικής αγοράς, όπως τούτο προβλέπεται στη διάταξη της παραγράφου 2 του άρθρου 26 ΣΛΕΕ.

Περαιτέρω, όπως ήδη έχει καταστεί σαφές εκ των ανωτέρω, η υιοθέτηση του Κανονισμού αποσκοπεί στον εκσυγχρονισμό του νομικού πλαισίου και συνακολούθως στην προσαρμογή του στις σύγχρονες τεχνολογικές εξελίξεις, ιδίως αν ληφθεί υπόψη ότι η κλίμακα της συλλογής, αποθήκευσης, ανταλλαγής και επεξεργασίας εν γένει δεδομένων προσωπικού χαρακτήρα έχει αυξηθεί σε σημαντικό βαθμό. Παράλληλα, γίνεται δεκτό ότι τόσο ιδιωτικές επιχειρήσεις όσο και δημόσιες αρχές χρησιμοποιούν προσωπικά δεδομένα, προκειμένου να επιτευχθούν οι επιχειρηματικοί σκοποί τους. Καθώς, λοιπόν, διευκολύνεται η ελεύθερη κυκλοφορία προσωπικών δεδομένων εντός της ΕΕ και η διαβίβαση σε τρίτες χώρες και διεθνείς οργανισμούς,



ο ΓΚΠΔ εισάγει καινοτόμες ρυθμίσεις, όπως επί παραδείγματι την αρχή της προστασίας δεδομένων εκ σχεδιασμού και εξ ορισμού (Μήτρου, 2013, σελ. 14 επ.) που συνιστά θεμελιώδη απαίτηση συμμόρφωσης του και θεμελιώνεται στο άρθρο 25, το δικαίωμα στη φορητότητα, το δικαίωμα στη λήθη (Ιγγλεζάκης 2014, σελ. 97 επ.), την εκτίμηση αντικτύπου στην προστασία των δεδομένων, την υποχρέωση διορισμού υπευθύνου επεξεργασίας σε ορισμένες περιπτώσεις και την εκπόνηση κωδίκων δεοντολογίας.

### **2.2.2. Το πεδίο εφαρμογής**

Ο Κανονισμός τυγχάνει εφαρμογής στην εν όλω ή εν μέρει αυτοματοποιημένη ή μη επεξεργασία προσωπικών δεδομένων, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε ένα οργανωμένο σύστημα αρχειοθέτησης (Κανέλλος, 2020, σελ. 174-176). Το εφαρμοστικό πεδίο του Κανονισμού εκτείνεται και στο δημόσιο τομέα, όπως τούτο συνάγεται από τον ορισμό του υπεύθυνου επεξεργασίας δεδομένων ως φυσικό ή νομικό πρόσωπο ή δημόσια αρχή (άρθρα 4 και 7, ΓΚΠΔ).

Αναλυτικότερα, ο Κανονισμός εφαρμόζεται στις περιπτώσεις κατά τις οποίες λαμβάνει χώρα επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία τεκμαίρεται ως κάθε πράξη ή σειρά πράξεων που εκτελείται, με τη χρήση αυτοματοποιημένων μέσων ή χωρίς αυτά, σε προσωπικά δεδομένα ή σε σύνολο προσωπικών δεδομένων, όπως επί παραδείγματι η καταχώριση, συλλογή, αποθήκευση, προσαρμογή, κάθε μεταβολή, χρήση, ανάκτηση και αναζήτηση πληροφοριών, διαβίβαση, διάδοση ή κάθε μορφή διάθεσης, καθώς και καταστροφή και διαγραφή (άρθρου 4 παρ. 2, ΓΚΠΔ). Οι πράξεις επεξεργασίας που ορίζει ο νομοθέτης στον Κανονισμό είναι ενδεικτικές και όχι περιοριστικές και εξ αυτού ο ορισμός της επεξεργασίας των δεδομένων παρέμεινε ανοιχτός, κυρίως καθότι ο ενωσιακός νομοθέτης αποσκοπεί στην αποτροπή σοβαρών κινδύνων καταστρατήγησης της προστασίας δεδομένων προσωπικού χαρακτήρα και επίσης ο ίδιος επεδίωξε να καταστεί η προστασία των φυσικών προσώπων τεχνολογικά ουδέτερα, δηλαδή ανεξάρτητη από τις τεχνικές επεξεργασίας δεδομένων προσωπικού χαρακτήρα (αιτ. σκέψη 15, ΓΚΠΔ).

### 2.3. Οδηγία 2002/58/EK

Η εν λόγω Οδηγία<sup>21</sup> αντικατέστησε την παλιά Οδηγία 97/66/EK<sup>22</sup> του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, καθόσον, λόγω των ραγδαίων τεχνολογικών εξελίξεων ήταν απαραίτητο να προσαρμοστούν οι υπηρεσίες ηλεκτρονικών επικοινωνιών στις νέες αυτές εξελίξεις των αγορών και τεχνολογιών. Η Οδηγία είναι γνωστή ως «ePrivacy Directive» και ο σκοπός της συνίσταται στην παροχή ισοδύναμου επιπέδου προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής σε όλους τους συνδρομητές και χρήστες υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό, ανεξάρτητα από τις χρησιμοποιούμενες παραδοσιακές τεχνολογίες, όπως είναι το διαδίκτυο. Η ως άνω Οδηγία με τις διατάξεις της εισήγαγε ένα σύγχρονο ρυθμιστικό πλαίσιο, το οποίο συμπεριλαμβάνει νέες και ειδικές τεχνικές λεπτομέρειες.

Εν συνεχεία, η Οδηγία 2002/58/EK τροποποιήθηκε δυνάμει της μεταγενέστερης Οδηγίας 2009/136/EK<sup>23</sup>, της γνωστής ως “cookies Directive”, οι διατάξεις της οποίας συνέβαλαν στην ενίσχυση της ασφάλειας των παρεχόμενων υπηρεσιών καθώς και στη θέσπιση αυξημένων υποχρεώσεων αναλυτικής πληροφόρησης των χρηστών, ενώ κατά το έτος 2013 εκδόθηκε ο υπ’

---

<sup>21</sup> Οδηγία 2002/58/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες), διαθέσιμη σε <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32002L0058>, ανακτήθηκε στις 24.1.2022.

<sup>22</sup> Οδηγία 97/66/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, διαθέσιμη σε <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A31997L0066>, ανακτήθηκε 25.1.2022.

<sup>23</sup> Οδηγία 2009/136/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, για τροποποίηση της οδηγίας 2002/22/EK για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/EK σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών (L 173), διαθέσιμη σε <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:32009L0136>, ανακτήθηκε 07.02.2022.

αριθμόν Κανονισμός (ΕΕ) 611/2013<sup>24</sup>, ο οποίος προσδιόρισε τα εφαρμοστέα μέτρα για τις περιπτώσεις κοινοποίησης παραβιάσεων προσωπικών δεδομένων δυνάμει της Οδηγίας 2002/58/ΕΚ. Πιο συγκεκριμένα, δυνάμει του ανωτέρω Κανονισμού ο πάροχος υποχρεούται να προβαίνει στην κοινοποίηση των παραβιάσεων δεδομένων προσωπικού χαρακτήρα στην αρμόδια εθνική αρχή, ενώ προβλέπεται υποχρέωση του παρόχου να κοινοποιήσει στο υποκείμενο των δεδομένων, στις περιπτώσεις κατά τις οποίες η εν λόγω παραβίαση ενδέχεται να επιφέρει δυσμενείς επιπτώσεις είτε στα δεδομένα προσωπικού χαρακτήρα είτε στην ιδιωτική ζωή ενός συνδρομητή ή χρήστη.

### **2.3.1. Ν.3471/2006**

Όπως αναφέρεται στον Ιγγλεζάκη (2021) η ePrivacy Directive ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν.3471/2006 και υπέστη σημαντικές τροποποιήσεις με την ενσωμάτωση των διατάξεων της Οδηγίας 2009/136. Στο άρθρο 3 του Ν. 3471/2006 καθορίζετε το εφαρμοστικό πεδίο του νόμου, το οποίο λαμβάνει χώρα κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών, στο πλαίσιο της παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα, περιλαμβανομένων αυτών που υποστηρίζουν συσκευές συλλογής δεδομένων και ταυτοποίησης. Συγκεκριμένα, στο πεδίο του νόμου υπάγονται ένα σύνολο υπηρεσιών, συμπεριλαμβανομένων των υπηρεσιών φωνητικής τηλεφωνίας, των υπηρεσιών που παρέχονται μέσω Διαδικτύου, όσων παρέχονται μέσω κινητών ψηφιακών δικτύων κ.ο.κ.

Τα σημαντικότερα σημεία του Ν.3471/2006 αφορούν τις διατάξεις που συμβάλλουν στην αύξηση της προστασίας του απορρήτου των επικοινωνιών (άρθρο 4, Ν.3471/2006), με κρίσιμο σημείο την επέκταση της προστασίας αυτής πέραν του περιεχομένου της επικοινωνίας και στα δεδομένα

---

24 ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) αριθ. 611/2013 ΤΗΣ ΕΠΙΤΡΟΠΗΣ της 24ης Ιουνίου 2013 σχετικά με τα εφαρμοστέα μέτρα για την κοινοποίηση παραβιάσεων προσωπικών δεδομένων βάσει της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, διαθέσιμος σε <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32013R0611&from=LV>, ανακτήθηκε 07.02.2022.

κίνησης και θέσης (άρθρο 5 παρ. 2 περ. β', Ν. 3471/2006), τα cookies, τους κανόνες επεξεργασίας και γενικότερα τα δικαιώματα των συνδρομητών και των χρηστών.

Πιο συγκεκριμένα η χρήση των cookies προβλέπεται στο άρθρο 170 του Ν.4070/2012, το οποίο αντικατέστησε το άρθρο 4 παρ. 5 του Ν.3471/2006, με σκοπό την εναρμόνιση με την Οδηγία 2009/136/ΕΚ. Σύμφωνα με τη διάταξη αυτή καταργήθηκε στο σύστημα «opt-out», σύμφωνα με το οποίο επιτρεπόταν στους χρήστες των αρχείων αυτών ή στους συνδρομητές μόνο η μεταγενέστερη δήλωση μη συγκατάθεσης.

Ο Ν.3471/2006, συμπορευόμενος με τον ΓΚΠΔ, στο άρθρο 5 παρ. 1 εξειδικεύει περαιτέρω την αρχή της αναγκαιότητας, καθώς τονίζει ότι η επεξεργασία των προσωπικών δεδομένων συμπεριλαμβανομένων των δεδομένων κίνησης και θέσης, πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των σκοπών της. Στον Ν.3471/2006 επίσης βασική προϋπόθεση για τη νομιμότητα της επεξεργασίας είναι η συγκατάθεση, με εξαίρεση νόμιμης επεξεργασίας χωρίς παροχή συγκατάθεσης στις περιπτώσεις αναγκαίας επεξεργασίας για την εκτέλεση σύμβασης όπου ο χρήστης ή ο συνδρομητής είναι συμβαλλόμενο μέρος και σε προσυμβατικό στάδιο κατά τη λήψη μέτρων μετά από αίτηση του συνδρομητή (άρθρο 5 παρ. 2 περ. β').

Καθοριστικής σημασίας είναι η συγκατάθεση με την απαραίτητη προηγηθείσα ενημέρωση για την επεξεργασία των δεδομένων κίνησης και θέσης, αφού σύμφωνα με το νόμο ο οποίος εμπεριέχει νέες ρυθμίσεις, περιλαμβάνουν πληροφορίες που μπορούν να ωθήσουν στη δημιουργία προφίλ των χρηστών για τη παρακολούθηση τους συνάγοντας κάθε είδους συμπεράσματα με σκοπό την άμεση προώθηση προϊόντων και υπηρεσιών. Μ' αυτό το τρόπο όπως και στα cookies υιοθετείται το σύστημα «opt-in».

Το σύστημα «opt-in» καθιερώνεται με το άρθρο 11 του Ν.3471/2006, για τη μη ζητηθείσα επικοινωνία, στην οποία περιλαμβάνεται και η ανεπιθύμητη ηλεκτρονική αλληλογραφία, θέτοντας ως βασική προϋπόθεση τη λήψη συγκατάθεσης εκ των προτέρων, τη παροχή όλων των μέσων ώστε ο παραλήπτης της επικοινωνίας να μπορεί να τη τερματίσει όποτε επιθυμεί, την απαγόρευση μη αιτηθείσας επικοινωνίας σε περίπτωση δήλωσης εκ των προτέρων για μη λήψη τέτοιων επικοινωνιών και απαγόρευση αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου με σκοπό την άμεση εμπορική προώθηση προϊόντων ή υπηρεσιών χωρίς την

ευδιάκριτη και σαφή αναφορά της ταυτότητας του αποστολέα και της διεύθυνσης σε περίπτωση βούλησης τερματισμού της επικοινωνίας.

## **2.4. Σχέδιο Κανονισμού E-Privacy**

### **2.4.1. Περί ePrivacy Regulation**

Στο πλαίσιο της ψηφιακής ενιαίας αγοράς κρίνεται αδήριτη η ανάγκη να διασφαλιστεί ένα υψηλότερο επίπεδο προστασίας της ιδιωτικής ζωής στους χρήστες υπηρεσιών ηλεκτρονικών επικοινωνιών και να παραχθούν ισότιμοι όροι ανταγωνισμού για όλους τους παράγοντες της αγοράς. Προς το σκοπό τούτο, είναι απαραίτητη η μεταρρύθμιση του πλαισίου για την προστασία δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, προκειμένου να διασφαλιστεί η προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών, κυρίως δε του σεβασμού της ιδιωτικής ζωής, το απόρρητο των επικοινωνιών και η προστασία των δεδομένων προσωπικού χαρακτήρα.

Αναγνωρίζοντας το ανωτέρω, η Ευρωπαϊκή Επιτροπή κατέθεσε πρόταση Κανονισμού αναφορικά με το σεβασμό της ιδιωτικής ζωής και την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες, γνωστό και ως e-Privacy Regulation<sup>25</sup>, η οποία τέθηκε προς διαβούλευση, προκειμένου ο ePrivacy Κανονισμός να συμβαδίζει με τον ΓΚΠΔ. Το νέο σχέδιο Κανονισμού, όπως αναλύεται κατωτέρω, θα καταργήσει την Οδηγία 2002/58/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, που αφορά στην επεξεργασία των προσωπικών δεδομένων και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Μήτρου, 2004, σελ. 371 επ., Νούσκαλης, 2003).

Λίγους μήνες μετά την ψήφιση του ΓΚΠΔ, το κείμενο της πρότασης του Κανονισμού παρουσιάστηκε για πρώτη φορά στην Ευρωπαϊκή Επιτροπή. Η τελευταία ενέκρινε την πρόταση για το σχέδιο ePrivacy Regulation και η Επιτροπή Πολιτικών Ελευθεριών, Δικαιοσύνης και

---

<sup>25</sup> Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για το σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της Οδηγίας 2002/58/EK (Κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες), COM/2017/010 final - 2017/03 (COD), διαθέσιμο σε <https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:52017PC0010>, ανακτήθηκε 07.02.2022.

Εσωτερικών Υποθέσεων στο Ευρωπαϊκό Κοινοβούλιο ενέκρινε την έκθεσή της στα τέλη του μηνός Οκτωβρίου του έτους 2017. Κατόπιν παρέλευσης τεσσάρων ολόκληρων ετών, ήτοι το μήνα Φεβρουάριο του έτους 2021, και κατόπιν έντονων διαπραγματεύσεων τα κράτη μέλη, εξαιρουμένης της Γερμανίας και της Αυστρίας, συμφώνησαν επί της διαπραγματευτικής εντολής για το σχέδιο του Κανονισμού ePrivacy.

Το ανωτέρω σχέδιο θα καταργήσει την ως άνω αναφερόμενη Οδηγία 2002/58/EK (Μήτρου, 2004, σελ. 371 επ., Νούσκαλης, 2003) και θα εξειδικεύσει και συμπληρώσει τον ΓΚΠΔ (Κανέλλος, 2020, σελ. 121), δεδομένου ότι τα εν λόγω νομοθετήματα τελούν μεταξύ τους σε σχέση γενικού και ειδικού νόμου. Σε αντίθεση με ό,τι ισχύει στον ΓΚΠΔ, ορισμένες διατάξεις του νέου σχεδίου θα είναι εφαρμοστές όχι μόνο σε φυσικά αλλά και σε νομικά πρόσωπα.

Το νέο σχέδιο που εμπεριέχει επικαιροποιημένους κανόνες και ρυθμίζει όλες εκείνες τις περιπτώσεις κατά τις οποίες οι πάροχοι υπηρεσιών επιτρέπεται να επεξεργάζονται δεδομένα ηλεκτρονικών επικοινωνιών ή να έχουν πρόσβαση σε δεδομένα αποθηκευμένα σε συσκευές τελικών χρηστών. Είναι χαρακτηριστικό ότι το νέο σχέδιο ePrivacy αναφέρεται τόσο στους παρόχους των παραδοσιακών ηλεκτρονικών επικοινωνιών, όπως για παράδειγμα στους παρόχους τηλεφωνίας, αλλά και στις υπηρεσίες που αναπτύχθηκαν κατά την 4<sup>η</sup> Βιομηχανικής Επανάστασης, όπως για παράδειγμα εφαρμογές Internet of Things («IoT») και διενέργειας προωθητικών επικοινωνιών (Βαρλά, 2021).

#### **2.4.2. Το χρονικό των διαπραγματεύσεων**

Ιδιαίτερο ενδιαφέρον παρουσιάζει η καθυστέρηση επίτευξης συμφωνίας επί του σχεδίου Κανονισμού ePrivacy. Δικαιολογητικός λόγος αυτής της καθυστέρησης ήταν η έλλειψη συμφωνίας των κρατών μελών της ΕΕ αναφορικά με τις βασικές διατάξεις του εν λόγω νομοθετήματος. Περαιτέρω, ενδιαφέρον παρουσιάζει ότι μέχρι και τον Φεβρουάριο του έτους 2021 οκτώ συνολικά χώρες είχαν καταβάλει προσπάθειες, οι οποίες τελικώς δεν τελεσφόρησαν, προκειμένου να συμβιβάσουν τα συμφέροντα των εμπλεκόμενων μερών και να καταλήξουν σε μια συμφωνία, αναφορικά με το κείμενο του σχεδίου ePrivacy. Στην καθυστέρηση αυτή συνέβαλε σε μεγάλο βαθμό ο προβληματισμός επί της αλληλεπίδρασης του ePrivacy με το ΓΚΠΔ (σχετική η υπ' αριθμόν 5/12.03.2019 Γνώμη του ΕΣΠΔ αναφορικά με την αλληλεπίδραση

μεταξύ της Οδηγίας για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του ΓΚΠΔ, ιδίως αναφορικά με τα ζητήματα αρμοδιότητας, καθηκόντων και εξουσιών των Αρχών Προστασίας Δεδομένων).

Επισημαίνεται, εν προκειμένω, ότι η εξέταση της πρότασης για το σχέδιο του Κανονισμού από το Συμβούλιο, η οποία έλαβε χώρα από την Ομάδα Εργασίας για τις τηλεπικοινωνίες και την Κοινωνία της Πληροφορίας ήταν μια αρκετά χρονοβόρος διαδικασία. Σε συνάρτηση με αυτήν την καθυστέρηση, σημαντικές καθυστερήσεις σημειώθηκαν ένεκα των αποκλιουσών απόψεων που διατυπώθηκαν μεταξύ των αντιπροσωπειών, οι οποίες, μολονότι οδήγησαν σε μείζονος σημασίας διευκρινίσεις επί του κειμένου της πρότασης, εν τούτοις στην πραγματικότητα καθυστέρησαν σε μεγάλο βαθμό την πρόοδο του Κανονισμού ePrivacy. Για παράδειγμα διευκρινίσεις απαιτήθηκαν καθόσον υπήρξαν ανησυχίες μεταξύ των αντιπροσωπειών ως προς τον τρόπο αλληλεπίδρασης του κανονισμού ePrivacy Regulation με νέες τεχνολογίες και μέσα, όπως για παράδειγμα είναι το IoT και η Τεχνητή Νοημοσύνη.

Οι μακροχρόνιες διαπραγματεύσεις που έλαβαν χώρα κατέδειξαν τη λεπτή ισορροπία ανάμεσα στην προστασία δεδομένων προσωπικού χαρακτήρα και την προάσπιση της καινοτομίας. Σε τούτο μάλιστα συνέβαλε ουσιωδώς και το γεγονός ότι πολλές υπερεθνικές ισχυρές εμπορικές και διαφημιστικές εταιρείες, καθώς και εταιρείες τεχνολογίας και πάροχοι τηλεπικοινωνιών άσκησαν έντονες πιέσεις, υποστηρίζοντας ότι οι προτεινόμενες διατάξεις του Κανονισμού λειτουργούν ως τροχοπέδη στην καινοτομία και παρακωλύουν τον πλουραλισμό των μέσων ενημέρωσης και επιδιώκοντας δραστικές εκπτώσεις στο εφαρμοστικό πεδίο του επικείμενου Κανονισμού. Τελικώς, έπειτα από το σύνολο των διαπραγματεύσεων, συνάγεται ότι το κείμενο που συνάδει με το στόχο που επιδιώκεται ήταν αυτό της φινλανδικής Προεδρίας το φθινόπωρο του 2019, που χαρακτηρίζεται «συμβιβαστικό» και στο οποίο βασίστηκε η Πορτογαλία κατά τη διαμόρφωση του οριστικού σχεδίου (Βαράλα, 2021).

#### ***2.4.3. Επισκόπηση ορισμένων εκ των βασικών διατάξεων που εισήχθησαν στο σχέδιο ePrivacy Regulation***

Αναλυτικότερα, στην αναθεωρημένη συμβιβαστική πρόταση, την οποία δημοσίευσε κατά το μήνα Φεβρουάριο 2019 το Συμβούλιο, έλαβαν χώρα ορισμένες τροποποιήσεις στην αιτιολογική

σκέψη 21 αναφορικά με την εξαίρεση συσκευών IoT. Περαιτέρω, βάσει της έκθεσης προόδου, θέματα που άπτονται της πρόληψης ή ανίχνευσης ή αναφοράς εικόνων, που απεικονίζουν κακοποιημένα παιδιά, έχουν, επίσης, καταστεί αντικείμενο διαφωνίας μεταξύ των αντιπροσωπειών, καθώς ερείδεται εάν πρέπει να εισαχθούν προς ρύθμιση στο ePrivacy Regulation. Συγκεκριμένα, μολονότι ορισμένα κράτη μέλη πρότειναν να αντιμετωπιστούν τα ως άνω ζητήματα με την εισαγωγή μιας διάταξης στο άρθρο 6 σχετικά με την επιτρεπόμενη επεξεργασία δεδομένων ηλεκτρονικών επικοινωνιών, εν τούτοις έτερα κράτη μέλη υποστήριξαν ότι είναι φρονιμότερο τα εν λόγω ζητήματα να αντιμετωπιστούν με μια ξεχωριστή νομική πράξη έναντι του άρθρου 11 αναφορικά με τους περιορισμούς.

Προς επίρρωση τούτου, το άρθρο 11 του Κανονισμού ePrivacy Regulation δίδει τη δυνατότητα στα κράτη μέλη να περιορίσουν το πεδίο εφαρμογής των δικαιωμάτων και υποχρεώσεων, στα οποία γίνεται αναφορά στα άρθρα 5 έως 8, αναφορικά με την εμπιστευτικότητα των δεδομένων ηλεκτρονικών επικοινωνιών, την επιτρεπόμενη επεξεργασία δεδομένων ηλεκτρονικών επικοινωνιών, την αποθήκευση και τη διαγραφή δεδομένων ηλεκτρονικών επικοινωνιών και την προστασία των πληροφοριών τετραγωνικού εξοπλισμού τελικών χρηστών.

Όπως συμβαίνει με τους περιορισμούς που τίθενται από τα κράτη μέλη στις διατάξεις των άρθρων 5, 12-22 και 34 του ΓΚΠΔ, έτσι και ένας περιορισμός που επιβάλλεται από μέρος ενός κράτους μέλους στα άρθρα 5-8 του ePrivacy Regulation θα είναι επιτρεπτός μονάχα υπό τον όρο να σέβεται *«...το περιεχόμενο των θεμελιωδών δικαιωμάτων και ελευθεριών και συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση ενός ή περισσοτέρων από τα γενικά δημόσια συμφέροντα του άρθρου 23 παράγραφος 1 στοιχείο α) έως ε) του κανονισμού (ΕΕ) 2016/679...»* (άρθρο 11 παρ.1, σχέδιο ePrivacy Regulation). Τα συμφέροντα αυτά αφορούν στη δημόσια ασφάλεια, την πρόληψη, διερεύνηση, τον εντοπισμό ή δίωξη ποινικών αδικημάτων ή και την εκτέλεση ποινικών κυρώσεων. Τέλος, περιλαμβάνουν και άλλους θεμελιώδεις στόχους γενικού δημοσίου συμφέροντος ενός κράτους μέλους της Ένωσης ή ακόμα και της Ένωσης εν όλω, όπως επί παραδείγματι δημοσιονομικά και φορολογικά ζητήματα και θέματα δημόσιας υγείας και κοινωνικής ασφάλειας.

Περαιτέρω, παρότι ο δρόμος μέχρι τη θέση σε εφαρμογή του νέου Κανονισμού ενδέχεται να είναι ιδιαίτερα μακρύς, εντούτοις οι νομοθετικές προβλέψεις του αναφορικά με την αυτόκλητη



εμπορική επικοινωνία (spam) αναμένεται να οδηγήσουν στον αποκλεισμό ή κατ' ελάχιστον στον περιορισμό της ηλεκτρονικής διαφήμισης, πλην των περιπτώσεων όπου ο παραλήπτης έχει παράσχει τη ρητή συγκατάθεσή του στη διαφήμιση μέσω της αποστολής εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου σε υφιστάμενους πελάτης για τη διαφήμιση όμοιων προϊόντων ή υπηρεσιών (Κανέλλος, 2020, σελ. 123). Είναι γνωστό ότι ο Κανονισμός θα καλύπτει το περιεχόμενο ηλεκτρονικών επικοινωνιών που μεταδίδεται μέσω διαθέσιμων στο κοινό υπηρεσιών και δικτύων, καθώς και τα μεταδεδομένα (metadata) (Ιγγλεζάκης, 2021, σελ. 158 επ.) που είναι συνυφασμένα με την επικοινωνία. Στην έννοια των μεταδεδομένων, τα οποία επεξεργάζονται οι πάροχοι για σκοπούς διαβίβασης και ανταλλαγής του περιεχομένου των επικοινωνιών, εσωκλείονται πληροφορίες αναφορικά με τη θέση, τον χρόνο και τον αποδέκτη της επικοινωνίας, οι οποίες θεωρούνται εξίσου ευαίσθητες με το περιεχόμενο. Περαιτέρω, στο περιεχόμενο των ηλεκτρονικών επικοινωνιών περιέχονται τα δεδομένα που μεταδίδονται κατά τη χρήση online υπηρεσιών, όπως το Viber και το Skype .

Ο νέος Κανονισμός θα είναι εφαρμοστέος στις περιπτώσεις που ο τελικός χρήστης ευρίσκεται εντός της Ευρωπαϊκής Ένωσης. Παράλληλα, το εφαρμοστικό πεδίο εκτείνεται και στις περιπτώσεις κατά τις οποίες η επεξεργασία πραγματοποιείται εκτός της Ευρωπαϊκής Ένωσης ή ο πάροχος υπηρεσιών είναι εγκατεστημένος ή ευρίσκεται εκτός Ευρωπαϊκής Ένωσης, δεδομένου ότι οι ρυθμίσεις του εν λόγω Κανονισμού δεν θα εξαρτώνται από εδαφικές παραμέτρους, όπως τούτο συμβαίνει στην περίπτωση του ΓΚΠΔ (Κανέλλος, 2020, σελ. 122).

Εκ των βασικότερων διατάξεων που περιέχει ο νέος Κανονισμός, ιδιαίτερο ενδιαφέρον παρουσιάζουν οι εξής:

- **White-lists**

Εξ αφορμής της συνεχούς συγκατάθεσης που ο χρήστης καλείται να χορηγεί για τα cookies, το νέο σχέδιο ορίζει ότι ο χρήστης θα δύναται να παρέχει τη συγκατάθεσή του για την εγκατάσταση και τη χρήση συγκεκριμένων τύπων cookies και ετέρων αναγνωριστικών κωδικών, καταχωρώντας έναν ή περισσότερους παρόχους σε κατάλογο εγκεκριμένων παρόχων για τη χρήση cookies στις ρυθμίσεις του browser.

Ο νέος Κανονισμός ωθεί, χωρίς να θέτει σχετική υποχρέωση, τους παρόχους λογισμικού να διευκολύνουν τους χρήστες στην εγκατάσταση και τροποποίηση καταλόγων εγκεκριμένων

παρόχων στους browser τους, ενώ παράλληλα παρέχει τη δυνατότητα ανάκλησης της συγκατάθεσης ανά πάσα στιγμή. Τούτο συνεπάγεται τη δημιουργία ενός κατάλληλου μηχανισμού, βάσει του οποίου οι τελικοί χρήστες θα έχουν τη δυνατότητα να διαχειρίζονται με εύκολο και διαφανή τρόπο τη συγκατάθεση που χορηγούν για τα cookies και να λαμβάνουν συγκεκριμένες και ενημερωμένες αποφάσεις σχετικά με την αποθήκευση και πρόσβαση στα δεδομένα που διατηρούνται στον τερματικό εξοπλισμό τους. Κατά συνέπεια, οι τελικοί χρήστες θα δύνανται να δημιουργούν και να τροποποιούν λίστες με τους εγκεκριμένους παρόχους (white-listing) ελέγχοντας με αυτόν τον τρόπο τη διαχείριση της συγκατάθεσής τους.

- **Cookie walls**

Το νέο σχέδιο του Κανονισμού ePrivacy προβλέπει ότι ο τελικός χρήστης θα πρέπει να έχει πραγματική επιλογή ως προς την αποδοχή των cookies ή παρεμφερών αναγνωριστικών κωδικών. Αναλυτικότερα, το νέο σχέδιο επιτρέπει στους παρόχους να θέτουν ως όρο για την πρόσβαση των χρηστών σε έναν δικτυακό τόπο τη χορήγηση από αυτούς συγκατάθεσης στη χρήση cookies για επιπρόσθετους σκοπούς, ως εναλλακτική λύση αντί της επί πληρωμή πρόσβασης σε αυτόν. Ωστόσο, για να είναι νόμιμο τούτο, θα πρέπει ο χρήστης να έχει στη διάθεσή του πραγματική επιλογή όσον αφορά στην αποδοχή των cookies, δηλαδή θα πρέπει ο χρήστης να είναι σε θέση να επιλέξει ανάμεσα στη συγκεκριμένη προσφορά και σε ισοδύναμη προσφορά του ίδιου παρόχου, η οποία δεν θέτει ως προϋπόθεση τη χορήγηση συγκατάθεσης για τα cookies. Επισημαίνεται εν προκειμένω ότι τεκμαίρεται ότι ο χρήστης δεν έχει πραγματική επιλογή στη χρήση cookies στην περίπτωση που έχει μονάχα ελάχιστες ή και καμία εναλλακτική επιλογή στη συγκεκριμένη υπηρεσία, κυρίως δε όταν ο πάροχος έχει δεσπόζουσα θέση στην ενιαία αγορά.

- **Επεξεργασία μεταδεδομένων**

Το νέο σχέδιο προβλέπει ότι τα μεταδεδομένα ηλεκτρονικών επικοινωνιών δύνανται να χρησιμεύσουν στις επιχειρήσεις, τους καταναλωτές, αλλά και την κοινωνία στο σύνολό της. Ωστόσο, λαμβανομένου υπόψη ότι το απόρρητο των επικοινωνιών και της διαδικτυακής δραστηριότητας έχει καιρία σημασία για τους χρήστες, η επεξεργασία των μεταδεδομένων από

τους παρόχους δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών καταρχήν επιτρέπεται μόνον κατόπιν χορήγησης της συγκατάθεσης του χρήστη (Λ. Κανέλλος, 2020, σελ. 122-123).

Ταυτόχρονα, προβλέπεται ότι οι πάροχοι δύνανται να επεξεργάζονται τα μεταδεδομένα ηλεκτρονικών επικοινωνιών ενός χρήστη στην περίπτωση που κρίνεται απαραίτητο για την παροχή υπηρεσίας ηλεκτρονικής επικοινωνίας βάσει σύμβασης, στην οποία ο χρήστης είναι συμβαλλόμενο μέρος, καθώς και για την τιμολόγηση της υπηρεσίας.

Τέλος, ο νέος Κανονισμός επιτρέπει τη δυνατότητα περαιτέρω επεξεργασίας των μεταδεδομένων χωρίς να δίδεται η συγκατάθεση του χρήστη για σκοπούς διαφορετικούς από τον αρχικό σκοπό συλλογής τους, εφόσον βέβαια οι εν λόγω σκοποί επεξεργασίας είναι συμβατοί προς τον αρχικό και ότι λαμβάνονται τα κατάλληλα μέτρα για την προστασία και ασφάλεια των δεδομένων.

## **2.5. Digital Services Act**

Η Ευρώπη, παρατηρώντας την επιταχυνόμενη ψηφιοποίηση της κοινωνίας και της οικονομίας, η οποία άνοιξε το δρόμο στις μεγάλες πλατφόρμες για τον έλεγχο των οικοσυστημάτων της ψηφιακής οικονομίας και των ψηφιακών αγορών, με την δύναμη να διαμορφώνουν από μόνες τους κανόνες, αξιώνει ένα σύγχρονο νομικό πλαίσιο με προτεραιότητα την ασφάλεια των χρηστών στο Διαδίκτυο, την καθιέρωση διακυβέρνησης με γνώμονα τη προστασία των θεμελιωδών δικαιωμάτων και τη διατήρηση ενός δίκαιου και ανοιχτού περιβάλλοντος διαδικτυακής πλατφόρμας (European Commission, 2022).

Η καθιέρωση ενός νομικού πλαισίου που να καλύπτει όλες τις απαιτήσεις της Ευρώπης για τη συμπόρευσή της με την ψηφιακή εποχή έγινε τον Δεκέμβριο του 2020, όταν η Ευρωπαϊκή Επιτροπή πρότεινε τον Digital Services Act (εφεξής «DSA»), για την ενίσχυση της ενιαίας αγοράς και την προστασία των πολιτών και των δικαιωμάτων τους. Τον Ιανουάριο του 2022 συμφωνήθηκε ένα σχέδιο μέτρων για την αντιμετώπιση του παράνομου περιεχομένου, τη διασφάλιση ότι οι πλατφόρμες λογοδοτούν για τους αλγορίθμους τους και τη βελτίωση της συγκράτησης του περιεχομένου. Η δήλωση του Christel Schaldemose, ηγέτη της διαπραγματευτικής ομάδας του Κοινοβουλίου, μετά τη ψηφοφορία δείχνει την επιθυμία των ευρωβουλευτών για μια φιλόδοξη ψηφιακή ρύθμιση κατάλληλη για το μέλλον. Συγκεκριμένα

δήλωσε: «Πολλά έχουν αλλάξει στα 20 χρόνια από τότε που εγκρίναμε την οδηγία για το ηλεκτρονικό εμπόριο. Οι διαδικτυακές πλατφόρμες έχουν γίνει όλο και πιο σημαντικές στην καθημερινή μας ζωή, φέρνοντας νέες ευκαιρίες, αλλά και νέους κινδύνους. Είναι καθήκον μας να διασφαλίσουμε ότι αυτό που είναι παράνομο εκτός σύνδεσης είναι παράνομο στο διαδίκτυο. Πρέπει να διασφαλίσουμε ότι θα θέσουμε σε εφαρμογή ψηφιακούς κανόνες προς όφελος των καταναλωτών και των πολιτών. Τώρα μπορούμε να ξεκινήσουμε διαπραγματεύσεις με το Συμβούλιο και πιστεύω ότι θα μπορέσουμε να υλοποιήσουμε αυτά τα ζητήματα». (Press Releases, 2022)

### **2.5.1. Φύση και πεδίο εφαρμογής**

Ο DSA λαμβάνει τη μορφή Κανονισμού, πράγμα που σημαίνει ότι θα εφαρμόζεται άμεσα στη έννομη τάξη των κρατών μελών. Ο DSA θα δώσει περισσότερο έλεγχο στους χρήστες επί του διαδικτυακού περιεχομένου και θα αποδώσει ευθύνες σε διάφορους τύπους υπηρεσιών, συμπεριλαμβανομένων των ενδιάμεσων υπηρεσιών<sup>26</sup>, των υπηρεσιών φιλοξενίας, των υπηρεσιών online πλατφορμών και των πολύ μεγάλων υπηρεσιών online πλατφορμών (VLOP) που έχουν περισσότερους από 45 εκατομμύρια μηνιαίους ενεργούς χρήστες στην ΕΕ. Αυτές οι εναρμονισμένες υποχρεώσεις σε επίπεδο ΕΕ αποσκοπούν στην ενίσχυση της ψηφιακής εσωτερικής αγοράς, στην αποσαφήνιση των ευθυνών όσον αφορά τις ψηφιακές υπηρεσίες και στη διασφάλιση της διαφάνειας, της λογοδοσίας και της ρυθμιστικής εποπτείας του online χώρου της ΕΕ (Fourberg κ.ά., 2021a).

### **2.5.2. Ουσιαστικά μέτρα σχετικά με τη στοχευμένη διαφήμιση**

Ο DSA καλύπτει κάθε είδους διαφήμιση, ακόμα και τις πολιτικές διαφημίσεις και συμπληρώνει τους υφιστάμενους κανόνες, όπως τον ΓΚΠΔ. Οι κανόνες του αποσκοπούν στο να διασφαλίσουν ότι οι χρήστες λαμβάνουν περισσότερες πληροφορίες που θα τους βοηθήσουν να κάνουν χρήση των δικαιωμάτων τους ως υποκείμενα των δεδομένων. Στόχος είναι να

---

<sup>26</sup> Σύμφωνα με την Ευρωπαϊκή Επιτροπή, οι online ενδιάμεσες υπηρεσίες είναι οι ψηφιακές υπηρεσίες που μεταδίδουν ή αποθηκεύουν το περιεχόμενο τρίτων. Θα περιλαμβάνουν, για παράδειγμα, παρόχους υπηρεσιών διαδικτύου, υπηρεσίες cloud, μηνύματα, αγορές ή κοινωνικά δίκτυα. (European Commission, 2022)

οδηγήσουν τους χρήστες στην κατανόηση και τη λήψη τεκμηριωμένων αποφάσεων σχετικά με τις διαφημίσεις που βλέπουν. Η άρνηση συγκατάθεσης δεν είναι πιο δύσκολη ή χρονοβόρα για τον αποδέκτη συγκριτικά με τη συγκατάθεση. Σε περίπτωση απόρριψης ή απόσυρσης της συγκατάθεσης, οι αποδέκτες έχουν άλλες επιλογές πρόσβασης στην online πλατφόρμα, συμπεριλαμβανομένων των «επιλογών που βασίζονται σε διαφημίσεις χωρίς παρακολούθηση».(European Commission 2022).

Εκτός από τις απαιτήσεις που απορρέουν από το άρθρο 6 της Οδηγίας για το ηλεκτρονικό εμπόριο, όλες οι online πλατφόρμες θα πρέπει να διασφαλίζουν ότι οι αποδέκτες της υπηρεσίας λαμβάνουν εξατομικευμένες πληροφορίες, ώστε να μπορούν να προσδιορίζουν, για κάθε συγκεκριμένη διαφήμιση που εμφανίζεται, με σαφή τρόπο και σε πραγματικό χρόνο:

- ότι οι πληροφορίες που εμφανίζονται είναι διαφήμιση,
- το (φυσικό ή νομικό) πρόσωπο για λογαριασμό του οποίου εμφανίζεται η διαφήμιση,
- ουσιαστικές πληροφορίες σχετικά με τις κύριες παραμέτρους που χρησιμοποιούνται για τον προσδιορισμό του παραλήπτη στον οποίο εμφανίζεται η διαφήμιση (Fourberg κ.ά., 2021a), και
- πληροφορίες σχετικά με τον τρόπο δημιουργίας εσόδων από τα δεδομένα τους.

Οι ευρωβουλευτές ενέκριναν με συντριπτική πλειοψηφία την απαγόρευση χρήσης ευαίσθητων δεδομένων με σκοπό τη στόχευση ατόμων βάσει ειδικών κατηγοριών δεδομένων που επακόλουθα επιτρέπουν τη στόχευση ευάλωτων ομάδων. Η τροποποίηση επίσης προβλέπει απαγόρευση των τεχνικών στόχευσης ή ενίσχυσης που αφορούν τα δεδομένα ανηλίκων με σκοπό την προβολή διαφημίσεων, καθώς και τη χρήση τεχνικών εξαπάτησης ή ώθησης από τις online πλατφόρμες με σκοπό τη επιρροή της συμπεριφοράς των χρηστών μέσω «σκοτεινών προτύπων». (European Commission, 2022a)

Όσον αφορά τις μεγάλες διαδικτυακές πλατφόρμες, τα κοινωνικά διακυβεύματα είναι υψηλότερα και οι κανόνες περιλαμβάνουν πρόσθετα μέτρα για τον μετριασμό των κινδύνων και την ενεργοποίηση της εποπτείας. Οφείλουν να συγκεντρώνουν και να δημοσιοποιούν μέσω διεπαφών προγραμματισμού εφαρμογών (API) ένα αποθετήριο που περιέχει ορισμένες πληροφορίες, διασφαλίζοντας παράλληλα ότι δεν περιέχει δεδομένα προσωπικού χαρακτήρα. Θα πρέπει να διατηρήσουν και να παρέχουν πρόσβαση στα αποθετήρια, επιτρέποντας στους

ερευνητές, την κοινωνία των πολιτών και τις αρχές να επιθεωρούν τον τρόπο εμφάνισης και στοχοποίησης των διαφημίσεων.

Η πρόταση συμπληρώνεται από μέτρα του νόμου για τις ψηφιακές αγορές<sup>27</sup>. Προβλέπονται διατάξεις για την αύξηση της διαφάνειας από τους gatekeepers, παρέχοντας πληροφορίες σχετικά με την τιμή των διαφημίσεων και την αμοιβή που καταβάλλεται στον Εκδότη. Πρέπει επίσης να παρέχουν πρόσβαση στα εργαλεία μέτρησης απόδοσης και στις πληροφορίες που είναι απαραίτητες για τους Διαφημιστές και τους Εκδότες για τη διεξαγωγή της δικής τους ανεξάρτητης επαλήθευσης του αποθεματικού (inventory).

### **2.5.3. Αντιδράσεις για τον επερχόμενο νόμο για τις ψηφιακές υπηρεσίες**

Ο DSA αποτελεί αντικείμενο ερίδων μεταξύ ακτιβιστών καταναλωτών και προασπιστών των ψηφιακών δικαιωμάτων από τη μία πλευρά και της αμερικανικής τεχνολογικής βιομηχανίας από την άλλη. «Οι ευρωβουλευτές ψήφισαν για την προστασία των δικαιωμάτων των πολιτών και επιθυμούν να περιορίσουν την επεμβατική πρακτική της διαφήμισης, σηματοδοτώντας την αρχή του τέλους για το τοξικό επιχειρηματικό μοντέλο της Big Tech», δήλωσε η Ναόμι Χίρστ, αγωνίστρια της ΜΚΟ ανθρωπίνων δικαιωμάτων Global Witness. Αντίθετα, ο IAB Europe, μετά τη δημοσίευση των αποτελεσμάτων της ψηφοφορίας, δημοσίευσε την εξής δήλωση «Απαιτείται μεγαλύτερη σαφήνεια σχετικά με τις προτάσεις, με τα σκοτεινά πρότυπα και την επιτυχή επιβολή απαγόρευσης στοχευμένων διαφημίσεων για ανηλίκους» (Meyer David, 2022).

Η IAB Europe, σε πρώτο επίπεδο προσέγγισε χωρίς προκαταλήψεις τον DSA, τονίζοντας το ιδιοτελές συμφέρον του κλάδου της ψηφιακής διαφήμισης για τη διασφάλιση της διαφάνειας και της εμπιστοσύνης. Παρόλα αυτά εξέφρασε την κάθετη διαφωνία του με την απαγόρευση της στοχευμένης διαφήμισης, καθώς υποστηρίζει σθεναρά ότι οι κανόνες συναίνεσης και το δικαίωμα εναντίωσης στην επεξεργασία προσωπικών δεδομένων καλύπτεται πλήρως από το ισχύον νομικό πλαίσιο της ΕΕ για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων και τυχόν νέες διατάξεις δεν πρέπει να υπονομεύουν ή να αντικρούουν αυτό το πλαίσιο, αλλά να το συμπληρώνουν. Τέλος, σύμφωνα με τον IAB Europe, μία τέτοια πρόταση

---

<sup>27</sup> Στις 24 Μαρτίου 2022 επετεύχθη πολιτική συμφωνία μεταξύ του Ευρωπαϊκού Κοινοβουλίου και των κρατών μελών της ΕΕ σχετικά με τον νόμο για τις ψηφιακές αγορές (DMA).

θα στερήσει όλα τα οφέλη των πολιτών που απορρέουν από τις υπηρεσίες στοχευμένης διαφήμισης και θα εμποδίσει την είσοδο στην αγορά των νεοσύστατων επιχειρήσεων, οι οποίες στηρίζονται σε τέτοιες μεθόδους ώστε να αποκτήσουν αναγνωρισιμότητα και μέσω αυτής να προσεγγίσουν τους πελάτες τους (IAB Europe, χ.χ)

### **3. Η ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ DIGITAL ADVERTISING**

#### **3.1. Η αρχή της διαφάνειας της επεξεργασίας/Το δικαίωμα ενημέρωσης**

Έναν εκ των βασικότερων κινδύνων για την προστασία των προσωπικών δεδομένων των χρηστών αποτελεί η έλλειψη της προβλεπόμενης εκ του άρθρου 12 ΓΚΠΔ διαφάνειας, η οποία λειτουργεί ως «γενική ρήτρα» για την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων (Ιγγλεζάκης, 2020, σελ. 148). Η αρχή της διαφάνειας, προϋποθέτει τη λήψη των κατάλληλων μέτρων από τον υπεύθυνο επεξεργασίας ώστε η ενημέρωση που παρέχεται στο υποκείμενο των δεδομένων για την επεξεργασία των δεδομένων του να είναι συνοπτική, εύκολα προσβάσιμη, κατανοητή με σαφή και απλή διατύπωση. Πιο συγκεκριμένα κατ' εφαρμογή της εν λόγω αρχής, ο υπεύθυνος επεξεργασίας υποχρεούται να παρέχει πληροφορίες και να ενημερώνει τα υποκείμενα των δεδομένων αναφορικά με την ταυτότητα του ίδιου, τους σκοπούς της επεξεργασίας, οι οποίοι απαιτείται να είναι σύννομοι και να έχουν προσδιοριστεί κατά το χρόνο συλλογής των προσωπικών δεδομένων (Αιτιολογική Σκέψη 39 ΓΚΠΔ). Επίσης, αξίζει να επισημανθεί ότι σύμφωνα με την αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας, θεμελιώδης αρχή που διέπει την επεξεργασία προσωπικών δεδομένων, απαιτείται η νόμιμη και θεμιτή επεξεργασία των προσωπικών δεδομένων με τρόπο διαφανή σε σχέση με το υποκείμενο των δεδομένων, όπως προβλέπεται στο άρθρο 5 παρ. 1 ΓΚΠΔ (Ιγγλεζάκης, 2020, σελ. 77).

Ωστόσο, στο πλαίσιο του Digital Advertising, έχει κριθεί ότι δεδομένης της πολυπλοκότητας της λειτουργίας των διάφορων διαφημιστικών εργαλείων που χρησιμοποιούνται δεν καθίσταται δυνατή η ενημέρωση του υποκειμένου σχετικά με τα είδη των εκτελούμενων δραστηριοτήτων

και με τις λοιπές αναγκαίες πληροφορίες με τους προβλεπόμενους τρόπους (WP 29, 2018). Η έλλειψη διαφάνειας είναι πιο εμφανής όσον αφορά τις πηγές και τους αποδέκτες των προσωπικών δεδομένων, κυρίως λόγω της δημιουργίας προφίλ, γι' αυτό και έχει εκτεταμένες συνέπειες στην ικανότητα των υποκειμένων των δεδομένων να ασκούν τα δικαιώματά τους ( Privacy International, 2018).

Σύμφωνα με τα άρθρα 13, 14 και 15 του ΓΚΠΔ, το υποκείμενο των δεδομένων δικαιούται πληροφορίες σχετικά με την πηγή προέλευσης των προσωπικών δεδομένων που επεξεργάζεται ο υπεύθυνος επεξεργασίας δεδομένων. Η WP 29 καθιστά σαφές ότι αυτή η υποχρέωση διαφάνειας ισχύει ακόμη και όταν το έργο είναι επαχθές. Αν μία βάση δεδομένων περιλαμβάνει προσωπικά δεδομένα τα οποία έχουν συγκεντρωθεί με τη χρήση περισσότερων πηγών δεν αρκεί για να άρει αυτήν την απαίτηση. Λαμβάνοντας υπόψη τις απαιτήσεις προστασίας δεδομένων από τον σχεδιασμό και εξ ορισμού, θα πρέπει εξ αρχής να ενσωματωθούν μηχανισμοί διαφάνειας στα συστήματα επεξεργασίας, έτσι ώστε όλες οι πηγές προσωπικών δεδομένων που λαμβάνονται σε έναν οργανισμό να μπορούν να παρακολουθούνται και να ανιχνεύονται στην πηγή τους σε οποιοδήποτε σημείο του κύκλου επεξεργασίας των δεδομένων. Επιπλέον, το υποκείμενο των δεδομένων δικαιούται να γνωρίζει τους παραλήπτες ή τις κατηγορίες αποδεκτών των προσωπικών του δεδομένων, συμπεριλαμβανομένων και αυτών που πρόκειται να λάβουν γνώση μελλοντικά ( Privacy International, 2018).

Η τήρηση της διαφάνειας όπως και η υποχρέωση ενημέρωσης διασφαλίζεται με τη παροχή επαρκών και αποτελεσματικών πληροφοριών με τις αντίστοιχες «φιλικές προς το χρήστη» μεθόδους ώστε να γίνονται κατανοητοί στους μέσους χρήστες, οι οποίοι σπάνια παρατηρούν μεθόδους ενημέρωσης όπως εικονίδια, λογότυπα ή άλλα banner διαφάνειας, ή λειτουργίες «AdChoices», είτε συχνά δεν τα κατανοούν. Οι έρευνες έχουν δείξει επίσης ότι οι χρήστες δεν επιθυμούν να παρακολουθούνται και να αντιλαμβάνονται ότι η Ψηφιακή Διαφήμιση παραβιάζει το απόρρητο τους. Έχει διαπιστωθεί ότι οι «άκρως εξατομικευμένες διαφημίσεις» μείωσαν τη πρόθεση συμπεριφοράς των χρηστών, ενώ η μεγαλύτερη διαφάνεια ωθεί τους καταναλωτές σε περισσότερα ποσοστά πρόθεσης κλικ στις διαδικτυακές Συμπεριφορικές Διαφημίσεις (Aiolfi, Bellini και Pellegrini, 2021). Συνεπώς, τα πιο διαφανή επιχειρηματικά



μοντέλα μπορούν να ωφελήσουν ταυτόχρονα τους χρήστες, τους παρόχους και τους διαφημιστές (Wachter, 2019).

### **3.2. Νομιμότητα επεξεργασίας για διαφημιστικούς σκοπούς**

#### **3.2.1. Γενικότερο κανονιστικό πλαίσιο**

Το σύνθετο νομικό πλαίσιο που εφαρμόζεται στις ηλεκτρονικές επικοινωνίες, αποτέλεσμα της αλληλεπίδρασης του ΓΚΠΔ και της Οδηγίας ePrivacy επηρεάζει τη νομική βάση επεξεργασίας στο πλαίσιο του Digital Advertising. Σημαντικό είναι να αναφέρουμε ότι τα συστήματα της Ψηφιακής Διαφήμισης τροφοδοτούνται με τα δεδομένα χρηστών, εκ των οποίων κάποια χαρακτηρίζονται ως προσωπικά και κάποια όχι. Τα δεδομένα που δεν χαρακτηρίζονται ως προσωπικά μολονότι δεν προστατεύονται από το πλαίσιο του ΓΚΠΔ, εντάσσονται στο πεδίο εφαρμογής της Οδηγίας ePrivacy. Τα ανωτέρω έχουν επισημανθεί ήδη από το 2011, καθώς η WP 29 και στη συνέχεια το Δικαστήριο της Ε.Ε., τονίζουν ότι τα διαβιβαζόμενα δεδομένα, στο πλαίσιο της Ψηφιακής Διαφήμισης, που δεν χαρακτηρίζονται, έστω και αρχικά ως προσωπικά, δεν εξαιρούνται από το πεδίο εφαρμογής της Οδηγίας ePrivacy.

Μοναδική νομική βάση στο τομέα των ηλεκτρονικών επικοινωνιών είναι η συγκατάθεση για την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή χρήστη, μετά από σαφή και εκτενή ενημέρωση. Η εμπλοκή πολλών μερών στις πράξεις αυτές δυσχεραίνει τη τεκμηρίωση των νομικών βάσεων και τον καθορισμό ρόλων επεξεργασίας. Επιπλέον ζήτημα αποτελεί και το γεγονός ότι η Οδηγία ePrivacy δεν περιλαμβάνει ειδικούς κανόνες για προγενέστερες ή μεταγενέστερες πράξεις επεξεργασίας που αφορούν τέτοιες πληροφορίες, με αποτέλεσμα στις περιπτώσεις που οι πληροφορίες αυτές χαρακτηριστούν ως προσωπικά δεδομένα, ίσως θα πρέπει να αναζητηθεί άλλη νομική βάση για την περαιτέρω επεξεργασία τους (Καρκατζούνης και Μήτρου, 2020).

Στις περιπτώσεις άμεσης εμπορικής προώθησης έχει υποστηριχθεί ότι το έννομο συμφέρον του Εκδότη μπορεί να είναι μία κατάλληλη νομική βάση για την περαιτέρω επεξεργασία προσωπικών δεδομένων. Όσον αφορά τη Στοχευμένη Διαφήμιση, οι ερμηνευτικές

κατευθυντήριες γραμμές που υιοθετούνται σε επίπεδο Ε.Ε. υπογραμμίζουν την αναγκαιότητα λήψης της συναίνεσης του υποκειμένου των δεδομένων, ενώ η WP 29 υποστηρίζει ότι το έννομο συμφέρον δεν αποτελεί κατάλληλη νομική βάση για διαφημιστικούς σκοπούς που αφορούν την παρακολούθηση των υποκειμένων των δεδομένων και τη συνεπαγόμενη δημιουργία προφίλ. Το ΕΣΠΔ έχει αποκλείσει την εκτέλεση σύμβασης ως νομική βάση στη Ψηφιακή Διαφήμιση, ενώ αναφορικά με το έννομο συμφέρον τονίζει ότι μπορεί να χαρακτηριστεί ως έγκυρος νομικός λόγος μόνο σε σχέση με τη στόχευση βάσει δεδομένων που παρέχονται απευθείας από τα υποκείμενα των δεδομένων (Fourberg et al., 2021). Οι υπεύθυνοι επεξεργασίας μπορεί να έχουν έννομο συμφέρον να γνωρίζουν τις προτιμήσεις των πελατών τους, για λόγους προσφοράς προϊόντων και υπηρεσιών, όμως πρακτικά συνδυάζουν τεράστιο όγκο δεδομένων από διαφορετικές πηγές που συλλέχθηκαν αρχικά σε άλλα πλαίσια και για διαφορετικούς σκοπούς, χωρίς να αντιλαμβάνονται τις υποχρεώσεις που ακολουθούν την επιλογή της συγκεκριμένης νομικής βάσης, πλέον της συγκατάθεσης, όπως είναι η υιοθέτηση ενός λειτουργικού μηχανισμού αντιρρήσεων για τη ικανοποίηση του δικαιώματος εναντίωσης ή την επιλογή της απαιτούμενης άσκησης ισορροπίας (balancing test) ανάμεσα στο επιδιωκόμενο συμφέρον τους και τα δικαιώματα των υποκειμένων (Privacy International, 2018).

Στην ελληνική έννομη τάξη, το άρθρο 11 παράγραφος 1 του Ν. 3741/2006 καθιστά σαφές ότι απαιτείται ελεύθερη, ειδική και ρητή προηγούμενη συγκατάθεση του συνδρομητή-παραλήπτη, προκειμένου να χρησιμοποιούνται νομίμως αυτόματα συστήματα κλήσης, συμπεριλαμβανομένου του ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης και για διαφημιστικούς σκοπούς πάσης φύσεως, σύμφωνα με το καλούμενο σύστημα «opt-in», με εξαίρεση όταν τα στοιχεία επαφής, έχουν αποκτηθεί στο πλαίσιο της σύμβασης πώλησης παρόμοιων προϊόντων ή υπηρεσιών στο πλαίσιο έτερης προγενέστερης συναλλαγής με τον αποστολέα (αρ.11 παρ.3). Σε αυτήν την περίπτωση, θεωρείται σύννομη η διαφήμιση παρόμοιων προϊόντων ή υπηρεσιών μέσω της χρήσης αυτοματοποιημένων μέσων, δεδομένου ότι θεωρείται απαραίτητο για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας. Ωστόσο απαιτείται να παρέχεται στον αποδέκτη, κατά τρόπο σαφή και ευδιάκριτο, η δυνατότητα να αντιτάσσεται, με ευχέρεια και χωρίς κόστος, στην περαιτέρω συλλογή και επεξεργασία των ηλεκτρονικών του στοιχείων σε κάθε ηλεκτρονικό

μήνυμα. Τέλος, η παράγραφος 4 του άρθρου 11 του Ν. 3741/2006 θεσπίζει ορισμένες επιπρόσθετες προϋποθέσεις σύννομης αποστολής ηλεκτρονικών μηνυμάτων για διαφημιστικούς σκοπούς, όπως η απαίτηση σε κάθε ηλεκτρονικό μήνυμα να περιλαμβάνει και να αναγράφει, με τρόπο σαφή και ευδιάκριτο, την ταυτότητα του αποστολέα ή του διαφημιζόμενου, καθώς και έναν τρόπο, με τον οποίο ο παραλήπτης του δύναται να αντιταχθεί στην περαιτέρω αποστολή παρόμοιων μηνυμάτων στο μέλλον.

### **3.2.2. Ειδικότερο ζήτημα συγκατάθεσης**

Η ειδικότερη νομική βάση της συγκατάθεσης του υποκειμένου των δεδομένων, προβλέπεται στο άρθρο 6 παρ. 1 περίπτωση α' ΓΚΠΔ ως απαραίτητη προϋπόθεση για να είναι σύννομη η επεξεργασία των προσωπικών δεδομένων. Στην ελληνική έννομη τάξη, η διάταξη του άρθρου 5 παρ. 3 Ν. 3741/2006 προβλέπει ότι ο υπεύθυνος επεξεργασίας υποχρεούται να διασφαλίζει ότι έκαστος χρήστης ή συνδρομητής παρέχει τη συγκατάθεσή του στην επεξεργασία των προσωπικών δεδομένων, που το αφορούν, για έναν ή περισσότερους σκοπούς, έχοντας πλήρη επίγνωση των συνεπειών που επιφέρει η σχετική δήλωση συγκατάθεσης, ενώ προβλέπεται ότι η δήλωση συγκατάθεσης απαιτείται να καταγράφεται με ασφαλή τρόπο, να υπάρχει δυνατότητα πρόσβασης σε εκείνη σε οποιαδήποτε χρονική στιγμή και να μπορεί να ανακαλείται ανά πάσα στιγμή.

Η συναίνεση ως νομική βάση θα πρέπει να αποδίδει στα άτομα τον τρόπο ελέγχου και επιλογής σχετικά με τον τρόπο επεξεργασίας των προσωπικών τους δεδομένων, όπως ορίζεται στο άρθρο 4 παράγραφος 11 του GDPR ως «κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν». Στην αιτιολογική σκέψη 43 του Κανονισμού, διευκρινίζεται ότι προκειμένου να διασφαλιστεί ότι η συγκατάθεση παρέχεται ελεύθερα, δεν θα πρέπει να παρέχει έγκυρη νομική βάση για την επεξεργασία προσωπικών δεδομένων σε περιπτώσεις όπου υπάρχει σαφής ανισορροπία μεταξύ του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας. Η συγκατάθεση τεκμαίρεται ότι δεν παρέχεται ελεύθερα εάν δεν επιτρέπει τη

χωριστή συγκατάθεση για διαφορετικές λειτουργίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ακόμη και αν ενδείκνυται στη συγκεκριμένη περίπτωση, ή όταν η εκτέλεση μιας σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, προϋποθέτει τη συγκατάθεση. Επίσης, η συγκατάθεση δεν μπορεί να δοθεί υπό όρους, πρέπει να είναι λεπτομερής χωρίς να συγχέει τους σκοπούς επεξεργασίας και δεν δύναται να δίδεται στο πλαίσιο γραπτής δήλωσης που αφορά επιπρόσθετα άλλα θέματα. Η συναίνεση υποβάλλεται με τρόπο που να διακρίνεται σαφώς από άλλα ζητήματα επεξεργασίας δεδομένων, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα. Προκειμένου λοιπόν να υπάρχει αδιαμφισβήτητη ένδειξη των επιθυμιών του υποκειμένου των δεδομένων, οι κατευθυντήριες γραμμές της WP 29 τονίζουν ότι σε περιπτώσεις όπου άλλοι υπεύθυνοι επεξεργασίας πρόκειται να μεταφέρουν ή να επεξεργαστούν προσωπικά δεδομένα βασιζόμενοι στην αρχική συγκατάθεση, πρέπει να κατονομαστούν όλοι (Privacy International, 2018).

Στη Στοχευμένη Διαφήμιση οι απαιτήσεις για έγκυρη συγκατάθεση είναι αυξημένες. Όταν η επεξεργασία δεδομένων βασίζεται στη συγκατάθεση, η οποία συνεπάγεται πραγματική επιλογή από το υποκείμενο των δεδομένων, αυτό ουσιαστικά σημαίνει ότι οι καταναλωτές επιλέγουν τη Στοχευμένη Διαφήμιση. Κατ' ακολουθίαν, οι υπεύθυνοι επεξεργασίας οφείλουν να παραχωρούν στα υποκείμενα των δεδομένων δικαιώματα που ενισχύουν τους χρήστες της Ψηφιακής Διαφήμισης. Αυτά τα δικαιώματα περιλαμβάνουν το δικαίωμα ενημέρωσης, το δικαίωμα ανάκλησης της συγκατάθεσης, το δικαίωμα διαγραφής και το δικαίωμα αντίρρησης στην επεξεργασία για σκοπούς μάρκετινγκ. Όταν ένα υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεσή του και ο υπεύθυνος επεξεργασίας δεδομένων δεν δύναται να επικαλεστεί άλλο νομικό λόγο ή αντιτίθεται στην επεξεργασία για σκοπούς άμεσου μάρκετινγκ, έχει τη δυνατότητα να ζητήσει τη διαγραφή των προσωπικών του δεδομένων που υπόκεινται σε επεξεργασία που συνδέεται με τη Στοχευμένη Διαφήμιση. Επομένως, ο υπεύθυνος επεξεργασίας οφείλει να κοινοποιεί σε κάθε αποδέκτη των προσωπικών δεδομένων το αίτημα διαγραφής του υποκειμένου των δεδομένων. Μεταξύ των υποχρεώσεών τους, οι υπεύθυνοι επεξεργασίας πρέπει να αξιολογούν τους κινδύνους για τα δικαιώματα και τις ελευθερίες που συνεπάγονται οι δραστηριότητες της επεξεργασίας και επιβάλλεται η διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (DPIA) (Fourberg et al., 2021).

Ένα ακόμα δικαίωμα των υποκειμένων δεδομένων όπως αναφέρεται ρητά στο άρθρο 22 ΓΚΠΔ είναι να μην υπόκεινται σε απόφαση που βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της δημιουργίας προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο, εκτός αν προηγουμένως έχουν συναινέσει ρητά σε μία τέτοια επεξεργασία. Σε αυτήν την περίπτωση, η Στοχευμένη Διαφήμιση θα υπόκειται σε επιλογή συμμετοχής του στοχευόμενου ατόμου. Η WP 29 επισημαίνει ότι: «Οι υπεύθυνοι επεξεργασίας που επιδιώκουν να βασιστούν στη συγκατάθεση ως βάση για τη δημιουργία προφίλ θα πρέπει να αποδείξουν ότι τα υποκείμενα των δεδομένων κατανοούν ακριβώς σε τι συναινούν και να θυμούνται ότι η συγκατάθεση δεν αποτελεί πάντα κατάλληλη βάση για την επεξεργασία. Σε όλες τις περιπτώσεις, τα υποκείμενα των δεδομένων θα πρέπει να έχουν αρκετές πληροφορίες σχετικά με την προβλεπόμενη χρήση και τις συνέπειες της επεξεργασίας για να διασφαλιστεί ότι οποιαδήποτε συγκατάθεση παρέχουν αντιπροσωπεύει μια τεκμηριωμένη επιλογή» (Fourberg et al., 2021) .

Προς το σκοπό της υιοθέτησης ορθών πρακτικών λήψης συγκατάθεσης με τη χρήση ηλεκτρονικών μέσων, η ΑΠΔΠΧ έχει προβεί στην έκδοση της υπ' αριθμόν 2/2011 Οδηγίας, στο πλαίσιο της οποίας παρέχονται βέλτιστες πρακτικές αναφορικά με τη διαδικασία δήλωσης της συγκατάθεσης για την επεξεργασία προσωπικών δεδομένων ενός συνδρομητή ή χρήστη με τη χρήση ηλεκτρονικών μέσων για σκοπούς απευθείας εμπορικής προώθησης. Σύμφωνα με την ως άνω Οδηγία θεμελιώνεται υποχρέωση του υπεύθυνου επεξεργασίας σχετικά με την εφαρμογή μηχανισμών επιβεβαίωσης της ηλεκτρονικής συγκατάθεσης σύμφωνα με το σύστημα «opt-in», οι οποίοι πρέπει να προσαρμόζονται στο εκάστοτε χρησιμοποιούμενο ηλεκτρονικό μέσο (ΑΠΔΠΧ, 2011).

Η συγκατάθεση αποτελεί την νομική βάση που επιλέγουν οι περισσότερες εποπτικές αρχές για αυτού του είδους την επεξεργασία, πρακτικά όμως παρουσιάζονται προβλήματα, τα οποία σχετίζονται με το ίδιο το περιεχόμενο της έννοιας της συγκατάθεσης, όπως η πλήρης επίγνωσή της και η ελεύθερη ανάκλησή της, στοιχεία που δύσκολα μπορούν να επιτευχθούν στη σύγχρονη Ψηφιακή Διαφήμιση. Δυσκολίες παρουσιάζονται επιπλέον όταν αντιμετωπίζουμε κενά στη νομοθεσία, όπως στις περιπτώσεις ορισμένων μηχανισμών παρακολούθησης, όπως

το δακτυλικό αποτύπωμα συσκευής, οι οποίοι ενδέχεται να μην απαιτούν αποθήκευση ή πρόσβαση σε πληροφορίες στον εξοπλισμό τελικού χρήστη, συνεπώς δεν καλύπτονται σαφώς από την Οδηγία για την προστασία της ιδιωτικής ζωής ηλεκτρονικών επικοινωνιών (Fourberg et al., 2021).

Στο πλαίσιο της Ψηφιακής Διαφήμισης, η απανταχού παρουσία των διαφημίσεων και η υποκείμενη ανάλυση δεδομένων που χρησιμοποιούνται για τη δημιουργία προφίλ υποδηλώνει ότι η ενημερωμένη συναίνεση είναι ιδιαίτερα δυσχερής. Σε κάποια σημεία όπως η αιτιολογία των χρήσεων των προσωπικών δεδομένων ή ο τρόπος χειρισμού από τους υπεύθυνους επεξεργασίας της άρνησης ενός υποκειμένου δεδομένων να συναινέσει ή να αντιταχθεί στην επεξεργασία παρατηρείται η αποτυχία της νομικής βάσης της συγκατάθεσης (Wachter, 2019). Η WP 29 παρατηρεί επίσης ότι αν και μπορεί σε ορισμένες περιπτώσεις να είναι επωφελές να παρέχεται στο υποκείμενο των δεδομένων ένας γενικός σκοπός, αυτό δεν ικανοποιεί τη νομική υποχρέωση. Συνακόλουθα συμπεραίνουμε τη σημασία της σαφούς ένδειξης των σκοπών για μία ενημερωμένη συγκατάθεση, καθώς χωρίς αυτή είναι αμφίβολο εάν οι καταναλωτές μπορούν ποτέ να ενημερωθούν πραγματικά.

Ωστόσο, δεδομένων των πρακτικών δυσκολιών που συνδέονται με την πραγματοποίηση οποιασδήποτε επιλογής του καταναλωτή, τίθεται το ερώτημα κατά πόσον η συγκατάθεση για τη συλλογή και επεξεργασία δεδομένων υποδηλώνει τη πραγματική συναίνεση του καταναλωτή να στοχοποιηθεί με εξατομικευμένες εμπορικές επικοινωνίες, που μπορεί να μην είναι σε θέση να αναγνωρίσει και, συνακόλουθα να θέσει υπό αμφισβήτηση τη σχετική προστασία από το δίκαιο της ΕΕ. Ο ΓΚΠΔ εστίασε στην αρχή της λογοδοσίας με σκοπό να μεταφέρει το βάρος της ευθύνης στους εκτελούντες την επεξεργασία, κάτι που δεν είναι βέβαιο ότι πρακτικά ενίσχυσε την αξία της συγκατάθεσης. Η δυσκολία της ικανότητας λήψης αποφάσεων των καταναλωτών φέρνει στην επιφάνεια απόψεις που υποστηρίζουν ότι οι τυποποιημένες συμβάσεις διαβρώνουν το βασικό δικαίωμα διαπραγμάτευσης και, ως εκ τούτου, αποτελούν μια μορφή ιδιωτικής νομοθέτησης από μεγάλες εταιρείες (Clifford και Verdoodt, 2017).

### 3.3. Ειδικές Κατηγορίες Δεδομένων

Η συλλογή και αξιολόγηση προσωπικών δεδομένων στο πλαίσιο της Ψηφιακής Διαφήμισης επιτρέπει στις εταιρείες να αποκτούν και να χρησιμοποιούν ευαίσθητες πληροφορίες για τη ζωή των πελατών τους, δηλαδή δεδομένα που αποκαλύπτουν, μεταξύ άλλων, τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή δεδομένα που αφορούν τον σεξουαλικό προσανατολισμό. Σύμφωνα με το άρθρο 9 του ΓΚΠΔ, παρέχεται αυξημένο πλαίσιο προστασίας για τις ειδικές αυτές κατηγορίες δεδομένων, καθιστώντας σαφές ότι η επεξεργασία τους απαγορεύεται ενώ εισάγει στην παράγραφο 2 ορισμένες εξαιρέσεις από τον κανόνα αυτό (Ιγγλεζάκης, 2014, σελ. 196)<sup>28</sup>. Τα δεδομένα αυτά μπορούν να προέλθουν από μία σειρά πηγών, με έμμεσο ή άμεσο τρόπο, και να αξιοποιηθούν συνδυαστικά με άλλες πληροφορίες εντός του πεδίου της Ψηφιακής Διαφήμισης με σκοπό τη στοχευμένη προβολή διαφημίσεων (Καρκατζούνης και Μήτρου, 2020). Συνεπώς, στην ειδική κατηγορία των ευαίσθητων προσωπικών δεδομένων εμπίπτουν αφενός μεν δεδομένα, που παρέχουν άμεση ένδειξη για την ένταξή τους στις ειδικές κατηγορίες δεδομένων, αφετέρου δε πληροφορίες, από τις οποίες δύναται κάποιος να συναγάγει πληροφορίες αυτού του τύπου<sup>29</sup>.

Η WP 29 σχετικά με τον ορισμό των ευαίσθητων προσωπικών δεδομένων και τη χρήση της λέξης «αποκαλύπτουν», κρίνει ασφαλές να υποθέσουμε ότι τα «δεδομένα ειδικής κατηγορίας» καλύπτουν τόσο τα ευαίσθητα δεδομένα όσο και τα δεδομένα που μπορούν να είναι ευαίσθητα δυνάμει συμπεράσματος. Όσον αφορά τη Συμπεριφορική Διαφήμιση, υποστηρίζει ότι εάν ένας πάροχος διαφημιστικού δικτύου επεξεργάζεται τη συμπεριφορά ενός ατόμου προκειμένου να το «τοποθετήσει» σε μια κατηγορία ενδιαφερόντων που υποδεικνύει μια συγκεκριμένη σεξουαλική προτίμηση θα επεξεργάζεται «ευαίσθητα δεδομένα» (Wachter, 2019).

---

<sup>28</sup> Η ομάδα εργασίας του άρθρου 29 προκειμένου να καλύψει πιθανές ελλείψεις καθώς δεν απαριθμούνται όλοι οι τύποι δεδομένων που πιθανόν να προκαλέσουν διακρίσεις, πρότεινε την επέκταση του ορισμού των ευαίσθητων δεδομένων ώστε να περιλαμβάνει τουλάχιστον πληροφορίες σχετικά με την οικονομική κατάσταση, τους ανηλίκους και τη γεωγραφική θέση, με αξιοσημείωτη τη παράλειψη του φύλου ως είδος ευαίσθητων δεδομένων (Wachter, 2019).

<sup>29</sup> Οράτε σχετικά WP 29, 2011, p. 6: «Profiling can create special category data by inference from data which is not special category data in its own right but becomes so when combined with other data. For example, it may be possible to infer someone's state of health from the records of their food shopping combined with data on the quality and energy content of foods».

Όσον αφορά την εξαγωγή δεδομένων βάσει συμπεράσματος, οι ακαδημαϊκοί διαφωνούν σχετικά με τις απαιτήσεις για να χαρακτηριστούν αυτά τα δεδομένα ως ευαίσθητα. Για ορισμένους, απαιτείται αφενός η πρόθεση εξαγωγής συμπερασμάτων, και αφετέρου να χρησιμοποιούν δεδομένα που παρέχουν αξιόπιστη βάση για να εξαχθούν ευαίσθητα δεδομένα. Παρομοίως, έχει προταθεί ότι εάν τα ευαίσθητα δεδομένα συλλέγονται μόνο συμπτωματικά δεν θα πρέπει να ταξινομούνται ως ευαίσθητα, εκτός εάν είναι γνωστό ότι περιέχουν ευαίσθητο περιεχόμενο. Μ' αυτό το τρόπο τα προσωπικά δεδομένα μετατρέπονται σε ευαίσθητα δεδομένα μόνο αν ο υπεύθυνος επεξεργασίας έχει την πρόθεση αυτή και έτσι οι αλγόριθμοι θα συμπεραίνουν ευαίσθητα στοιχεία ανεξάρτητα από την πρόθεση των χρηστών (Wachter, 2019).

Ο κοινός τόπος στη βιομηχανία της Ψηφιακής Διαφήμισης είναι η συλλογή των δεδομένων αυτών από τους υπεύθυνους επεξεργασίας προκειμένου να δημιουργηθούν προφίλ χρηστών βάσει των χαρακτηριστικών τους γνωρισμάτων, των προτιμήσεων και των ενδιαφερόντων τους, όπως αναφέρεται στο άρθρο 4 παρ. 4 ΓΚΠΔ, δεδομένου ότι διενεργείται αυτοματοποιημένη επεξεργασία των προσωπικών δεδομένων του χρήστη προς τον σκοπό της αξιολόγησης ορισμένων προσωπικών πτυχών του (Ιγγλεζάκης, 2020, σελ. 62). Στο πλαίσιο της Συμπεριφορικής Διαφήμισης μελετώνται τα χαρακτηριστικά της συμπεριφοράς των χρηστών, όπως επί παραδείγματι επαναλαμβανόμενες επισκέψεις σε ιστότοπους, διαδραστικές ενέργειες, key-words, επιγραμμική παραγωγή περιεχομένου, προκειμένου να δημιουργηθεί συγκεκριμένο προφίλ και εν συνεχεία να διενεργηθεί προώθηση στοχοθετημένης διαφήμισης, που ανταποκρίνεται στις προτιμήσεις του προσώπου (WP 29, 2010).

Η «κατάρτιση προφίλ προτιμήσεων» που απαντάτε στο πλαίσιο της Συμπεριφορικής Διαφήμισης είναι η κατάρτιση προφίλ που δεν συμπεραίνει άμεσα τα ευαίσθητα δεδομένα ενός χρήστη, αλλά χρησιμοποιεί άλλα δεδομένα για να ανακαλύψει τη «προτίμηση» του χρήστη σύμφωνα με μία ομάδα. Αυτή η διαδικασία αναζητά την ομοιότητα μεταξύ των υποτιθέμενων ενδιαφερόντων ενός χρήστη και των ενδιαφερόντων μιας ομάδας. Ο ΓΚΠΔ ενδέχεται να μην αναγνωρίζει μια πιθανή σχέση μεταξύ υποτιθέμενων ενδιαφερόντων και ευαίσθητων προσωπικών χαρακτηριστικών, κάτι που καθιστούσε τα υψηλότερα πρότυπα προστασίας δεδομένων ανεφάρμοστα, παρά το γεγονός ότι έχουν ισχυρή και δυναμική επεμβατική δύναμη



διακρίσεων. Το επιχείρημα ότι δεν θα πρέπει να εφαρμόζονται τέτοιου είδους πρότυπα εάν τα δεδομένα χρησιμοποιούνται για να συναχθεί συμπέρασμα για τη προτίμηση για παράδειγμα βάση εθνικότητας και όχι άμεσα από αυτήν, καθίσταται προβληματικό, διότι παρέχει στενή ερμηνεία του πεδίου εφαρμογής των δεδομένων ειδικής κατηγορίας (Wachter, 2019).

Στην περίπτωση της Ψηφιακής Διαφήμισης η μοναδική προϋπόθεση νόμιμης επεξεργασίας ειδικών κατηγοριών προσωπικών δεδομένων για έναν ή πλείονες σκοπούς επεξεργασίας, που θα μπορούσε να τύχει εφαρμογής, συνίσταται στην προβλεπόμενη εκ του άρθρου 9 παρ. 2 περίπτωση α' ΓΚΠΔ προϋπόθεση της ρητής συγκατάθεσης του υποκειμένου των δεδομένων. Η WP 29 τόνισε ότι στο πλαίσιο Συμπεριφορικής Διαφήμισης οι υπεύθυνοι επεξεργασίας δεδομένων απαιτείται να ζητούν ρητή συγκατάθεση για τη συλλογή ευαίσθητων δεδομένων και σε καμία περίπτωση ο μηχανισμός συγκατάθεσης εξαίρεσης δεν ικανοποιεί την απαίτηση του νόμου. Αυξημένες δυσκολίες εντοπίζονται στον τρόπο με τον οποίο λαμβάνεται και αποδεικνύεται η ρητή συγκατάθεση, αλλά και στον περιορισμό του σκοπού για τον οποίο παρέχονται τα δεδομένα. Στην πράξη, όπως παρατηρεί η βρετανική εποπτική αρχή στην πρόσφατη έκθεσή της σχετικά με το AdTech και το RTB, οι ισχύοντες μηχανισμοί συγκατάθεσης στην προγραμματική διαφήμιση δεν συμμορφώνονται με το πλαίσιο για την προστασία ειδικών κατηγοριών δεδομένων (Καρκατζούνης και Μήτρου, 2020).

### **3.4. Προστασία προσωπικών δεδομένων ανηλίκων**

#### **3.4.1. Πρόσβαση ανηλίκων σε ψηφιακές υπηρεσίες**

Τα προσωπικά δεδομένα των ανηλίκων χρήζουν ειδικής προστασίας, λόγω της έλλειψης επίγνωσης των κινδύνων, των συνεπειών και των δικαιωμάτων τους αναφορικά με την επεξεργασία των δεδομένων τους. Η χρήση των διαδικτυακών υπηρεσιών εκ μέρους των ανηλίκων και η έκθεσή τους σε πληθώρα πληροφοριών λόγω της απεριόριστης πρόσβασής τους, ή λόγω της σχετιζόμενης με την ηλικία τους ανωριμότητας ελλοχεύει ποικίλους κινδύνους. Ειδικότερα τα ανήλικα θεωρούνται ως η πιο ευάλωτη ομάδα στις επιρροές της διαφήμισης λόγω της ελλιπούς κριτικής σκέψης και των παρορμήσεων τους. Οι ανήλικοι παρότι αναγνωρίζουν τη

διαφήμιση σίγουρα δεν κατανοούν την πολυπλοκότητα του τρόπου συλλογής, ανάλυσης και χρήσης των προσωπικών δεδομένων για εμπορικούς σκοπούς, καθώς έχουν περισσότερο διαπροσωπική και λιγότερο τεχνική αντίληψη της ιδιωτικής ζωής. Έχει διαπιστωθεί μέσω έρευνας ότι τα παιδιά και οι γονείς δεν διαβάζουν τους όρους και τις προϋποθέσεις ή τις ειδοποιήσεις απορρήτου στις πλατφόρμες, αισθάνονται πιεσμένοι να αποδέχονται cookies και γενικότερα αισθάνονται περίεργα με τη χρήση των δεδομένων τους για Στοχευμένη Διαφήμιση. Επιπλέον, τα ανήλικα άτομα στην ίδια μελέτη θεωρούν ότι θα έπρεπε να έχουν το δικαίωμα να διαγράφουν ή να περιορίζουν τη χρήση των προσωπικών τους δεδομένων (Radesky et al., 2020).

Συνάγεται λοιπόν η ανάγκη νομοθετικής επέμβασης για την ενίσχυση της προστασίας των προσωπικών δεδομένων των ανηλίκων, η οποία σαφώς πρέπει να συνδυάζεται με την εμπειριστατωμένη ενημέρωση των ανηλίκων, των γονέων και εκπαιδευτικών σε σχέση με τις υπηρεσίες της κοινωνίας της πληροφορίας και με την ευαισθητοποίηση των παρόχων υπηρεσιών στο Διαδίκτυο (Αλεξανδροπούλου - Αιγυπτιάδου, 2007, σελ. 848-849). Οι λόγοι της ενισχυμένης προστασίας προσδιορίζονται στην αιτιολογική σκέψη 38 του ΓΚΠΔ, η οποία τονίζει οι ανήλικοι έχουν περιορισμένη επίγνωση των σχετικών κινδύνων, συνεπειών, εγγυήσεων και δικαιωμάτων σε σχέση με την επεξεργασία των δεδομένων τους.

Επίσης στην ίδια σκέψη αναφέρεται ότι «η ειδική προστασία θα πρέπει να ισχύει ιδίως στη χρήση των δεδομένων προσωπικού χαρακτήρα με σκοπό την εμπορία ή τη δημιουργία προφίλ και τη συλλογή δεδομένων προσωπικού χαρακτήρα όσον αφορά παιδιά κατά τη χρήση υπηρεσιών που προσφέρονται άμεσα σε ένα παιδί». Η λέξη «ιδίως» υποδηλώνει ότι η ειδική προστασία δεν προϋποθέτει για παράδειγμα τη δημιουργία προφίλ αλλά επεκτείνεται στη γενικότερη «συλλογή δεδομένων προσωπικού χαρακτήρα όσον αφορά παιδιά». Εντούτοις, η ενισχυμένη προστασία των προσωπικών δεδομένων των παιδιών δεν προβλέπεται από κάποιο άλλο σημείο του Κανονισμού. Η μοναδική σχετική διάταξη είναι το άρθρο 8 παρ. 1, στο οποίο ορίζονται οι προϋποθέσεις που ισχύουν για τη συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών (ΕΣΠΔ, 2020).

Περαιτέρω, η αμερικάνικη νομοθεσία που ρυθμίζει την προστασία της ιδιωτικής ζωής των ανηλίκων στο διαδίκτυο (COPPA)<sup>30</sup>, έχει ως στόχο να «θέσει τους γονείς υπό τον έλεγχο των πληροφοριών που συλλέγονται από τα παιδιά τους στο διαδίκτυο» και παρότι επιθυμεί να περιορίσει τα δεδομένα που συλλέγονται, χρησιμοποιούνται ή κοινοποιούνται, ωστόσο, δεν προστατεύει τα παιδιά όταν χρησιμοποιούν ιστότοπους ή εφαρμογές που θεωρούνται ότι απευθύνονται σε γενικό κοινό, τουναντίον είναι απαραίτητο η ηλεκτρονική υπηρεσία να απευθύνεται αποκλειστικά σε ανήλικα άτομα (Radesky et al., 2020).

### **3.4.2. Το ζήτημα της συγκατάθεσης**

#### *α. Εγκυρότητα λήψης συγκατάθεσης από ανήλικο πρόσωπο*

Αξιοσημείωτο είναι ότι στον Κανονισμό δεν υπάρχει ορισμός για την έννοια του «παιδιού». Βάσει της κυρωθείσας δυνάμει του Ν. 2101/1992 (ΦΕΚ Α' 192/2.12.1992) Διεθνούς Σύμβασης των Ηνωμένων Εθνών για τα δικαιώματα του παιδιού σε συνδυασμό με το πρώτο άρθρο του Ν. 3625/2007 (ΦΕΚ Α' 290/24.12.2007), δίδεται ορισμός σύμφωνα με τον οποίο παιδί θεωρείται ένα άτομο που δεν έχει συμπληρώσει το 18<sup>ο</sup> έτος της ηλικίας του. Το άρθρο 8 παρ. 1 του ΓΚΠΔ, προβλέπει ότι στην περίπτωση που έχει χορηγηθεί η συγκατάθεση του υποκειμένου των δεδομένων, βάσει του άρθρου 6 παρ. 1 α' ΓΚΠΔ, η συγκατάθεση που παρέχεται από παιδί για την επεξεργασία των προσωπικών του δεδομένων, στο πλαίσιο προσφοράς υπηρεσιών της κοινωνίας των πληροφοριών απευθείας σε αυτό, είναι έγκυρη εάν το παιδί είναι τουλάχιστον 16 χρονών. Αναφορικά με το όριο ηλικίας για την παροχή έγκυρης συγκατάθεσης, ο ΓΚΠΔ παρέχει την ευχέρεια στα κράτη μέλη να προβλέπουν διά εθνικού νόμου τη κατώτερη ηλικία συγκατάθεσης, η οποία δεν μπορεί να είναι κάτω των 13 ετών. Στην ελληνική έννομη τάξη με τη διάταξη του άρθρου 21 του Ν. 4624/2019 ορίζεται το 15<sup>ο</sup> έτος ως ηλικιακό όριο παροχής συγκατάθεσης για πρόσβαση σε υπηρεσίες της κοινωνίας της πληροφορίας που αφορούν σε παιδιά.

Επιπλέον, σύμφωνα με τη διάταξη του άρθρου 8 του ΓΚΠΔ και ειδικότερα σύμφωνα με τη φράση «απευθείας σε παιδί», εμφανίζεται ότι η διάταξη εφαρμόζεται σε ορισμένες υπηρεσίες της

---

<sup>30</sup> Children's Online Privacy Protection Act (2000).

κοινωνίας της πληροφορίας. Ακολούθως, στην περίπτωση που ένας πάροχος συναφών υπηρεσιών καθιστά σαφές στους δυνητικούς χρήστες ότι προσφέρει τις υπηρεσίες του μονάχα σε ενήλικους και αυτό δεν υπονομεύεται από άλλα στοιχεία όπως τα σχέδια εμπορικής προώθησης, τότε τεκμαίρεται ότι η υπηρεσία δεν προσφέρεται «απευθείας σε παιδί» και συνεπώς δεν εφαρμόζεται το ανωτέρω άρθρο (ΕΣΠΔ, 2020).

#### *β. Επιμέρους ζητήματα περί συγκατάθεσης*

Όμως στη πράξη όταν ένα παιδί καλείται να επιβεβαιώσει την ακριβή του ηλικία σε μία εφαρμογή ή σε μία ιστοσελίδα, είναι πολύ εύκολο, είτε να μη δηλώσει την πραγματική του ηλικία, είτε να συναινέσει το ίδιο αντί των κηδεμόνων του μέσω της πρόσβασής του στους κωδικούς του e-mail τους, με αποτέλεσμα να καταστεί παράνομη η επεξεργασία των προσωπικών του δεδομένων.

Εκ των ανωτέρω συνεπάγεται η αυξημένη ευθύνη των υπεύθυνων επεξεργασίας δεδομένων κατά το στάδιο της συγκατάθεσης των παιδιών. Η WP 29 εξηγεί, ότι ενώ δεν προβλέπεται ρητά από τον ΓΚΠΔ ο τρόπος καταβολής εύλογων προσπαθειών εξακρίβωσης της ηλικίας των παιδιών και η επαλήθευσή της, ωστόσο θα πρέπει να τεκμαίρεται σιωπηρά, όταν ένα παιδί συναινεί στη επεξεργασία των προσωπικών του δεδομένων μη έχοντας τη νόμιμη ηλικία ψηφιακής συγκατάθεσης, τότε αυτομάτως η επεξεργασία θεωρείται παράνομη. Οι υπεύθυνοι επεξεργασίας σε περιπτώσεις παροχής υπηρεσιών σε παιδιά βάσει συγκατάθεσης, θα πρέπει να λαμβάνουν σχετικά και ανάλογα μέτρα προς τη φύση και τους κινδύνους των δραστηριοτήτων επεξεργασίας. Στις περιπτώσεις δήλωσης νόμιμης ηλικίας για την ψηφιακή συγκατάθεση, ο υπεύθυνος επεξεργασίας μπορεί να διενεργεί κατάλληλους ελέγχους για να επαληθεύει ότι η δήλωση αυτή είναι αληθής (WP 29, 2018).

Ο τρόπος που επιλέγεται για την επαλήθευση της ηλικίας υποκειμένου των δεδομένων θα πρέπει να περιλαμβάνει αξιολόγηση του κινδύνου της σχεδιαζόμενης επεξεργασίας ενώ δεν θα πρέπει να οδηγεί σε επεξεργασία υπερβολικής ποσότητας δεδομένων. Σε κάποιες καταστάσεις χαμηλού κινδύνου, πιθανόν να κρίνεται αναγκαίο να ζητείται η γνωστοποίηση του έτους γέννησής του υποκειμένου ή η συμπλήρωση εντύπου στο οποίο να δηλώνει ότι είναι ανήλικος.

Συνεπώς, είναι προφανής η δυσκολία εγγύησης της νομιμότητας της επεξεργασίας μέσω των μέτρων που προβλέπει ο ΓΚΠΔ. Οι υπεύθυνοι επεξεργασίας προκειμένου να εξακριβώσουν την πραγματική ηλικία των ανηλίκων ή την αληθή συγκατάθεση των κηδεμόνων τους επιβάλλεται να υιοθετούν δικλείδες ασφαλείας μέσω τεχνολογικών εργαλείων ώστε να η συγκατάθεση να αποτελεί ουσιαστική νομιμοποιητική βάση επεξεργασίας των προσωπικών δεδομένων των ανηλίκων (Παπακωνσταντίνου, 2020).

### *γ. Λήψη γονικής συγκατάθεσης*

Στην περίπτωση που το παιδί δεν έχει συμπληρώσει το 16<sup>ο</sup> έτος της ηλικίας του, η επεξεργασία των δεδομένων του θεωρείται νόμιμη μόνο εάν και στο βαθμό που η εν λόγω συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική του μέριμνα. Βάσει της ανωτέρω ρύθμισης, δεν απαιτείται η εκ των προτέρων συναίνεση του γονέα, αρκούμενη και στην εκ των υστέρων συγκατάθεση, ήτοι στην έγκρισή του, κατά παρέκκλιση από τον γενικό κανόνα της συναίνεσης (Αλεξανδροπούλου - Αιγυπτιάδου, 2016, σελ. 87). Ειδικότερα για σκοπούς Συμπεριφορικής Διαφήμισης που απευθύνεται σε παιδιά, οι πάροχοι πρέπει να ενημερώνουν τους γονείς σχετικά με τη συλλογή και τη χρήση των πληροφοριών σχετικά με τα παιδιά και να λαμβάνουν τη συγκατάθεσή τους πριν από τη συλλογή και την περαιτέρω χρήση των πληροφοριών αυτών. Λαμβανομένου υπόψη του ευάλωτου χαρακτήρα των παιδιών, η WP 29 τονίζει ότι οι πάροχοι διαφημιστικών δικτύων δεν πρέπει να προσφέρουν κατηγορίες ενδιαφερόντων για σκοπούς Συμπεριφορικής Διαφήμισης ή επηρεασμού των παιδιών (WP 29, 2011).

Όσον αφορά την έγκριση του προσώπου που έχει τη γονική μέριμνα, ο ΓΚΠΔ δεν προσδιορίζει πρακτικούς τρόπους λήψης της συγκατάθεσης του γονέα ούτε εξακρίβωσης του δικαιώματος ενός προσώπου να προβεί στην ενέργεια αυτή. Ως εκ τούτου, η WP 29 συνιστά την εφαρμογή αναλογικής προσέγγισης, σύμφωνα με το άρθρο 8 παράγραφος 2 και της διάταξης του ΓΚΠΔ για την ελαχιστοποίηση των δεδομένων, η οποία επιτρέπει την προσήλωση στην εξασφάλιση περιορισμένης ποσότητας πληροφοριών, όπως των στοιχείων επικοινωνίας του γονέα ή του κηδεμόνα (WP 29, 2018).

Δέον να σημειώσουμε ότι σύμφωνα με την αιτιολογική σκέψη 38, η συγκατάθεση από γονέα ή κηδεμόνα δεν απαιτείται σε συνάρτηση με υπηρεσίες πρόληψης ή παροχής συμβουλών που προσφέρονται άμεσα σε παιδί. Η εξαίρεση αυτή στοχεύει στη προστασία των παιδιών καθώς μπορούν να καταγγέλλουν ελεύθερα επιβλαβείς πράξεις και συμπεριφορές, χωρίς να απαιτείται η προηγούμενη συγκατάθεση των γονέων ή κηδεμόνων τους ( Παπακωνσταντίνου 2020).

Στην παρ. 2 του αρθρ. 8 του Κανονισμού, ορίζεται ότι ο υπεύθυνος επεξεργασίας «καταβάλλει εύλογες προσπάθειες για να επαληθεύσει στις περιπτώσεις αυτές ότι η συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού, λαμβάνοντας υπόψη την τεχνολογία». Το ΕΣΠΔ αναγνωρίζει ότι ενδέχεται να υπάρχουν περιπτώσεις στις οποίες η επαλήθευση είναι δύσκολη, το οποίο λαμβάνεται υπόψη όταν κρίνεται ποιες προσπάθειες είναι εύλογες, αλλά δεν αναιρεί την υποχρέωση των υπεύθυνων επεξεργασίας να επανεξετάζουν συνεχώς τις διαδικασίες τους και τη διαθέσιμη τεχνολογία. Κάποιες τεχνικές ελέγχου που χρησιμοποιούνται, προκειμένου να εξακριβωθεί ότι η συγκατάθεση πράγματι παρέχεται από τον γονέα του ανηλίκου είναι ενδεικτικά, η υπογραφή από το γονέα ηλεκτρονικής φόρμας συγκατάθεσης από την ιστοσελίδα του παρόχου, η δημιουργία ειδικού λογαριασμού e-mail από τον πάροχο της υπηρεσίας και η εισαγωγή χρεωστικής ή πιστωτικής κάρτας ή άλλου ηλεκτρονικού συστήματος πληρωμών, που παρέχει άμεση ειδοποίηση μέσω SMS για συναλλαγές που πραγματοποιεί ο κάτοχος του λογαριασμού (Κανέλλος, 2020, σελ. 262).

Όσον αφορά την αυτονομία συγκατάθεσης του υποκειμένου των δεδομένων στην επεξεργασία των προσωπικών του δεδομένων, στις περιπτώσεις των ανηλίκων η συγκατάθεση για την επεξεργασία των δεδομένων τους η οποία παρέχεται ή εγκρίνεται από τα πρόσωπα που έχουν τη γονική μέριμνα τους μπορεί να επιβεβαιωθεί, να τροποποιηθεί ή να ανακληθεί όταν το υποκείμενο των δεδομένων συμπληρώσει την προβλεπόμενη ηλικία για την ψηφιακή συγκατάθεση<sup>31</sup>. Σύμφωνα με τις αρχές της αντικειμενικότητας και της λογοδοσίας, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει το παιδί για τη δυνατότητα αυτή (WP 29, 2018).

### **3.4.3. Το δικαίωμα ενημέρωσης**

Το δικαίωμα ενημέρωσης είναι εύλογο ότι πρέπει να προσαρμόζεται στις ιδιαιτερότητες των ανηλίκων. Βάσει τούτου, λαμβανομένης υπόψη της υπ' αριθ. 58 αιτιολογικής σκέψης του ΓΚΠΔ, η ενημέρωση που παρέχεται πρέπει να είναι ευχερώς κατανοητή στους ανηλίκους και να διατυπώνεται σε σαφή και απλή γλώσσα, προκειμένου ο ανήλικος να είναι σε θέση να την κατανοήσει ευχερώς. Το άρθρο 12 παρ. 1 ΓΚΠΔ προβλέπει ότι η λήψη κατάλληλων μέτρων και ο τρόπος παροχής των οφειλόμενων πληροφοριών από τον υπεύθυνο επεξεργασίας πρέπει να εφαρμόζονται ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη σε παιδιά. Εξ αυτού συνάγεται ότι η ενημέρωση που απευθύνεται σε ανηλίκους πρέπει να έχει έναν ευρύτερο χαρακτήρα συγκριτικά με την ενημέρωση που παρέχεται στους ενήλικους (Αλεξανδροπούλου-Αιγυπτιάδου, 2007).

Σύμφωνα με τη Γνώμη 2/2009 της WP 29 για τους τρόπους ενημέρωσης των ανηλίκων, τονίζει ότι «στο πλαίσιο παροχής πληροφοριών σε παιδιά ή νόμιμους αντιπροσώπους τους, πρέπει να δοθεί έμφαση στην παροχή πολύπτυχων ανακοινώσεων που βασίζονται στη χρήση απλής, περιεκτικής και εκπαιδευτικής γλώσσας που μπορεί να γίνει εύκολα αντιληπτή. Μία συντομότερη ανακοίνωση πρέπει να περιέχει τα βασικά στοιχεία που πρέπει να παρέχονται κατά τη συλλογή δεδομένων προσωπικού χαρακτήρα είτε απευθείας από το πρόσωπο στο οποίο αναφέρονται τα δεδομένα είτε από τρίτο. Αυτό πρέπει να συνοδεύεται από λεπτομερή ανακοίνωση, ίσως μέσω υπερσυνδέσεων όπου παρέχονται όλες οι σχετικές λεπτομέρειες.» (WP 29, 2009).

### **3.4.4. Προβληματισμοί σχετικά με τη προστασία των ανηλίκων στο ψηφιακό οικοσύστημα**

Παρά τη βούληση του ενωσιακού νομοθέτη να εξειδικεύσει τη προστασία των ανηλίκων, εντοπίζονται ζητήματα που εμποδίζουν την πρακτική αποτελεσματικότητα και στην εφαρμοστικότητα του Κανονισμού. Καταρχάς υπάρχουν προβληματισμοί αναφορικά με την διακριτική ευχέρεια που παρέχεται στα κράτη μέλη για τον καθορισμό του κατώτατου ορίου ηλικίας σύμφωνα με το οποίο επιτρέπεται η επεξεργασία δεδομένων. Μ' αυτό το τρόπο διακρίνεται η διάσταση με τον σκοπό νομοθετικής εναρμόνισης της ΕΕ, καθιστώντας δύσκολη την επίλυση της ανομοιομορφίας των πολιτικών προστασίας, παράλληλα με τα ζητήματα των διασυνοριακών διαβιβάσεων προσωπικών δεδομένων προς τρίτες χώρες.

Επιπλέον, αμφισβητείται το κατά πόσο το άρθρο 8 του ΓΚΠΔ ερμηνεύεται σύμφωνα με το άρθρο 24 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ και προς το απόλυτο συμφέρον των παιδιών, λαμβάνοντας υπόψη την ψηφιακή εξοικείωση των παιδιών. Ενδεχομένως μια ορθότερη ερμηνεία του άρθρου 8 βάσει του αρθρ. 24 του Χάρτη να ήταν πιο σύγχρονη και αποτελεσματική σταθμίζοντας αναλογικά τα δικαιώματα, συνδυαστικά με τη συνεχώς επιταχυνόμενη τεχνολογική εξέλιξη των παιδιών (Παπακωνσταντίνου, 2020).

Τέλος, στις περισσότερες περιπτώσεις, η ασφάλεια "γενικής χρήσης" και οι έλεγχοι προστασίας της ιδιωτικής ζωής έχουν εφαρμοστεί σε πλαίσια στα οποία εμπλέκεται η ιδιωτική ζωή των παιδιών, ενώ ένας ελάχιστος αριθμός τεχνικών ελέγχων έχουν σχεδιαστεί ειδικά για την προστασία της ιδιωτικής ζωής των παιδιών (Crepax et al., 2022). Γι' αυτό και είναι απαραίτητο οι πάροχοι διασυνοριακών υπηρεσιών να διαθέτουν κατάλληλες πολιτικές ασφαλείας, ελέγχου ταυτότητας, διαχείρισης της συναίνεσης των γονέων, καθώς και ρυθμίσεις απορρήτου εναρμονισμένες πλήρως με τις εθνικές ρυθμίσεις περί της νόμιμης ηλικίας συμμετοχής των ανηλίκων στις ψηφιακές υπηρεσίες (Παπακωνσταντίνου, 2020).

## **4. ΕΙΔΙΚΟΤΕΡΑ ΖΗΤΗΜΑΤΑ**

### **4.1. Cookies και Συμπεριφορική Διαφήμιση (Behavioral Advertising)**

#### **4.1.1. Η Συμπεριφορική Διαφήμιση και οι κίνδυνοι της Online παρακολούθησης**

Όπως αναλύσαμε ανωτέρω στο υποκεφάλαιο 1.4, η στόχευση Χρηστών μέσω της παρακολούθησης και ανάλυσης των προσωπικών τους δεδομένων αποτελεί βασικό συστατικό της ψηφιακής διαφήμισης. Ζητήματα παραβίασης προσωπικών δεδομένων ανακύπτουν ιδιαίτερα στο πλαίσιο εφαρμογής της Συμπεριφορικής Διαφήμισης υπό την έννοια της παρακολούθησης και μελέτης των χαρακτηριστικών της διαδικτυακής συμπεριφοράς ενός Χρήστη, προκειμένου να σκιαγραφηθεί συγκεκριμένο προφίλ του για την προώθηση Στοχευμένης Διαφήμισης προσαρμοσμένης και ανταποκρινόμενης στις προτιμήσεις του (WP 29, 2010). Η ανωτέρω παρακολούθηση της διαδικτυακής συμπεριφοράς των Χρηστών, η οποία διενεργείται μέσω των cookies και όμοιων τεχνολογιών παρακολούθησης, καθιστά την εν λόγω



μορφή διαφημιστικής πρακτικής επικίνδυνη για την προστασία των δεδομένων προσωπικού χαρακτήρα των Χρηστών καθώς και την παραβίαση της ιδιωτικότητάς τους.

Στο πλαίσιο της Συμπεριφορικής Διαφήμισης, μέσω των cookies και όμοιων τεχνολογιών, λαμβάνει χώρα καταρχήν η συλλογή και επεξεργασία διευθύνσεων IP<sup>32</sup> και η δημιουργία και επεξεργασία μοναδικών αναγνωριστικών στοιχείων ID, προκειμένου να μπορούν να ταυτοποιούνται οι Χρήστες, ακόμη και εάν τα πραγματικά τους ονόματα δεν γίνονται γνωστά (WP 29, 2010). Εν συνεχεία, συλλέγονται πληροφορίες σχετικά με τα χαρακτηριστικά και την πλοηγική συμπεριφορά των χρηστών προς το σκοπό της διαμόρφωσης προφίλ χρηστών βάσει των οποίων επιλέγονται και προβάλλονται οι σχετικές διαφημίσεις. Σύμφωνα με τη WP 29 (2010), για τα προφίλ χρηστών που δημιουργούνται υπάρχουν δύο βασικές προσεγγίσεις: «i) Τα προφίλ πρόβλεψης που δημιουργούνται επαγωγικά από την παρακολούθηση της ατομικής και συλλογικής συμπεριφοράς των χρηστών σε βάθος χρόνου, ιδίως με παρακολούθηση της επισκεψιμότητας των σελίδων και των διαφημίσεων που οι χρήστες έχουν παρακολουθήσει ή κάνει κλικ σε αυτές. ii) Τα συγκεκριμένα προφίλ δημιουργούνται από προσωπικά στοιχεία που οι ίδιοι οι χρήστες έχουν παράσχει σε δικτυακή υπηρεσία, π.χ. μέσω της εγγραφής τους. Οι δύο προσεγγίσεις μπορούν να χρησιμοποιηθούν συνδυαστικά. Επιπλέον, τα προφίλ πρόβλεψης μπορούν να γίνουν συγκεκριμένα σε μετέπειτα στάδιο, όταν ένας χρήστης δημιουργεί διαπιστευτήρια εισόδου για συγκεκριμένους δικτυακούς τόπους.» Τα προφίλ που δημιουργούνται με τη σειρά τους μπορεί να εμπλουτίζονται από δεδομένα που προκύπτουν από Χρήστες με παρόμοια συμπεριφορά. Με βάση τα στοιχεία που συγκεντρώνονται οι Χρήστες εν συνεχεία ταξινομούνται σε ευρύτερες κατηγορίες, όπως για παράδειγμα ανάλογα με τα ενδιαφέροντα τους ή βάσει του προϊόντος ή υπηρεσίας για την οποία έχουν εκδηλώσει ενδιαφέρον (π.χ. «κηπουρική»).

Από τα ανωτέρω καθίσταται σαφές ότι η τόσο εκτεταμένη παρακολούθηση, συγκέντρωση και ανάλυση δεδομένων που φτάνει έως τη πρόβλεψη της συμπεριφοράς του εκάστοτε Χρήστη σε

---

<sup>32</sup> Για τις διευθύνσεις IP ως προσωπικά δεδομένα, εάν συνδυαστούν και με άλλες πληροφορίες ώστε να ταυτοποιούνται οι χρήστες βλ. Απόφαση του ΔΕΕ της 19/10/2016 επί της υπόθεσης C-582/2014 “Patrick Breyer κατά Bundesrepublik Deutschland, Δίκαιο Μέσων Μαζικής Ενημέρωσης και Επικοινωνίας (ΔΙΜΕ&Ε), τόμος 13/2016, σελ. 650.

πολύ προσωπικό, ατομικό επίπεδο εγείρει σοβαρά ζητήματα που άπτονται της προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας. Ήδη από το 2010 ο Eric Schmidt, πρώην διευθύνων σύμβουλος της Google δήλωνε: «Ξέρουμε πού βρίσκεστε. Ξέρουμε πού ήσασταν. Εμείς μπορούμε λίγο πολύ να ξέρουμε τι σκέφτεστε» (Thompson, 2010).

Ένας από τους μεγαλύτερους κινδύνους της Online παρακολούθησης είναι η παγκόσμια επιτήρηση, η οποία μπορεί να πραγματοποιείται είτε από κυβερνήσεις είτε από εταιρείες για εμπορικούς λόγους. Σαν επιχείρημα υπέρ της σχετικής πρακτικής προβάλλεται η άποψη ότι ένας Χρήστης δεν έχει λόγο να ανησυχεί για την ιδιωτική του ζωή αν δεν έχει τίποτα να κρύψει. Σύμφωνα με τον Solove (2011), η σχετική άποψη είναι επιφανειακή καθότι πηγάζει από μια στενή αντίληψη της ιδιωτικής ζωής ως μυστικό ή απόκρυψη πληροφοριών. Οι κίνδυνοι όμως της παρακολούθησης μπορεί να μην εκδηλώνονται σαν μία άμεση ζημία αλλά μπορεί να απορρέουν από λανθασμένες ή διαστρεβλωμένες πληροφορίες, που με τη σειρά τους μπορεί να οδηγήσουν σε λανθασμένες αποφάσεις, κατάχρηση και έλλειψη διαφάνειας και λογοδοσίας (Solove, 2011). Οι παρακολούθηση μπορεί πολύ άμεσα να οδηγήσει σε διακρίσεις ως προς την παροχή ή όχι μιας υπηρεσίας ή την τιμολόγηση. Ένα προφίλ χρήστη μπορεί να αποκαλύπτει δεδομένα υγείας, τα οποία μπορεί να οδηγήσουν μια ασφαλιστική εταιρεία για παράδειγμα είτε να μην ασφαλίσει το σχετικό χρήστη ή να του αυξήσει τα ασφάλιστρα (ENISA EU, 2012). Από την άλλη πλευρά, οι εκτεταμένες πληροφορίες σχετικά με το ιστορικό αγορών, τις συνήθειες περιήγησης και την οικονομική κατάσταση ενός Χρήστη μπορεί να αξιοποιηθούν για το καθορισμό της μέγιστης τιμής που αυτός είναι διατεθειμένος να πληρώσει για ένα προϊόν ή υπηρεσία, με σκοπό την ανάλογη τιμολόγηση του. Το φαινόμενο αυτό προφανώς έχει δυσμενείς συνέπειες για τους καταναλωτές. Για παράδειγμα, εάν η τιμή ενός προϊόντος ή υπηρεσίας διαφέρει σε ατομικό επίπεδο, θα είναι αδύνατο για τους καταναλωτές να συγκρίνουν τις τιμές τους (Consumer Council of Norway, 2020).

Όπως περιγράψαμε ανωτέρω, η Συμπεριφορική Διαφήμιση οδηγεί στην εξατομίκευση του περιεχομένου που προβάλλεται στους Χρήστες. Οι διαδικτυακές διαφημίσεις συνεπώς που βλέπει ένας χρήστης εξατομικεύονται με βάση τη συμπεριφορά και το προφίλ του. Με την εξατομίκευση συνεπώς των υπηρεσιών, οι χρήστες συχνά βρίσκονται παγιδευμένοι σε μία

κατάσταση που συνηθίζεται να ονομάζεται “filter bubble”, δηλαδή γύρω τους δημιουργείται περίβλημα που επιτρέπει να εισέρχεται στο εσωτερικό του μόνο η πληροφορία που κρίνεται ως κατάλληλη για το συγκεκριμένο Χρήστη με βάση την προηγούμενη συμπεριφορά του. Αυτό όμως έχει ως αποτέλεσμα την απομόνωση του Χρήστη και επομένως τη στέρηση του από άλλες πληροφορίες ή ευκαιρίες (ENISA EU, 2012).

#### ***4.1.2. Τα cookies ως βασικό εργαλείο της OnLine παρακολούθησης***

Τα cookies αποτελούν το βασικότερο εργαλείο της OnLine παρακολούθησης. Επί της ουσίας συνιστούν αναγνωριστικά στοιχεία των συσκευών πλοήγησης και προέλευσης κάθε Χρήστη μιας ιστοσελίδας (Κανέλλος, 2020, σελ. 377). Τα Cookies δημιουργούνται όταν ο browser “φορτώνει” μια ιστοσελίδα προκειμένου ο χρήστης να την επισκεφτεί. Η ιστοσελίδα συλλέγει πληροφορίες αναφορικά με τη συσκευή του χρήστη και την κίνησή του στο πρόγραμμα περιήγησης και εν συνεχεία δημιουργεί ένα μικρό αρχείο κειμένου (cookies). Κατ’ αυτόν τον τρόπο, κάθε φορά που ο χρήστης επισκεφτεί εκ νέου τη συγκεκριμένη ιστοσελίδα, το πρόγραμμα περιήγησης (browser) ανακτά και αποστέλλει το ανωτέρω αρχείο με τις ως άνω πληροφορίες στο διακομιστή της ιστοσελίδας, η οποία τον αναγνωρίζει και παρουσιάζει στοιχεία και υπηρεσίες, που έχουν προσαρμοστεί στις ανάγκες και τις προτιμήσεις του, δυνάμει των αρχών της Συμπεριφορικής Διαφήμισης (WP 29, 2010).

Ανάλογα με το είδος και τον τρόπο λειτουργίας των cookies, οι πληροφορίες που αποθηκεύουν αφορούν σε ποικίλες προσωπικές πληροφορίες αναγνώρισης και ταυτοποίησης του χρήστη, όπως για παράδειγμα όνομα, διεύθυνση κατοικίας, διεύθυνση ηλεκτρονικού ταχυδρομείου, αριθμό τηλεφώνου, διεύθυνση IP, κωδικό πρόσβασης (password). Σε αυτό το σημείο αξίζει να σημειωθεί ότι από μία μελέτη που διενεργήθηκε κατά το έτος 2015 από μία ομάδα ειδικών των ευρωπαϊκών αρχών ιδιωτικότητας, κατόπιν ελέγχου και σάρωσης τετρακοσίων εβδομήντα οκτώ (478) ιστοσελίδων, εντοπίστηκαν συνολικά δεκαέξι χιλιάδες πεντακόσια πενήντα πέντε (16.555) cookies, δηλαδή κατά μέσο όρο 34,6 cookies ανά ιστοσελίδα (WP 29, 2015).

Συνήθως η ιχνηλάτηση των Χρηστών διενεργείται μέσω third-party cookies, που εγκαθίστανται όχι από τον πάροχο της ιστοσελίδας αλλά από τρίτους Διαφημιστές. Ωστόσο, λόγω της δυνατότητας των περισσότερων browsers να μπλοκάρουν τα third-party cookies, τα

διαφημιστικά δίκτυα προέβησαν στην ανάπτυξη εναλλακτικών λύσεων, όπως τα προηγμένης τεχνολογίας Flash cookies, των οποίων η διαγραφή δεν καθίσταται εφικτή μέσω των παραδοσιακών ρυθμίσεων ενός browser (Soltani, Ashkan, Canty, Shannon, Mayo, Quentin, Thomas, Lauren και Hoofnagle, Chris Jay, 2009).

Δεν χρησιμοποιούνται όμως όλα τα cookies για την παρακολούθηση των χρηστών μιας ιστοσελίδας. Η αποθήκευση και εγκατάστασή ορισμένων ειδών cookies στον ηλεκτρονικό υπολογιστή ή στο κινητό τηλέφωνο του Χρήστη μπορεί να αποσκοπεί στην εύρυθμη λειτουργία των ιστοσελίδων και στην βελτίωση της λειτουργικότητας τους ή στη βελτίωση της διαδικτυακής εμπειρίας του χρήστη μέσω της αποκρυστάλλωσης των προτιμήσεων του τελευταίου και της συνακόλουθης προβολής περιεχομένου και υπηρεσιών προσαρμοσμένων στις προτιμήσεις του. Ζήτημα παραβίασης των αρχών της προστασίας προσωπικών δεδομένων γεννάται στις περιπτώσεις κατά τις οποίες μέσω των cookies συλλέγονται και χρησιμοποιούνται παρανόμως δεδομένα προσωπικού χαρακτήρα των Χρηστών διαδικτυακών ιστότοπων, με αποτέλεσμα να επέρχεται κατάφωρη παραβίαση του δικαιώματός τους στην ιδιωτικότητα.

Στον ΓΚΠΔ δεν υφίσταται ρητή νομοθετική πρόβλεψη για τη χρήση των cookies. Ρητή πρόβλεψη για τα cookies και τις παρόμοιες τεχνολογίες υπάρχει στην Οδηγία ePrivacy 2002/59/EK αναφορικά με την επεξεργασία προσωπικών δεδομένων και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, η οποία πρόκειται να αντικατασταθεί από τον Κανονισμό ePrivacy, κατά τα ανωτέρω αναφερόμενα στο κεφάλαιο 2 της παρούσας. Η σχετική Οδηγία συνεπώς είναι το νομοθετικό εργαλείο το οποίο καταρχήν χρησιμοποιείται για τη προστασία της ιδιωτικής ζωής από τη χρήση των cookies και την εν γένει OnLine παρακολούθηση μέσω της εγκατάστασης κατασκοπευτικών τεχνολογιών στους τερματικούς εξοπλισμούς των Χρηστών του διαδικτύου.

#### **4.1.3. Η ρύθμιση των cookies**

- **Ρητή συγκατάθεση για την εγκατάσταση των cookies**

Δυνάμει της διάταξης του άρθρου 5 παρ. 3 της Οδηγίας ePrivacy 2002/59/EK, όπως αυτή έχει ενσωματωθεί στην ελληνική έννομη τάξη δυνάμει του άρθρου 4 παρ. 5 Ν. 3741/2006, επιτρέπεται να αποθηκεύονται πληροφορίες ή να αποκτάται πρόσβαση σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη μιας ιστοσελίδας μόνο στις περιπτώσεις κατά τις οποίες ο συνδρομητής ή ο χρήστης έχει παράσχει τη συγκατάθεσή του προς τούτο βάσει σαφών και εκτεταμένων πληροφοριών που του έχουν παρασχεθεί και ο υπεύθυνος ελέγχου των δεδομένων παρέχει στο συνδρομητή ή χρήστη το δικαίωμα να αρνείται την επεξεργασία αυτή, σύμφωνα με τις αρχές του ΓΚΠΔ, όπως εμφανίζονται στο παρακάτω infographic του Lawspot:

**Συγκατάθεση**  
σύμφωνα με τον GDPR

**Πρέπει να:**

- Προκύπτει από δήλωση ή σαφή θετική ενέργεια
- Είναι ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει
- Ανακαλείται ελεύθερα και όσο εύκολα παρέχεται
- Παρέχεται σε γραπτή, ηλεκτρονική ή προφορική μορφή
- Μπορεί να αποδειχθεί από τον Υπεύθυνο Επεξεργασίας

**Δεν πρέπει να:**

- Προκύπτει από σιωπή, προσυμπληρωμένα τετραγωνίδια ή αδράνεια
- Τίθεται ως προϋπόθεση για την εκτέλεση σύμβασης (π.χ. παροχή υπηρεσίας), όταν δεν είναι αναγκαίο
- Παρέχεται με βάση αίτημα που δεν είναι σε κατανοητή και εύκολα προσβάσιμη μορφή

LAWSPOT  
GDPR  
www.lawspot.gr/gdpr

Εικόνα 3: <https://www.lawspot.gr/nomika-nea/online-diafimisi-kai-prosopika-dedomena-mia-simantiki-apofasi-gia-mellon-toy-ad-tech-apof>

Εκ των ανωτέρω καθίσταται σαφές ότι τα cookies εγκαθίστανται νομίμως στις περιπτώσεις όπου ο χρήστης ή συνδρομητής έχει παράσχει τη ρητή συγκατάθεση του στην αποθήκευση πληροφοριών ή στην απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες και υπό την επιπρόσθετη προϋπόθεση ότι ο χρήστης ή συνδρομητής έχει ενημερωθεί επαρκώς προς τούτο (Κανέλλος, 2020, σελ. 381-382). Η διεργασία αυτή είναι γνωστή ως σύστημα opt – in. Η ενημέρωση του χρήστη ή του συνδρομητή απαιτείται να είναι ειδική και να έχει αναρτηθεί σε εμφανές σημείο, ενώ δεν επαρκεί γενική ενημέρωση, που διενεργείται στο πλαίσιο των ΓΟΣ

(π.χ. Όροι Χρήσης ιστοσελίδας) ή μιας μακροσκελούς Πολιτικής Απορρήτου ενός ιστότοπου, η οποία ρυθμίζει κι άλλα ζητήματα. Ακόμη, με απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ), που εκδόθηκε στις 01.10.2019 επί της υπόθεσης C-673/2017 Bundesverband der Verbraucherzentralen und Verbraucherverbände-Verbraucherzentrale Bundesverband eV v. Planet 29 GmbH, έγινε δεκτό ότι η αποθήκευση cookies προϋποθέτει την ενεργό συγκατάθεση του χρήστη ή συνδρομητή και ότι δεν είναι επιτρεπτή η χρήση εκ των προτέρων συμπληρωμένων τετραγωνιδίων προορισμένων για την παροχή συγκατάθεσης.

Ωστόσο, υφίστανται ορισμένες περιπτώσεις, κατά τις οποίες δεν κρίνεται απαραίτητη η παροχή συγκατάθεσης του χρήστη ή συνδρομητή αναφορικά με τη χρήση cookies. Πιο συγκεκριμένα, δεν απαιτείται συγκατάθεση, πρώτον στην περίπτωση που η οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση αποσκοπεί αποκλειστικά και μόνο στη διενέργεια της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών και δεύτερον στην περίπτωση που η χρήση cookies κρίνεται απολύτως απαραίτητη, προκειμένου να έχει τη δυνατότητα ο πάροχος μιας υπηρεσίας της Κοινωνίας της Πληροφορίας να παρέχει τη συγκεκριμένη υπηρεσία την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής.

Από τα διάφορα είδη cookies που μπορεί να υπάρχουν και να χρησιμοποιούνται από μία ιστοσελίδα, για τα περισσότερα απαιτείται η ρητή προγενέστερη συγκατάθεση του χρήστη ή συνδρομητή για τη νόμιμη εγκατάσταση τους στον browser ενός χρήστη. Υπάρχουν όμως cookies που χρησιμοποιούνται άπαξ και προσωρινά ανά συνεδρία ή για το σκοπό της τεχνικής υποστήριξης της σύνδεσης, όπως λόγω χάριν session cookies, user input, plug-ins, content sharing (WP 29, 2015) για τα οποία δεν απαιτεί συγκατάθεση του χρήστη ή συνδρομητή.

Για τους σκοπούς της συμμόρφωσης με το άρθρο 5 παρ. 3 της Οδηγίας ePrivacy 2002/59/EK είναι άσχετο αν οι πληροφορίες που αποθηκεύονται ή στις οποίες παρέχεται πρόσβαση είναι δεδομένα προσωπικού χαρακτήρα ή δεδομένα ειδικής κατηγορίας. Η σχετική Οδηγία έχει εφαρμογή σε όλα τα δεδομένα που ανακτώνται μέσω των cookies και στο μέτρο που τα δεδομένα αυτά περιλαμβάνουν και προσωπικά δεδομένα εφαρμόζεται από κοινού με τον ΓΚΠΔ. Στη διαφημιστική πρακτική οι εν λόγω απαιτήσεις δεν τηρούνται, δεδομένου ότι είτε δεν ενημερώνονται επαρκώς οι χρήστες ή συνδρομητές, είτε δεν λαμβάνεται νόμιμα η

συγκατάθεση του Χρήστη, είτε εγκαθίστανται cookies παρακολούθησης της διαδικτυακής συμπεριφοράς του Χρήστη εκ μέρους τρίτων μερών χωρίς τη συγκατάθεση του. Σύμφωνα με πανεπιστημιακή μελέτη που διενεργήθηκε τον Οκτώβριο 2019 (Utz, Degeling, Fahl, Schaub, Holz, 2019) η λήψη συγκατάθεσης των Χρηστών για τη χρήση cookies μέσω διαδικτυακών ιστότοπων δεν έχει ουσιαστική σημασία, καθότι δεν πληροί τις απαιτήσεις του ΓΚΠΔ, ενώ ωθεί τους Χρήστες στην αποδοχή όλων των cookies.

- **Οι Συστάσεις της ΑΠΔΠΧ**

Σημαντικό είναι να αναφέρουμε ότι δυνάμει του υπ' αριθμόν πρωτοκόλλου Γ/ΕΞ/1525 και από 25.02.2020 Δελτίου Τύπου, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα («ΑΠΔΠΧ») εξέδωσε ειδικές «Συστάσεις προς το σκοπό της συμμόρφωσης των υπευθύνων επεξεργασίας δεδομένων με την ειδική νομοθεσία για τις ηλεκτρονικές επικοινωνίες»<sup>33</sup>, καθώς μετά από έλεγχο που διεξήγαγε διαπιστώθηκε σημαντική έλλειψη της συμμόρφωσης των παρόχων υπηρεσιών της Κοινωνίας της Πληροφορίας στο ειδικό νομοθετικό πλαίσιο αναφορικά με την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών και του Γενικού Κανονισμού Προστασίας Δεδομένων αναφορικά με τη διαχείριση cookies και συναφών τεχνολογιών (ΑΠΔΠΧ, 2020). Στο εν λόγω κείμενο Συστάσεων η ΑΠΔΠΧ διατυπώνει ότι η εγκατάσταση ενός ιχνηλάτη (tracker) σε τερματική συσκευή προϋποθέτει καταρχήν τη συγκατάθεση του Χρήστη, ανεξαρτήτως του εάν μέσω αυτού διενεργείται εν τέλει επεξεργασία δεδομένων προσωπικού χαρακτήρα, ενώ εξαίρεση από την υποχρέωση προηγούμενης συγκατάθεσης του Χρήστη θεσπίζεται στις περιπτώσεις, κατά τις οποίες οι ιχνηλάτες κρίνονται «τεχνικά απαραίτητοι για την πραγματοποίηση της σύνδεσης στην ιστοσελίδα ή για την παροχή της υπηρεσίας διαδικτύου την οποία έχει ζητήσει ο ίδιος ο χρήστης». Η επιλογή της ΑΠΔΠΧ για την χρήση του όρου «ιχνηλάτης (tracker)» και όχι cookies σαφώς έχει ως σκοπό τη συμπερίληψη στην ρύθμιση όλων των τεχνολογιών παρακολούθησης είτε ήδη υπάρχοντων είτε αυτών που πιθανώς να δημιουργηθούν με την εξέλιξη της τεχνολογίας.

---

33 Πλήρες κείμενο είναι διαθέσιμο στον ακόλουθο σύνδεσμο:

<https://www.dpa.gr/el/enimerwtiko/deltia/systaseis-gia-ti-symmorfosi-ypeythynon-epexergasias-dedomenon-me-tin-eidiki>

Τέλος, ρητή πρόβλεψη γίνεται από την ΑΠΔΠΧ σχετικά με την εγκατάσταση ιχνηλατών προς το σκοπό της ψηφιακής διαφήμισης, καθότι επισημαίνεται ότι οι εν λόγω ιχνηλάτες δεν υπάγονται στην εξαίρεση από τον κανόνα της υποχρέωσης λήψης προγενέστερης συγκατάθεσης του χρήστη. **Ως εκ τούτου η ΑΠΔΠΧ καταλήγει στην κρίση της ότι η εγκατάσταση ιχνηλατών στο πλαίσιο της ψηφιακής διαφήμισης είναι σύννομη, μόνο εφόσον ο Χρήστης έχει παράσχει προηγουμένως τη συγκατάθεσή του και εφόσον ο τελευταίος έχει ενημερωθεί καταλλήλως.** Περαιτέρω, η υποχρέωση προηγούμενης λήψης της συγκατάθεσης του Χρήστη καθώς και η κατάλληλη ενημέρωση του τελευταίου απαιτείται, αφενός μεν στην κατηγορία των **"first-party" cookies**, αφετέρου δε στην κατηγορία των **"third-party" cookies**. Ειδικά στην περίπτωση των cookies τρίτου μέρους κρίνεται απαραίτητο να ληφθεί η συγκατάθεση του Χρήστη, ακόμη και στην περίπτωση όπου τα cookies αναφέρονται σε στατιστικά στοιχεία και στην ανάλυση της αγοράς, χωρίς δηλαδή τα cookies να συσχετίζονται άμεσα με την ταυτοποίηση του χρήστη.

Κατά πολλούς η ΑΠΔΠΧ υιοθέτησε μία αυστηρή γραμμή απέναντι στη χρήση των τεχνολογιών αυτών με αποτέλεσμα να εμποδίζει την λειτουργία της ψηφιακής αγοράς. Πράγματι, η ΑΠΔΠΧ ερμηνεύει αυστηρά τις σχετικές διατάξεις της Οδηγίας ePrivacy 2002/59/EK, τον ΓΚΠΔ και το εν γένει νομοθετικό πλαίσιο που έχει διαμορφωθεί δυνάμει των ερμηνευτικών κειμένων που έχουν εκδοθεί από άλλες εποπτικές αρχές, την WP 29, τα Δικαστήρια, με γνώμονα την προστασία του τελικού Χρήστη. Η θέση αυτή της ΑΠΔΠΧ όμως είναι απόλυτα δικαιολογημένη καθώς ακολουθεί την πρακτική των υπόλοιπων ευρωπαϊκών εποπτικών αρχών ενώ θα ήταν παράλογο να προτείνει ως βέλτιστες πρακτικές, πρακτικές απαρχαιωμένες ή συμβιβαστικές (Καρκατζούνης και Σκόνδρα, 2020). Αντιθέτως, παρέχοντας σαφείς και αναλυτικές οδηγίες συνδράμει στη διαμόρφωση ενός ικανοποιητικού επιπέδου προστασίας και στη διασφάλιση ενιαίας εφαρμογής της σχετικής νομοθεσίας.

- **Πολιτική Cookies και πλατφόρμες διαχείρισης συγκατάθεσης**

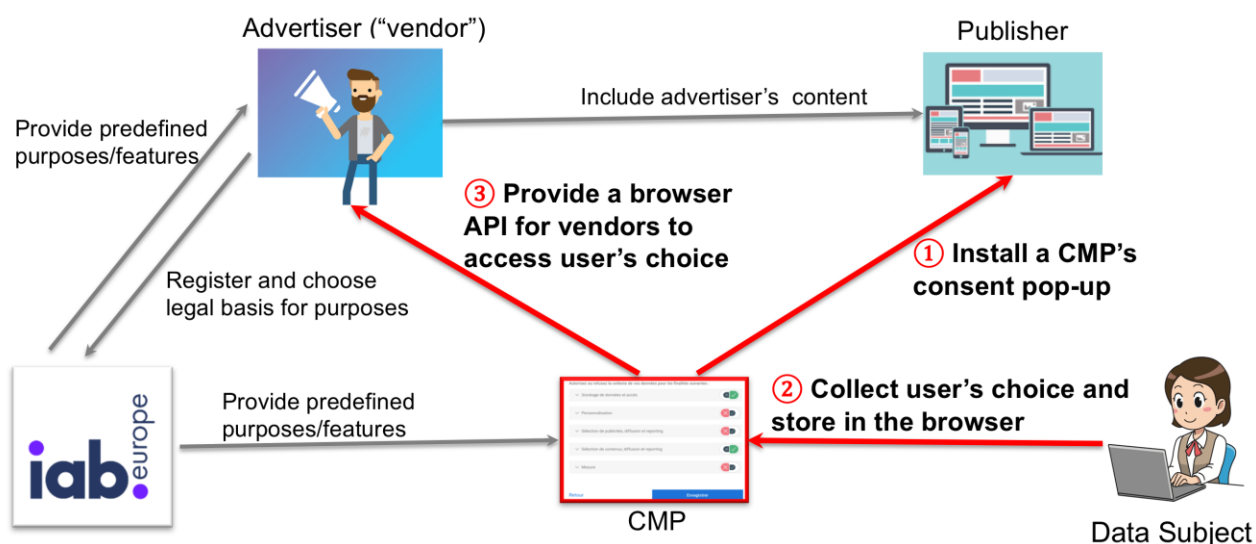
Όπως τούτο προβλέπεται από τη διάταξη του άρθρου 4 παρ. 5 Ν. 3741/2006, οι διαχειριστές των διαδικτυακών ιστότοπων, που κάνουν χρήση τεχνικών και τεχνολογιών εντοπισμού των Χρηστών υποχρεούνται να συντάσσουν και να αναρτούν στον ιστότοπό/εφαρμογή τους την



καλούμενη Πολιτική Cookies (Cookies Policy). Ειδικότερα, με την εν λόγω Πολιτική Cookies ενημερώνεται ο χρήστης του ιστότοπου και έπειτα ζητείται η απαιτούμενη κατά τα ως άνω ρητή συγκατάθεση του αναφορικά με τη χρήση cookies ή παρόμοιων τεχνολογιών οποιασδήποτε μορφής, ενώ στην περίπτωση που ο χρήστης αρνηθεί να παράσχει τη συγκατάθεσή του ο τελευταίος δεν μπορεί να παρεμποδιστεί από την ανώνυμη περιήγηση στο ψηφιακό περιεχόμενο της εν λόγω ιστοσελίδας (απαγόρευση “cookies walls”) (Κανέλλος, 2020, σελ. 382 επ.).

Πιο συγκεκριμένα, η Πολιτική Cookies απαιτείται να διευκρινίζει σε κάθε χρήστη σε τί συνίσταται η λειτουργικότητα και ο σκοπός της χρήσης της κάθε κατηγορίας cookies, ενώ ταυτοχρόνως πρέπει να διαχωρίζεται με σαφήνεια και ευκρίνεια η χρήση και η υποχρεωτική ή προαιρετική φύση τους. Η υλοποίηση της Πολιτικής Cookies είναι το ελάχιστο επίπεδο συμμόρφωσης για μια ιστοσελίδα ή εφαρμογή που χρησιμοποιεί cookies. Πρέπει να συντάσσεται με ιδιαίτερη προσοχή και επιμέλεια, καθότι σε διαφορετική περίπτωση ενδέχεται να κριθεί μη συμμορφωμένη με το ισχύον νομοθετικό πλαίσιο.

Αναφορικά με τον τρόπο παροχής της συγκατάθεσης του χρήστη, αξίζει να σημειωθεί ότι υφίστανται ποικίλες τεχνικές λύσεις λήψης και διαχείρισης της συγκατάθεσης που παρέχουν τεχνολογικές λύσεις «Consent as a Service» για να βοηθήσουν τους ιδιοκτήτες δικτυακών τόπων να διασφαλίσουν τη συμμόρφωση τους, καλούμενες Consent Management Platforms (CMPs). Οι πάροχοι CMP παρέχουν αναδυόμενα παράθυρα συγκατάθεσης (όπως cookie pop-up ή banner) που ενσωματώνονται σε δικτυακούς τόπους για να καταγράφουν τη συγκατάθεση του χρήστη πριν από την παρακολούθηση, τη συλλογή και την επεξεργασία των δεδομένων του. Τα CMP ενημερώνουν τους χρήστες σχετικά με τους τρόπους με τους οποίους μπορεί να παρακολουθούνται οι διαδικτυακές δραστηριότητές τους και τους σκοπούς της παρακολούθησης. Για την προτυποποίηση της τεχνικής υλοποίησης των CMP, μεταξύ άλλων, ο IAB Europe ανέπτυξε πρότυπο γνωστό ως «Transparency and Consent Framework» (TCF). Το TCF αναπτύχθηκε για να διαφυλάξει την ανταλλαγή δεδομένων στο οικοσύστημα του digital advertising και τη συμμόρφωση με τον ΓΚΠΔ και την ePrivacy Directive (Santos et al, 2021). Οι παράγοντες και οι βασικές διεργασίες στο TCF εμφανίζονται στην πιο κάτω εικόνα:



**Εικόνα 4:** Ο IAB Europe παρέχει τους προκαθορισμένους σκοπούς και λειτουργίες που προβάλλονται στους χρήστες. Οι εγγεγραμμένοι Διαφημιστές επιλέγουν νομική βάση για τους σκοπούς. Τα CMP παρέχουν το αναδύομενο παράθυρο για τη συγκατάθεση, αποθηκεύουν την επιλογή του χρήστη ως browser cookie και παρέχουν σε Διαφημιστές πρόσβαση στις πληροφορίες (C. Santos et al.).

- **Σημαντική απόφαση της γαλλικής Αρχής Προστασίας Δεδομένων (CNIL) για τη λήψη συγκατάθεσης και το πρότυπο TCF**

Με την υπ' αριθμ. 2018-042 απόφαση της, που δημοσιεύθηκε στις 9 Νοεμβρίου 2018, η CNIL έκρινε ότι ο μηχανισμός λήψης συγκατάθεσης (CMP) που χρησιμοποιεί η εταιρεία Vectaury δεν συμμορφώνεται με τις απαιτήσεις του ΓΚΠΔ για τη συγκατάθεση και επέβαλε στην εν λόγω εταιρεία συστάσεις με τις οποίες τη διέταξε να τροποποιήσει το σχετικό μηχανισμό και να διαγράψει όλα τα δεδομένα που είχε συλλέξει με τον μηχανισμό αυτό. Η εταιρεία Vectaury είναι διαφημιστικό πρακτορείο, που μεταξύ άλλων, παρείχε στους πελάτες του (Διαφημιστές) ένα λογισμικό πρόγραμμα για τη συλλογή δεδομένων και της τοποθεσίας των Χρηστών των εφαρμογών τους και τη δημιουργία προφίλ τους, βάσει του οποίου στη συνέχεια εκτελούσε διαφημιστικές καμπάνιες στόχευσης (Online διαφήμιση και προσωπικά δεδομένα, 2018).

Οι εφαρμογές που ενσωμάτωναν το σχετικό πρόγραμμα χρησιμοποιούσαν το μηχανισμό συγκατάθεσης (CMP), βασισμένο στο πρότυπο TCF του IAB Europe, με μια σύντομη ειδοποίηση ότι η εφαρμογή συγκεντρώνει τις σχετικές πληροφορίες για σκοπούς Στοχευμένης Διαφήμισης,

παρέχοντας στο Χρήστη στις επιλογές: αποδοχή, άρνηση ή τη διαχείριση των προτιμήσεών του. Κατά την άποψη της CNIL, το σχετικό CMP που χρησιμοποιούσε η Vectaury είχε τις πιο κάτω ελλείψεις (Karur S και Savare M, 2018):

1. Οι Χρήστες δεν ενημερώνονταν κατάλληλα για όλους τους σκοπούς επεξεργασίας δεδομένων πριν από την εμφάνιση των επιλογών συνολικής συγκατάθεσης. Σύμφωνα με την CNIL, η αρχική ειδοποίηση πρέπει να αναφέρει τους διάφορους σκοπούς ενώ οι περισσότερες πληροφορίες συνίσταται να παρέχονται με πολυεπίπεδο (layered) τρόπο (π.χ. κάνοντας κλικ στην επιλογή "Διαχείριση Προτιμήσεων").
2. Οι σκοποί ήταν "προεπιλεγμένοι", αντίθετα με την απαίτηση της ενεργού συγκατάθεσης του Χρήστη, δηλαδή opt-out αντί για opt-in. Επιπλέον, πρέπει να είναι διαθέσιμες επιλογές συγκατάθεσης ανά σκοπό.
3. Η ειδοποίηση παραπλανούσε τους Χρήστες. Η CNIL έκρινε ότι ορισμένες διατυπώσεις μπορούσαν να παραπλανήσουν τους Χρήστες και να τους κάνουν να νομίζουν ότι η άρνηση συγκατάθεσης συνεπάγεται αμοιβές ή πιο παρεμβατική διαφήμιση.
4. Η ειδοποίηση δεν απαριθμούσε τους υπεύθυνους επεξεργασίας στους οποίους θα διαμοιράζονταν τα δεδομένα, ούτε παρείχε άμεσο σύνδεσμο προς τέτοιο κατάλογο.
5. Οι σκοποί στερούνταν διαφάνειας.

Οι σχετικές κρίσεις της CNIL κατά πολλούς θεωρήθηκε ότι στέφονται κατά του προτύπου TCF και της ψηφιακής διαφήμισης στο σύνολό της, εφόσον το πρότυπο TCF χρησιμοποιείται ευρέως στο οικοσύστημα της. Ωστόσο, η απόφαση αυτή της CNIL δεν στρεφόταν άμεσα κατά του προτύπου TCF, παρά κατά της εκδοχής που είχε επιλέξει να χρησιμοποιεί η Vectaury. Άλλωστε, πολλές από τις απαιτήσεις αναφέρει η CNIL επιβάλλονται επίσης από τις πολιτικές TCF (π.χ. σκοποί επεξεργασίας και ο κατάλογος υπευθύνων επεξεργασίας στο πρώτο επίπεδο της ενημέρωσης και ενεργός συγκατάθεση). Πράγματι, στο πλαίσιο της εν λόγω απόφασης, η CNIL δεν έκρινε ότι το TCF είναι πρότυπο στο οποίο δεν μπορεί να βασιστεί κανείς για να λάβει έγκυρη συγκατάθεση. Αλλά παρεμπιπτόντως ανέδειξε κάποιες αδυναμίες του. Για παράδειγμα στο πλαίσιο του TCF παρέχονται ορισμένοι ορισμοί σκοπών επεξεργασίας οι οποίοι κατά την CNIL δεν έχουν επαρκή διαφάνεια για την λήψη έγκυρης συγκατάθεσης. Ως μοναδικό

παράδειγμα, η CNIL έφερε τον ορισμό της "προσωποποίησης" κρίνοντας ότι ήταν ασαφώς διατυπωμένος. Σε συνέχεια της σχετικής παρατήρησης, ο IAB Europe δήλωσε ότι έχει αναθεωρήσει τους ορισμούς του, μετά από διαβούλευση με την CNIL και άλλες εποπτικές αρχές (IAB Europe, 2018). Αποτέλεσμα αυτών ήταν το TCF v. 2.0.

Αξίζει να σημειωθεί ότι έκτοτε και παρά τις αναθεωρήσεις στις οποίες προχώρησε ο IAB Europe υποβλήθηκαν νέες καταγγελίες και κατά του προτύπου TCF v. 2.0, ιδιαίτερα για τον ρόλο του στην Προγραμματική Διαφήμιση και στο Real Time Bidding («RTB»), που θα αναλύσουμε κατωτέρω. Αποτέλεσμα αυτών των καταγγελιών ήταν η πρόσφατη απόφαση της Βελγικής εποπτικής αρχής της 2 Φεβρουαρίου του 2022, με την οποία μάλιστα επιβλήθηκε εις βάρος του IAB Europe πρόστιμο ποσού 250.000,00 ευρώ. Η εν λόγω απόφαση εστιάζει στον ρόλο του IAB Europe στο TCF (και ειδικότερα σε σχέση με την καταχώρηση των συγκαταθέσεων των χρηστών) ως Υπεύθυνου Επεξεργασίας, κρίνοντας ότι υπό τη σχετική του ιδιότητα απέτυχε να συμμορφωθεί με τις απαιτήσεις του ΓΚΠΔ. Στο πλαίσιο δε της ίδιας απόφασης έκρινε και πάλι ότι οι πληροφορίες που παρέχονταν στους χρήστες μέσω των CMP είναι πολύ γενικές και ασαφείς όσον αφορά τη φύση και το πεδίο εφαρμογής της επεξεργασίας, καθιστώντας δύσκολο για τους χρήστες να διατηρήσουν τον έλεγχο των προσωπικών τους δεδομένων (Kim W. και White L, 2022).

## **4.2. Social Media Advertising**

### **4.2.1. Τα μέσα κοινωνικής δικτύωσης («social media»)**

Είναι αναμφισβήτητο ότι τα social media» συνέβαλαν στη μετάβαση στο Συμμετοχικό Διαδίκτυο (WEB 2.0). Η ολοένα αυξανόμενη χρήση των social media σε παγκόσμια κλίμακα οφείλεται κατά κύριο λόγο στα εξελιγμένα εργαλεία που διαθέτουν, τα οποία παρέχουν τη δυνατότητα στους χρήστες, αφού δημιουργήσουν δωρεάν προφίλ ή άλλως λογαριασμό, να επικοινωνούν μεταξύ τους, να μοιράζονται φωτογραφίες, μουσική, κοινά ενδιαφέροντα κλπ. Τούτο σημαίνει ότι ο καθένας έχει τη δυνατότητα να δημιουργήσει έναν λογαριασμό στο Facebook, Twitter, Instagram, YouTube κλπ. χωρίς κανένα κόστος, κάνοντας μια απλή εγγραφή στις εν λόγω πλατφόρμες. Λόγω του αχανούς αριθμού χρηστών των μέσων κοινωνικής δικτύωσης

καθίσταται ευχερώς κατανοητό ότι ο όγκος των προσωπικών δεδομένων που παράγεται από τους χρήστες αυτούς είναι εξίσου αχανής. Τούτο δε θέτει σε κίνδυνο θεμελιώδη δικαιώματα και τις ελευθερίες των χρηστών, μεταξύ των οποίων και αυτό της προστασίας προσωπικών δεδομένων, όπως θα αναλύσουμε κατωτέρω.

Προκειμένου τα κοινωνικά δίκτυα να ενισχύονται οικονομικά, δηλαδή να αποφέρουν έσοδα, οι πάροχοι των σχετικών υπηρεσιών έχουν βασίσει σε μεγάλο ποσοστό το επιχειρηματικό τους μοντέλο σε υπηρεσίες στόχευσης των χρηστών των social media έναντι αντιτίμου, οι οποίες παρέχονται σε οντότητες που επιθυμούν να τους μεταδώσουν συγκεκριμένα μηνύματα με σκοπό την προώθηση των συμφερόντων τους. Όπως γίνεται κατανοητό το Social Media Advertising (όπως το έχουμε ορίσει στο κεφάλαιο 1.2.1 Βασικοί Τύποι Digital Advertising) αποτελεί σημαντικό τρόπο για τους παρόχους social media να παράγουν έσοδα, καθώς τα κοινωνικά δίκτυα είναι ιδιαίτερα ελκυστικά για προβολή στοχευμένης διαφήμισης, η οποία προϋποθέτει συλλογή και επεξεργασία μεγάλων ποσοτήτων δεδομένων (Kahl κ.ά., 2011).

#### **4.2.2. Οι κίνδυνοι**

Αναγνωρίζοντας τους κινδύνους που ενέχει η στόχευση για τους χρήστες των social media το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων («ΕΣΠΔ») εξέδωσε τις υπ' αριθμ. 8/2020 κατευθυντήριες γραμμές σχετικά με τη στόχευση χρηστών μέσω κοινωνικής δικτύωσης («Κατευθυντήριες Γραμμές»), η πιο πρόσφατη μορφή των οποίων εγκρίθηκε την 13.04.2021. Σκοπός του ΕΣΠΔ ήταν να αποσαφηνίσει τους ρόλους και τις αρμοδιότητες των εμπλεκόμενων μερών και να προσδιορίσει τις υποχρεώσεις τους σχετικά με τη προστασία προσωπικών δεδομένων. Στις Κατευθυντήριες Γραμμές, το ΕΣΠΔ εντοπίζει ποικίλους κινδύνους για τα δικαιώματα και τις ελευθερίες των χρηστών λόγω της επεξεργασίας των προσωπικών τους δεδομένων, χωρίς ωστόσο να παρέχει εξαντλητικό κατάλογο των ειδών των κινδύνων. Ενδεικτικά αναφέροντας, το ΕΣΠΔ αρχικά τονίζει ότι η χρήση δεδομένων για τη στόχευση στα social media ξεπερνάει κατά πολύ τις εύλογες προσδοκίες των χρηστών των μέσω κοινωνικής δικτύωσης και συνεπώς παραβιάζει τις αρχές προστασίας προσωπικών δεδομένων.

Ως πρώτη κατηγορία κινδύνων το ΕΣΠΔ αναφέρει τους κινδύνους που προκύπτουν από το συνδυασμό των δεδομένων που συλλέγονται από τρίτες πηγές και από τους χρήστες απευθείας,

με αποτέλεσμα τη χρήση των δεδομένων πέραν του αρχικού σκοπού συλλογής τους και με τρόπο που ο χρήστης δεν μπορούσε εύλογα να προβλέψει. Επιπλέον, ο συνδυασμός δεδομένων για κατάρτιση προφίλ μπορεί να έχει ως αποτέλεσμα να γίνονται γνωστά προσωπικά γνωρίσματα και πληροφορίες για τον χρήστη που εκείνος δεν γνωστοποίησε ενεργά, με αποτέλεσμα ο χρήστης να καταλήγει να χάνει τον έλεγχο επί των προσωπικών του δεδομένων. Ακόμη, η εμπλοκή διάφορων οργανισμών και οντοτήτων στη διαδικασία της επεξεργασίας των δεδομένων εμποδίζει ή και αποτρέπει την αποτελεσματική άσκηση των δικαιωμάτων των χρηστών σχετικά με τα δεδομένα τους. Οι φορείς στα social media είναι φυσικά οι χρήστες τους (έννοια που περιλαμβάνει φυσικά πρόσωπα τόσο εγγεγραμμένα όσο και μη εγγεγραμμένα στην υπηρεσία) και οι πάροχοι μέσων κοινωνικής δικτύωσης που προσδιορίζουν τις λειτουργίες των social media (όπως μεταξύ άλλων τα δεδομένα που θα υπόκεινται σε επεξεργασία στο πλαίσιο της υπηρεσίας στόχευσης). Το ΕΣΠΔ ονομάζει τις οντότητες που χρησιμοποιούν στις υπηρεσίες στόχευσης ως «Στοχεύοντες φορείς», δηλαδή φυσικά ή νομικά πρόσωπα που επιθυμούν να μεταδώσουν ένα μήνυμα σε συγκεκριμένους χρήστες των social media βάσει χαρακτηριστικών, ενδιαφερόντων και άλλων κριτηρίων (πρακτική καλούμενη συχνά και ως «μικροστόχευση»). Οι στοχεύοντες φορείς μπορεί να χρησιμοποιούν για το σκοπό αυτό δικά τους εργαλεία μέσω της χρήσης API<sup>34</sup> ή SDK<sup>35</sup>. Τέλος, έχουμε τους ενδιάμεσους παρόχους υπηρεσιών που δεν είναι άλλοι από τα γνωστά σε μας AdTech, Data Brokers, Measurement and Verification Providers, που έχουμε αναλύσει ανωτέρω (ΕΣΠΔ, 2021).

Ως δεύτερη κατηγορία κινδύνων το ΕΣΠΔ αναφέρει το ενδεχόμενο διακρίσεων και αποκλεισμού των χρηστών βάσει κριτηρίων σχετικά με τη φυλετική ή εθνοτική καταγωγή τους, την υγεία ή

---

34 «Η Διεπαφή Προγραμματισμού Εφαρμογών (*Application Programming Interface*), γνωστή και ως Διασύνδεση Προγραμματισμού Εφαρμογών (για συντομία διεπαφή ή διασύνδεση), είναι η διεπαφή των προγραμματιστικών διαδικασιών που παρέχει ένα λειτουργικό σύστημα, βιβλιοθήκη ή εφαρμογή προκειμένου να επιτρέπει να γίνονται προς αυτά αιτήσεις από άλλα προγράμματα ή/και ανταλλαγή δεδομένων.», Wikipedia (2021), διαθέσιμο σε [https://el.wikipedia.org/wiki/Διεπαφή\\_προγραμματισμού\\_εφαρμογών](https://el.wikipedia.org/wiki/Διεπαφή_προγραμματισμού_εφαρμογών), ανακτήθηκε 07.4.2022.

35 «Ένα Κιτ Ανάπτυξης Λογισμικού (*Software Development Kit - SDK ή devkit*) είναι ένα σύνολο εργαλείων ανάπτυξης που επιτρέπουν σε έναν προγραμματιστή να δημιουργήσει λογισμικό εφαρμογών για ένα συγκεκριμένο πακέτο λογισμικού, πλατφόρμα, παιχνιδιομηχανή, λειτουργικά συστήματα κτλ.», Wikipedia, (2022), διαθέσιμο σε [https://el.wikipedia.org/wiki/Κιτ\\_Ανάπτυξης\\_Λογισμικού](https://el.wikipedia.org/wiki/Κιτ_Ανάπτυξης_Λογισμικού), ανακτήθηκε 07.4.2022.

τον γενετήσιο προσανατολισμό. Παράδειγμα τέτοιας διάκρισης είναι για παράδειγμα η προβολή διαφημίσεων για προσφορά εργασίας ή πίστωσης σε ορισμένες μόνο ομάδες χρηστών, με αποκλεισμό άλλων ομάδων χρηστών με κριτήριο την υγεία τους. Η δυνατότητα των Διαφημιστών για στόχευση γίνεται ευκολότερη λόγω εργαλείων και της ποικιλίας και ποσότητας δεδομένων που συγκεντρώνονται στα social media. Δυσμενείς δε διακρίσεις δεν συνεπάγεται η επεξεργασία μόνο των ειδικών κατηγοριών δεδομένων αλλά και των απλών δεδομένων, σύμφωνα με τα αποτελέσματα σχετικής έρευνας (Speicher κ.ά., 2018).

Ως τρίτη κατηγορία κινδύνων το ΕΣΠΔ αναφέρει τη χειραγώγηση των χρηστών που μπορεί να φτάνει στο σημείο του περιορισμού της ατομικής ελευθερίας και αυτονομίας τους. Για παράδειγμα η ανάλυση των αλληλεπιδράσεων του χρήστη στα social media μπορεί να αποκαλύπτει τη συναισθήματα του σε μία δεδομένη στιγμή, πράγμα που μπορεί να χρησιμοποιηθεί για τη στόχευσή του με συγκεκριμένα μηνύματα στα οποία θα είναι επιρρεπής τη συγκεκριμένη χρονική στιγμή, επηρεάζοντας τι σκέφτεται, τι αισθάνεται και τελικά τη συμπεριφορά του (Kramer, Guillory και Hancock, 2014).

Ως τέταρτη κατηγορία κινδύνων το ΕΣΠΔ αναφέρει τον περιορισμό του χρήστη στη πρόσβαση σε διάφορες απόψεις και πηγές πληροφοριών για ένα συγκεκριμένο θέμα, με αποτέλεσμα ο χρήστης να καταλήγει να παγιδεύεται σε “filter bubble” που περιγράψαμε ανωτέρω ή λόγω της «υπερπληροφόρησης» να καταλήγει να μην μπορεί να λάβει απόφαση (καθώς εκτίθεται σε πολλές πληροφορίες για το ίδιο θέμα, χωρίς να γνωρίζει ποιες είναι αξιόπιστες).

Τέλος, το ΕΣΠΔ αναγνωρίζει τους κινδύνους που ενέχουν τα social media για τις αρχές του ανταγωνισμού, καθώς οι τεράστιες ποσότητες δεδομένων που διαθέτουν οι πλατφόρμες social media τις καθιστούν αναγκαστικούς επιχειρηματικούς συνεργάτες για τους φορείς του digital advertising. Το ΕΣΠΔ (2018) τονίζει ότι ο ρόλος και η ισχύς των social media στην αγορά «ενδέχεται να απειλήσει το επίπεδο προστασίας των δεδομένων και την ελευθερία των καταναλωτών ψηφιακών υπηρεσιών» .

Κατά το ΕΣΠΔ η επέλευση των ως άνω κινδύνων εξαρτάται μεταξύ άλλων από τον μηχανισμό στόχευσης και από τον τρόπο και το σκοπό για τον οποίο αυτός μπορεί να χρησιμοποιηθεί.

#### 4.2.3. Οι μηχανισμοί στόχευσης στο *Social Media Advertising*

Το ΕΣΠΔ (2021) κατατάσσει τους μηχανισμούς στόχευσης στις εξής κατηγορίες:

α) **Στόχευση προσώπων βάσει παρεχόμενων δεδομένων** δηλαδή δεδομένων που ο χρήστης παρέχει εκουσίως στον πάροχο μέσω κοινωνικής δικτύωσης και/ή στον στοχεύοντα φορέα. Τέτοια στόχευση χρησιμοποιεί τα δεδομένα που παρέχει ο χρήστης κατά την εγγραφή του στην υπηρεσία (π.χ. ηλικία) ή δεδομένα που παρέχει ο χρήστης στον στοχεύοντα φορέα στο πλαίσιο πελατειακών σχέσεων (π.χ. e-mail), τα οποία στη συνέχεια συνδυάζονται με τα δεδομένα που διαθέτει ο πάροχος μέσω κοινωνικής δικτύωσης ώστε η διαφήμιση να στοχεύει τους χρήστες αυτούς.

β) **Στόχευση βάσει παρατηρούμενων δεδομένων**, τα οποία είναι δεδομένα τα οποία παρέχει ο χρήστης στο πλαίσιο της χρήσης μιας υπηρεσίας ή συσκευής. Τέτοια στόχευση διενεργείται με κριτήριο:

- ❖ τη δραστηριότητα του χρήστη στο πλαίσιο των social media (π.χ. likes),
- ❖ τη χρήση συσκευών που χρησιμοποιεί κατά τη πρόσβαση στα social media (π.χ. τοποθεσία GPS),
- ❖ δεδομένα που προέρχονται από τρίτο σχεδιαστή εφαρμογών, με τη χρήση API ή SDK,
- ❖ δεδομένα που συλλέχθηκαν από ιστότοπους τρίτων που έχουν ενσωματώσει στα social media,
- ❖ δεδομένα που συλλέχθηκαν από άλλους τρίτους (π.χ. επιχείρηση από την οποία αγόρασε ένα προϊόν, στην οποία έγινε συνδρομητής με κάρτα πελάτη),
- ❖ δεδομένα που συλλέχθηκαν από υπηρεσίες τις οποίες παρέχουν εταιρείες συμφερόντων του παρόχου social media.

γ) **Στόχευση βάσει συναγόμενων δεδομένων**, τα οποία δημιουργούνται από τον εκάστοτε υπεύθυνο επεξεργασίας βάσει των δεδομένων που παρέχει ο χρήστης. Επί της ουσίας πρόκειται για συμπεράσματα που βγάζει ο υπεύθυνος επεξεργασίας σχετικά με τον χρήστη και τις προτιμήσεις του (π.χ. με βάση τη πλοηγική συμπεριφορά του χρήστη, μπορεί να συνάγεται ότι ενδιαφέρεται για ένα προϊόν).



### **4.3. Real Time Bidding («RTB»)**

#### **4.3.1 Τι είναι RTB;**

Το RTB είναι η αυτοματοποιημένη διαδικασία κατά την οποία δημοπρατείται η προσοχή που δίνει ένας χρήστης σε κάποιον ιστότοπο (EDRi, 2019). Σύμφωνα με το Information Commissioner's Office<sup>36</sup> (2019) το RTB χρησιμοποιεί AdTech για να επιτρέψει την αγοραπωλησία διαφημιστικού αποθεματικού ανά Εμφάνιση σε πραγματικό χρόνο (δηλαδή σε χρόνο που χρειάζεται ένας ιστότοπος να εμφανιστεί στο browser ενός χρήστη), συνήθως με τη χρήση ενός μηχανισμού κοστολόγησης μέσω δημοπρασίας. Πιο συγκεκριμένα, ένας Εκδότης αποστέλλει «αίτημα προσφοράς», το οποίο περιέχει πληροφορίες μεταξύ των οποίων συνήθως προσωπικά δεδομένα, σε εκατοντάδες Διαφημιστές, οι οποίοι με τη σειρά τους τοποθετούν προσφορές για το διαθέσιμο ψηφιακό χώρο διαφήμισης εντός χιλιοστών του δευτερολέπτου, αφού προηγουμένως έχει προηγηθεί ανάλυση των προτιμήσεων των χρηστών των συγκεκριμένων εφαρμογών και ιστοσελίδων. Το RTB είναι υποκατηγορία της Προγραμματικής Διαφήμισης και χρησιμοποιείται κυρίως για την πώληση εικαστικού αποθεματικού ενός ιστότοπου ή εφαρμογής (Information Commissioner's Office, 2019). Στη διαδικασία συμμετέχουν όλα τα μέρη και τεχνολογίες AdTech που έχουμε αναλύσει στο πρώτο κεφάλαιο της παρούσας. Τα δε προσωπικά δεδομένα που διαμοιράζονται και αναλύονται μπορεί να είναι είτε απλά είτε ειδικής κατηγορίας.

#### **4.3.2 Οι κίνδυνοι**

Εκ των ανωτέρω καθίσταται σαφές ότι το RTB εγείρει σημαντικούς προβληματισμούς αναφορικά με την προστασία προσωπικών δεδομένων των χρηστών του Διαδικτύου. Οι δημοπρασίες που διενεργούνται λειτουργούν επί της ουσίας μέσω της συλλογής, αναμετάδοσης και επεξεργασίας προσωπικών δεδομένων ενός χρήστη που επισκέπτεται μια ιστοσελίδα ή κάνει χρήση μιας εφαρμογής (για παράδειγμα, οι προτιμήσεις του, η διαδικτυακή του δραστηριότητα κλπ.) σε εκατοντάδες εταιρείες (όπως Διαφημιστές, AdTech και Advertising

---

<sup>36</sup> Βρετανική ανεξάρτητη αρχή επιφορτισμένη μεταξύ άλλων με τη προστασία προσωπικών δεδομένων φυσικών προσώπων. Οράτε σχετικά στο <https://ico.org.uk/about-the-ico/>

Agencies). Και όλα αυτά συμβαίνουν κάθε φορά που κάποιος χρήστης επισκέπτεται έναν ιστότοπο, σε κλάσματα δευτερολέπτου (Privacy International, 2019). Το RTB, εκ της φύσεως του και του τρόπου επεξεργασίας των δεδομένων, εγκυμονεί κινδύνους για το δικαίωμα της ιδιωτικότητας και της προστασίας προσωπικών δεδομένων. Μεταξύ αυτών, η δημιουργία προφίλ και αυτοματοποιημένη λήψη αποφάσεων, η επεξεργασία δεδομένων μεγάλης κλίμακας (συμπεριλαμβανομένων ειδικών κατηγοριών δεδομένων), η χρήση καινοτόμων τεχνολογιών, ο συνδυασμός και η αντιστοίχιση δεδομένων από πολλαπλές πηγές, η παρακολούθηση της γεωγραφικής θέσης και/ή της συμπεριφοράς των χρηστών και η αδιαφανής επεξεργασία τους (Information Commissioner's Office, 2019).

#### **4.3.3 Βασικά ζητήματα που εγείρονται σχετικά με την επεξεργασία προσωπικών δεδομένων**

Το RTB έχει μπει στο στόχαστρο διάφορων οργανώσεων της κοινωνίας των πολιτών μεταξύ των οποίων και η ελληνική Homo Digitalis, η οποία κατέθεσε ενώπιον της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα την αριθ. Πρωτ. 8478/10-12-2020 καταγγελία της κατά της Google και του IAB Europe σχετικά με τις πρακτικές επεξεργασίας προσωπικών δεδομένων στο πλαίσιο του RTB (Homo Digitalis, 2020), επί της οποίας η ΑΠΔΠΧ ακόμη δεν έχει λάβει θέση. Σύμφωνα με την εν λόγω καταγγελία (2020) τα βασικότερα ζητήματα που εγείρονται σχετικά με την επεξεργασία προσωπικών δεδομένων είναι τα εξής:

- Ανυπαρξία των προβλεπόμενων εκ του άρθρου 5 περίπτωση στ' του ΓΚΠΔ κατάλληλων τεχνικών και οργανωτικών μέτρων που πρέπει να χρησιμοποιούνται, προκειμένου να διασφαλίζεται η ενδεδειγμένη ασφάλεια των προσωπικών δεδομένων, ιδίως δε η προστασία τους έναντι της μη εξουσιοδοτημένης ή παράνομης επεξεργασίας τους και τυχαίας απώλειας, καταστροφής ή φθοράς, όπως τούτο επιτάσσουν οι αρχές της εμπιστευτικότητας και ακεραιότητας, που διέπουν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Τα προσωπικά δεδομένα αναμεταδίδονται χωρίς να υφίστανται οι τεχνικές εγγυήσεις σχετικά με την ασφάλεια, την ακεραιότητα και την εμπιστευτικότητα τους.
- Αδυναμία ενημέρωσης των χρηστών των σχετικών ιστοσελίδων και εφαρμογών υπό την ιδιότητά τους ως υποκείμενα των δεδομένων με βάση τα άρθρα 13 και 14 του ΓΚΠΔ. Εκ της φύσεως του, το RTB καθιστά αδύνατη την αποτύπωση όλων των πραγματικών χρήσεων και

των συνολικών αποδεκτών των δεδομένων, καθώς δεν υπάρχει η δυνατότητα ελέγχου της επεξεργασίας μόλις τα προσωπικά δεδομένα αναμεταδοθούν. Η δε αναμετάδοση των δεδομένων προσωπικού χαρακτήρα των χρηστών διενεργείται χωρίς οι τελευταίοι να λαμβάνουν γνώση και να έχουν έλεγχο επί των συγκεκριμένων πράξεων επεξεργασίας των προσωπικών δεδομένων που τους αφορούν.

- Στα δεδομένα προσωπικού χαρακτήρα εκάστου χρήστη που επεξεργάζονται στο πλαίσιο του RTB ενδέχεται να υπάγονται, μεταξύ άλλων, προσωπικά δεδομένα ειδικής κατηγορίας, σύμφωνα με τον ΓΚΠΔ. Πιο συγκεκριμένα, οι ιστοσελίδες ή εφαρμογές, που επισκέπτεται ο χρήστης-υποκείμενο των δεδομένων ενδέχεται να περιλαμβάνουν πληροφορίες και στοιχεία, που λειτουργούν ως δείκτες σχετικά με τον σεξουαλικό του προσανατολισμό, την εθνικότητά του, την προέλευση, τις πολιτικές ή θρησκευτικές πεποιθήσεις κ.α., με αποτέλεσμα να τίθεται σοβαρό ζήτημα παράνομης επεξεργασίας ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, ενώ οι δείκτες τέτοιας φύσεως δύναται να είναι σαφείς ή να δύναται να συναχθούν εύκολα, αποτελεσματικά και με ακρίβεια μέσω της χρήσης σύγχρονων τεχνικών ανάλυσης δεδομένων<sup>37</sup>.
- Καταστρατήγηση των βασικών αρχών που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τον ΓΚΠΔ (άρθρο 5). Ειδικότερα, στο πλαίσιο του RTB συγκεντρώνεται ένα ευρύ φάσμα πληροφοριών για τους χρήστες, που υπερβαίνει τις απαιτούμενες πληροφορίες που χρειάζονται για την παροχή των σχετικών διαφημίσεων. Τα δε δεδομένα αυτά συλλέγονται και επεξεργάζονται για σκοπούς που υπερβαίνουν κατά πολύ τους σκοπούς που ο χρήστης μπορεί να κατανοήσει ή συναινέσει ή αντιταχθεί.

---

37 «Η κατάρτιση προφίλ μπορεί να δημιουργήσει δεδομένα ειδικών κατηγοριών διά της συναγωγής από δεδομένα που δεν ανήκουν σε ειδική κατηγορία καθαυτά, αλλά τα οποία καθίστανται δεδομένα ειδικών κατηγοριών όταν συνδυάζονται με άλλα δεδομένα. Για παράδειγμα, μπορεί να είναι εφικτή η συναγωγή της κατάστασης της υγείας ενός φυσικού προσώπου από τα αρχεία των αγορών τροφίμων που πραγματοποιεί σε συνδυασμό με δεδομένα σχετικά με την ποιότητα και την ενέργεια που περιέχεται στα τρόφιμα.», WP 29, Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679, (wp251rev.01).

## ΣΥΜΠΕΡΑΣΜΑΤΑ

Εκ των αναλυθέντων στην παρούσα εργασία συνάγεται αρχικά ότι η προώθηση των σύγχρονων επιχειρήσεων μέσω της ψηφιακής διαφήμισης συμβάλλει σε σημαντικό βαθμό στην ενίσχυση της οικονομίας του διαδικτύου. Η ραγδαία ανάπτυξη του διαδικτύου και η συνεχής ανάδυση νέων τεχνολογικών επιτευγμάτων, η ανάπτυξη των μέσων κοινωνικής δικτύωσης, το φαινόμενο της παγκοσμιοποίησης, οι ολοένα αυξανόμενες απαιτήσεις των καταναλωτών και η αλληλεπίδραση των χρηστών καθιστούν αναγκαία την παρουσία των επιχειρήσεων στις διαδικτυακές πλατφόρμες, οι οποίες σαφώς ενισχύονται οικονομικά από τις τελευταίες μέσω της προβολής τους στο δίκτυό τους. Κατά συνέπεια, η εκτενής παρουσία των επιχειρήσεων στο χώρο του διαδικτύου συνέβαλε σταδιακά στην ανάπτυξη του digital advertising. Στο γενικότερο πλαίσιο της σύγχρονης Κοινωνίας της Πληροφορίας και των ραγδαίων τεχνολογικών εξελίξεων, η ανάπτυξη της ψηφιακής διαφήμισης κατά τον ανωτέρω τρόπο εγείρει ποικίλους προβληματισμούς αναφορικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. Τούτο καθότι τα παραπάνω συνεπάγονται ολοένα και μεγαλύτερη ανάγκη για συλλογή και κατ' επέκταση επεξεργασία των προσωπικών δεδομένων με σκοπό την εξατομίκευση των διαφημιστικών εμπειριών των εν δυνάμει πελατών και τη συστηματική παρακολούθηση της συμπεριφοράς τους στο διαδίκτυο. Εν ολίγοις, μέσα από τις στρατηγικές του digital advertising διαρρέουν υπέρογκες ποσότητες προσωπικών δεδομένων των χρηστών του διαδικτύου, οι οποίες αποθηκεύονται και χρησιμοποιούνται είτε από εταιρείες είτε από ιδιώτες και συνεπώς καθίστανται αντικείμενο εμπορικής εκμετάλλευσης και αποκόμισης κέρδους. Μάλιστα, ουκ ολίγες είναι οι εταιρείες που επιδιώκουν να διαμορφώσουν ένα πολιτικό, πολιτισμικό, μορφωτικό και καταναλωτικό προφίλ για τον κάθε χρήστη που δραστηριοποιείται διαδικτυακά, αποκωδικοποιώντας την προσωπική του ζωή και καταγράφοντας τα ψηφιακά του ίχνη με απώτερο σκοπό τη Στοχευμένη Διαφήμιση και την προώθηση προϊόντων και υπηρεσιών. Όλα αυτά σαφώς συνεπάγονται κατάφωρη παραβίαση των προσωπικών δεδομένων των χρηστών του διαδικτύου και επιπροσθέτως δημιουργούν την αίσθηση της συστηματικής παρακολούθησης.

Στο πλαίσιο τούτο, οι έννοιες της ψηφιακής διαφήμισης και της επιχειρηματικής ηθικής αποκτούν ιδιαίτερη σημασία σε συνάρτηση με το σεβασμό, την προστασία και τη θωράκιση των προσωπικών δεδομένων των χρηστών του διαδικτύου. Δεδομένων τούτων, λοιπόν, η προστασία των δεδομένων προσωπικού χαρακτήρα εμφανίζεται ως επιτακτική ανάγκη. Στο πλαίσιο τούτο, η έλευση του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (GDPR) και η θέση του σε ισχύ το Μάιο του έτους 2018, ο Κανονισμός e-Privacy και όλα τα νομοθετικά καθεστώτα περί προστασίας των προσωπικών δεδομένων κατέστησαν σημαντική πρόκληση για το digital advertising. Κατά συνέπεια, κατά την προετοιμασία μιας στρατηγικής του digital advertising, πρέπει να ακολουθούνται ορισμένοι κανόνες δεοντολογίας, όπως επί παραδείγματι η παροχή ορθών πληροφοριών για τα προϊόντα ή τις υπηρεσίες που διαφημίζονται μέσω ψηφιακών πλατφόρμων, ο σεβασμός στις διαφορετικές θρησκευτικές και πολιτικές πεποιθήσεις και επίσης να εφαρμόζονται οι διατάξεις όλων των νομοθετημάτων, που σκοπούν στο σεβασμό και την προστασία των προσωπικών δεδομένων των χρηστών του διαδικτύου.

Λαμβάνοντας υπόψη όλα τα ανωτέρω, δέον να επισημανθεί ότι τα νομοθετήματα που εξετάστηκαν στην παρούσα και ρυθμίζουν την προστασία προσωπικών δεδομένων δεν έχουν σκοπό να καταστούν τροχοπέδη στο διαδικτυακό κόσμο, παρά να ενθαρρύνουν τις επιχειρήσεις σε πιο ηθικές και ειλικρινείς στρατηγικές του digital advertising. Κάθε επιχείρηση ή οργανισμός που ασχολείται με την ψηφιακή διαφήμιση πρέπει να τηρεί και να συμμορφώνεται με τις νομοθετικές διατάξεις των νομοθετημάτων αναφορικά με την προστασία προσωπικών δεδομένων.

Ωστόσο, δεδομένου ότι ο τομέας του digital advertising είναι ένας χώρος με συνεχείς και ιδιαίτερες προκλήσεις και με διαρκώς αναδυόμενες πτυχές, καθώς τα τεχνολογικά και λογισμικά εργαλεία που διαθέτει διαρκώς αναπτύσσονται και εξελίσσονται, είναι ιδιαίτερος κρίσιμο τα νομοθετήματα που ρυθμίζουν την προστασία των προσωπικών δεδομένων να επικαιροποιούνται συνεχώς από το νομοθέτη, προκειμένου οι διατάξεις τους να είναι αποτελεσματικές και ικανές να προστατεύσουν τους χρήστες και σε κάθε περίπτωση το ρυθμιστικό τους πεδίο να ανταποκρίνεται επαρκώς σε οποιαδήποτε ανάπτυξη σημειώνεται στον εν λόγω τομέα.

## ΠΑΡΑΡΤΗΜΑ ΒΙΒΛΙΟΓΡΑΦΙΚΩΝ ΑΝΑΦΟΡΩΝ

Clearcode (χ.χ.), *The AdTech Book*. Διαθέσιμο σε: <https://adtechbook.clearcode.cc/introduction/>, ανακτήθηκε 07.01.2022.

Michael Chibuzor (χ.χ.), *Digital Advertising Vs. Digital Marketing – What’s the Difference?*. Διαθέσιμο σε: <https://fabrikbrands.com/digital-advertising-vs-digital-marketing-whats-difference/>, ανακτήθηκε την 07.01.2022.

Amazon Europe. (χ.χ.), *What is adtech and why is it important?*. Διαθέσιμο σε: <https://advertising.amazon.com/library/guides/what-is-adtech>. ανακτήθηκε 05.01.2022.

IAB Europe (χ.χ.). Διαθέσιμο σε: <https://iabeurope.eu>, ανακτήθηκε 04.01.2022.

IAB Hellas (χ.χ.), *Digital Advertising Guide*. Διαθέσιμο σε: <https://www.iab.gr/digital-advertising-guide>, ανακτήθηκε 04.01.2022.

IAB, Europe (χ.χ.), *Digital Services Act*. Διαθέσιμο στο: <https://iabeurope.eu/digital-services-act/>, ανακτήθηκε την 15 Μάρτιος 2022.

Kim W. και White L (2022), *Belgian DPA fines IAB Europe over its consent framework’s GDPR violations*, (2022, Φεβρουάριος), Διαθέσιμο σε: <https://www.dataprotectionreport.com/2022/02/belgian-dpa-fines-iab-europe-over-its-consent-frameworks-gdpr-violations/>, ανακτήθηκε την 7.4.2022.

Crepax, T. et al. (2022) *‘Information technologies exposing children to privacy risks: Domains and children-specific technical controls’*, *Computer Standards and Interfaces*, 82(January).

European Commission (2022) *‘The Digital Services Act: ensuring a safe and accountable online environment’*. Διαθέσιμο στο: [https://ec.europa.eu/info/digital-services-act-ensuring-safe-and-accountable-online-environment\\_en](https://ec.europa.eu/info/digital-services-act-ensuring-safe-and-accountable-online-environment_en), ανακτήθηκε την 6.4.2022.

European Commission (2022) *‘The Digital Services Act package’*. Διαθέσιμο στο: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>, ανακτήθηκε την 6.4.2022.

MEYER DAVID (2022) *‘European lawmakers vote to ban online advertising based on sensitive information like sexuality and political orientation’*, *FORTUNE*. Διαθέσιμο στο: <https://fortune.com/2022/01/20/surveillance-capitalism-targeted-ads-digital-services-act-dsa-amendments-european-parliament/>, ανακτήθηκε την 6.4.2022.

Press Releases (2022) *‘Digital Services Act: regulating platforms for a safer online space for users’*, *European*

Parliament. Διαθέσιμο στο: <https://www.europarl.europa.eu/news/en/press-room/20220114IPR21017/digital-services-act-regulating-platforms-for-a-safer-online-space-for-users>, ανακτήθηκε την 6.4.2022.

Toreini Ehsan Mehrmezhad Maryam, Coopamootoo Kovila, 'How Can and Would People Protect From Online Tracking?', *Sciento*, 2022, 105–25.

Aiolfi, S., Bellini, S. και Pellegrini, D. (2021) 'Data-driven digital advertising: benefits and risks of online behavioral advertising', *International Journal of Retail and Distribution Management*, 49(7), σσ 1089–1110.

Fourberg, N. et al. (2021), *Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice*.

European Parliament. Luxembourg (2021, Ιούνιος). Διαθέσιμο σε: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662913/IPOL\\_STU\(2021\)662913\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662913/IPOL_STU(2021)662913_EN.pdf).

Cristiana Santos, Midas Nouwens, Michael Toth, Nataliia Bielova, Vincent Roca (2021), *Consent Management Platforms under the GDPR: processors and/or controllers?*, Proceedings of the 9th Annual Privacy Forum (APF), (2021, Ιούνιος), Oslo, Norway. pp.47-69, 10.1007/978-3-030-76663-4\_3. hal-03169436

Βαρλά, Α. (2021), *The ePrivacy Saga: το χρονικό για την ψήφιση ενός κανονισμού*, (2021, Ιούνιος 16). Διαθέσιμο σε: <https://lawyermagazine.gr/the-eprivacy-saga-to-xroniko-gia-thn-psifisi-enos-kanonismou/>, ανακτήθηκε 20.02.2022

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021), *Κατευθυντήριες γραμμές 8/2020 σχετικά με τη στόχευση χρηστών μέσω κοινωνικής δικτύωσης*, Έκδοση 2.0, (2021, Απρίλιος 3), Διαθέσιμο σε: [https://edpb.europa.eu/system/files/2021-11/edpb\\_guidelines\\_082020\\_on\\_the\\_targeting\\_of\\_social\\_media\\_users\\_el\\_0.pdf](https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_el_0.pdf), ανακτήθηκε την 20.4.2022.

Η *Homo Digitalis* καταθέτει καταγγελία κατά της Google και της IAB Europe για τις επιβλαβείς πρακτικές συμπεριφορικής διαφήμισης, (2020, Δεκέμβριος 10). Διαθέσιμο σε: <https://www.homodigitalis.gr/posts/8137>, ανακτήθηκε 07.4.2022.

Η αριθ. Πρωτ. 8478/10-12-2020 καταγγελία της *Homo Digitalis* κατά της Google και του IAB Europe σχετικά με τις πρακτικές επεξεργασίας προσωπικών δεδομένων στο πλαίσιο του RTB, (2020,

Δεκέμβριος 10). Διαθέσιμο σε: [https://www.homodigitalis.gr/wp-content/uploads/2020/12/HomoDigitalis\\_κατά\\_Google\\_IABEurope\\_Censored.pdf](https://www.homodigitalis.gr/wp-content/uploads/2020/12/HomoDigitalis_κατά_Google_IABEurope_Censored.pdf), ανακτήθηκε 07.4.2022.

Ιγγλεζάκης, Ι. (2021). Δίκαιο Πληροφορικής, Δ' έκδοση, Αθήνα- Θεσσαλονίκη: Εκδ. Σάκκουλα  
Καρκατζούνης, Β./ Σκόνδρα Μ. (2020), *Cookies και παρακολούθηση χρηστών στο διαδίκτυο: Γιατί οι οδηγίες της ΑΠΔΠΧ κινούνται στη σωστή κατεύθυνση*, (2020, Απρίλιος 10). Διαθέσιμο σε [https://www.lawspot.gr/nomika-blogs/magdalini\\_skondra/cookies-kai-parakoloythisi-hriston-sto-diadiktyo-giati-oi-odigies-tis](https://www.lawspot.gr/nomika-blogs/magdalini_skondra/cookies-kai-parakoloythisi-hriston-sto-diadiktyo-giati-oi-odigies-tis), ανακτήθηκε 07.4.2022

ΑΠΔΠΧ (2020), *Συστάσεις για τη συμμόρφωση υπευθύνων επεξεργασίας δεδομένων με την ειδική νομοθεσία για τις ηλεκτρονικές επικοινωνίες*, (2020, Φεβρουάριος 25). Διαθέσιμο σε <https://www.dpa.gr/el/enimerwtiko/deltia/systaseis-gia-ti-symmorfosi-ypeythynon-epexergasias-dedomenon-me-tin-eidiki>, ανακτήθηκε 07.04.2022.

Consumer Council of Norway (2020), *Out of control - How consumers are exploited by the online advertising industry*, (2020, Ιανουάριος 14). Διαθέσιμο σε: <https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>, ανακτήθηκε 07.04.2022

Geradin και Katsifis (2020), *Online platforms and digital advertising: Market study final report*, SSRN Electronic Journal, (Market Study Final Report), (2020, Ιούλιος 1) pp. 1–437. Διαθέσιμο σε: [https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final\\_report\\_Digital\\_AL\\_T\\_TEXT.pdf](https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_AL_T_TEXT.pdf), ανακτήθηκε 07.01.2022.

Καρκατζούνης, Β./Μήτρου, Λ. (2020), *Online διαφήμιση και προστασία προσωπικών δεδομένων*, ΔιΜΕΕ, 1/2020, pp. 5–16.

Κανέλλος, Λ. (2020), *The GDPR Handbook, Για DPOs, Επιχειρήσεις & Οργανισμούς*, Αθήνα: Νομική Βιβλιοθήκη.

European Data Protection Board (2020) *Κατευθυντήριες γραμμές 5 / 2020 σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016 / 679*, σσ 1–40.

Radesky, J. et al. (2020) *'Digital advertising to children'*, *Pediatrics*, 146(1), σσ 1–8.

Παπακωνσταντίνου, Σ. (2020) *'Η προστασία των προσωπικών δεδομένων των παιδιών σε ψηφιακό περιβάλλον με βάση τον Κανονισμό 2016/679'*, *Επιθεώρηση Δικαίου Πληροφορικής*, 2. Διαθέσιμο στο: <http://ejournals.lib.auth.gr/infolawj/%0AH>.



Dr Gurudutta P Japee (2019), *Digital Marketing*. New Delhi: Authorspress.

Μπούκη, Α. (2019), *Τι είναι οι data brokers και πως εκμεταλλεύονται τα προσωπικά δεδομένα των καταναλωτών*, Διαθέσιμο σε: <https://www.capital.gr/me-apopsi/3377427/ti-einai-oi-data-brokers-kai-pos-ekmetalleuontai-ta-prosopika-dedomena-ton-katanaloton>, ανακτήθηκε 04.01.2022.

Worledge, M. and Bamford, M. (2019), *Adtech Market Research Report*. Διαθέσιμο σε: <https://ico.org.uk/media/about-theico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf>, ανακτήθηκε 07.01.2022.

Information Commissioner's Office (2019), *Update report into adtech and real time bidding*. Διαθέσιμο σε: <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf>, ανακτήθηκε 07.01.2022.

Utz, C./Degeling, M./Fahl, S./ Schaub, F./Holz, T. (2019), *(Un)informed Consent: Studying GDPR Consent Notices in the Field*, University of Michigan/Ruhr-Universität Bochum, Διαθέσιμο σε: <https://arxiv.org/pdf/1909.02638.pdf>, ανακτήθηκε 07.04.2022

Privacy International (2019), "Why am I really seeing that ad? The answer might be Real Time Bidding (RTB)", (2019, Μάιος 21). Available at: <https://privacyinternational.org/explainer/2974/why-am-i-really-seeing-ad-answer-07might-be-real-time-bidding-rtb>, ανακτήθηκε την 07.04.2022.

EDRi, (2019), *Real Time Bidding: The auction for your attention*, (2019, Ιούλιος 4). Διαθέσιμο σε: <https://edri.org/our-work/real-time-bidding-the-auction-for-your-attention/>, ανακτήθηκε 07.04.2022.

Geradin, D. και Katsifis, D. (2019) 'An EU competition law analysis of online display advertising in the programmatic age', *European Competition Journal*, 15(1), σσ 55–96.

Wachter, S. (2019) 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising', *SSRN Electronic Journal*, σσ 380–385.

Tobias Urban κ.λ., «Μια μελέτη σχετικά με την πρόσβαση των δεδομένων σε θέματα στην ηλεκτρονική διαφήμιση μετά τον ΓΚΠΔ», Σημειώσεις διάλεξης στην Επιστήμη των Υπολογιστών (συμπεριλαμβανομένων των υποσημειωμένων Σημειώσεων Διαλέξεων τεχνητής νοημοσύνης και σημειώσεων διαλέξεων στη Βιοπληροφορική), 11737 LNCS. Σεπτέμβριος (2019), 61-79.

ΑΠΔΠΧ, 11/2019 Απόφαση, 10.05.2019, διαθέσιμο σε <https://www.dpa.gr/sites/default/files/2019->

[09/apofasi112019.pdf](#), ανακτήθηκε 20.02.2022.

Mahalakshmi, R. και Rajasekaran, D. (2018), *Customers Perception on Online Advertising*, International Journal of Computational Research and Development, (January 2018), pp. 1–6. doi: 10.5281/zenodo.1224470.

European Commission (2018), *Consumer market study on online market segmentation through personalised pricing*, Διαθέσιμο σε: [http://ec.europa.eu/dgs/communication/services/visual\\_identity/pdf/guidelines-studies-publications-by-](http://ec.europa.eu/dgs/communication/services/visual_identity/pdf/guidelines-studies-publications-by-), ανακτήθηκε 07.01.2022.

*Online διαφήμιση και προσωπικά δεδομένα: Μία σημαντική απόφαση για το μέλλον του Ad Tech από την CNIL*, (2018, Νοέμβριος 22), Διαθέσιμο σε <https://www.lawspot.gr/nomika-nea/online-diafimisi-kai-prosopika-dedomena-mia-simantiki-apofasi-gia-mellon-toy-ad-tech-apo>, ανακτήθηκε την 7.4.2022

Kapur S και Savare M (2018), *The Vectaury decision is not an obituary for digital advertising*, (2018, Δεκέμβριος 13), Διαθέσιμο σε: <https://iapp.org/news/a/the-vectaury-decision-is-not-an-obituary-for-digital-advertising/>, ανακτήθηκε την 7.4.2022.

IAB Europe (2018), *The CNIL's VECTAURY Decision and the IAB Europe Transparency & Consent Framework*, (2018, Νοέμβριος 21). Διαθέσιμο σε <https://iabeurope.eu/all-news/the-cnils-vectaury-decision-and-the-iab-europe-transparency-consent-framework/>, ανακτήθηκε την 7.4.2022.

Speicher, T. et al. (2018), *Potential for Discrimination in Online Targeted Advertising*, Proceedings of Machine Learning Research, 81, pp. 1–15. Διαθέσιμο σε: <https://business.linkedin.com/marketing->, ανακτήθηκε την 20.4.2022.

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2018), *Δήλωση του ΕΣΠΔ σχετικά με τις επιπτώσεις της οικονομικής συγκέντρωσης στην προστασία των δεδομένων*. Διαθέσιμο σε: [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_statement\\_economic\\_concentration\\_el\\_0.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_economic_concentration_el_0.pdf), ανακτήθηκε την 20.4.2022.

Privacy International (2018) *'Submission to the Information Commissioner - Request for an assessment notice / Complaint of Adtech Data Brokers Criteo, Quantcast and Tapad'*.

Party, A. 29 W. (2018) *'Guidelines on transparency under Regulation 2016/679'*, σ 22.

Clifford, D. και Verdoodt, V. (2017) *'Integrative advertising: the marketing 'dark side' or merely the*

*emperor's new clothes?*, *European Journal of Law and Technology*, 8(1), σσ 1–43.

ENISA EU (2017), *Online Tracking and User Protection Mechanisms*, European Network and Information Security Agency (ENISA), Διαθέσιμο σε: <file:///C:/Users/user/Downloads/WP2017%20O-2-2-1%20Do%20Not%20Track%20Methods%20and%20Techniques.pdf> , ανακτήθηκε 07.01.2022.

McStay, A. (2017), *3.1 Micro-Moments, Liquidity, Intimacy and Automation: Developments in Programmatic Ad-tech*, *Commercial Communication in the Digital Age*, (January), pp. 143–160. doi: 10.1515/9783110416794-009.

Chen, G. et al. (2016), *'In-depth survey of digital advertising technologies'*, *IEEE Communications Surveys and Tutorials*, 18(3), pp. 2124–2148. doi: 10.1109/COMST.2016.2519912.

ΑΠΔΠΧ (2016) *'ΑΠΟΦΑΣΗ ΑΡ. 78/2016'*, σσ 5–8.

Data Protection Working Party (2015), *Cookie Sweep Combined Analysis – Report*. Διαθέσιμο σε: <https://ec.europa.eu/newsroom/article29/items/640605/en> , ανακτήθηκε 07.04.2022.

Goldfarb, A. (2014) *'What is Different About Online Advertising?'*, *Review of Industrial Organization*, 44(2), σσ 115–129. doi: 10.1007/s11151-013-9399-3.

Kramer, A. D. I., Guillory, J. E. και Hancock, J. T. (2014), *Experimental evidence of massive-scale emotional contagion through social networks*, *Proceedings of the National Academy of Sciences of the United States of America*, 111(24), pp. 8788–8790.

Ιγγλεζάκης, Ι. (2014). *Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του*, Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα

ENISA EU (2012), *Privacy considerations of online behavioural tracking*, European Network and Information Security Agency (ENISA), Διαθέσιμο σε: <https://www.enisa.europa.eu/publications/privacy-considerations-of-online-behavioural-tracking> , ανακτήθηκε 07.01.2022.

Solove, Daniel J. (2011), *Nothing to Hide: The False Tradeoff between Privacy and Security*, GWU Law School Public Law Research Paper No. 571.

Kahl, C. et al. (2011), *Privacy respecting targeted advertising for social networks*, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6633 LNCS, pp. 361–370. doi: 10.1007/978-3-642-21040-2\_26.

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2011) *Οδηγία 2/2011 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σχετικά με την ηλεκτρονική συγκατάθεση στο πλαίσιο του άρθρου 11*. Διαθέσιμο στο: <https://www.dpa.gr/el/enimerwtiko/deltia/odigia-22011-tis-arhis-prostasias-dedomenon-prosopikoy-haraktira-shetika-me-tin>, ανακτήθηκε 8.3.2022.

Data Protection Working Party (2010), *Opinion 2/2010 on online behavioural advertising*, European Commission. Διαθέσιμο σε: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf), ανακτήθηκε 07.01.2022.

Data Protection Working Party (2011), *Γνώμη 16/2011 σχετικά με τη σύσταση βέλτιστων πρακτικών EASA/IAB για την επιγραμμική συμπεριφορική διαφήμιση*, 4(1), σσ 1–23.

Thompson D. (2010), *“Google’s CEO: ‘The Laws Are Written by Lobbyists’”*, Διαθέσιμο σε: <https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/>, ανακτήθηκε 07.04.2022

Soltani, Ashkan, Canty, Shannon, Mayo, Quentin, Thomas, Lauren and Hoofnagle, Chris Jay (2009), *Flash Cookies and Privacy*. Διαθέσιμο μέσω του SSRN στο δικτυακό τόπο <http://ssrn.com/abstract=1446862>, ανακτήθηκε 07.04.2022.

Αλεξανδροπούλου- Αιγυπτιάδου Ε. 2007). *Η πλοήγηση ανηλίκων στο Διαδίκτυο και η νομική προστασία των προσωπικών δεδομένων*, Αρμ 2007, σελ. 849-851.