ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΕΥΡΩΠΑΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ – ΔΙΟΙΚΗΣΗ ΟΛΙΚΗΣ ΠΟΙΟΤΗΤΑΣ

Διπλωματική Εργασία
«Ζητήματα λόγω της εκμετάλλευσης προσωπικών δεδομένων»

Όνομα: Ζάννη Αγγελική
Α.Μ.: ΜΔΕ-ΟΠ1706

Επιβλέπουσα Καθηγήτρια: κα Κ. Δελούκα-Ιγγλέση

Πειραιάς, 2019

ΠΑΡΑΡΤΗΜΑ Δ : **ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ** **ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ**

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

Μεταπτυχιακό Πρόγραμμα Σπουδών

στη «Διοίκηση Επιχειρήσεων – Ολική Ποιότητα» με διεθνή προσανατολισμό

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

(περιλαμβάνεται ως ξεχωριστή [δεύτερη] σελίδα στο σώμα της διπλωματικής εργασίας)

Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών, του Πανεπιστημίου Πειραιώς, στη Διοίκηση Επιχειρήσεων - Ολική Ποιότητα με διεθνή προσανατολισμό με τίτλο:

"ΖΗΤΗΜΑΤΑ ΛΟΓΩ ΤΗΣ ΕΚΜΕΤΑΛΛΕΥΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ"

έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

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

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

Υπογραφή Μεταπτυχιακού Φοιτητή/ τριας .....

Ονοματεπώνυμο ΖΑΝΝΗ ΑΓΓΕΛΙΚΗ

Ημερομηνία 22/7/2019

Πρόλογος

Τα ανθρώπινα δικαιώματα έχουν δυναμικό χαρακτήρα και εξελίσσονται συνεχώς, γεγονός που οφείλεται στη διαρκώς μεταβαλλόμενη κοινωνική πραγματικότητα, καθώς και στη σύνδεση τους με τους ταχύτατους ρυθμούς της τεχνολογικής εξέλιξης. Η εμφάνιση νέων μέσων επικοινωνίας (μέσα κοινωνικής δικτύωσης, smartphones) και η επέκταση της χρήσης τους οδηγούν στην «αποκρυστάλλωση» νέων δικαιωμάτων (πχ το δικαίωμα προστασίας προσωπικών δεδομένων ανήκει στη λεγόμενη τρίτη γενιά δικαιωμάτων), ταυτόχρονα όμως «εγκυμονούν» πολλαπλούς κινδύνους για την καταστρατήγηση τους. Η συγκεκριμένη σκέψη αποτέλεσε το έναυσμα του ερευνητικού μου προβληματισμού για τη διερεύνηση του νέου Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (GDPR). Αναμφισβήτητα, ήδη από τη θέσπιση του έχουν εκπονηθεί πολυάριθμες έρευνες με αντικείμενο τον νέο Κανονισμό. Ωστόσο, κατά την άποψη μου η πρωτοτυπία της παρούσας διπλωματικής έγκειται στο ότι επιχειρεί μία διεπιστημονική ανάλυση του GDPR, εν αντιθέσει με τις έρευνες που έχουν προηγηθεί έως τώρα, οι οποίες στην πλειοψηφία τους έχουν αμιγώς νομικό χαρακτήρα.

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω την Καθηγήτρια μου κα. Κ. Δελούκα Ιγγλέση, η οποία με τη διδασκαλία και την καθοδήγηση της μου παρείχε τα απαραίτητα γνωστικά εφόδια για την εκπόνηση της ανά χείρας μελέτης.

Πίνακας Περιεχομένων

Συντομογραφίες

GDPR:	General Data Protection Regulation
απ.:	απόφαση
ΑΠΔΠΧ:	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Βλ.:	Βλέπε
ΓΚΠΔ:	Γενικός Κανονισμός Προστασίας Δεδομένων
ΔΕΚ-ΔΕΕ:	Δικαστήριο της Ευρωπαϊκής Ένωσης
ΕΔΔΑ:	Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου
ΕΕ:	Ευρωπαϊκή Ένωση
ΕΕΠΔ-EDPS:	Ευρωπαίος Επόπτης Προστασίας Δεδομένων-European Data Protection Supervisor
ΕΚ:	Ευρωπαϊκό Κοινοβούλιο
Εκδ.:	Εκδόσεις
ΕΟΚ:	Ευρωπαϊκή Οικονομική Κοινότητα
επ.:	επόμενα
ΕΣΔΑ:	Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου
ΕΣΠΔ:	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
ν.:	νόμος
Ολ.:	Ολομέλεια
ΟΟΣΑ:	Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη
όπ.π.:	όπου παραπάνω
Πρβλ.:	Παράβαλε
σ.:	σελίδα
Σ:	Σύνταγμα
ΣΛΕΕ:	Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης

Περίληψη

Η πληθώρα ευρωπαϊκών νομοθετημάτων για την προστασία των προσωπικών δεδομένων των Ευρωπαίων πολιτών που προηγήθηκαν χρονικά του Γενικού Κανονισμού ΕΕ 2016/679 για την προστασία των προσωπικών δεδομένων, γνωστού ως GDPR (General Data Protection Regulation), αναδεικνύει δύο βασικές δυσχέρειες: Εν πρώτοις, αναδεικνύει τη δυσκολία που παρουσιάζει η επαρκής ρύθμιση της προστασίας των προσωπικών δεδομένων, λόγω της άμεσης συνάρτησης του συγκεκριμένου δικαιώματος με τις ραγδαίες τεχνολογικές εξελίξεις (συνεχής ανάπτυξη νέων «εφαρμογών», smarthphones κ.τ.λ.), οι οποίες σε ταχύτατα χρονικά διαστήματα καθιστούν τις προηγούμενες ρυθμίσεις παρωχημένες. Δευτερευόντως, αναδεικνύει τη δυσκολία εφαρμογής ενός ενιαίου κανονιστικού πλαισίου σε όλες τις χώρες της ΕΕ, λόγω της ανομοιόμορφης τεχνολογικής ανάπτυξης και της ασύμμετρης εφαρμογής των παλαιότερων σχετικών Οδηγιών από τα κράτη μέλη. Η επιλογή της μορφής της νέας ρύθμισης (Κανονισμός που έχει άμεση και υποχρεωτική εφαρμογή έναντι της παλαιότερης Οδηγίας) είναι ενδεικτική της πρόθεσης της ΕΕ να διαδραματίσει έναν πιο κομβικό ρόλο στη ρύθμιση της προστασίας των προσωπικών δεδομένων στα ευρωπαϊκά κράτη. Ωστόσο, εκτός από την ύπαρξη λιγοστών σημαντικών νέων προβλέψεων (όπως πχ η σύσταση του Ευρωπαϊκού Συμβουλίου για την προστασία των προσωπικών δεδομένων), ο GDPR εν πολλοίς «συστηματοποιεί» σε ενιαίο κείμενο ρυθμίσεις που είτε υπήρχαν διάσπαρτες σε υπερνομοθετικά κείμενα, είτε είχαν ήδη συναχθεί από τη διαπλαστική ερμηνεία των Αρχών και των Δικαστηρίων. Αποδεικνύεται λοιπόν ότι η προστασία των προσωπικών δεδομένων δεν διασφαλίζεται μόνο από την πρόβλεψη αυστηρών κανονιστικών ρυθμίσεων, αλλά πρωτίστως από την ενίσχυση των μηχανισμών που εξασφαλίζουν την εφαρμογή τους.

Στο πρώτο κεφάλαιο της εργασίας επιχειρείται η εννοιολογική και νομική προσέγγιση των προσωπικών δεδομένων και της επεξεργασίας τους και στο κεφάλαιο 2 επιδιώκεται η εξέταση της ιστορικής εξέλιξης της κατοχύρωσης του δικαιώματος της προστασίας των προσωπικών δεδομένων στο παράγωγο ενωσιακό δίκαιο πριν από τον GDPR. Επιπροσθέτως, στο κεφάλαιο 3 παρουσιάζονται οι συνθήκες που οδήγησαν στη θέσπιση του νέου Κανονισμού, ενώ στο κεφάλαιο 4 γίνεται η ανάλυση των βασικών διατάξεων του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων. Τέλος, στο κεφάλαιο 5 αναλύονται οι προβλέψεις του Κανονισμού για τις Ανεξάρτητες Αρχές που είναι επιφορτισμένες με την παρακολούθηση της εφαρμογής του, στο κεφάλαιο 6 αναλύεται η έννοια της στοχευμένης διαφήμισης και παρουσιάζονται προβεβλημένες υποθέσεις εκμετάλλευσης προσωπικών δεδομένων.

Τέλος, στο 7ο και τελευταίο κεφάλαιο πραγματοποιείται μία εκτενής επισκόπιση όλης της διπλωματικής εργασίας και παρουσιάζονται τα συμπεράσματα της μελέτης.

Λέξεις-Κλειδιά: Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR), Ευρωπαϊκή Ένωση, Οδηγία 95/46/ΕΚ, Ευρωπαίος Επόπτης Προστασίας Δεδομένων

Abstract

The numerous European laws for data protection that preceded the GDPR reveal two main difficulties. First of all, it highlights the difficulty of adequately regulating the protection of personal data, due to the connection of them with the rapid technological developments, which rapidly make the previous regulations obsolete. Secondly, it highlights the difficulty of implementing a single regulatory framework in all EU countries due to the uneven technological development and the asymmetrical application of the older directives by the Member States. The choice of the form of the new European law (a regulation istead of the earlier directive) is indicative of the EU's intention to play a more crucial role in securing the protection of personal data in the European states. However, in addition to the existence of few significant new provisions (such as the European Council on the Protection of Personal Data), the GDPR systematizes in a single text provisions that either were scattered in supranational laws and conventions or were already deduced from the interpretation of the Authorities and Courts. Therefore, it's proved that the protection of personal data is not guaranteed only by the adoption of strict regulations but, above all, by the reinforcement of the mechanisms that ensure their implementetion.

The first chapter of this research paper presents a conceptual and legal approach of personal data and its processing, and the second chapter seeks to examine the historical evolution of the right to the protection of personal data in secondary EU law prior to GDPR. Additionally, the third chapter presents the conditions that led to the adoption of the new Regulation, while the fourth chapter analyzes the basic provisions of the GDPR. Finally, chapter 5 analyzes the provisions of the Regulation on Independent Authorities responsible for monitoring its implementation, chapter 6 analyzes the concept of targeted advertising and presents prominent cases of exploitation of personal data and Chapter 7 presents the conclusions of the research.

Key-Words: General Data Protection Regulation, European Union, Directive 95/46/EC, European Data Protection Supervisor

Εισαγωγή

Όσο εκτεταμένη τυγχάνει πλέον η χρήση του Διαδικτύου στην εποχή μας, άλλο τόσο αυξάνονται και οι κίνδυνοι που διατρέχουν οι χρήστες του για παραβίαση των προσωπικών τους δεδομένων. Η ταχύτατη τεχνολογική εξέλιξη έχει συμβάλει στην «αποκρυστάλλωση» μίας νέας κατηγορίας δικαιωμάτων[1] και ειδικότερα του δικαιώματος της πληροφοριακής αυτοδιάθεσης και της προστασίας των προσωπικών δεδομένων από την αθέμιτη επεξεργασία, η οποία επιτάσσει την επαρκή ενημέρωση των υποκειμένων για τον τρόπο συλλογής και επεξεργασίας των προσωπικών τους δεδομένων στους διαδικτυακούς ιστοτόπους που επισκέπτονται.

Επομένως, εκ πρώτης όψεως, φαίνεται πως η ανάπτυξη των αντίστοιχων θεσμικών κειμένων, δηλαδή ευρωπαϊκών[2] και εθνικών νομοθετικών πράξεων[3], καθιστά τους πολίτες απόλυτους κυρίαρχους των προσωπικών τους δεδομένων. Είναι όμως επαρκής και αποτελεσματική η ανάπτυξη πολιτικής απορρήτου, όταν οι χρήστες στην πλειοψηφία τους ενδέχεται να μην την διαβάσουν και να μην ενημερωθούν καν για τα δικαιώματα τους; Είναι ενδεικτική πρόσφατη έρευνα σύμφωνα με την οποία το 74% των χρηστών του διαδικτύου δεν διαβάζουν καν την πολιτική απορρήτου[4].

Ειδικότερα, όταν οι χρήστες υποχρεώνονται από τους ιστοτόπους να διαβάζουν και να αποδέχονται μακροσκελή νομικά κείμενα στα οποία περιγράφεται η πολιτική απορρήτου που ακολουθούν, συχνά αποθαρρύνονται και καταβάλλονται επειδή το κείμενο είναι υπερβολικά μεγάλο ή δυσνόητο[5]. Πράγματι, οι χρήστες συχνά λαμβάνουν υπερβολικά πολλές πληροφορίες για την προστασία της ιδιωτικότητάς τους[6] με αποτέλεσμα να μην έχουν καν το χρόνο να τις διαβάσουν, ενόσω, αρκετές

---

[1] Πρβλ. Σ. Βλαχόπουλος, «Θεμελιώδη Δικαιώματα», Εκδ. Νομική Βιβλιοθήκη, 2016, σ. 5-8 Η νέα κατηγορία δικαιωμάτων αποτελεί τη λεγόμενη «τρίτη γενιά δικαιωμάτων» που περιλαμβάνει μεταξύ άλλων το δικαίωμα προστασίας του περιβάλλοντος κτλ.

[2] Βλ. ενδεικτικά Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ 1995, L 281, σ 31), Κανονισμό (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ 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, κτλ.

[3] Βλ. πχ ν. 2496/1997

[4] Βλ. J. Obar & A. Oeldorf-Hirsch, «The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services», York University, 2018, Διαθέσιμο σε: https://poseidon01.ssrn.com/delivery.php?ID=191017121025029007091077081094122117118011008021008010118087102004104064108069078105024021120009040036108011075127126120123087110055007050032012065067106075122007000020073086087127121111000093124119002024112020064064085103070096000019088010088073026&EXT=pdf

[5] Βλ. J. Reidenberg et al., «Ambiguity in Privacy Policies and the Impact of Regulation», σε: *Journal of Legal Studies*, v. 45, 2015, σ. 3, Διαθέσιμο σε: http://www.cs.cornell.edu/~shmat/courses/cs5436/reidenberg.pdf

[6] Βλ. L. Anderson, (2014): «The effects of interannual climate variability on the moraine record», σε: *Geology,* v. 42(1), 2014, σ. 55-58

φορές δεν γνωρίζουν τις ακριβείς ενέργειες που πρέπει να κάνουν για να διασφαλίσουν την προστασία των δεδομένων τους.

Συνεπώς, οι Οδηγίες προσβασιμότητας περιεχομένου ιστού θα πρέπει να είναι εύληπτες, λειτουργικές και κατανοητές, γεγονός που δεν φαίνεται να συμβαίνει στην πραγματικότητα. Το γεγονός αυτό μειώνει την αποτελεσματικότητα των ειδοποιήσεων και «εκθέτει» τους χρήστες στον κίνδυνο να πραγματοποιούν εν αγνοία τους ενέργειες που θέτουν σε κίνδυνο την ιδιωτική τους ζωή.

Η έλευση του GDPR προσθέτει ένα ακόμη επίπεδο πολυπλοκότητας στο σχεδιασμό των πολιτικών απορρήτου. Πιο συγκεκριμένα, η καθοδήγηση που παρέχεται από το Γραφείο του Επιτρόπου Πληροφοριών υπογραμμίζει τη σημασία της κοινοποίησης των απαραίτητων πληροφοριών σχετικά με την προστασία της ιδιωτικής ζωής στους ενδιαφερόμενους και την «ευαισθητοποίηση» σχετικά με τον αντίκτυπο του τρόπου με τον οποίο ο οργανισμός εφαρμόζει τις απαιτήσεις του GDPR.

Επιπλέον, ο Κανονισμός GDPR απαιτεί οι πολιτικές απορρήτου να παραδίδουν το μήνυμά τους αποτελεσματικά, αποδοτικά και με χρήσιμο τρόπο. Οι συγκεκριμένες μέθοδοι χρηστικότητας επιδιώκουν να κάνουν τις πολιτικές να μοιάζουν λιγότερο με νομικά κείμενα, τα οποία είναι συνήθως διατυπωμένα με εξαιρετικά «νομικίστικο» τρόπο, ώστε να εξασφαλίσουν ότι οι απλοί χρήστες θα είναι σε θέση να τα κατανοήσουν. Εξάλλου, η εξειδικευμένη νομική ορολογία εμποδίζει την κατανόηση των ειδοποιήσεων από τους χρήστες υπολογιστών.

Εκ των ανωτέρω λοιπόν συνάγεται πόσο αναγκαία είναι η διερεύνηση του νέου Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων, προκειμένου να εξεταστεί κατά πόσον η εν λόγω ρύθμιση ανταποκρίνεται στο αίτημα της αποτελεσματικής προστασίας των δεδομένων και στην παροχή ενός εύληπτου κειμένου που να ενημερώνει επαρκώς τους χρήστες για τα δικαιώματα τους. Κατά συνέπεια, αναδεικνύεται και το επιστημονικό ενδιαφέρον της ανά χείρας μελέτης, η οποία έχει ως σκοπό την ανάλυση του νέου Γενικού Κανονισμού Προσωπικών Δεδομένων, προκειμένου να αναδειχθεί αν πρόκειται πράγματι για μία ρύθμιση που συμβάλλει στην ενίσχυση της προστασίας των προσωπικών δεδομένων, ή αν πρόκειται για απλά μία ακόμη ευρωπαϊκή ρύθμιση που απλώς συστηματοποιεί και εμπλουτίζει τις ήδη υπάρχουσες ρυθμίσεις. Η πρωτοτυπία της έρευνας έγκειται, θεωρώ, στο ότι ενώ οι περισσότερες έρευνες που έχουν διεξαχθεί μέχρι στιγμής με αυτό το θέμα έχουν αμιγώς νομικό χαρακτήρα, η παρούσα διπλωματική επιχειρεί μία πιο διεπιστημονική προσέγγιση του GDPR.

Κεφάλαιο 1: Εννοιολογική και θεσμική θεώρηση των προσωπικών δεδομένων

Είναι σαφές ότι ο σεβασμός και η προστασία της ιδιωτικής ζωής, της αυτονομίας της ιδιωτικής βουλήσεως και της ανάπτυξης της προσωπικότητας αποτελούν ένα από τους σημαντικότερους σκοπούς κάθε δημοκρατικής κοινωνίας. Θα πρέπει να επισημάνουμε ότι[7], η Ευρωπαϊκή Επιτροπή είχε υποβάλει ήδη από το 1990 μια πρόταση Οδηγίας προκειμένου να επιτευχθεί η εναρμόνιση των εθνικών νομοθεσιών των κρατών – μελών σχετικά με την προστασία των προσωπικών δεδομένων. Μετά μια τετραετή διαπραγμάτευση, την 22η.10.1995, θεσπίστηκε η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», η οποία ενσωματώθηκε στην εθνική έννομη τάξη μας με τον Ν. 2472/1997. Ετσι, η ΕΕ κατάφερε, μέσα από μια μακρά εξελικτική πορεία να κατοχυρώσει το δικαίωμα προστασίας από την αθέμιτη επεξεργασία των προσωπικών δεδομένων των φυσικών προσώπων.

Ωστόσο, η προστασία αυτή, στην πορεία του χρόνου, ιδίως κάτω από την πίεση των νέων τεχνολογιών δημιουργήσαν νέες προκλήσεις και νέους κινδύνους για τα δεδομένα προσωπικού χαρακτήρα των ατόμων. Κρίθηκε λοιπόν απαραίτητος ο εκσυγχρονισμός της Οδηγίας 95/46/ΕΚ και η μεταρρύθμισή της σε ένα γενικό Κανονισμό. Έτσι, στις 6 Απριλίου 2016, ψηφίστηκε ο Γενικός Κανονισμός για την Προστασία Προσωπικών Δεδομένων ΕΕ 2016/679, ο οποίος αντικατέστησε την Οδηγία, η οποία είχε εκδοθεί προ εικοσαετίας. Στις 25 Μαΐου 2018 ο Κανονισμός τέθηκε σε ισχύ και έκτοτε παράγει άμεσα αποτελέσματα στο εσωτερικό των κρατών μελών, ανοίγοντας ένα νέο κεφάλαιο στην προστασία των προσωπικών δεδομένων στο Ενωσιακό δίκαιο.

Για την καλύτερη κατανόηση του θέματος της διπλωματικής και της προεκτεθείσας «εξέλιξης» του δικαιώματος προστασίας των προσωπικών δεδομένων στην ενωσιακή έννομη τάξη κρίνεται απαραίτητη αρχικώς η εξοικείωση του αναγνώστη με βασικές έννοιες της θεματικής των προσωπικών δεδομένων, καθώς και των νομικών ερεισμάτων του δικαιώματος της προστασίας των προσωπικών δεδομένων στο πρωτογενές ενωσιακό δίκαιο. Για το σκοπό αυτό στο πρώτο υποκεφάλαιο του παρόντος κεφαλαίου αναλύεται η έννοια και ο ρόλος των προσωπικών δεδομένων, έτσι όπως αυτός «αντανακλάται» στα σημαντικότερα ευρωπαϊκά νομοθετήματα πριν τον Γενικό Κανονισμό, στο δεύτερο υποκεφάλαιο αναλύεται ο νομικός ορισμός της επεξεργασίας των προσωπικών δεδομένων, ενώ στο τρίτο υποκεφάλαιο εξετάζονται τα νομικά ερείσματα του εν λόγω δικαιώματος στο πρωτογενές ενωσιακό δίκαιο.

1.1: Η έννοια και ο ρόλος των προσωπικών δεδομένων

Βασικό χαρακτηριστικό της νέας ψηφιακής εποχής είναι η εξάρτηση της κοινωνίας από την συλλογή και την επεξεργασία της πληροφορίας. Οι δυνατότητες αλληλοσυσχετισμών των δεδομένων, η ευκολία πρόσβασης και η αμεσότητα επικοινωνίας, χάρη στην επιστήμη της Πληροφορικής, κατέστησαν εφικτή την επεξεργασία μεγάλου όγκου δεδομένων σε σύντομο χρονικό διάστημα.

[7] Βλ. αναλυτικά κεφάλαια 2 και 3 της παρούσας διπλωματικής εργασίας

Μέσα λοιπόν σ' αυτόν τον «όγκο» δεδομένων περιλαμβάνονται και τα προσωπικά δεδομένα, τα οποία συνίστανται σε κάθε είδους πληροφορία που αφορά ένα φυσικό πρόσωπο, ανεξαρτήτως αν η πηγή προέλευσης αυτής σχετίζεται με τον ιδιωτικό, τον επαγγελματικό ή τον δημόσιο βίο του. Για το λόγο αυτό, τα προσωπικά δεδομένα ποικίλλουν και υφίστανται σε όλες σχεδόν τις καθημερινές δραστηριότητες π.χ ένα ονοματεπώνυμο, μια φωτογραφία, μια διεύθυνση ηλεκτρονικού ταχυδρομείου, τα στοιχεία που έχουν αναρτηθεί σε ιστότοπους κοινωνικής δικτύωσης[8] κτλ.

Ο ορισμός των «προσωπικών δεδομένων[9]» διατυπώνεται στην Οδηγία 95/46/ΕΚ ως: «κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή είναι δυνατόν να εξακριβωθεί άμεσα ή έμμεσα ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική[10]».

Είναι αποδεκτό ότι το όνομα είναι το πιο συνηθισμένο προσδιοριστικό της ταυτότητας ενός προσώπου, όμως με το όνομα μπορούν να εξομοιωθούν και άλλα στοιχεία όπως ο αριθμός μητρώου της κοινωνικής ασφάλισης (Α.Μ.Κ.Α.), ο αριθμός του δελτίου αστυνομικής ταυτότητας, ο αριθμός φορολογικού μητρώου κτλ. Επιπλέον, στοιχεία που δηλώνουν την ταυτότητα ενός προσώπου και νομιμοποιητικά στοιχεία που αποδίδονται σε πρόσωπα ή επιλέγονται από αυτά είναι δυνατόν να είναι ο κωδικός αναγνώρισης ή πρόσβασης.

Στην Ελλάδα με το ν. 2472/1997 τα προσωπικά δεδομένα ορίζονταν ως «κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως προσωπικά δεδομένα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν να προσδιοριστούν τα υποκείμενα των δεδομένων[11]».

Προσωπική πληροφορία είναι δυνατόν να χαρακτηριστεί και οποιαδήποτε πληροφορία μπορεί να συνδεθεί με το πρόσωπο, όπως για παράδειγμα η ψυχική κατάσταση ενός ατόμου, οι απόψεις του, οι επιθυμίες του, ο τρόπος συμπεριφοράς, η περιουσιακή και οικογενειακή κατάσταση, η επαγγελματική και οικονομική δραστηριότητα, ή η καταναλωτική του συμπεριφορά[12]. Είναι λοιπόν φανερό, ότι αν από την πληροφορία δεν ταυτοποιείται το πρόσωπο (ανωνυμοποίηση), τότε δεν πρόκειται για προσωπικά δεδομένα.

Διαπιστώθηκε ότι η προσωπική πληροφορία καθώς και ο ορισμός που δόθηκε για τα προσωπικά δεδομένα από την Οδηγία 95/46/ΕΚ αποτελούν ευρείς ορισμούς. Το περιεχόμενο της πληροφορίας

---

[8] Βλ. Europa, Press Release Database, 2014, Διαθέσιμο σε: http://europa.eu/rapid/search.htm

[9] Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου, «Προσωπικά Δεδομένα», Εκδ. Νομική Βιβλιοθήκη, 2016, σ. 44

[10] Βλ. Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995, άρθρο 2 στοιχ.α΄

[11] Βλ. νόμος 2472/1997, άρθρο 2 στοιχ. α΄

[12] Βλ. Λ. Μήτρου, «Προστασία προσωπικών δεδομένων – νόμος 2472/97», Εκδ. Σάκκουλα, 2017, σ. 59

καθορίζει την διάκριση των δεδομένων προσωπικού χαρακτήρα σε «απλά» και σε «ειδικής κατηγορίας δεδομένα» ή «ευαίσθητα[13]».

Τα προσωπικά δεδομένα ειδικών κατηγοριών, τα οποία αναφέρονται στα άρθρα 9 και 10 του Κανονισμού, αποτελούν στην πράξη τα ευαίσθητα προσωπικά δεδομένα του καταργηθέντος ν. 2472/97. Τα ευαίσθητα δεδομένα περιέχουν πληροφορίες για τη φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις, την υγεία και τη σεξουαλική ζωή σύμφωνα με την Οδηγία 95/46/ΕΚ, ενώ ο Έλληνας νομοθέτης με το ν. 2472/1997 είχε συμπληρώσει τα στοιχεία σχετικά με την κοινωνική πρόνοια και με τις ποινικές διώξεις ή καταδίκες.

Ο ν. 3471/2006 διαφοροποίησε τον ορισμό των ευαίσθητων δεδομένων[14]. Συγκεκριμένα ορίσθηκε ότι η συμμετοχή σε ενώσεις προσώπων, οι οποίες δραστηριοποιούνται σε πεδία και τομείς σχετικές με τα ευαίσθητα δεδομένα πολιτικού, εθνικού, θρησκευτικού περιεχομένου κτλ. συνιστά ευαίσθητο δεδομένο. Αντίθετα, η συμμετοχή σε ενώσεις, όπως π.χ. σε ένα αθλητικό ή πολιτιστικό σωματείο, δεν θεωρείται ευαίσθητο δεδομένο, διότι κρίθηκε ότι η δημοσιοποίησή του δεν διατρέχει σημαντικούς κινδύνους για τα θεμελιώδη δικαιώματα και την ελευθερία του ατόμου[15].

Επιπρόσθετα, ο ν. 3625/2007 συμπληρώνει ότι ειδικά για τις ποινικές διώξεις ή καταδίκες επιτρέπεται η δημοσιοποίηση συγκεκριμένων αδικημάτων μόνο με άδεια από την εισαγγελική αρχή, με σκοπό την προστασία του ευρύτερου κοινωνικού συνόλου και ευάλωτων πληθυσμιακών ομάδων[16]. Ακολούθησε ο ν. 4139/2013 ο οποίος συμπλήρωσε το ν. 3625/2007, εξειδικεύοντας τον τρόπο με τον οποίο θα γίνεται η δημοσιοποίηση των αδικημάτων[17].

Ο νέος Κανονισμός 2016/679 ΕΕ και η Οδηγία 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 εμπλουτίζουν τον ορισμό των δεδομένων προσωπικού χαρακτήρα και συγκεκριμένα τα ορίζουν ως «Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, του οποίου η ταυτότητα είναι δυνατόν να εξακριβωθεί άμεσα ή έμμεσα, από κάποιο αναγνωριστικό στοιχείο της ταυτότητας, από τα δεδομένα θέσης, από επιγραμμικό αναγνωριστικό ταυτότητας ή από έναν ή περισσότερους παράγοντες που αφορούν τη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του προσώπου[18]». Επιπλέον, ο νέος Κανονισμός και η ανωτέρω Οδηγία περιέχουν τα ευαίσθητα δεδομένα της Οδηγίας 95/46/ΕΚ και προσθέτουν τα στοιχεία που αφορούν γενετικά ή βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου και τον γενετήσιο προσανατολισμό.

---

[13] Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου, «Προσωπικά Δεδομένα», Εκδ. Νομική Βιβλιοθήκη, 2016, σ. 45

[14] Βλ. Νόμο 3471/2006, άρθρο 18 παρ.1 στοιχ.β΄

[15] Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου, «Προσωπικά Δεδομένα», Εκδ. Νομική Βιβλιοθήκη, 2016, σ. 50-51

[16] Βλ. Νόμο 3625/2007, άρθρο 8 παρ.3

[17] Βλ. Νόμο 4139/2017, άρθρο 79

[18] Βλ. Κανονισμό 2016/679 ΕΕ, άρθρο 4 στοιχ. 1 και Οδηγία 216/680 ΕΕ, άρθρο 3 στοιχ. 1

1.2: Η διαδικασία της επεξεργασίας των προσωπικών δεδομένων

Η επεξεργασία των προσωπικών δεδομένων αποτελεί κρίσιμο παράγοντα λήψης αποφάσεων και σχεδιασμού σε οικονομικό, διοικητικό, πολιτικό και κοινωνικό επίπεδο τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Η επεξεργασία των προσωπικών δεδομένων είναι μία έννοια ευρύτατη[19]. Σύμφωνα με την Οδηγία 95/46/ΕΚ (άρθρο 2) αλλά και με το ν. 2472/1997 ως υλοποίηση της Οδηγίας, η επεξεργασία προσωπικών δεδομένων[20] ορίζεται ως «Κάθε εργασία ή σειρά εργασιών που πραγματοποιούνται με ή χωρίς τη βοήθεια αυτοματοποιημένων διαδικασιών και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, εργασίες όπως συλλογή, καταχώρηση, οργάνωση, αποθήκευση, προσαρμογή ή τροποποίηση, ανάκτηση, αναζήτηση πληροφοριών, χρήση, ανακοίνωση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, εναρμόνιση ή συνδυασμός, καθώς και κλείδωμα, διαγραφή ή καταστροφή[21]».

Επίσης, ορίζεται η έννοια του υπεύθυνου επεξεργασίας ως: «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος φορέας που μόνος ή από κοινού με άλλους καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Όταν οι στόχοι και ο τρόπος της επεξεργασίας καθορίζονται από νομοθετικές ή κανονιστικές διατάξεις, εθνικές ή κοινοτικές, ο υπεύθυνος της επεξεργασίας ή τα ειδικά κριτήρια για τον ορισμό του μπορούν να καθορίζονται από το εθνικό ή κοινοτικό δίκαιο[22]».

Το άρθρο 10 του ν. 2472/1997, αναφέρει ότι: «Η επεξεργασία των προσωπικών δεδομένων είναι απόρρητη και εκτελείται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνον κατ' εντολή του». Οι υπεύθυνοι επεξεργασίας, ανεξαρτήτως αν απαλλάσσονται από την υποχρέωση γνωστοποίησης και λήψης άδειας από την Αρχή Προστασίας Προσωπικών Δεδομένων[23], οφείλουν να επιλέγουν πρόσωπα με επαρκείς τεχνικές γνώσεις και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. Επίσης, πρέπει να λαμβάνουν κατάλληλα οργανωτικά και τεχνικά μέτρα που να

[19] Βλ. Π. Αρμαμέντος, & Β. Σωτηρόπουλος, «Προσωπικά δεδομένα-Ερμηνεία Ν.2472/1997», Εκδ. Σάκκουλα, 2005, σ. 47-68

[20] Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου, «Προσωπικά Δεδομένα», Εκδ. Νομική Βιβλιοθήκη, 2016, σ. 53

[21] Βλ. Νόμος 2472/1997, άρθρο 2, στοιχ. δ΄. Παρόμοιος είναι και ο ορισμός επεξεργασία των προσωπικών δεδομένων, που δίδεται από άρθρο 4 παρ. 2 του Νέου Κανονισμού: Ως «επεξεργασία των προσωπικών δεδομένων» ορίζεται κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή».

[22] Βλ. Νόμος 2472/1997, άρθρο 2, στοιχ. ζ΄

[23] Βλ. Νόμος 2472/1997, άρθρο 7

εξασφαλίζουν ένα επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που απορρέουν από την επεξεργασία και τη φύση των δεδομένων που επεξεργάζονται[24].

Ο υπεύθυνος επεξεργασίας πρέπει να εκτιμήσει τους κινδύνους και τις απειλές στις οποίες είναι εκτεθειμένο το πληροφοριακό σύστημα στο οποίο λαμβάνει χώρα η επεξεργασία των προσωπικών δεδομένων, μέσω της ανάλυσης επικινδυνότητας και βάσει των αποτελεσμάτων από αυτήν, να λάβει κατάλληλα μέτρα ασφαλείας ώστε να μειώσει τον κίνδυνο σε ένα αποδεκτό επίπεδο[25].

Στην περίπτωση που η επεξεργασία εκτελείται για λογαριασμό του υπευθύνου επεξεργασίας από τρίτο πρόσωπο μη εξαρτώμενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως και προβλέπει ότι ο ενεργών την επεξεργασία την διεξάγει μόνο κατόπιν εντολής του υπευθύνου επεξεργασίας και ότι οι λοιπές υποχρεώσεις του άρθρου 10 του ν. 2472/1997 βαρύνουν αναλόγως και αυτόν. Η συλλογή και επεξεργασία προσωπικών δεδομένων, απλών και ευαίσθητων απαγορεύεται, εκτός εάν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του[26]. Επιτρέπεται, κατ' εξαίρεση, και χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων όταν συντρέχουν συγκεκριμένες προϋποθέσεις[27]. Η συγκατάθεση του υποκειμένου πρέπει να είναι ρητή, εν λόγω και να δίδεται μετά από λεπτομερής πληροφόρηση. Κατά συνέπεια δεν συμπεριλαμβάνεται η σιωπηρή συγκατάθεση.

Ταυτόχρονα, όμως, θα πρέπει να διερευνάται αν εφαρμόζονται οι γενικές αρχές[28] της νόμιμης επεξεργασίας των προσωπικών δεδομένων, όπου κάθε νόμιμη επεξεργασία θα πρέπει να εξυπηρετεί καθορισμένο, σαφή και νόμιμο σκοπό (αρχή της νομιμότητας του σκοπού και του τρόπου επεξεργασίας). Τα δεδομένα που υφίστανται επεξεργασία, θα πρέπει να είναι συναφή και πρόσφορα και, όχι περισσότερα από όσα απαιτεί κάθε φορά ο σκοπός της επεξεργασίας (αρχή της αναλογικότητας). Επιπλέον, πρέπει να είναι ακριβή, επικαιροποιημένα ώστε να εξακολουθούν να ανταποκρίνονται στην πραγματικότητα και να διατηρούνται σε μορφή που να προσδιορίζεται η ταυτότητα των υποκειμένων κατά τη διάρκεια της επεξεργασίας (αρχή της ακρίβειας των τηρουμένων δεδομένων).

Τέλος, η διάρκεια τήρησης των δεδομένων καθορίζεται από την Αρχή Προστασίας Προσωπικών Δεδομένων, για όσο χρονικό διάστημα απαιτείται για την διευθέτηση των σκοπών της συλλογής και της επεξεργασίας. Μετά το πέρας του ανωτέρω χρόνου, τα δεδομένα καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας, ενώ η Αρχή με αιτιολογημένη απόφασή της έχει το δικαίωμα να διατηρήσει προσωπικά δεδομένα για ιστορικούς, επιστημονικούς ή στατιστικούς σκοπούς, εφόσον

[24] Βλ. Νόμος 2472/1997, άρθρο 10 παρ. 2 και 3

[25] Βλ. Νόμος 2472/1997, άρθρο 10 παρ. 4

[26] Βλ. Νόμος 2472/1997, άρθρο 5 παρ.1 και άρθρο 7 παρ. 1

[27] Βλ. Άρθρο 5 παρ. 2 του ν. 2472/1997 για τα απλά δεδομένα, στο άρθρο 7 παρ.2 για τα ευαίσθητα δεδομένα καθώς και γνωστοποίηση στην Α.Π.Δ.Π.Χ. σύμφωνα με το άρθρο 6

[28] Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου, «Προσωπικά Δεδομένα», Εκδ. Νομική Βιβλιοθήκη, 2016, σ. 69-85

δεν θίγονται τα δικαιώματα των υποκειμένων ή τρίτων (αρχή της χρονικής διάρκειας τήρησης των δεδομένων).

Συνεπώς, κάθε επεξεργασία προσωπικών δεδομένων για να θεωρείται νόμιμη θα πρέπει να τηρούνται οι τέσσερις αρχές επεξεργασίας, να υπάρχει η συγκατάθεση του υποκειμένου των δεδομένων, διαφορετικά να εξεταστούν αν πληρούνται οι προϋποθέσεις μη συγκατάθεσης, να ενημερωθεί το υποκείμενο και να γνωστοποιηθεί η πρόθεση της συλλογής και επεξεργασίας προσωπικών δεδομένων στην Αρχή Προστασίας Προσωπικών Δεδομένων ή να ληφθεί η άδεια της Αρχής σε περίπτωση ευαίσθητων δεδομένων. Όλα τα προαναφερόμενα, αναπροσαρμόζονται σύμφωνα τον νέο Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων[29].

1.3: Η νομική βάση προστασίας των προσωπικών δεδομένων στο πρωτογενές Ενωσιακό δίκαιο[30]

Είναι, καταρχάς, αξιοσημείωτο ότι το παράγωγο Ενωσιακό δίκαιο προηγήθηκε χρονικά του πρωτογενούς. Όταν το δικαίωμα προστασίας των προσωπικών δεδομένων έτυχε αναγνώρισης και στο πρωτογενές Ενωσιακό δίκαιο τόσο στο Χάρτη Θεμελιωδών Δικαιωμάτων της Ε.Ε., όσο και με τη Συνθήκη της Λισαβώνας, η Οδηγία 95/46/ΕΚ μετρούσε ήδη πολλά χρόνια εφαρμογής.

Το δικαίωμα στην προστασία των προσωπικών δεδομένων κατοχυρώνεται ρητώς στο άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων το οποίο ορίζει ότι: «Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν, καθώς και ότι η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους λόγους που προβλέπονται από το νόμο».

---

[29] Ειδικότερα, στο άρθρο 5 του Κανονισμού, εισάγονται ορισμένες βασικές αρχές που θα πρέπει να τηρούνται σε κάθε περίπτωση επεξεργασίας δεδομένων προσωπικού χαρακτήρα από μία τράπεζα, προκειμένου αυτή να είναι σύννομη και σύμφωνη με το πνεύμα και το σκοπό του Κανονισμού.
Οι αρχές που εισάγονται με τον Κανονισμό 679/2016 είναι οι εξής:

1. Η αρχή της νομιμότητας, της αντικειμενικότητας και της διαφάνειας (άρθρο 5 παρ. 1, περ. α').
2. Η αρχή του περιορισμού του σκοπού της επεξεργασίας (άρθρο 5 παρ. 1, περ. β').
3. Η αρχή της ελαχιστοποίησης των δεδομένων (άρθρο 5 παρ. 1, περ. γ').
4. Η αρχή της ακρίβειας (άρθρο 5 παρ. 1, περ. δ').
5. Η αρχή του περιορισμού της περιόδου αποθήκευσης (άρθρο 5 παρ. 1, περ. ε').

[30] Ως πρωτογενές δίκαιο χαρακτηρίζεται το δίκαιο των τριών ιδρυτικών Συνθηκών της ΕΕ (Συνθήκη για την Ευρωπαϊκή Ένωση, Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης και Συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας, καθώς και οι γενικές αρχές που πηγάζουν από αυτές. Σημειωτέον ότι οι ανωτέρω συνθήκες τροποποιήθηκαν με τη Συνθήκη της Λισαβόνας, η οποία περαιτέρω ενσωμάτωσε στο πρωτογενές δίκαιο τον Χάρτη των Θεμελιωδών Δικαιωμάτων Βλ. Π. Ιωακειμίδης, «Η Συνθήκη της Λισαβόνας», Εκδ. Θεμέλιο, 2010, σ. 14 επ.

Περαιτέρω, ορίζεται ότι: «Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωση τους[31]».

Η μεγάλη τομή που επέφερε η Συνθήκη της Λισαβώνας στο δικαίωμα προστασίας προσωπικών δεδομένων έγκειται στην προσθήκη του άρθρου 16 στην εν λόγω Συνθήκη. Το άρθρο αυτό αφενός κατοχυρώνει την προστασία του δικαιώματος προστασίας των προσωπικών δεδομένων με σχεδόν πανομοιότυπο λεκτικό με αυτό του άρθρου 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ε.Ε. και αφετέρου προβλέπει στην παρ. 2 μια νέα νομική βάση για το Συμβούλιο και το Κοινοβούλιο με την οποία μπορούν, σύμφωνα με τη συνήθη νομοθετική διαδικασία, να θεσπίζουν κανόνες σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των προσωπικών δεδομένων τους.

Ετσι, ρητή αναφορά στο δικαίωμα της προστασίας των προσωπικών δεδομένων γίνεται στο άρθρο 16 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης το οποίο ορίζει στην παράγραφο 1 ότι: «Κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν», και στην παράγραφο 2 ότι: «Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία, θεσπίζουν τους κανόνες σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του δικαίου της Ένωσης, και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών. Η τήρηση των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητων αρχών[32]».

Επομένως, το άρθρο 16 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης, ως διάταξη γενικής εφαρμογής, όχι μόνο κατοχυρώνει δικαίωμα στην προστασία των προσωπικών δεδομένων, αλλά δημιουργεί και νέα νομική βάση, στη λογική κατάργησης των πυλώνων, αφού προβλέπει την ίδια νομοθετική διαδικασία τόσο για την εσωτερική αγορά όσο και για την εσωτερική ασφάλεια[33] (πρώην αστυνομική και δικαστική συνεργασία). Παρατηρείται λοιπόν ότι η προστασία των προσωπικών δεδομένων κατοχυρώνεται επαρκώς στο πρωτογενές ενωσιακό δίκαιο. Ωστόσο, όπως αναφέραμε και πιο πάνω, σε μεγάλο βαθμό η κατοχύρωση της προστασίας των προσωπικών δεδομένων στο πρωτογενές δίκαιο έγινε αφού πρώτα είχε θεσπιστεί και συγκεκριμενοποιηθεί το περιεχόμενο της στο παράγωγο δίκαιο, κυρίως με τη μορφή Οδηγιών όπως θα αναδειχθεί στο επόμενο κεφάλαιο.

1.4: Συμπεράσματα

[31] Βλ. Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, «Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης», Διαθέσιμο σε: http://www.europarl.europa.eu/charter/pdf/text_el.pdf

[32] Βλ. Ενοποιημένη απόδοση της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:12012E/TXT

[33] Πρβλ. Ζ. Καρδασιάδου, «Στον απόηχο της Οδηγίας 95/46/ΕΚ», Ευρωπαίων Πολιτεία, 2011, σ. 209 επ.

Οι σημαντικότερες έννοιες της θεματικής της εργασίας είναι πρωτίστως η έννοια και ο νομικός ορισμός των προσωπικών δεδομένων, της επεξεργασίας τους, καθώς και του υπεύθυνου επεξεργασίας. Όπως αναδείχθηκε ανωτέρω η ευρωπαϊκή και εθνική έννομη τάξη (με τον εφαρμοστικό νόμο 2472/1997) έχει συγκεκριμενοποιήσει επαρκώς τις συγκεκριμένες έννοιες, υιοθετώντας ως επί το πλείστον ευρείς ορισμούς που να περιλαμβάνουν οποιαδήποτε μορφή πληροφορίας που μπορεί να συνδεθεί με την ταυτότητα συγκεκριμένου προσώπου. Περαιτέρω, αποδείχθηκε ότι το δικαίωμα προστασίας των προσωπικών δεδομένων έχει σημαντικά ερείσματα στο πρωτογενές ενωσιακό δίκαιο, αποκαλύφθηκε ωστόσο και μία συγκεκριμένη ιδιαιτερότητα του δικαιώματος η οποία σχετίζεται με το γεγονός ότι η κατοχύρωση του χρονικά ακολούθησε της «συγκεκριμενοποίησης» και κατοχύρωσης του στο παράγωγο ενωσιακό δίκαιο.

Κεφάλαιο 2: Ιστορική εξέλιξη της κατοχύρωσης της προστασίας των προσωπικών δεδομένων στην ενωσιακή έννομη τάξη

Η εναργέστερη κατανόηση του GDPR προϋποθέτει την εξέταση των προηγούμενων νομοθετικών πράξεων με τις οποίες τα θεσμικά όργανα της ΕΕ επιχείρησαν να ρυθμίσουν την προστασία των προσωπικών δεδομένων. Και τούτο διότι τα περισσότερα στοιχεία του GDPR αντλούνται σχεδόν αυτούσια από τις προηγούμενες νομοθετικές ρυθμίσεις της ΕΕ. Επί παραδείγματι, οι βασικότεροι νομικοί ορισμοί (προσωπικά δεδομένα, επεξεργασία, υπεύθυνος επεξεργασίας) αντλούνται από την Οδηγία 95/46/ΕΚ, ενώ ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων, που βάσει του νέου κανονισμού συμμετέχει στο νεοσυσταθέν Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, είχε ήδη συσταθεί με τον Κανονισμό 45/2001.

Για το σκοπό αυτό στο παρόν κεφάλαιο επιχειρείται η «παρακολούθηση» της ιστορικής εξέλιξης της ρύθμισης της προστασίας των προσωπικών δεδομένων στο παράγωγο ενωσιακό δίκαιο. Πιο συγκεκριμένα, στο πρώτο υποκεφάλαιο εξετάζεται η Οδηγία 95/46/ΕΚ, στο δεύτερο υποκεφάλαιο εξετάζεται η Οδηγία 97/66/ΕΚ, ενώ στο τρίτο υποκεφάλαιο αναλύεται ο Κανονισμός 45/2001. Τέλος, στο τέταρτο υποκεφάλαιο αναλύεται η απάντηση του Δικαστηρίου της Ευρωπαϊκής Ένωσης σε προδικαστικό ερώτημα Ισπανικού Δικαστηρίου επ' αφορμή συγκεκριμένης υπόθεσης, προκειμένου να αναδειχθεί ο τρόπος ερμηνείας της Οδηγίας 95/46/ΕΚ από το ΔΕΚ.

2.1: Η Οδηγία 95/46/ΕΚ

Η Οδηγία[34] για την προστασία δεδομένων προσωπικού χαρακτήρα (επίσημη ονομασία: 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 την ελεύθερη κυκλοφορία αυτών[35]) υιοθετήθηκε το 1995 και αποτέλεσε για αρκετά χρόνια (μέχρι την αντικατάσταση της από τον εξεταζόμενο Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων[36]) τη σημαντικότερη ενωσιακή νομοθετική πράξη ρύθμισης της επεξεργασίας προσωπικών δεδομένων στο χώρο της Ευρωπαϊκής Ένωσης. Αναμφισβήτητα η συγκεκριμένη Οδηγία συνιστά νομοθέτημα υψίστης σημασίας για τα ανθρώπινα δικαιώματα και την προστασία της ιδιωτικής ζωής στην ΕΕ, καθώς αποτέλεσε την πρώτη προσπάθεια συστηματοποίησης και

[34] Η Οδηγία είναι μία μορφή νομοθετικής πράξης της Ευρωπαϊκής Ένωσης (η συνηθέστερη μορφή δράσης της ΕΕ μαζί με τον Κανονισμό) η οποία προϋποθέτει από τα κράτη μέλη να πετύχουν ένα συγκεκριμένο αποτέλεσμα, χωρίς να υπαγορεύονται τα μέσα με τα οποία θα επιτευχθεί αυτό το αποτέλεσμα. Επομένως η Οδηγία αφήνει στα κράτη μέλη «ένα περιθώριο ελευθερίας» ως προς τα ακριβή μέτρα που θα υιοθετήσουν για την επίτευξη του επιδιωκόμενου αποτελέσματος Βλ. άρθρο 288 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης καθώς και P. Nanda (επιμ.), «European Union law after Maastricht: a practical guide for lawyers outside the common market», Εκδ. Kluwer, 1996, σ. 5

[35] Πρβλ. ΕΕ L 281 της 23/11/1995 σ. 31-50

[36] Βλ. άρθρο 94 του Γενικού Κανονισμού για την Προστασία Δεδομένων-GDPR (ΕΕ L 119 της 4/5/2016, σ. 1-88) όπου ρητά αναφέρεται ότι με την έναρξη της ισχύος του καταργείται η Οδηγία 95/46/ΕΚ.

κωδικοποίησης του νομικού πλαισίου που έως τότε ρύθμιζε την επεξεργασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση.

2.1.1: Η πορεία προς την Οδηγία[37]

Είναι γεγονός πως και πριν την υιοθέτηση της συγκεκριμένης Οδηγίας το δικαίωμα στην ιδιωτική ζωή ήταν αρκετά ανεπτυγμένο στο εθνικό δίκαιο των περισσότερων κρατών μελών της Ευρωπαϊκής Ένωσης[38]. Τούτο οφειλόταν αφ' ενός στην κοινή συνταγματική παράδοση των περισσότερων κρατών μελών της ΕΕ[39] και αφ' ετέρου στο ότι όλα τα κράτη μέλη είχαν επικυρώσει την Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου. Πιο συγκεκριμένα, το άρθρο 8 της ΕΣΔΑ κατοχυρώνει το δικαίωμα στην ιδιωτική και οικογενειακή ζωή, στην κατοικία και στην αλληλογραφία. Μάλιστα, το Δικαστήριο της Ευρωπαϊκής Ένωσης έχει υιοθετήσει μία διασταλτική ερμηνεία του συγκεκριμένου άρθρου, γεγονός που ενισχύει την προστασία του εν λόγω δικαιώματος.

Το 1980, σε μία προσπάθεια δημιουργίας ενός αποτελεσματικού συστήματος προστασίας των προσωπικών δεδομένων στην Ευρώπη, ο ΟΟΣΑ υπέβαλε συγκεκριμένες προτάσεις («Κατευθυντήριες Αρχές») στην ΕΟΚ για την προστασία της ιδιωτικότητας και της διασυνοριακής διαβίβασης των προσωπικών δεδομένων[40]. Η σχετική πρόταση του ΟΟΣΑ χαρακτηριζόταν από επτά γενικές αρχές. Η πρώτη ήταν η αρχή προειδοποίησης των υποκειμένων των δεδομένων όταν αυτά συλλέγονταν, ενώ η δεύτερη ήταν η αρχή του σκοπού, βάσει της οποίας τα δεδομένα μπορούσαν να χρησιμοποιηθούν μόνο για το σκοπό που αναφέρθηκε στο υποκείμενο των δεδομένων. Η τρίτη αρχή ήταν αυτή της συγκατάθεσης, σύμφωνα με την οποία δεν μπορούσε να γίνει συλλογή δεδομένων χωρίς τη συγκατάθεση του υποκειμένου, ενώ η τέταρτη αρχή υπαγόρευε ότι τα δεδομένα έπρεπε να «προστατεύονται» από πιθανές παραβιάσεις.

---

[37] Βλ. Κ. Δελούκα-Ιγγλέση, «Νομικά Θέματα Ηλεκτρονικού Εμπορίου», Εκδ. Σάκκουλα, 2015, σ. 265 επ.

[38] Αξίζει να σημειωθεί ότι το πρόβλημα της προστασίας του πολίτη από την απεριόριστη δυνατότητα συλλογής, επεξεργασίας και καταχώρησης σε αρχεία προσωπικών πληροφοριών ανεφύη με ιδιαίτερη ένταση στην Ομοσπονδιακή Δημοκρατία της Γερμανίας και σε σχέση με τη συνταγματικότητα του νόμου του 1983 για την απογραφή του πληθυσμού (Volkszaelungsgesetz), καθώς αυτός προσέφερε στον κρατικό φορέα τη δυνατότητα κατοχής ενός εξαιρετικά μεγάλου αριθμού προσωπικών πληροφοριών των πολιτών. Τελικά, στην περίφημη Απόφασή του της 15.12.1983 το γερμανικό Ομοσπονδιακό Συνταγματικό Δικαστήριο δέχθηκε πράγματι την αντισυνταγματικότητα ορισμένων διατάξεων του εν λόγω νόμου, και γίνεται ρητή επίκληση του «δικαιώματος πληροφοριακού αυτοκαθορισμού», ήτοι «του δικαιώματος του ατόμου να αποφασίζει και να συμπροδιορίζει πότε και υπό ποιες προϋποθέσεις είναι δυνατή η επεξεργασία των πληροφοριών που το αφορούν». Βλ. Κ. Δελούκα-Ιγγλέση, ό.π., σ. 267, υποσ. 618.

[39] Σε ένα βαθμό η ομοιογένεια των Συνταγμάτων των κρατών μελών στον τομέα των δικαιωμάτων οφείλεται στις αποφάσεις του Δικαστηρίου της Ευρωπαϊκής Ένωσης το οποίο, λόγω της υπέροχης του ενωσιακού έναντι του εσωτερικού δικαίου-ακόμη και του συνταγματικού-, εμμέσως δέσμευε τα κράτη μέλη να θεσπίσουν νομοθετήματα που να εναρμονίζονται με το ενωσιακό δίκαιο Βλ. V. Louis, Η κοινοτική έννομη τάξη, Εκδ. Επιτροπής των Ευρωπαϊκών Κοινοτήτων, 1981, σ. 97-98

[40] Βλ. The Organization for Economic Co-Operation and Development, «Guidelines on the Protection of Privacy and Transborder Flows of Personal Data», Διαθέσιμο σε: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Τέλος, σύμφωνα με την πέμπτη αρχή τα υποκείμενα των δεδομένων έπρεπε να ενημερώνονται για την ταυτότητα αυτών που τα συλλέγουν, βάσει της έκτης αρχής τα υποκείμενα έπρεπε να έχουν πρόσβαση στα δεδομένα τους και επιπλέον να έχουν τη δυνατότητα να κάνουν τις απαιτούμενες αλλαγές σε πιθανά ανακριβή στοιχεία, ενώ σύμφωνα με την τελευταία αρχή τα υποκείμενα των δεδομένων έπρεπε να έχουν στη διάθεσή τους μία κατάλληλη μέθοδο που θα διασφάλιζε τη δυνατότητα τους να εγκαλούν όσους παραβαίνουν τις ανωτέρω αρχές[41].

Μολονότι η πρόταση του ΟΟΣΑ δεν ήταν δεσμευτική, όπως θα διαπιστωθεί και στα επόμενα κεφάλαια όπου θα επιχειρηθεί η ανάλυση του ισχύοντος νομικού πλαισίου, οι ανωτέρω αρχές αποτέλεσαν το θεμέλιο των μεταγενέστερων νομοθετικών ρυθμίσεων της προστασίας των προσωπικών δεδομένων από τα θεσμικά όργανα της ΕΕ[42]. Πάντως, ο μη δεσμευτικός χαρακτήρας των Κατευθυντηρίων Αρχών του ΟΟΣΑ είχε ως αποτέλεσμα το νομικό πλαίσιο ρύθμισης των προσωπικών δεδομένων να εξακολουθεί να διαφέρει σημαντικά μεταξύ των κρατών μελών της ΕΟΚ.

Ένα χρόνο αργότερα το Συμβούλιο της Ευρώπης ξεκίνησε τις διαπραγματεύσεις για τη Σύμβαση για την Προστασία των ιδιωτών σε σχέση με την Αυτοματοποιημένη Επεξεργασία των Προσωπικών Δεδομένων. Η συγκεκριμένη σύμβαση υποχρέωσε τα συμβαλλόμενα κράτη να θεσπίσουν κατάλληλη νομοθεσία για τη ρύθμιση της αυτοματοποιημένης επεξεργασίας των προσωπικών δεδομένων. Σύντομα ωστόσο η Ευρωπαϊκή Επιτροπή συνειδητοποίησε ότι η διαφορετική νομοθεσία για την προστασία των δεδομένων μεταξύ των κρατών μελών της ΕΕ εμπόδιζε την ελεύθερη ροή δεδομένων εντός της ΕΕ και, ως εκ τούτου, πρότεινε τη θέσπιση μίας Οδηγίας για την προστασία των δεδομένων.

2.1.2: Το περιεχόμενο της Οδηγίας

Η σημασία της Οδηγίας έγκειται πρωτίστως στο ότι περιέχει ορισμούς των βασικών εννοιών που αφορούν την προστασία προσωπικών δεδομένων και οι οποίοι, όπως συμπληρώθηκαν μέσω δικαστικής ερμηνείας, χρησιμοποιούνται ως βάση στο σύνολο του ισχύοντος ενωσιακού πλαισίου για τα προσωπικά δεδομένα. Ειδικότερα, στην Οδηγία ως προσωπικά δεδομένα ορίζονται «κάθε πληροφορία που αναφέρεται σε συγκεκριμένο φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί[43]». Οι τρόποι ταυτοποίησης του ατόμου περιλαμβάνουν είτε τον

[41] Βλ. A. Shimanek, «Do you Want Milk with those Cookies?: Complying with Safe Harbor Privacy Principles», Journal of Corporation Law, 26 (2): 455, 2001, σ. 462–463

[42] Χαρακτηριστικό παράδειγμα αποτελεί η αρχή του σκοπού Βλ. Άρθρο 5 παρ. 1 υποενότητα β': «Τα δεδομένα προσωπικού χαρακτήρα συλλέγονται για καθορισμένους, ρητούς και θεμιτούς σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς»

[43] Βλ. Άρθρο 2 παρ. 1 της Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995, Διαθέσιμο σε: http://drivingschool.gr/nomothesia/eu_odigies/95-46-ek.pdf

αριθμό ταυτότητας είτε περισσότερα στοιχεια που χαρακτηρίζουν την υπόσταση του από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη[44].

Όπως ανφέρθηκε και στο προηγούμενο κεφάλαιο, είναι αποδεκτό ότι το όνομα είναι το πιο σύνηθες προσδιοριστικό της ταυτότητας ενός προσώπου, όμως με το όνομα μπορούν να εξομοιωθούν και άλλα στοιχεία όπως ο αριθμός μητρώου της κοινωνικής ασφάλισης (Α.Μ.Κ.Α.), ο αριθμός του δελτίου αστυνομικής ταυτότητας και ο αριθμός φορολογικού μητρώου[45]. Επιπλέον, στοιχεία που δηλώνουν την ταυτότητα ενός προσώπου και νομιμοποιητικά στοιχεία που αποδίδονται σε πρόσωπα ή επιλέγονται από αυτά είναι δυνατόν να είναι ο κωδικός αναγνώρισης ή πρόσβασης[46].

Αυτό που παρατηρείται επομένως είναι ότι ο ορισμός των προσωπικών δεδομένων στην εξεταζόμενη Οδηγία είναι ικανοποιητικά ευρύς. Και τούτο διότι ως δεδομένα προσωπικού χαρακτήρα χαρακτηρίζονται αυτά που μπορούν να συνδεθούν με την ταυτότητα ενός συγκεκριμένου ατόμου, ακόμη και όταν το πρόσωπο που τα συλλέγει δεν μπορεί να κάνει αυτή τη σύνδεση. Επί παραδείγματι, δεδομένα προσωπικού χαρακτήρα αποτελούν η διεύθυνση, ο αριθμός πιστωτικής κάρτας, οι τραπεζικές καταθέσεις και το ποινικό μητρώο μεταξύ άλλων.

Έπειτα, ως επεξεργασία προσωπικών δεδομένων ορίζεται «το σύνολο των εργασιών επεξεργασίας των προσωπικών δεδομένων που πραγματοποιείται με ή χωρίς τη βοήθεια αυτοματοποιημένων διαδικασιών από τη συλλογή μέχρι την καταχώρηση, την οργάνωση, την αποθήκευση, την προσαρμογή ή τροποποίηση, την ανάκτηση, την αναζήτηση πληροφοριών, τη χρήση, την ανακοίνωση με διαβίβαση, τη διάδοση ή κάθε άλλη μορφή διάθεσης, την εναρμόνιση, η διαγραφή ή καταστροφή των δεδομένων[47]». Μάλιστα στην Οδηγία περιλαμβάνεται ενδεικτική απαρίθμηση τέτοιων εργασιών.

Ως τέτοια νοείται και η δημοσίευση δεδομένων προσωπικού χαρακτήρα στο Διαδίκτυο[48]. Η επεξεργασία αποσκοπεί στη δημιουργία αρχείου προσωπικών δεδομένων και ως τέτοιο ορίζεται «κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα προσιτών με γνώμονα συγκεκριμένα κριτήρια[49]». Τούτο είναι σημαντικό διότι ως επεξεργασία νοείται τόσο εκείνη που πραγματοποιείται με τη βοήθεια αυτοματοποιημένων διαδικασιών (με χαρακτηριστικό παράδειγμα την αυτοματοποιημένη συλλογή, επεξεργασία και διάρθρωση στο Διαδίκτυο) όσο και η καθαρά χειρόγραφη επεξεργασία εφόσον όμως αποσκοπεί στη δημιουργία αρχείου δεδομένων με την

[44] Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου, «Προσωπικά Δεδομένα», Εκδ. Νομική Βιβλιοθήκη, 2016, σ. 44

[45] Ε. Αλεξανδροπούλου-Αιγυπτιάδου, όπ.π., σ. 44

[46] Σημειωτέον ότι στο άρθρο 2 του εφαρμοστικού νόμου 2472/1997 της Οδηγίας στην ελληνική έννομη τάξη τα προσωπικά δεδομένα ορίζονται ως «κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως προσωπικά δεδομένα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν να προσδιοριστούν τα υποκείμενα των δεδομένων». Επομένως και ο ελληνικός νόμος «περιχαρακώνει» με τον ίδιο τρόπο όπως και η Οδηγία την έννοια των προσωπικών δεδομένων αυστηρά σε όσα στοιχεία δύνανται να προσδιορίζουν τα υποκείμενα των δεδομένων.

[47] Βλ. Άρθρο 2 παρ. 2 της Οδηγίας 95/46/ΕΚ

[48] Βλ. Απόφαση ΔΕΚ (πλέον ΔΕΕ) της 6ης Νοεμβρίου 2003, C-101/01, Lindqvist, σ. 47

[49] Βλ. Άρθρο 2 παρ. 3 της Οδηγίας 95/46/ΕΚ

προαναφερθείσα έννοια (για παράδειγμα η καταγραφή σε χειρόγραφα πρακτικά των ονομάτων συμμετεχόντων σε επιχειρηματική διάσκεψη).

Περαιτέρω, ως υπεύθυνος επεξεργασίας ορίζεται «ο φορέας που καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα[50]», ενώ ο εκτελών την υπηρεσία είναι «ο φορέας ο οποίος επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας[51]».

Αξίζει μάλιστα στο σημείο αυτό να αναφερθεί ότι η εξεταζόμενη Οδηγία δεν ήταν εφαρμοστέα μόνο στις περιπτώσεις που ο υπεύθυνος επεξεργασίας ήταν εγκατεστημένος σε χώρα της Ευρωπαϊκής Ένωσης, αλλά και γενικότερα στις περιπτώσεις που ο υπεύθυνος επεξεργασίας χρησιμοποιούσε εξοπλισμό εγκατεστημένο στην ΕΕ για αυτή τη διαδικασία[52]. Συναφώς, υπεύθυνοι επεξεργασίας με έδρα εκτός της ΕΕ ήταν υποχρεωμένοι να τηρούν αυτή την Οδηγία[53]. Οποιαδήποτε διαδικτυακή συναλλαγή των κατοίκων της ΕΕ αναπόφευκτα περιελάμβανε την επεξεργασία ορισμένων προσωπικών δεδομένων και τη χρήση εξοπλισμού στην ΕΕ για τη διεκπεραίωση αυτών των δεδομένων (τον υπολογιστή του πελάτη). Κατά συνέπεια, ο διαχειριστής του δικτυακού τόπου ήταν υποχρεωμένος να συμμορφώνεται με την ευρωπαϊκή Οδηγία προστασίας προσωπικών δεδομένων.

Επιπλέον, σημαντική καινοτομία της Οδηγίας αποτελεί η κατοχύρωση των αρχών της διαφάνειας, της νομιμότητας και της αναλογικότητας, οι οποίες πρέπει να διέπουν την επεξεργασία των προσωπικών δεδομένων και οι οποίες εξειδικεύονται στα άρθρα της. Πιο συγκεκριμένα, η διαφάνεια περιλαμβάνει το δικαίωμα του υποκειμένου να ενημερώνεται για την επεξεργασία των προσωπικών του δεδομένων. Συναφώς, ο υπεύθυνος επεξεργασίας πρέπει να γνωστοποιεί το όνομα και τη διεύθυνσή του, τον σκοπό της επεξεργασίας, τους αποδέκτες των δεδομένων και γενικότερα όλες τις υπόλοιπες πληροφορίες που απαιτούνται για να εξασφαλιστεί ότι η επεξεργασία είναι διαφανής[54].

Συναφώς, η επεξεργασία των δεδομένων είναι επιτρεπτή μόνο στις περιπτώσεις που απαριθμούνται περιοριστικά στο άρθρο 7 της Οδηγίας δηλαδή όταν το υποκείμενο των δεδομένων έχει δώσει τη

---

[50] Βλ. Άρθρο 2 παρ. 4 της Οδηγίας 95/46/ΕΚ

[51] Βλ. Άρθρο 2 παρ. 5 της Οδηγίας 95/46/ΕΚ

[52] Βλ. Άρθρο 4 παρ. 1 εδ. γ'

[53] Οι συγκεκριμένοι κανόνες ερμηνεύθηκαν διασταλτικά στην απόφαση Google Spain (C-131/12, Google Spain, 13 Μαϊού 2014, Διαθέσιμο σε: http://curia.europa.eu/juris/document/document.jsf;jsessionid=8B16E4B7657EA3BB00C0B34D0E92B65D?text=&docid=152065&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=11720450) Και τούτο διότι η δυνατότητα αυτόματης αναζήτησης και ευρετηρίασης βάσει ονοματεπωνύμου υπήχθη στην έννοια της «επεξεργασίας», η δε εκ μέρους των μηχανών αναζήτησης του διαδικτύου προσωρινή αποθήκευση των ευρετηριαζόμενων πληροφοριών υπήχθη στην περίπτωση της χρήσης μέσων που βρίσκονται σε ενωσιακό έδαφος, γεγονός που κατέστησε τη Google Inc. «υπεύθυνο επεξεργασίας» με την έννοια της Οδηγίας 95/46/ΕΚ

[54] Βλ. Άρθρα 10 και 11 της Οδηγίας 95/46/ΕΚ

συγκατάθεσή του, όταν η επεξεργασία είναι αναγκαία για την εκτέλεση ή τη σύναψη σύμβασης, όταν η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με μια νομική υποχρέωση, όταν η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων, και τέλος όταν η επεξεργασία είναι αναγκαία για την εκτέλεση καθήκοντος που εκτελείται για το δημόσιο συμφέρον ή για την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας ή σε τρίτο μέρος στον οποίο αποκαλύπτονται τα δεδομένα.

Παράλληλα, το υποκείμενο των δεδομένων διατηρεί το δικαίωμα πρόσβασης σε όλα τα δεδομένα που έχουν υποστεί επεξεργασία, καθώς και το δικαίωμα να ζητήσει τη διόρθωση ή τη διαγραφή δεδομένων που είναι ελλιπή ή ανακριβή[55]. Στο σημείο αυτό παρατηρείται μία ακόμη ομοιότητα του περιεχομένου της Οδηγίας με τις Κατευθυντήριες Αρχές του ΟΟΣΑ και ειδικότερα με την έκτη αρχή η οποία υπαγόρευε τη ανάγκη τα υποκείμενα να έχουν πρόσβαση στα δεδομένα τους και τη δυνατότητα να κάνουν τις απαιτούμενες αλλαγές σε πιθανά ανακριβή στοιχεία.

Η αρχή της νομιμότητας του σκοπού επεξεργασίας των προσωπικών δεδομένων εξειδικεύεται στο άρθρο 6 εδ. β' όπου ορίζεται ότι τα προσωπικά δεδομένα μπορούν να υποβάλλονται σε επεξεργασία μόνο για σαφείς και νόμιμους σκοπούς και δεν επιτρέπεται να υποβάλλονται σε περαιτέρω επεξεργασία με τρόπο ασυμβίβαστο προς τους σκοπούς αυτούς. Επιπροσθέτως, στο κείμενο της Οδηγίας κατοχυρώνεται και η αρχή της αναλογικότητας που επιχειρεί να συνδέσει το μέτρο επεξεργασίας των προσωπικών δεδομένων με τους σκοπούς για τους οποίους συλλέγονται. Περαιτέρω, τα δεδομένα πρέπει να είναι ακριβή και εφόσον κρίνεται αναγκαίο να ενημερώνονται, ενώ πρέπει να διατηρούνται σε μορφή που να αποτρέπει τον προσδιορισμό των προσώπων στα οποία αναφέρονται τα δεδομένα για μεγαλύτερο χρονικό διάστημα από αυτό που είναι αναγκαίο για τους σκοπούς για τους οποίους συλλέχθηκαν τα δεδομένα ή για τα οποία υποβάλλονται σε περαιτέρω επεξεργασία[56].

Τέλος, σημαντική καινοτομία της Οδηγίας είναι και η κατοχύρωση της υποχρέωσης των κρατών μελών να συστήσουν εποπτική αρχή ως ανεξάρτητο όργανο, με αρμοδιότητα την παρακολούθηση του επιπέδου προστασίας των προσωπικών δεδομένων, την παροχή συμβουλών και γνωμοδοτήσεων στις εθνικές κυβερνήσεις, και την ανάληψη νομικής δράσης όταν παραβιάζεται ο κανονισμός προστασίας δεδομένων[57].

2.2: Η Οδηγία 97/66/ΕΚ

Με την Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρώπης της 15ης Δεκεμβρίου του 1997 επιχειρήθηκε να ρυθμιστεί στο πλαίσιο του δευτερογενούς ενωσιακού δικαίου για την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας στο χώρο της τηλεπικοινωνίας. Η σημασία της συγκεκριμένης Οδηγίας βασίζεται αφ' ενός στο ότι αποτέλεσε τη δεύτερη ευρωπαϊκή νομοθετική πράξη με παρεμφερές ρυθμιστικό αντικείμενο μετά από την

[55] Βλ. Άρθρα 12 της Οδηγίας 95/46/ΕΚ

[56] Βλ. Άρθρα 6 της Οδηγίας 95/46/ΕΚ

[57] Βλ. Άρθρα 28 της Οδηγίας 95/46/ΕΚ

ψήφιση της θεμελιώδους Οδηγίας 95/46/ΕΚ που εξετάστηκε στο προηγούμενο υποκεφάλαιο και αφ' ετέρου ότι επιχειρεί να «εισάγει» το κεκτημένο της ανωτέρω Οδηγίας στον τομέα των τηλεπικοινωνιών.

Ιδιαίτερη μνεία γίνεται στους λόγους που οδήγησαν στη θέσπιση της (υποκ. 2.2.1), καθώς και στις καινοτομίες που εισήγαγε η Οδηγία (υποκ. 2.2.2). Εν πολλοίς η Οδηγία επαναλαμβάνει τους ορισμούς και τις ρυθμίσεις της 95/46/ΕΚ. Ως εκ τούτου, οι καινοτομίες που εισάγει περιορίζονται στον νομικό ορισμό των βάσεων δεδομένων, καθώς και στην κατοχύρωση του αποκλειστικού πνευματικού δικαιώματος του δημιουργού της βάσης δεδομένων.

2.2.1: Οι λόγοι που οδήγησαν στη θέσπιση

Στην αιτιολογική έκθεση της Οδηγίας[58] αναφέρεται πως οι δύο βασικοί λόγοι που οδήγησαν στη θέσπιση της ήταν το γεγονός ότι δεν παρεχόταν σε όλα τα κράτη μέλη επαρκής προστασία για τις βάσεις δεδομένων, καθώς και ότι όπου αυτή υπήρχε διέφερε σημαντικά μεταξύ των κρατών. Συνεπώς οι λόγοι που οδήγησαν στη θέσπιση της σχετίζονταν τόσο με την ανεπάρκεια της νομικής προστασίας των βάσεων δεδομένων, όσο και με την ανομοιόμορφη νομική της ρύθμιση μεταξύ των ευρωπαϊκών κρατών. Περαιτέρω, στην αιτιολογική έκθεση τονίζονται οι αρνητικές επιπτώσεις της υφιστάμενης κατάστασης, δηλαδή η στρέβλωση της εσωτερικής αγοράς όσον αφορά τις βάσεις δεδομένων, και ιδιαίτερα τα εμπόδια που τίθενται στην ελευθερία των φυσικών και νομικών προσώπων να διαθέτουν προϊόντα και να παρέχουν υπηρεσίες σχετικές με βάσεις δεδομένων άμεσης επικοινωνίας.

Σημαντικό ρόλο αναμφισβήτητα διαδραμάτισε και η ιδιαιτερότητα του δικαιώματος του δημιουργού των βάσεων δεδομένων ως αποκλειστικό δικαίωμα και η ανάγκη ενίσχυσης της προστασίας του, προκειμένου να αποτραπεί η εξαγωγή ή και η επαναχρησιμοποίηση χωρίς προηγούμενη άδεια του περιεχομένου βάσεων δεδομένων. Επισημαίνεται λοιπόν ότι οι συγκεκριμένοι λόγοι δεν εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας 95/46/ΕΚ ο οποίος είχε τελείως διαφορετικό σκοπό, δηλαδή την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και η κατοχύρωση της ελεύθερης κυκλοφορίας αυτών των δεδομένων βάσει εναρμονισμένων κανόνων που προστατεύουν τα θεμελιώδη δικαιώματα του υποκειμένου.

2.2.2: Το περιεχόμενο της Οδηγίας

[58] Πρβλ. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31997L0066

Οι βασικότερες καινοτομίες που περιέχει η συγκεκριμένη Οδηγία περιλαμβάνουν το νομικό ορισμό της βάσης δεδομένων, καθώς και την κατοχύρωση του πνευματικού δικαιώματος του δημιουργού της βάσης δεδομένων. Πιο συγκεκριμένα, στο άρθρο 1 παρ. 2 της Οδηγίας ως βάση δεδομένων ορίζεται «η συλλογή έργων, δεδομένων ή άλλων ανεξάρτητων στοιχείων, διευθετημένων κατά συστηματικό ή μεθοδικό τρόπο και ατομικώς προσιτών με ηλεκτρονικά μέσα ή κατ' άλλον τρόπο[59]». Περαιτέρω, στα άρθρα 3 και 4 της Οδηγίας κατοχυρώνεται το πνευματικό δικαίωμα του δημιουργού της βάσης δεδομένων.

2.3: Ο Κανονισμός[60] 45/2001

Αναντίρρητα, η σημαντικότερη καινοτομία του Κανονισμού 45/2001 είναι η σύσταση της ανεξάρτητης ευρωπαϊκής εποπτικής αρχής «Ευρωπαίος Επόπτης Προστασίας Δεδομένων». Ειδικότερα, στο άρθρο 41 παρ. 2 του Κανονισμού προσδιορίζονται οι αρμοδιότητες του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, οι οποίες περιλαμβάνουν «την παρακολούθηση και την εξασφάλιση της εφαρμογής των διατάξεων του συγκεκριμένου κανονισμού, καθώς και κάθε άλλης κοινοτικής πράξης στον τομέα της προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από όργανο ή οργανισμό της Κοινότητας και επίσης την παροχή συμβουλών προς τα όργανα της Κοινότητας και προς τα υποκείμενα των δεδομένων για κάθε θέμα σχετικό με την επεξεργασία δεδομένων προσωπικού χαρακτήρα[61]».

Περαιτέρω, η επιλογή του Ευρωπαίου Επόπτη είναι τέτοια ώστε να διασφαλίζεται η αμερόληπτη και αποτελεσματική άσκηση των καθηκόντων του. Πιο συγκεκριμένα, στο άρθρο 42 του Κανονισμού ορίζεται ότι «ο Ευρωπαίος Επόπτης διορίζεται με κοινή συμφωνία από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρώπης για θητεία πέντε ετών, η οποία μπορεί να ανανεωθεί, βάσει καταλόγου που συντάσσει η Επιτροπή κατόπιν δημόσιας πρόσκλησης για υποβολή υποψηφιοτήτων[62]». Επιπλέον, στην παράγραφο 2 του ίδιου άρθρου διευκρινίζεται ότι ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων επιλέγεται μεταξύ προσώπων τα οποία παρέχουν εχέγγυα

[59] Βλ. Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, Διαθέσιμο σε: http://3lykeiolamias.gr/sites/default/files/files/pdf/odhgia_97-66.pdf

[60] Εναντιθέσει με την Οδηγία, ο Κανονισμός δεν απαιτεί την ενσωμάτωση του στο εθνικό δίκαιο των κρατών για να τεθεί σε ισχύ, αλλά αντίθετα εφαρμόζεται απευθείας και υποχρεωτικά σε όλα τα κράτη μέλη της ΕΕ ταυτοχρόνως.

[61] Βλ. Κανονισμός 45/2001/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Δεκεμβρίου 2000, Διαθέσιμο σε: https://www.lawspot.gr/nomikes-plirofories/nomothesia/kanonismos-45-2001-ek-toy-eyropaikoy-koinovoylioy-kai-toy-symvoylioy

[62] Βλ. ΕΕ L 008 της 12/01/2001 σ. 1-22

ανεξαρτησίας και που διαθέτουν αξιόλογη εμπειρία και ικανότητες για την εκπλήρωση των καθηκόντων τους[63].

2.4: Η σχετική νομολογία του ΔΕΕ

Στο συγκεκριμένο υποκεφάλαιο επιδιώκεται να εξεταστεί ο τρόπος με τον οποίο το Δικαστήριο της Ευρωπαϊκής Ένωσης επεξεργάστηκε και ερμήνευσε τα προηγουμένως εξετασθέντα νομοθετήματα με αφορμή την υπόθεση Agencia Espanola κατά Google Spain (1996).

2.4.1: Η υπόθεση[64]

Το 1996 ο Ισπανός πολίτης Mario Costeja Gonzalez δεν κατόρθωσε να αποπληρώσει τα χρέη του στο Ταμείο Κοινωνικής Ασφάλισης του, γεγονός που οδήγησε στη δημοπρασία της ακίνητης περιουσίας του. Όπως ήταν φυσικό, η δημοπρασία δημοσιεύθηκε σε μία καταλανική εφημερίδα. Ωστόσο, παρά το γεγονός ότι το χρέος του κ. Gonzalez αποπληρώθηκε, το σχετικό άρθρο για τη δημοπρασία που ανέφερε και το όνομα του παρέμενε διαθέσιμο στο διαδίκτυο.

Έπειτα από δεκατέσσερα χρόνια συνέχισης της εν λόγω κατάστασης, ο κ. Gonzalez υπέβαλε αναφορά στην Ισπανική Αρχή Προστασίας Προσωπικών Δεδομένων, καταγγέλοντας ότι όταν πληκτρολογούσε το όνομα του στη μηχανή αναζήτησης του Google search engine, εμφανιζόταν το άρθρο που αφορούσε τη δημοπρασία της περιουσίας του για την αποπληρωμή του χρέους του.

Το επιχείρημα του κ. Gonzalez ήταν ότι εφόσον η δημοπρασία πραγματοποιήθηκε 14 χρόνια πριν και ότι πλέον το χρέος του είχε αποπληρωθεί, οποιαδήποτε υπόμνηση της υπόθεσης ήταν ανούσια και έπρεπε να αφαιρεθεί από το διαδίκτυο. Ετσι, ο αιτών ζητούσε, η εφημερίδα να διαγράψει το όνομά του από τα σχετικά δημοσιεύματα και η Google να αφαιρέσει τα συγκεκριμένα προσωπικά του δεδομένα από τα αποτελέσματα που παρέχει στους χρήστες της.

Η Ισπανική Αρχή Προστασίας Προσωπικών Δεδομένων εν μέρει αποδέχθηκε τα επιχειρήματα του κ.Gonzalez, αναφέροντας ότι ενώ η δημοσίευση του άρθρου ήταν νόμιμη, καθώς ήταν απαραίτητη για την προσέλκυση του μεγαλύτερου δυνατού αριθμού υποψηφίων αγοραστών, η Google όφειλε να αφαιρέσει πλέον το άρθρο.

Όπως ήταν αναμενόμενο η Google Inc. προσέφυγε έναντι της απόφασης στο Ανώτατο Ισπανικό Δικαστήριο. Με τη σειρά του το Ανώτατο Δικαστήριο υπέβαλε προδικαστικό ερώτημα στο Δικαστήριο της Ευρωπαϊκής Ένωσης αναφορικά με την ερμηνεία συγκεκριμένων διατάξεων της

---

[63] Βλ. H. Kranenborg, Άρθρο 8, σε: S. Peers (επιμ.), «The EU Charter of Fundamental Rights, A Commentary», 2014, σ. 223 επ.

[64] Οι πληροφορίες για το πραγματικό της υπόθεσης αντλούνται πρωτίστως από το άρθρο E. Karchimakis, «The Right to be Forgotten», Constitutionalism.gr, Διαθέσιμο σε: https://www.constitutionalism.gr/karchimakis-the-right-to-be-forgotten/

Οδηγίας 95/46/ΕΚ καθώς και του Χάρτη των Θεμελιωδών δικαιωμάτων σε σχέση με την πληροφοριακή αυτοδιάθεση.

2.4.2: Η θέση του Δικαστηρίου της Ευρωπαϊκής Ένωσης

Εν πρώτοις, το Δικαστήριο της Ευρωπαϊκής Ένωσης υπήγαγε στην έννοια της επεξεργασίας προσωπικών δεδομένων της Οδηγίας 95/46/ΕΚ τις συγκεκριμένες δραστηριότητες της Google. Επομένως, η Google μπορεί να χαρακτηριστεί ως υπεύθυνος επεξεργασίας προσωπικών δεδομένων υπό την έννοια της Οδηγίας 95/46/ΕΚ. Στο συγκεκριμένο σημείο η άποψη του Δικαστηρίου συμπίπτει με αυτήν της Ισπανικής Αρχής Προστασίας Προσωπικών Δεδομένων.

Επιπλέον, στην ανάλυση του το Δικαστήριο της Ευρωπαϊκής Ένωσης επιβεβαίωσε τις βασικές αρχές της Οδηγίας, δηλαδή το δικαίωμα του κάθε ατόμου να ελέγχει τις πληροφορίες που αναφέρονται στο όνομα του. Η χρήση των συγκεκριμένων πληροφοριών, οι οποίες εμπίπτουν στην έννοια των προσωπικών δεδομένων, χωρίς τη συγκατάθεση του υποκειμένου απαγορεύεται.

Περαιτέρω, το Δικαστήριο ανέφερε ότι το δικαίωμα στη λήθη, αποτελεί πτυχή του δικαιώματος της ιδιωτικής ζωής και είναι σπουδαιότερο τόσο από το δικαίωμα της πληροφόρησης. Η μόνη εξαίρεση σε αυτό τον κανόνα είναι στην περίπτωση ενός δημόσιου προσώπου που διαδραματίζει κάποιο σημαντικό ρόλο στην κοινωνική ζωή. Στην προκειμένη περίπτωση πάντως το Δικαστήριο απεδέχθη τη δημοσίευση αυτών των πληροφοριών ακόμη και χωρίς τη συγκατάθεση του υποκειμένου.

Στο ίδιο πλαίσιο, το Δικαστήριο επιβεβαίωσε τις βασικές αρχές επεξεργασίας προσωπικών δεδομένων δηλαδή το ότι τα δεδομένα μπορούν να επεξεργάζονται μόνο για συγκεκριμένο, εξειδικευμένο και θεμιτό-νόμιμο σκοπό με ασφάλεια και ακρίβεια. Η επεξεργασία ευαίσθητων δεδομένων όπως η φυλή, η εθνικότητα, η εθνική ή θρησκευτική ταυτότητα, όπως επίσης και πληροφορίες για την υγεία και τη σεξουαλικότητα των ατόμων διέπονται από αυστηρότερους κανόνες.

Βάσει των ανωτέρω σκέψεων λοιπόν το Δικαστήριο της Ευρωπαϊκής Ένωσης αναγνώρισε το δικαίωμα των υποκειμένων να ζητούν τη διαγραφή των δεδομένων τους, ακόμη και στις περιπτώσεις που η αρχική επεξεργασία τους έγινε νόμιμα.

Συνεπώς το δικαστήριο συμπέρανε ότι ο υπεύθυνος επεξεργασίας ο οποίος δημοσιεύει δεδομένα σε τρίτο πρόσωπο χωρίς τη συγκατάθεση του υποκειμένου υποχρεούται να τα διαγράψει κατ' απαίτηση του ακόμη και στην περίπτωση που η δημοσίευση τους ήταν αρχικώς σύννομη όταν τα δεδομένα δεν εκπληρώνουν πλέον το σκοπό για τον οποίο έγινε η επεξεργασία τους, όταν τα δεδομένα είναι πλέον ανακριβή και δεν ανταποκρίνονται στην πραγματικότητα και παραβιάζουν την

αρχή της αναλογικότητας[65] (δηλαδή το μέτρο που είναι αναγκαία για την εκπλήρωση του σκοπού τους).

Είναι φυσικά γνωστό ότι, η Google αποτελεί έναν από τους μεγαλύτερους επεξεργαστές προσωπικών δεδομένων παγκοσμίως. Ετσι, η προαναφερθείσα απόφαση του ΔικΕΕ αναγνώρισε ουσιαστικά το «δικαίωμα στη λήθη» για τα υποκείμενα των δεδομένων και ταυτόχρονα τη σχετική υποχρέωση του κατόχου των δεδομένων, ενόσω, η απόφαση Google Spain κατά Costeja Gonzalez αποτελεί ορόσημο για την προστασία των προσωπικών δεδομένων σε ευρωπαϊκό, αλλά και σε παγκόσμιο επίπεδο.

2.5: Συμπεράσματα

Στο παρόν κεφάλαιο επιχειρήθηκε να εξεταστεί η ιστορική εξέλιξη της κατοχύρωσης της προστασίας των προσωπικών δεδομένων στο παράγωγο ενωσιακό δίκαιο. Όπως αναδείχθηκε, η ρύθμιση της προστασίας των προσωπικών δεδομένων πριν την ψήφιση του νέου κανονισμού στηρίχθηκε σε πολυάριθμες ατελείς ευρωπαϊκές νομοθετικές πράξεις, ενδεικτικό στοιχείο του πολυκερματισμού που επικρατούσε επί χρόνια στο ευρωπαϊκό νομικό πλαίσιο προστασίας των προσωπικών δεδομένων. Αναμφισβήτητα, οι βασικότερες νομοθετικές πράξεις ήταν η Οδηγία 95/46/ΕΚ που έδωσε τους βασικούς νομικούς ορισμούς των προσωπικών δεδομένων, της επεξεργασίας και του φορέα επεξεργασίας, καθώς και ο Κανονισμός 45/2001 που συνέστησε την Ευρωπαίο Επόπτη Προστασίας Προσωπικών Δεδομένων. Αυτό που αποδεικνύεται από την ανωτέρω ανάλυση είναι η ιδιαιτερότητα και ο δυναμικός χαρακτήρας του δικαιώματος της πληροφοριακής αυτοδιάθεσης, στοιχεία που δυσχεραίνουν την επαρκή ρύθμιση του. Ο δυναμικός χαρακτήρας οφείλεται στο γεγονός ότι η προστασία των δεδομένων συναρτάται με τη διαρκώς μεταβαλλόμενη και ταχύτατη τεχνολογική εξέλιξη, η οποία καθιστά σε σύντομο χρονικό διάστημα τη νομική της ρύθμιση παρωχημένη. Περαιτέρω, βασικό εμπόδιο στην επαρκή ρύθμιση της προστασίας των δεδομένων αποτέλεσε η άνιση τεχνολογική εξέλιξη μεταξύ των χωρών της ΕΕ και αντιστοίχως η ασύμμετρη ανάπτυξη του νομικού «οπλοστασίου» των κρατών για την προστασία του δικαιώματος. Χαρακτηριστικό παράδειγμα επιβεβαίωσης του ανωτέρω ισχυρισμού αποτελεί η προσπάθεια της Ένωσης ήδη από τα μέσα της δεκαετίας του 90’ να ρυθμίσει το ζήτημα σε επίπεδο Οδηγίας και αργότερα σε επίπεδο Κανονισμού.

[65] Βλ. Case C-131/12, Ct.J.EU (Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González) Διαθέσιμο σε: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d543eebb46b73f4314b9d5db2974a717d8.e34KaxiLc3qMb40Rch0SaxuSbhn0?text=&docid=138782&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=396824

Κεφάλαιο 3: Η πορεία προς τη μεταρρύθμιση του νομικού πλαισίου

Σε αυτό το κεφάλαιο επιχειρείται να παρουσιαστούν οι συνθήκες που κατέστησαν απαραίτητη τη θέσπιση του νέου Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων. Ειδικότερα, στο πρώτο υποκεφάλαιο αναλύονται οι πρόσφατες εξελίξεις που συντελέστηκαν στον τομέα των προσωπικών δεδομένων (ανάπτυξη των εφαρμογών-μέσων κοινωνικής δικτύωσης, ηλεκτρονική διακυβέρνηση, επέκταση των ηλεκτρονικών συναλλαγών) και τους κινδύνους που αυτά «εγκυμονούν» για τα προσωπικά δεδομένα, στο δεύτερο υποκεφάλαιο παρουσιάζεται η ασύμμετρη εφαρμογή των Οδηγιών από τα κράτη μέλη της ΕΕ, ενώ στο τρίτο υποκεφάλαιο εξετάζεται συνοπτικά το ιστορικό θέσπισης του Γενικού Κανονισμού, το οποίο θα μας βοηθήσει να κατανοήσουμε καλύτερα το περιεχόμενο του.

3.1: Οι πρόσφατες εξελίξεις στον τομέα των προσωπικών δεδομένων στην ΕΕ

Η τεχνολογία και οι εφαρμογές της αναπτύσσονται καθημερινά με αλματώδεις ρυθμούς. Αυτή η ραγδαία ανάπτυξη έχει επιφέρει πολλές αλλαγές, μια εκ των οποίων και στον τρόπο αντίληψης του όρου και του περιεχόμενού της ιδιωτικότητας. Αυτό συμβαίνει διότι πλέον πλήθος δεδομένων συλλέγονται, επεξεργάζονται και μεταφέρονται καθημερινά κυρίως μέσω της χρήσης ηλεκτρονικών υπολογιστών με γεωμετρικά αυξανόμενο ρυθμό.

Αυτό φυσικά ενισχύεται από τις πρακτικές της σύγχρονης δημόσιας διοίκησης, η οποία απαιτεί ευέλικτες και διαφανείς διαδικασίες με σκοπό τον περιορισμό του γραφειοκρατικού συστήματος, τη μείωση του διοικητικού και λειτουργικού κόστους, την καλύτερη αξιοποίηση του υφιστάμενου ανθρώπινου δυναμικού και γενικότερα τη συρρίκνωση των δημόσιων δαπανών (ηλεκτρονική διακυβέρνηση). Στο γενικό αυτό πλαίσιο, παρατηρείται μεγάλη ενίσχυση αυτής της κατάστασης μέσω της «απλόχερης» διάθεσης των προσωπικών πληροφοριών των φυσικών προσώπων σε παγκόσμιο επίπεδο, αφού στο διαδίκτυο δεν υφίστανται σύνορα, ενώ ταυτόχρονα η χρησιμοποίηση του «υπολογιστικού νέφους» επιτρέπει την αποστολή και επεξεργασία πάσης φύσεως δεδομένων, όπως, λ.χ. των δεδομένων υγείας σε οποιοδήποτε μέρος.

Έτσι, γίνεται αντιληπτό, ότι η πρωτόγνωρη χρήση των τεχνολογικών εφαρμογών έχει επιφέρει νέες προκλήσεις στην προστασία των προσωπικών δεδομένων. Το γεγονός αυτό αποκτά βαρύνουσα σημασία αν αναλογιστεί κανείς ότι η αποκάλυψη των δεδομένων είναι δυνατόν να επηρεάσει τη ζωή, την εξέλιξη και την πορεία ενός ατόμου, καθώς εκθέτει το άτομο σε στιγματισμό, σε πιθανές διακρίσεις και κατ' επέκταση σε περιορισμό των επιλογών του.

Επομένως, οι σημαντικές εξελίξεις που συντελέστηκαν περιλαμβάνουν την αλματώδη ανάπτυξη και επέκταση της χρήσης των μέσων κοινωνικής δικτύωσης[66] (Facebook, Instagram, Google+), την

[66] Βλ. J. Kietzmann, «Social media? Get serious! Understanding the functional building blocks of social media», σε: *Business Horizons*, 54 (3), 2011, σ. 241–251

ηλεκτρονική διακυβέρνηση, καθώς και την επέκταση των ηλεκτρονικών συναλλαγών (τραπεζικές συναλλαγές κτλ.). Οι συγκεκριμένες εξελίξεις εγκυμονούν νέους σημαντικούς κινδύνους για τα προσωπικά δεδομένα και κατέστησαν απαραίτητη τη μεταρρύθμιση του νομικού πλαισίου.

3.2: Η ασύμμετρη εφαρμογή των Οδηγιών από τα κράτη μέλη

Ένας παράγοντας που επίσης διαδραμάτισε σημαντικό ρόλο στη μεταρρύθμιση του νομικού πλαισίου για την προστασία των προσωπικών δεδομένων ήταν η ασύμμετρη εφαρμογή των προηγούμενων Οδηγιών από τα κράτη μέλη. Η ασύμμετρη εφαρμογή οφειλόταν αφ' ενός στην ιδιαιτερότητα ορισμένων μελών που βρίσκονται σε εξαιρετικό καθεστώς (πχ Βρετανία), στην ανομοιόμορφη τεχνολογική εξέλιξη στις χώρες της ΕΕ, καθώς και στη μορφή των νομοθετικών πράξεων της ΕΕ, δηλαδή στην επιλογή της Οδηγίας έναντι του κανονισμού που «αφήνει» μεγαλύτερη ελευθερία στα κράτη μέλη όσον αφορά την ενσωμάτωση τους στην εθνική έννομη τάξη[67].

Σε μεγάλο βαθμό η ανάγκη για ενιαία και συνεκτική ρύθμιση της προστασίας των προσωπικών δεδομένων στις χώρες της ΕΕ με τη μορφή Κανονισμού δρομολογήθηκε από τη ραγδαία τεχνολογική ανάπτυξη, που άρχισε πλέον να «ομογενοποιείται» σε όλες τις χώρες της Ευρωπαϊκής Ένωσης. Η ραγδαία ανάπτυξη και διάδοση των μέσων κοινωνικής δικτύωσης, σε συνδυασμό με τη νομολογιακή επεξεργασία που οι προηγούμενες ρυθμίσεις (παλαιότερες Οδηγίες) είχαν τύχει από τα εθνικά δικαστήρια και τις Εποπτικές Αρχές των κρατών μελών, δημιούργησαν «πρόσφορο» έδαφος για τη θέσπιση του νέου Κανονισμού.

3.2.1: Στη Βρετανία

Στο Ηνωμένο Βασίλειο, το οποίο δεν έχει γραπτό σύνταγμα, η προστασία των δεδομένων δεν είχε αρχικά ιδιαίτερο καθεστώς, αλλά η χώρα έχει ενσωματώσει τώρα την Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα στο εσωτερικό της σύστημα και έχει δώσει αυξημένη τυπική ισχύ.

Μπορεί μάλιστα επομένως να υποστηριχθεί ότι η προστασία των δεδομένων απορρέει από τα δικαιώματα που κατοχυρώνονται στη Σύμβαση, όπως για παράδειγμα το δικαίωμα της «ιδιωτικής και οικογενειακής ζωής» το οπίο μάλιστα τώρα έχει ενισχυμένη προστασία στη χώρα αυτή, σε σχέση με τα υπόλοιπα δικαιώματα της Σύμβασης. Σε πολλά άλλα κράτη μέλη, η σχέση μεταξύ προστασίας δεδομένων και ΕΣΔΑ έχει συνέπειες λόγω του ειδικού καθεστώτος (ενίοτε υπερβολικά συνταγματικού) χαρακτήρα της Σύμβασης στο οικείο εθνικό σύστημα.

3.2.2: Στη Δανία

Στη Δανία δεν υπάρχει πολύ σταθερή συνταγματική βάση για την προστασία των δεδομένων. Δεν υπάρχει δηλαδή ειδική συνταγματική διάταξη που να αναφέρεται σε αυτήν, ούτε και διάταξη για

[67] Βλ. Hunton & Williams, «The Proposed EU General Data Protection Regulation A guide for in-house lawyers», 2015, σ. 14

την ιδιωτική ζωή. Η Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα εφαρμόζεται άμεσα στη Δανία αλλά δεν διαθέτει ενισχυμένο καθεστώς.

3.2.3: Συγκριτική παρουσίαση των ορισμών στα εθνικά νομοθετήματα[68]

Οι νόμοι στα περισσότερα κράτη μέλη που έχουν εφαρμόσει την Οδηγία ορίζουν την έννοια των «προσωπικών δεδομένων» ουσιαστικά σύμφωνα με τον (βασικό) ορισμό της Οδηγίας, όπως εκτίθεται ανωτέρω. Αυτό μπορεί να θεωρηθεί ότι συμβαίνει στο Βέλγιο, τη Δανία, τη Φινλανδία, τη Γερμανία, την Ελλάδα, την Ολλανδία, την Πορτογαλία, την Ισπανία, τη Σουηδία και το Ηνωμένο Βασίλειο. Ο προτεινόμενος νέος (τροποποιημένος) νόμος στη Γαλλία περιέχει επίσης (νέο) ορισμό των «προσωπικών δεδομένων» σύμφωνα με τους ορισμούς της Οδηγίας, αν και με κάποιες διαφορές, όπως αναφέρεται παρακάτω.

Οι νόμοι σε ορισμένες από τις προαναφερθείσες χώρες (Ελλάδα, Δανία, Σουηδία και Ισπανία) δεν παρέχουν τη λεπτομερή διευκρίνιση που παρέχεται από την Οδηγία για το τι πρέπει να θεωρείται ως πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, αλλά αυτό φαίνεται να είναι κυρίως θέμα τεχνικής νομοθετικής σύνταξης: όπως περιγράφεται παρακάτω, διασαφηνίζεται και αυτό στους νόμους αυτούς οι διευκρινίσεις σχετικά με πρόσωπα που μπορούν να ταυτοποιηθούν «άμεσα ή έμμεσα».

Ο προτεινόμενος νέος νόμος στη Γαλλία, επί παραδείγματι, αναφέρεται σε φυσικά πρόσωπα τα οποία μπορούν να εντοπιστούν, άμεσα ή έμμεσα, με αναφορά σε έναν αριθμό αναγνώρισης ή σε έναν ή περισσότερους παράγοντες που είναι συγκεκριμένοι για το συγκεκριμένο πρόσωπο, δηλαδή ο νόμος δεν διευκρινίζει είδη των παραγόντων που αναφέρονται στην Οδηγία, αλλά από την άλλη δεν χρησιμοποιεί και τον όρο ειδικότερα. Ο προτεινόμενος νέος νόμος επίσης δεν αναφέρει ρητώς ότι η έννοια των προσωπικών δεδομένων καλύπτει δεδομένα οποιασδήποτε μορφής (όπως αυτά που τίθενται στον ισχύοντα νόμο).

Ο νόμος στο Ηνωμένο Βασίλειο κάνει μια τυπική διάκριση μεταξύ δεδομένων και πληροφοριών που περιπλέκει την ορολογία που χρησιμοποιείται στον νόμο, αλλά δεν έχει ουσιαστικό αποτέλεσμα. Σημαντικότερο είναι το γεγονός ότι ο νόμος σε αυτό το κράτος, αντί να αναφέρεται σε δεδομένα που μπορούν να συνδεθούν άμεσα ή έμμεσα με ένα συγκεκριμένο άτομο, αναφέρεται σε δεδομένα που αφορούν ένα ζωντανό άτομο που μπορεί να αναγνωριστεί από αυτά τα δεδομένα ή και άλλες πληροφορίες που βρίσκονται στην κατοχή του ή είναι πιθανόν να τεθούν στην κατοχή του.

Όταν ο νόμος επανεξετάστηκε από την κυβέρνηση στο πλαίσιο του λεγόμενου αρκετά ενδιαφερόμενα μέρη δήλωσαν ότι αντιμετωπίζουν δυσκολίες με αυτόν τον ορισμό. Ο νόμος για την προστασία των δεδομένων στην Ιρλανδία (προ της εφαρμογής) υιοθετεί την ίδια προσέγγιση με τον νόμο του Ηνωμένου Βασιλείου, ορίζοντας τα δεδομένα προσωπικού χαρακτήρα ως δεδομένα σχετικά με ένα άτομο που είναι ή μπορεί να προσδιορίζεται είτε από τα δεδομένα είτε από τα

[68] Τα στοιχεία του υποκεφαλαίου αντλούνται από τη μελέτη του D. Korff, «EC Study on Implementation Of Data Protection Directive-comparative summary of national laws», University of Cambrige, 2002, Διαθέσιμο σε: https://gegevensbeschermingsrecht.nl/onewebmedia/douwe.pdf

δεδομένα σε συνδυασμό με άλλες πληροφορίες που βρίσκονται στην κατοχή του υπεύθυνου επεξεργασίας δεδομένων.

Εν τούτοις, πρέπει να σημειωθεί ότι ο νέος ιρλανδικός νόμος περιέχει επίσης μια διάταξη σύμφωνα με την οποία μια λέξη ή μια έκφραση που χρησιμοποιείται στην παρούσα Πράξη, καθώς και στην Οδηγία (95/46/ΕΚ), εκτός εάν το κείμενο απαιτεί διαφορετικά, έχει την ίδια έννοια με αυτή την Πράξη όπως στην Οδηγία.

Καταρχάς είναι σημαντικό να ανφέρουμε ότι, το άρθρο 35 του Πορτογαλικού Συντάγματος του 1975 παρείχε σε όλους τους πολίτες το δικαίωμα πληροφόρησης για το περιεχόμενο των δεδομένων τους που βρίσκονται αποθηκευμένα σε τράπεζες δεδομένων, απαγόρευε την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων και έθετε σαφείς κανόνες για τη χρήση εθνικών αριθμών ταυτοποίησης. Επίσης, ο ειδικός για την προστασία των δεδομένων προσωπικού χαρακτήρα νόμος της Πορτογαλίας[69] προσθέτει ρητώς ότι κάθε πληροφορία σημαίνει κάθε είδους πληροφορία ανεξάρτητα από το είδος του μέσου που εμπλέκεται, συμπεριλαμβανομένων των δεδομένων ήχου και εικόνων.

Ο νόμος στο Λουξεμβούργο[70] τονίζει επίσης ότι η έννοια καλύπτει πληροφορίες κάθε είδους, ανεξάρτητα από το μέσο αποθήκευσης, συμπεριλαμβανομένων των δεδομένων ήχου και εικόνων. Και στη Γαλλία, εδώ και πολύ καιρό θεωρείται ότι τα δεδομένα ήχου και εικόνας αποτελούν προσωπικά δεδομένα εάν είναι σε ψηφιακή μορφή και μπορούν να σχετίζονται με ένα αναγνωρίσιμο άτομο. Όπως σημειώνεται περαιτέρω παρακάτω, ο νόμος στη Φινλανδία[71] δηλώνει ρητά ότι εφαρμόζεται όχι μόνο σε πληροφορίες σχετικά με ένα άτομο, αλλά και σε πληροφορίες για μια οικογένεια ή ένα νοικοκυριό. Επομένως, οι ορισμοί στις ανωτέρω χώρες τείνουν να καλύψουν και τις λεγόμενες «ψηφιακές πληροφορίες» δηλαδή ήχους ή εικόνες που μπορούν να ταυτοποιήσουν συγκεκριμένα πρόσωπα, καθώς και οικογένειες.

Προβληματικό είναι το γεγονός ότι οι νόμοι στην Αυστρία, την Ιταλία και το Λουξεμβούργο επεκτείνουν την έννοια του υποκειμένου των δεδομένων σε νομικά πρόσωπα. Αυτό σημαίνει ότι, στις χώρες αυτές, οι περιορισμοί στη συλλογή, αποθήκευση, γνωστοποίηση κ.λπ. δεδομένων σχετικά με φυσικά πρόσωπα (κατ' αρχήν) ισχύουν και για τα νομικά πρόσωπα και ότι τα νομικά πρόσωπα μπορούν (πάλι κατ' αρχήν) να ασκούν τα δικαιώματα των υποκειμένων των δεδομένων. Εδώ, οι διαφορές ορισμού οδηγούν σε σαφείς αποκλίσεις όσον αφορά την εφαρμογή του νόμου.

Το άλλο βασικό ζήτημα που σχετίζεται με τον ορισμό των προσωπικών δεδομένων είναι το ερώτημα κατά πόσο η έννοια αυτή είναι σχετική. Μπορούμε να διαβάσουμε τον ορισμό της Οδηγίας που υποδηλώνει ότι οποιαδήποτε δεδομένα που μπορεί να συνδέονται με ένα άτομο (με οποιονδήποτε τρόπο) πρέπει να θεωρούνται ως «προσωπικά» (ακόμα και αν κάποιος μπορεί να κάνει παραχωρήσεις ή να εφαρμόσει τους κανόνες με πιο χαλαρό τρόπο, αν και αυτή η δυνατότητα είναι

[69] Το κείμενο του αντίστοιχου πορτογαλικού νόμου είναι διαθέσιμο σε: https://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM στα αγγλικά

[70] Το κείμενο του αντίστοιχου νόμου είναι διαθέσιμο σε: https://cnpd.public.lu/en/legislation/droit-lux.html

[71] Το κείμενο του αντίστοιχου νόμου είναι διαθέσιμο σε: https://www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf

κάπως περιορισμένη). Ή κάποιος θα μπορούσε να ερμηνεύσει τη λέξη «μπορεί» ως αναφορά στις δυνατότητες κάποιου συγκεκριμένου προσώπου ή οργανισμού που μπορεί να έχει πρόσβαση στα δεδομένα. Τότε τα δεδομένα είναι «προσωπικά» για κάποιον που (ή κάποια οργάνωση) που «μπορεί» να συνδέσει τα δεδομένα σε ένα ταυτοποιημένο άτομο, αλλά όχι σε κάποιον που δεν μπορεί να δημιουργήσει μία τέτοια σύνδεση.

Η πρώτη προσέγγιση έχει το πλεονέκτημα ότι ο νομοθέτης και οι εποπτικές αρχές διασφαλίζουν καλύτερα τα δεδομένα. Δηλαδή, τα δεδομένα δεν «διαφεύγουν» από το κανονιστικό πλαίσιο αποκλειστικά και μόνο επειδή μεταβιβάζονται σε κωδικοποιημένη μορφή. Η δεύτερη προσέγγιση αντίθετα, έχει το πλεονέκτημα ότι δεν επεκτείνει τις υποχρεώσεις που επιβάλλονται από τους νόμους για την προστασία των δεδομένων σε πρόσωπα και οργανώσεις που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα τα οποία δεν έχουν καμία πρόθεση ούτε συνδέονται με συγκεκριμένα άτομα. Πράγματι, μερικές φορές θα είναι αδύνατο για τα άτομα που επεξεργάζονται κωδικοποιημένα δεδομένα να συμμορφώνονται με αυτές τις υποχρεώσεις (π.χ. όσον αφορά την ενημέρωση των υποκειμένων των δεδομένων με τα οποία δεν μπορούν να επικοινωνήσουν).

Το ζήτημα δεν επιλύεται με σαφήνεια στην Οδηγία. Οι άλλες γλωσσικές εκδοχές είναι εξίσου διφορούμενες από την άποψη αυτή. Ωστόσο, το 15ο προοίμιο προτείνει μια διαφορετική προσέγγιση. Αυτό το προοίμιο (το οποίο ασχολείται με δεδομένα ήχου και εικόνας) επιβεβαιώνει καταρχάς ότι η επεξεργασία τέτοιων δεδομένων υπόκειται μόνο στην Οδηγία, εάν η επεξεργασία αυτή είναι αυτοματοποιημένη ή εάν τα δεδομένα περιέχονται σε σύστημα υποβολής δεδομένων προσωπικού χαρακτήρα, ώστε να επιτρέπεται η εύκολη πρόσβαση στα εν λόγω προσωπικά δεδομένα. Αυτό μπορεί να θεωρηθεί ότι υπονοεί τη «σχετική» προσέγγιση, δηλαδή ένα άτομο που δεν έχει τα μέσα να συνδέσει συγκεκριμένα δεδομένα ήχου και εικόνας με ένα φυσικό πρόσωπο (ή που μπορεί να κάνει αυτή τη σύνδεση με δυσκολία) δεν έχει πρόσβαση στα δεδομένα.

Αυτό φαίνεται επίσης ότι είναι η προσέγγιση που ακολουθείται από τα περισσότερα κράτη μέλη. Ειδικότερα, ο νόμος του Λουξεμβούργου ορίζει ρητώς ότι εφαρμόζεται στη συλλογή, επεξεργασία και διάδοση δεδομένων ήχου και εικόνας που επιτρέπουν την αναγνώριση φυσικών ή νομικών προσώπων.

Οι νόμοι ή οι επίσημες διευκρινίσεις ή ερμηνείες των νόμων στην Αυστρία, τη Γερμανία, την Ελλάδα, την Ολλανδία και το Ηνωμένο Βασίλειο καθιστούν σαφές ότι στις χώρες αυτές τα κωδικοποιημένα δεδομένα πρέπει να θεωρούνται προσωπικά σε σχέση με πρόσωπο που έχει πρόσβαση σε αυτά. Ο όρος προσωπικά δεδομένα θεωρείται επίσης σχετικός στην Πορτογαλία. Στην Ιρλανδία, η αρχή προστασίας δεδομένων ήδη λαμβάνει υπόψιν την πιθανότητα ένα συγκεκριμένο άτομο να μπορεί να εντοπίσει ένα πρόσωπο από δεδομένα που έχει στην κατοχή του και οι λέξεις που προστέθηκαν στον ορισμό του νέου νόμου, πιο πάνω, να ενισχύει αυτή την προσέγγιση.

Το Βέλγιο έχει υιοθετήσει επίσημα την δεύτερη προσέγγιση, τουλάχιστον όσον αφορά τα κωδικοποιημένα δεδομένα έρευνας, δεδομένου ότι έχει εγκρίνει λεπτομερείς κανόνες σχετικά με την επεξεργασία για ερευνητικούς σκοπούς δεδομένων που είναι ασαφώς αναγνωρίσιμα,

κωδικοποιημένα και πλήρως ανώνυμα. Οι νόμοι στη Δανία[72], τη Φινλανδία, τη Γαλλία, την Ιταλία, την Ισπανία και τη Σουηδία είναι διφορούμενοι από αυτή την άποψη, αλλά οι αρχές τείνουν να συμφωνούν με τη βελγική προσέγγιση και να θεωρούν καταρχήν όλα τα δεδομένα που εξακολουθούν να συνδέονται με ένα άτομο προσωπικά, ακόμη και αν τα δεδομένα επεξεργάζονται από κάποιον που δεν μπορεί να κάνει αυτή τη σύνδεση.

Εντούτοις, είναι πρόθυμοι να είναι ευέλικτοι (λιγότερο απαιτητικοί) όσον αφορά την επεξεργασία δεδομένων που δεν μπορούν να προσδιοριστούν άμεσα, δεδομένου ότι το ερώτημα αν εφαρμόζεται ο νόμος σχετίζεται με την πιθανότητα ταυτοποίησης του υποκειμένου των δεδομένων και τη συνεκτίμηση της φύσης των δεδομένων. Όσο πιο ευαίσθητα είναι τα δεδομένα, τόσο πιο προσεκτική θα είναι η αρχή προστασίας δεδομένων, η οποία θα εξετάζει την πιθανότητα τα δεδομένα να είναι αναγνωρίσιμα και, κατά συνέπεια, την ανάγκη εφαρμογής του νόμου.

Οι αρχές της Δανίας έπρεπε, για παράδειγμα, να αποφανθούν για υπόθεση που αφορούσε τη διαβίβαση κωδικοποιημένων δεδομένων σε χώρα εκτός της ΕΕ και έκρινε, μεταξύ άλλων, ότι, επειδή τα δεδομένα κωδικοποιήθηκαν, εξασφαλίστηκε επαρκής προστασία, ενώ η νομοθεσία στη συγκεκριμένη τρίτη χώρα δεν παρέχει τέτοια προστασία. Αναγνωρίζουν επίσης ότι, ειδικά όσον αφορά τα δεδομένα ήχου και εικόνας, αυτό δεν αποτελεί ξεκάθαρο ζήτημα, διότι θα καθιστούσε όλες τις εικόνες που αναγνωρίζονται μέσω λογισμικού αναγνώρισης προσώπου προσωπικά δεδομένα. Από την άποψη αυτή, θα εξαρτήσουν την εφαρμογή του νόμου από τις συνθήκες και την πιθανότητα αναγνώρισης των προσώπων-υποκειμένων των δεδομένων.

Στον παρακάτω πίνακα παρουσιάζονται συγκεντρωτικά οι παράμετροι που οδήγησαν στη θέσπιση του Κανονισμού:

Παράμετροι που οδήγησαν στην ανάγκη για τον νέο Κανονισμό[73]	
άμεσες εξελίξεις σε επίπεδο τεχνολογίας	✓ Αύξηση της έκτασης και έντασης της συλλογής, ανταλλαγής και επεξεργασίας στοιχείων προσωπικού χαρακτήρα ✓ Αύξηση περιπτώσεων παραβίασης της ασφάλειας στοιχείων προσωπικού χαρακτήρα

[72] Το κείμενο του Δανικού νόμου είναι διαθέσιμο σε: https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf

[73] Βλ. Ευρωβαρόμετρο, Προστασία προσωπικών δεδομένων, Έρευνα 431, Στοιχεία 2015

ασύμμετρες εφαρμογές της Οδηγίας 95/46/ΕΚ από τα κράτη-μέλη	✓ Ανασφάλεια δικαίου - Αποκλίσεις κατά την εκτέλεση και εφαρμογή ✓ Στρέβλωση του ανταγωνισμού μεταξύ κρατών-μελών

3.3: Ιστορικό θέσπισης του Κανονισμού

Η εφαρμογή του Γενικού Κανονισμού για την Προστασία Στοιχείων (GDPR) ξεκίνησε επίσημα την 25η Μαΐου 2018, οδηγώντας στην κατάργηση της Οδηγίας 95/46/ΕΚ η οποία ως την ημερομηνία εκείνη αποτελούσε το βασικό νομικό πλαίσιο για την προστασία των στοιχείων προσωπικού χαρακτήρα στην Ευρώπη.

Ο Κανονισμός αποτέλεσε αντικείμενο έντονων διαβουλεύσεων και ενδεικτικό είναι το γεγονός ότι η Ευρωπαϊκή Επιτροπή επισήμανε την ανάγκη τροποποίησης της Οδηγίας από τον Ιανουάριο του 2012, το Ευρωπαϊκό Κοινοβούλιο υπερψήφισε το σχέδιο Κανονισμού το Μάρτιο του 2014 και η τελική συμφωνία μεταξύ του Κοινοβουλίου, της Επιτροπής και του Συμβουλίου επήλθε το Δεκέμβριο του 2015. Ο Κανονισμός ψηφίστηκε το Μάιο του 2016 και δόθηκε διετής περίοδος προσαρμογής στα κράτη-μέλη έως το Μάιο του 2018[74].

Η πολυετής (6,5 έτη) και σχετικά συγκρουσιακή πορεία έως την κατάρτιση του τελικού κειμένου του Κανονισμού καταδεικνύει την πολυπλοκότητα του συγκεκριμένου πεδίου πολιτικής, την υψηλή τεχνικότητα που το διέπει και την ταχύτητα με την οποία μεταβάλλονται οι τεχνολογικοί όροι που το επηρεάζουν (συχνά πριν προλάβει να ρυθμιστεί το πεδίο η τεχνολογία το έχει ήδη ξεπεράσει). Το τελικό κείμενο αποτέλεσε αντικείμενο έντονων διαπραγματεύσεων μεταξύ των διαφορετικών ομάδων συμφερόντων και τελικά πρόκειται για ένα «προϊόν» συμβιβασμού, γεγονός που αποδεικνύει τη σπουδαιότητα και τις οικονομικές του επεκτάσεις.

3.4: Συμπεράσματα

Στο σύντομο αυτό κεφάλαιο επιχειρήθηκε να αναδειχθούν συνοπτικά οι συνθήκες που κατέστησαν αναγκαία τη μεταρρύθμιση του νομικού πλαισίου και τη θέσπιση του Γενικού Κανονισμού Προστασίας Δεδομένων. Οι βασικότερες εξελίξεις που οδήγησαν στον GDPR υπήρξε η ραγδαία τεχνολογική ανάπτυξη, η επέκταση των ηλεκτρονικών συναλλαγών, η επέκταση της χρήσης των μέσων κοινωνικής δικτύωσης, καθώς και η ανάγκη για «σύγκλιση» των εθνικών νόμων των κρατών μελών που έως τότε ρύθμιζαν την προστασία των προσωπικών δεδομένων.

[74] Βλ. Hunton & Williams, «The Proposed EU General Data Protection Regulation-A guide for in house lawyers», 2015, σ. 14

Κεφάλαιο 4: Βασικά Χαρακτηριστικά του Κανονισμού

Καταρχάς, θα πρέπει να τονίσουμε ότι, σύμφωνα με το άρθρο 1 του Κανονισμού 679/2016 ο βασικός σκοπός του είναι η ελεύθερη ροή δεδομένων σε ολόκληρη την ενιαία ψηφιακή αγορά, η προστασία της ιδιωτικής ζωής των Ευρωπαίων και ενίσχυση της εμπιστοσύνης και της ασφάλειας των καταναλωτών και ταυτόχρονα η δημιουργία νέων ευκαιριών για τις επιχειρήσεις, κυρίως τις μικρότερες. Δημιουργείται ένα ενιαίο νομοθετικό πλαίσιο σε όλο το τον Ευρωπαικό χώρο, κάτι που μπορεί να συντελέσει αποφασιστικά στην ασφάλεια δικαίου για τις επιχειρήσεις. Οι ίδιοι κανόνες ισχύουν για όλες τις επιχειρήσεις που δραστηριοποιούνται στην ΕΕ, ακόμα κι εάν έχουν την έδρα τους εκτός της Ένωσης. Θεσπίζονται, ακόμη, νέα δικαιώματα για τους πολίτες όπως το δικαίωμα ενημέρωσης, πρόσβασης, ενώ το δικαίωμα στη λήθη ενισχύεται. Τέλος, τίθενται αυστηροί κανόνες και αποτρεπτικά πρόστιμα, καθώς όλες οι εθνικές αρχές προστασίας των προσωπικών δεδομένων θα έχουν την εξουσία να επιβάλλουν πρόστιμα έως 20 εκατ. ευρώ ή, σε περίπτωση εταιρείας, έως το 4% του παγκόσμιου ετήσιου κύκλου εργασιών της.

Στο παρόν κεφάλαιο επιχειρείται η παρουσίαση των βασικότερων στοιχείων του Κανονισμού. Ειδικότερα, στο πρώτο υποκεφάλαιο αναλύονται τα δικαιώματα του Υποκειμένου των δεδομένων όπως αυτά κατοχυρώνονται στο Κεφάλαιο 3 του Κανονισμού, στο δεύτερο υποκεφάλαιο εξετάζονται οι βασικότερες αλλαγές που επέφερε ο Κανονισμός, ενώ στο τρίτο υποκεφάλαιο αναλύεται η έναρξη της εφαρμογής του Κανονισμού. Επιπροσθέτως, το τρίτο υποκεφάλαιο περιέχει πίνακα με τις βασικές έννοιες και ρυθμίσεις του Κανονισμού για την εύληπτη παρουσίαση του, στο τέταρτο υποκεφάλαιο παρουσιάζεται το πεδίο ισχύος του Κανονισμού, και στο πέμπτο υποκεφάλαιο η νομιμοποιητική βάση της επεξεργασίας των δεδομένων. Τέλος, στο έκτο υποκεφάλαιο εξετάζεται η θεματική της ευθύνης και λογοδοσίας όπως ρυθμίζεται στον Κανονισμό, στο έβδομο υποκεφάλαιο οι προβλέψεις του Κανονισμού για την προστασία των δεδομένων κατά το σχεδιασμό και στο τελευταίο υποκεφάλαιο μελετάται ο αντίκτυπος του Κανονισμού.

4.1: Δικαιώματα του Υποκειμένου

Το Κεφάλαιο 3 του Κανονισμού για την Προστασία των Προσωπικών Δεδομένων κατοχυρώνει τα δικαιώματα του Υποκειμένου και επιμερίζεται σε πέντε τμήματα. Ειδικότερα, το πρώτο τμήμα τιτλοφορείται ως «Διαφάνεια και ρυθμίσεις» και περιλαμβάνει το, μεγάλης έκτασης, άρθρο 12.

Στην παράγραφο 1 του άρθρου 12 κατοχυρώνεται η υποχρέωση του υπεύθυνου επεξεργασίας να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία που αναφέρεται στα άρθρα 13 και 14 και κάθε ανακοίνωση στο πλαίσιο των άρθρων 15-22 και 34 (δηλαδή την ταυτότητα και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας και υπεύθυνου προστασίας των δεδομένων, τους σκοπούς και τη νομική βάση της επεξεργασίας, τους αποδέκτες των δεδομένων, την πρόθεση του υπεύθυνου επεξεργασίας για διαβίβαση των δεδομένων σε τρίτη χώρα ή οργανισμό, τη χρονική διάρκεια αποθήκευσης των συγκεκριμένων δεδομένων, τα έννομα συμφέροντα που επιδιώκονται

από την επεξεργασία, και τέλος το δικαίωμα του υποκειμένου για υποβολή διόρθωσης ανακριβών στοιχείων, καταγγελίας σε εποπτική αρχή και ανάκλησης της συγκατάθεσης[75]).

Περαιτέρω, ο υπεύθυνος επεξεργασίας βάσει του άρθρου είναι υποχρεωμένος να παρέχει τις ανωτέρω πληροφορίες σε συνοπτική, διαφανή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση. Συνεπώς παρατηρείται ότι η παράγραφος 1 του εξεταζόμενου άρθρου συγκεντρώνει ουσιαστικά όλες τις προστατευτικές ρυθμίσεις για τα προσωπικά δεδομένα που είχαν θεσπιστεί με παλαιότερα ευρωπαϊκά νομοθετήματα (επί παραδείγματι η υποχρέωση για γνωστοποίηση της ταυτότητας και των στοιχείων επικοινωνίας του υπεύθυνου επεξεργασίας έχει κατοχυρωθεί ήδη από την Οδηγία 95/46/ΕΚ).

Σημαντικές καινοτομίες που ωστόσο ενδέχεται να δημιουργήσουν ερμηνευτικά προβλήματα στην πράξη είναι οι προβλέψεις για αντίστοιχες υποχρεώσεις και από τον υπεύθυνο προστασίας των δεδομένων, καθώς και για την παροχή των εν λόγω πληροφοριών σε συνοπτική, διαφανή και εύκολα προσβάσιμη μορφή. Δοθέντος ότι οι συγκεκριμένες έννοιες είναι αρκετά γενικές και ότι δεν έχουν εξειδικευθεί επαρκώς ερμηνευτικά από τα Δικαστήρια, αναμένεται να ανακύψουν πολλαπλά ερμηνευτικά προβλήματα σε σχέση με το ποιές μορφές ανταποκρίνονται στο περιεχόμενο τους.

Στην παράγραφο 2 του ίδιου άρθρου κατοχυρώνεται η υποχρέωση του υπεύθυνου επεξεργασίας να διευκολύνει την άσκηση των δικαιωμάτων που αναφέρθηκαν ανωτέρω (πχ δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή, δικαίωμα πρόσβασης και υποβολής διορθώσεων σε ανακριβή στοιχεία κτλ). Το σημαντικό στοιχείο που κατοχυρώνεται σε αυτή την παράγραφο είναι ότι τονίζεται πως εφόσον η εκπλήρωση των στόχων της επεξεργασίας δεν απαιτεί πλέον τη συλλογή και αποθήκευση των προσωπικών δεδομένων, ο υπεύθυνος επεξεργασίας δεν δικαιούται να τα διατηρεί προκειμένου να συμμορφώνεται με τον παρόντα κανονισμό. Ουσιαστικά δηλαδή ξεκαθαρίζεται ότι δεν επιτρέπεται η επίκληση της συμμόρφωσης στις προβλέψεις του Κανονισμού για τη διασφάλιση της άσκησης των δικαιωμάτων του Υποκειμένου, όταν πλέον η διατήρηση και η επεξεργασία των δεδομένων δεν απαιτείται για το σκοπό που έχει δηλωθεί.

Έπειτα στην παράγραφο 3 του άρθρου κατοχυρώνεται η υποχρέωση του υπεύθυνου επεξεργασίας να παρέχει στο υποκείμενο δεδομένων τις πληροφορίες που απαιτούνται για την ενέργεια του αιτήματος που προβλέπεται στα άρθρα 15-22 το αργότερο εντός μηνός από την παραλαβή του αιτήματος. Ο Κανονισμός πάντως είναι μάλλον ελαστικός όσον αφορά τη χρονική προθεσμία, καθώς προβλέπει ότι αυτή μπορεί να παραταθεί κατά δύο ακόμη μήνες, λόγω της πολυπλοκότητας του αιτήματος και της πολλαπλότητας των αιτημάτων, υπό την προϋπόθεση όμως ότι το υποκείμενο των δεδομένων ενημερώνεται για αυτή την παράταση.

Στην παράγραφο 4 προβλέπεται ότι σε περίπτωση αδυναμίας του υπεύθυνου επεξεργασίας να ενεργήσει κατόπιν του αιτήματος του υποκειμένου, οφείλει να ενημερώσει εντός μηνός για τους λόγους για τους οποίους δεν ενήργησε, αλλά και να ενημερώσει επαρκώς το υποκείμενο των

[75] Πρβλ. το κείμενο του Κανονισμού στην ιστοσελίδα: https://www.lawspot.gr/nomikes-plirofories/nomothesia/genikos-kanonismos-gia-tin-prostasia-dedomenon?lspt_context=gdpr

δεδομένων για τη δυνατότητα άσκησης καταγγελίας αλλά και δικαστικής προσφυγής. Στο σημείο αυτό όπως είναι φυσικό ανακύπτει το ερώτημα ποιό όργανο ελέγχει τη συγκεκριμένη υποχρέωση του υπεύθυνου επεξεργασίας να παράσχει τις συγκεκριμένες πληροφορίες, σε περίπτωση για παράδειγμα που επιλέξει να παραπληροφορήσει το υποκείμενο και εάν αυτό συνεπάγεται κάποιο χρηματικό πρόστιμο.

Στο άρθρο 5 προβλέπεται μία μάλλον προστατευτική ρύθμιση για τους υπεύθυνους επεξεργασίας. Και τούτο διότι ορίζεται πώς σε περίπτωση που το αίτημα του υποκειμένου των δεδομένων είναι προδήλως αβάσιμα και υπερβολικά, ο υπεύθυνος επεξεργασίας μπορεί είτε να επιβάλει την καταβολή εύλογου τέλους, είτε να αρνηθεί να ικανοποιήσει το αίτημα. Πάντως στο άρθρο ορίζεται ότι η παροχή των πληροφοριών που προβλέπεται στα άρθρα 15-22 γίνεται δωρεάν.

Επιπλέον στην παράγραφο 6 ορίζεται ότι στην περίπτωση που ο υπεύθυνος επεξεργασίας έχει εύλογες αμφιβολίες για την ταυτότητα του υποκειμένου που υποβάλλει το αίτημα, μπορεί να ζητήσει την παροχή πρόσθετων πληροφοριών που απαιτούνται για την εξακρίβωση της ταυτότητας του. Η συγκεκριμένη διάταξη μάλλον περιπλέκει το περιεχόμενο του Κανονισμού, διότι προβλέπει με την επιφύλαξη όσων αναφέρθηκαν στο άρθρο 11 τη δυνατότητα του υπεύθυνου επεξεργασίας να ζητήσει επιπρόσθετες πληροφορίες για την ταυτοποίηση του υποκειμένου[76].

Το επόμενο τμήμα Κεφαλαίου τιτλοφορείται ως «Ενημέρωση και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα» και περιέχει τα άρθρα 13, 14 και 15. Ουσιαστικά στην παράγραφο 1 του άρθρου 13 προσδιορίζονται οι πληροφορίες που πρέπει να παρέχει ο υπεύθυνος επεξεργασίας στο υποκείμενο των δεδομένων οι οποίες περιλαμβάνουν την ταυτότητα και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας, τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων, τους σκοπούς και τη νομική βάση της επεξεργασίας, τους αποδέκτες των δεδομένων, τα έννομα συμφέροντα που επιδιώκονται από την επεξεργασία, καθώς και την πρόθεση, εάν υπάρχει, του υπεύθυνου επεξεργασίας να διαβιβάσει τα δεδομένα σε τρίτη χώρα ή σε άλλον οργανισμό.

Στο σημείο αυτό θα μπορούσε να παρατηρηθεί ότι οι πληροφορίες που υποχρεούται να παράσχει ο υπεύθυνος επεξεργασίας είναι επαρκείς για την προστασία των προσωπικών δεδομένων. Περαιτέρω, είναι σημαντικό ότι σε αυτές τις πληροφορίες περιλαμβάνονται και τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας των δεδομένων, χωρίς όμως αυτό να περιλαμβάνει και την ταυτότητα του.

Έπειτα στην παράγραφο 2 ορίζονται οι επιπρόσθετες πληροφορίες που υποχρεούται να παράσχει ο υπεύθυνος επεξεργασίας οι οποίες περιλαμβάνουν το χρονικό διάστημα αποθήκευσης των προσωπικών δεδομένων, την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων, την ύπαρξη δικαιώματος

[76] Βλ. Β. Τζώρτζη, «Προστασία Δεδομένων Προσωπικού Χαρακτήρα», Εκδ. Νομική Βιβλιοθήκη, 2018, σ. 198 επ.

ανάκλησης της συγκατάθεσης του υποκειμένου, καθώς και το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή.

Τέλος, στην παράγραφο 3 ότι προβλέπεται η υποχρέωση του υπεύθυνου επεξεργασίας να ενημερώνει το υποκείμενο των δεδομένων σε περίπτωση μεταβολής του σκοπού επεξεργασίας των δεδομένων. Οι συγκεκριμένες προβλέψεις κρίνονται επαρκείς για την προστασία των προσωπικών δεδομένων. Κατ' ουσίαν το άρθρο 14 αποτελεί μία επανάληψη των προβλέψεων του άρθρου 13, δηλαδή προβλέπει την υποχρέωση του υπεύθυνου επεξεργασίας για παροχή των ίδιων πληροφοριών στο υποκείμενο και στις περιπτώσεις που τα δεδομένα δεν συλλέγονται από αυτό.

Η μόνη διαφορά εντοπίζεται στην παράγραφο 5 η οποία ουσιαστικά ορίζει ότι οι ανωτέρω υποχρεώσεις δεν εφαρμόζονται στις περιπτώσεις που τα υποκείμενα δεδομένων διαθέτουν ήδη τις πληροφορίες, όταν η παροχή αυτών των πληροφοριών αποδεικνύεται αδύνατη, καθώς και στις περιπτώσεις που τα δεδομένα πρέπει να παραμείνουν εμπιστευτικά δυνάμει επαγγελματικού απορρήτου που ρυθμίζεται από το δίκαιο της Ένωσης ή από το εθνικό δίκαιο (για παράδειγμα ιατρικό απόρρητο[77]).

Έπειτα, στο άρθρο 15 κατοχυρώνονται τα δικαιώματα του υποκειμένου για πρόσβαση στις πληροφορίες που αφορούν τους σκοπούς της επεξεργασίας, τις σχετικές κατηγορίες των δεδομένων, τους αποδέκτες τους, το χρόνο αποθήκευσης τους, την ύπαρξη δικαιώματος υποβολής αιτήματος για διόρθωση ή διαγραφή των δεδομένων και το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή. Μάλιστα τονίζεται ότι σε περίπτωση διαβίβασης των δεδομένων σε τρίτη χώρα ή οργανισμό το υποκείμενο δικαιούται να λαμβάνει ενημέρωση για τις κατάλληλες εγγυήσεις και κατοχυρώνεται η υποχρέωση του υπεύθυνου επεξεργασίας για παροχή αντιγράφου των δεδομένων που υποβάλλονται σε επεξεργασία.

Το τμήμα 3 του κεφαλαίου τιτλοφορείται ως Διόρθωση και διαγραφή και περιλαμβάνει τα άρθρα 16-20 του Κανονισμού. Πιο συγκεκριμένα, στο άρθρο 16 κατοχυρώνεται το δικαίωμα του υποκειμένου να απαιτεί από τον υπεύθυνο επεξεργασίας τη διόρθωση τυχόν ανακριβών στοιχείων που το αφορούν, είτε τη συμπλήρωση τους εφόσον το απαιτεί ο σκοπός της επεξεργασίας.

Έπειτα, στο άρθρο 17 κατοχυρώνεται το λεγόμενο «δικαίωμα στη λήθη», δηλαδή το δικαίωμα του υποκειμένου να απαιτεί τη διαγραφή των προσωπικών του δεδομένων από τον υπεύθυνο επεξεργασίας όταν πλέον η διατήρηση τους δεν κρίνεται απαραίτητη για τους αρχικούς στόχους της επεξεργασίας, όταν το υποκείμενο ανακαλεί τη συγκατάθεση του, όταν τα δεδομένα υποβλήθηκαν σε επεξεργασία παράνομα και όταν τα δεδομένα πρέπει να διαγραφούν λόγω νομικής υποχρέωσης που προκύπτει από το ενωσιακό ή το εθνικό δίκαιο.

Στο άρθρο 18 κατοχυρώνεται το δικαίωμα του υποκειμένου να αξιώνει τον περιορισμό της επεξεργασίας όταν η ακρίβεια των δεδομένων αμφισβητείται από το υποκείμενο, όταν η επεξεργασία είναι παράνομη, όταν η επεξεργασία των δεδομένων δεν απαιτείται πλέον για την

[77] Βλ. Λ. Κοτσαλή, «Γενικός Κανονισμός Προστασίας Δεδομένων», Εκδ. Νομική Βιβλιοθήκη, 2018, σ. 147

εκπλήρωση των στόχων της, καθώς και όταν το υποκείμενο προβάλλει αντιρρήσεις για τη νομιμότητα του σκοπού επεξεργασίας των δεδομένων κατά το άρθρο 21 παρ. 1.

Στο άρθρο 19 κατοχυρώνεται η υποχρέωση του υπεύθυνου επεξεργασίας να ενημερώνει τόσο το ίδιο το υποκείμενο, όσο και τους αποδέκτες των δεδομένων σχετικά με οποιαδήποτε διόρθωση και αλλαγή συντελείται σε αυτά βάσει των άρθρων 16, 17 παρ. 1 και 18. Εν συνεχεία, το άρθρο 20 κατοχυρώνει το δικαίωμα του υποκειμένου να λαμβάνει τα προσωπικά του δεδομένα σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να τα διαβιβάζει σε άλλον χωρίς την αντίρρηση του υπεύθυνου επεξεργασίας εφόσον η επεξεργασία γίνεται με τη συγκατάθεση του[78] και καθώς η επεξεργασία γίνεται με αυτοματοποιημένα μέσα.

Επομένως, μέσα από αυτή τη ρύθμιση καθίσταται γνωστό ότι η παροχή συγκεκριμένων προσωπικών δεδομένων σε ορισμένο υπεύθυνο επεξεργασίας δύνανται να διαβιβαστούν και σε τρίτο εφόσον το ζητήσει το υποκείμενο και μάλιστα το υποκείμενο μπορεί να ζητήσει και από τον ίδιο τον υπεύθυνο επεξεργασίας να τα διαβιβάσει, εφόσον αυτό είναι τεχνικά εφικτό (παρ. 2).

Πάντως στις παραγράφους 3 και 4 ορίζεται ότι το συγκεκριμένο δικαίωμα δεν ισχύει όταν η επεξεργασία είναι απαραίτητη όταν γίνεται για την εκπλήρωση δημοσίου συμφέροντος ή κατά την άσκηση δημόσιας εξουσίας, ούτε βέβαια όταν επηρεάζει δυσμενώς δικαιώματα και ελευθερίες άλλων. Τα άρθρα 21 και 22 του Γενικού Κανονισμού περιλαμβάνονται στο Τμήμα 4 με τίτλο «Δικαίωμα εναντίωσης και αυτοματοποιημένη ατομική λήψη αποφάσεων».

Κατ' ουσίαν τόσο το άρθρο 21, το οποίο απαρτίζεται από 6 παραγράφους, όσο και το άρθρο 22 κατοχυρώνουν το δικαίωμα αντίταξης του υποκειμένου στην επεξεργασία των δεδομένων του και κυρίως στις περιπτώσεις που τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία για εμπορικούς σκοπούς (εμπορική προώθηση, κατάρτιση προφίλ κτλ.).

Περαιτέρω στις παραγράφους 5 και 6 του άρθρου 21 κατοχυρώνεται το δικαίωμα εναντίωσης του υποκειμένου στην περίπτωση επεξεργασίας των δεδομένων του από αυτοματοποιημένα μέσα που χρησιμοποιούν τεχνικές προδιαγραφές (με την επιφύλαξη της Οδηγίας 2002/58/ΕΚ), αλλά και στην περίπτωση επεξεργασίας για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιτστικούς σκοπούς.

Στο συγκεκριμένο σημείο θα μπορούσε να παρατηρηθεί[79] ότι το συγκεκριμένο άρθρο «αντανακλά» τις ανησυχίες των θεσμικών οργάνων της ΕΕ αναφορικά με την εμπορική χρήση των προσωπικών δεδομένων. Είναι πράγματι γεγονός ότι πριν από την ψήφιση του Κανονισμού αναπτύχθηκε ιδιαίτερα στο χώρο της Ευρωπαϊκής Ένωσης η αυτοματοποιημένη επεξεργασία των προσωπικών δεδομένων για την κατάρτιση «προφίλ» των αγοραστών, που χρησίμευε στην ανίχνευση της

[78] Βλ. Λ. Μήτρου, «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων», Εκδ. Σάκκουλα, 2017, σ. 69

[79] Βλ. Φ. Παναγοπούλου-Κουτνατζή, «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016/ΕΕ», Εκδ. Σάκκουλα, 2017, σ. 256 επ.

εμπορικής-αγοραστικής τους δραστηριότητας (εμπορική συμπεριφορά, προτίμηση συγκεκριμένων προϊόντων κτλ).

Ένα χαρακτηριστικό παράδειγμα αυτοματοποιημένης επεξεργασίας των προσωπικών δεδομένων για την κατάρτιση προφίλ αποτελεί η χρήση διαδικτυακής τράπεζας για τη χορήγηση δανείου. Με την καταχώριση των απαιτούμενων δεδομένων στο διαδικτυακό ιστότοπο της τράπεζας, ο αλγόριθμος της τράπεζας ενημερώνει τον υποκείμενο των δεδομένων αν η τράπεζα θα του χορηγήσει δάνειο και με τί τόκο.

Ακόμη και σε αυτή την περίπτωση λοιπόν, βάσει του Κανονισμού μπορεί να ελεγχθεί η αυτοματοποιημένη επεξεργασία των δεδομένων από φυσικό πρόσωπο. Σίγουρα πρόκειται για μία σημαντική πρόβλεψη, ωστόσο δεν είναι βέβαιο κατά πόσο αποτελεσματική μπορεί να αποβεί όταν δεν στρέφεται ενάντια σε συκγκεκριμένο φυσικό ή νομικό πρόσωπο.

Το τελευταίο τμήμα του Κεφαλαίο τιτλοφορείται ως «Περιορισμοί» και περιλαμβάνει το άρθρο 23 το οποίο απαριθμεί τους περιορισμούς που μπορούν να τεθούν νομοθετικώς στα δικαιώματα του Υποκειμένου. Ειδικότερα, ο Κανονισμός προβλέπει ότι στα δικαιώματα που κατοχυρώνονται στα άρθρα 12-22 μπορούν να τεθούν περιορισμοί υπό την προϋπόθεση ότι σέβονται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών και διασφαλίζει την ασφάλεια του κράτους, την εθνική άμυνα, τη δημόσια ασφάλεια, της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, σημαντικού οικονομικού ή χρηματοοικονομικού συμφέροντος της Ένωσης ή κράτους μέλους, προστασίας της ανεξαρτησίας της δικαιοσύνης, της πρόληψης και δίωξης παραβάσεων δεοντολογίας σε νομοθετικώς κατοχυρωμένα επαγγέλματα, της προστασίας του υποκειμένου των δεδομένων και των δικαιωμάτων τρίτων και τέλος της εκτέλεσης αστικών αξιώσεων.

Πάντως και σε αυτές τις περιπτώσεις προβλέπεται ότι σε κάθε νομοθετικό μέτρο, που θέτει περιορισμούς σε αυτά τα δικαιώματα, να αναφέρονται οι σκοποί της επεξεργασίας, οι κατηγορίες των δεδομένων προσωπικού χαρακτήρα, τις εγγυήσεις για την πρόληψη καταχρήσεων, την περιγραφή του υπευθύνου επεξεργασίας, τη χρονική διάρκεια της διατήρησης τους και τους κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων. Αυτό που επιβάλλεται να σημειωθεί είναι ότι τα περιθώρια που «αφήνονται» στον εθνικό νομοθέτη για την επιβολή περιορισμών στα δικαιώματα των υποκειμένων είναι αρκετά διευρυμένα[80].

Περαιτέρω, το άρθρο 37 μολονότι δεν κατατάσσεται συστηματικώς στο Κεφάλαιο με τα δικαιώματα των χρηστών, είναι επίσης εξέχουσας σημασίας. Και τούτο διότι με το άρθρο 37 του Κανονισμού καθιερώνεται θεσμός του Υπεύθυνου Προστασίας (για τον συγκεκριμένο θεσμό βλέπε υποκεφάλαιο 5.3). Ο Υπεύθυνος Προστασίας αναμένεται να αποτελέσει θεμέλιο λίθο του συστήματος επιμερισμού της ευθύνης, που θεσπίζει ο Κανονισμός. Ας σημειωθεί ότι, αν και η προσωπική ευθύνη του Υπεύθυνου Προστασίας για οποιαδήποτε μη συμμόρφωση αποκλείεται εξαρχής, η παρουσία του σε συνδυασμό με τον αυξημένο βαθμό αυτονομίας που εκ του νόμου απαιτείται να

[80] Βλ. Λ. Κοτσαλής, «Προσωπικά Δεδομένα», Εκδ. Νομική Βιβλιοθήκη, 2016, σ. 101 επ.

απολαμβάνει αποσκοπούν στην εξασφάλιση ότι τόσο ο υπεύθυνος όσο και ο εκτελών την επεξεργασία θα έχουν επαρκή βοήθεια στο έργο που καλούνται να επιτελέσουν. Σύμφωνα με τα προβλεπόμενα στο άρθρο 37 ο διορισμός Υπευθύνου Προστασίας είναι υποχρεωτικός σε τρεις περιπτώσεις: α) στην περίπτωση που η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, β) στην περίπτωση που οι βασικές δραστηριότητες επεξεργασίας προσωπικών δεδομένων απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα ή (γ) όταν απαιτούν μεγάλης κλίμακας επεξεργασία κατηγοριών ευαίσθητων δεδομένων (βλ. άρθρα 9 και 10).

4.2: Οι βασικές αλλαγές που επέφερε ο Κανονισμός

Ο νέος Κανονισμός 2016/679 ΕΕ και η Οδηγία 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 εμπλουτίζουν τον ορισμό των δεδομένων προσωπικού χαρακτήρα και συγκεκριμένα τα ορίζουν ως «Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, του οποίου η ταυτότητα είναι δυνατόν να εξακριβωθεί άμεσα ή έμμεσα, από κάποιο αναγνωριστικό στοιχείο της ταυτότητας, από τα δεδομένα θέσης, από επιγραμμικό αναγνωριστικό ταυτότητας ή από έναν ή περισσότερους παράγοντες που αφορούν τη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του προσώπου[81]». Επιπλέον, ο νέος Κανονισμός και η ανωτέρω Οδηγία περιέχουν τα ευαίσθητα δεδομένα της Οδηγίας 95/46/ΕΚ και προσθέτουν σε αυτά τα στοιχεία που αφορούν γενετικά ή βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση του προσώπου και τον γενετήσιο προσανατολισμό.

Στόχος του GDPR είναι να προστατεύσει την ιδιωτική ζωή όλων των πολιτών της ΕΕ από τις παραβιάσεις των στοιχείων στον σύγχρονο κόσμο που βασίζεται σε δεδομένα. Μολονότι οι βασικές αρχές της προστασίας της ιδιωτικής ζωής εξακολουθούν να ισχύουν στην προηγούμενη Οδηγία, έχουν προταθεί πολλές αλλαγές στις ρυθμιστικές πολιτικές.

Αναμφισβήτητα η μεγαλύτερη αλλαγή στο ρυθμιστικό περιβάλλον της ιδιωτικής ζωής έρχεται με την «κανονιστική εμβέλεια» του GDPR, καθώς ισχύει για όλες τις εταιρείες που επεξεργάζονται τα προσωπικά στοιχεία των υποκειμένων των στοιχείων που διαμένουν στην Ένωση, ανεξάρτητα από την έδρα της εταιρείας. Αντίθετα, προηγουμένως υπήρχε η «εδαφική ισχύς» της Οδηγίας που περιόριζε αρκετά την κανονιστική της εμβέλεια.

Ο GDPR ισχύει για την επεξεργασία προσωπικών δεδομένων από ελεγκτές και μεταποιητές στην ΕΕ, ανεξάρτητα από το εάν η επεξεργασία πραγματοποιείται εντός ή εκτός της ΕΕ. Ο GDPR ισχύει επίσης για την επεξεργασία στοιχείων προσωπικού χαρακτήρα των υποκειμένων των στοιχείων στην ΕΕ από υπεύθυνο επεξεργασίας ή μεταποιητή που δεν είναι εγκατεστημένος στην ΕΕ και όπου οι δραστηριότητες αφορούν είτε προσφορά αγαθών ή υπηρεσιών σε πολίτες της ΕΕ (ανεξάρτητα από το αν απαιτείται πληρωμή). Οι επιχειρήσεις εκτός ΕΕ που επεξεργάζονται τα στοιχεία των πολιτών της ΕΕ πρέπει επίσης να διορίσουν εκπρόσωπο στην ΕΕ.

[81] Βλ. άρθρο 4 στοιχ.1 Κανονισμός 2016/679 ΕΕ και άρθρο 3 στοιχ.1 Οδηγία 216/680 ΕΕ

Στους οργανισμούς που παραβιάζουν τον GDPR είναι δυνατόν να επιβληθεί πρόστιμο έως και 4% του ετήσιου συνολικού κύκλου εργασιών ή 20 εκατ. ευρώ (το οποίο είναι και το μεγαλύτερο). Πρόκειται για το μέγιστο πρόστιμο που μπορεί να επιβληθεί για τις πιο σοβαρές παραβάσεις, π.χ. όταν δεν υπάρχει επαρκής συναίνεση του πελάτη για επεξεργασία δεδομένων.

Περαιτέρω, υπάρχει μια κλιμακωτή προσέγγιση στα πρόστιμα, π.χ. σε μια εταιρεία μπορεί να επιβληθεί πρόστιμο ύψους 2% για μη τήρηση των αρχείων της (άρθρο 28), χωρίς να ενημερώνει την εποπτεύουσα αρχή και το υποκείμενο των δεδομένων για παραβίαση ή μη διενέργεια αξιολόγησης αντικτύπου. Είναι σημαντικό να σημειωθεί ότι αυτοί οι κανόνες ισχύουν τόσο για τους υπεύθυνους επεξεργασίας όσο και για τους επεξεργαστές.

Οι όροι για τη συγκατάθεση έχουν ενισχυθεί και οι εταιρείες δεν μπορούν πια να χρησιμοποιούν μακρούς δυσανάγνωστους όρους και συνθήκες γεμάτους νομική ορολογία[82]. Ειδικότερα, η αίτηση συγκατάθεσης πρέπει να παρέχεται σε κατανοητή και εύκολα προσβάσιμη μορφή, με σκοπό την επεξεργασία στοιχείων που επισυνάπτεται στη συναίνεση αυτή. Η συγκατάθεση πρέπει να είναι σαφής και διακριτή από άλλα θέματα και να παρέχεται με κατανοητή και εύκολα προσιτή μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα. Μία επιπρόσθετη σημαντική αλλαγή που επέφερε ο Κανονισμός είναι ότι πλέον, ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του για την επεξεργασία. Το υποκείμενο διατηρεί το δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή, χωρίς η ανάκληση αυτή να θίγει τη νομιμότητα της επεξεργασίας.

Περαιτέρω, μεταξύ του GDPR, οι ειδοποιήσεις παραβίασης είναι πια υποχρεωτικές σε όλα τα κράτη μέλη όπου μια παραβίαση στοιχείων ενδέχεται να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων. Αυτό πρέπει να γίνει εντός 72 ωρών από την πρώτη στιγμή της συνειδητοποίησης της παραβίασης. Οι επεξεργαστές στοιχείων υποχρεούνται επίσης να ειδοποιούν τους πελάτες τους, τους ελεγκτές, χωρίς αδικαιολόγητη καθυστέρηση, αφού πρώτα καταλάβουν την παραβίαση δεδομένων.

Μέρος των διευρυμένων δικαιωμάτων των προσώπων στα οποία αναφέρεται ο GDPR είναι το δικαίωμα για τα υποκείμενα δεδομένων να λαμβάνουν επιβεβαίωση από τον υπεύθυνο επεξεργασίας για το κατά πόσον τα στοιχεία προσωπικού χαρακτήρα που τους αφορούν υποβάλλονται σε επεξεργασία, πού και για ποιό σκοπό. Επιπλέον, ο ελεγκτής παρέχει δωρεάν αντίγραφο των προσωπικών στοιχείων σε ηλεκτρονική μορφή.

Επίσης το δικαίωμα στη λήθη, το οποίο παρέχει στο υποκείμενο των δεδομένων τη δυνατότητα να διαγράψει τα προσωπικά του στοιχεία, να σταματήσει την περαιτέρω διάδοση τους και ενδεχομένως να σταματήσει την επεξεργασία των δεδομένων από τρίτους ενισχύεται σημαντικά. Οι

[82] Βλ. Θ. Γεωργακόπουλος, «Η ευρωπαϊκή ισχύς και ο κανονισμός GDPR», 18/5/2018, Καθημερινή, Διαθέσιμο σε: https://www.kathimerini.gr/964984/opinion/epikairothta/politikh/h-eyrwpaikh-isxys-kai-o-kanonismos-gdpr

όροι για τη διαγραφή, όπως περιγράφονται στο άρθρο 17, περιλαμβάνουν τα στοιχεία που δεν έχουν πια σχέση με τους αρχικούς σκοπούς επεξεργασίας ή το υποκείμενο των δεδομένων που αποσύρει τη συναίνεση.

Το GDPR εισάγει επίσης τη φορητότητα των δεδομένων, δηλαδή το δικαίωμα για ένα υποκείμενο να λαμβάνει τα προσωπικά δεδομένα που το αφορούν και τα οποία έχουν παράσχει προηγουμένως σε μια «ευρέως χρησιμοποιούμενη και μηχανικά αναγνώσιμη μορφή», έχοντας το δικαίωμα να διαβιβάσουν τα στοιχεία αυτά και σε άλλο ελεγκτή.

Η προστασία της ιδιωτικής ζωής από την επεξεργασία καθίσταται νομική υποχρέωση βάσει του GDPR. Στον «πυρήνα» της, η προστασία της ιδιωτικής ζωής απαιτεί την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων κατά τρόπο αποτελεσματικό, προκειμένου να ανταποκρίνεται στις απαιτήσεις του παρόντος κανονισμού και να προστατεύει τα αποτελεσματικά τα δικαιώματα των υποκειμένων.

Ο Κανονισμός, προκειμένου να προστατεύει τα στοιχεία προσωπικού χαρακτήρα έχει τα ακόλουθα στοιχεία:

α) Ισχύει τόσο για τις ιδιωτικές εταιρείες όσο και για τους δημόσιους φορείς

β) Εφαρμόζεται άμεσα από την έναρξη της ισχύος του

γ) Καίτοι κανονισμός παρέχει ορισμένα στοιχεία «ευελιξίας» στα κράτη για αποτελεσματικότερη νομοθετική εξειδίκευση ορισμένων στοιχείων του[83].

δ) Προβλέπει υψηλά πρόστιμα διοικητικού χαρακτήρα, ανάλογα με το είδος της παραβίασης των κανονισμών.
ε) Ήταν το αποτέλεσμα έντονων διαπραγματεύσεων[84] μεταξύ ποικίλων ομάδων και συνιστά ένα «προϊόν» συμβιβασμού μεταξύ των αντικρουόμενων κοινωνικών ομάδων.

Περαιτέρω ο Κανονισμός έφερε αλλαγές αναφορικά με τους υπεύθυνους επεξεργασίας στοιχείων, στα εξής επίπεδα:

4.2.1: Συγκατάθεση

[83] Βλ. Σε 28 άρθρα του Κανονισμού υπάρχει περιθώριο παρέκκλισης για τα κράτη-μέλη

[84] Ενδεικτικό είναι το γεγονός ότι η Ευρωπαϊκή Επιτροπή επισήμανε την ανάγκη τροποποίησης της Οδηγίας από τον Ιανουάριο του 2012, το Ευρωπαϊκό Κοινοβούλιο υπερψήφισε το σχέδιο Κανονισμού το Μάρτιο του 2014 και η τελική συμφωνία μεταξύ του Κοινοβουλίου, της Επιτροπής και του Συμβουλίου επήλθε το Δεκέμβριο του 2015. Ο Κανονισμός ψηφίστηκε το Μάιο του 2016 και δόθηκε διετής περίοδος προσαρμογής στα κράτη-μέλη έως το Μάιο του 2018

Καταρχάς, ως γνωστόν, ο όρος «συγκατάθεση» εμφανίζεται σε πολλούς κλάδους του δικαίου ως νομιμοποιητικό γεγονός, ως όρος δηλαδή που αίρει την απαγόρευση μιας καταρχήν μη επιτρεπόμενης ενέργειας. Αλλά και στο δίκαιο των προσωπικών δεδομένων δεν εισάγεται για πρώτη φορά με τον GDPR. Ειδικότερα, υπό το προισχύσαν καθεστώς της Οδηγίας 95/46/ΕΚ, η συγκατάθεση του υποκειμένου έχει την έννοια δήλωσης βουλήσεως, η οποία θα πρέπει να είναι ελεύθερη, ρητή και να δίδεται με πλήρη επίγνωσης για τα έννομα αποτελέσματά της. Ο GDPR, δίνει τον ορισμό της συγκατάθεσης στο (στοιχ. 11' άρθρου 4) και εν πολλοίς αποτελεί αντιγραφή της προηγούμενης ρύθμισης. Η συγκατάθεση για την επεξεργασία στοιχείων προσωπικού χαρακτήρα απαιτείται κάθε φορά που δεν έχει αποφασιστεί και καταγραφεί από την οργάνωση άλλη νομική βάση για τη μεταποίηση. Όταν απαιτείται συγκατάθεση για επεξεργασία, οι οργανισμοί δεν είναι δυνατόν να «κρύβονται» πίσω από λέξεις με ιδιαίτερες νόμιμες έννοιες. Η αίτηση συναίνεσης πρέπει να παρέχεται με σαφή και εύληπτη μορφή και δεν μπορεί να αναμειγνύεται με άλλα άσχετα θέματα.

Η συγκατάθεση του υποκειμένου των δεδομένων θα πρέπει να είναι ελεύθερη, ρητή και ειδική, και να παρέχεται από το άτομο εν πλήρη επιγνώσει και αφού προηγουμένως έχει ενημερωθεί πλήρως. Ελεύθερη είναι η συγκατάθεση, η οποία δεν αποτελεί προϊόν ελαττωματικής βουλήσεως (πλάνη, απάτη, απειλή), ούτε προϊόν ανάγκης ή σχέσης εξάρτησης του υποκειμένου με τον υπεύθυνο επεξεργασίας. Το υποχρεωτικό της συγκατάθεσης του υποκειμένου των δεδομένων προκειμένου να καταστεί η επεξεργασία αυτών νόμιμη αποτελεί τη «ραχοκοκαλιά» του δικαίου προστασίας προσωπικών δεδομένων και έχει ιδιαίτερα μεγάλη σημασία, καθώς διασφαλίζει το δικαίωμα του πληροφοριακού αυτοκαθορισμού του ατόμου[85].

Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς βεβαίως αναδρομικό αποτέλεσμα. Γίνεται επομένως σαφές πως αποκλείεται η εικαζόμενη ή τεκμαιρόμενη συγκατάθεση του υποκειμένου, πολλώ δε μάλλον η σιωπηρή αποδοχή της[86]. Με άλλα λόγια, η συγκατάθεση πρέπει να είναι τόσο εύκολο να αποσυρθεί όσο εύκολη είναι και η χορήγησή της. Για παράδειγμα, εάν μια εφαρμογή παρέχει ειδοποίηση συμμετοχής για κάποια μορφή επεξεργασίας, ο μηχανισμός απόσυρσης αυτής της συγκατάθεσης δεν πρέπει να «κρυφτεί» σε ένα μη προσβάσιμο τμήμα της εφαρμογής.

4.2.2: Ειδοποίηση παραβίασης

Η πλειοψηφία των κρατών μελών δεν προέβλεπε προηγουμένως την υποχρέωση κοινοποίησης παραβιάσεων, αλλά τώρα, σύμφωνα με το GDPR, η κοινοποίηση παραβίασης θα καταστεί υποχρεωτική σε όλα τα κράτη μέλη κάθε φορά που μια παραβίαση είναι πιθανό να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων. Περαιτέρω, η κοινοποίηση πρέπει να ολοκληρώνεται χωρίς αδικαιολόγητη καθυστέρηση και όπου αυτό είναι εφικτό εντός 72 ωρών από τη στιγμή που θα γίνει γνωστή η παραβίαση των προσωπικών δεδομένων. Είναι λοιπόν αξιοσημείωτες οι προβλέψεις του Κανονισμού για την υποχρέωση έγκαιρης ειδοποίησης των υποκειμένων για το ενδεχόμενο παραβίασης των δεδομένων τους.

4.2.3: Προστασία στοιχείων από το σχεδιασμό

[85] Βλ. Κ. Δελούκα-Ιγγλέση, Νομικά Θέματα Ηλεκτρονικού Εμπορίου, ό.π., σ. 311.

[86] Βλ. Κ. Δελούκα-Ιγγλέση, ό.π., σ. 310.

Το Privacy by Design[87] («PbD»), που περιλαμβάνεται και στη νομοθεσία του Καναδά και «ενθαρρύνεται» από την Ομοσπονδιακή Επιτροπή Εμπορίου των Η.Π.Α., γίνεται τώρα νομική απαίτηση του GDPR. Σημαντικές αρχές του «PbD» είναι η προστασία της ιδιωτικής ζωής και της ασφάλειας από προεπιλογή (και εξαρχής), χρησιμοποιώντας τον ελάχιστο απαραίτητο όγκο προσωπικών δεδομένων για την επίτευξη ενός σκοπού. Αυτή η νομική απαίτηση υποχρεώνει τους οργανισμούς να απασχολούν προσωπικό κατάλληλα εκπαιδευμένο για την προστασία της ιδιωτικής ζωής στις διαδικασίες ανάπτυξης λογισμικού.

Όπως προαναφέρθηκε, ο Κανονισμός για την προστασία των προσωπικών δεδομένων, συμφωνήθηκε από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο τον Απρίλιο του 2016, και αντικατέστησε την Οδηγία 95/46/ΕΚ το Μάϊο του 2018 ως τον πρωτογενή νόμο που ρυθμίζει τον τρόπο με τον οποίο οι επιχειρήσεις προστατεύουν τα προσωπικά δεδομένα των πολιτών της ΕΕ. Οι εταιρείες που ήδη συμμορφώνονται με την Οδηγία πρέπει να διασφαλίσουν ότι συμμορφώνονται επίσης με τις νέες απαιτήσεις του GDPR. Οι εταιρείες που δεν συμμορφώνονται με την GDPR πριν από την προθεσμία υπόκεινται σε αυστηρές κυρώσεις και πρόστιμα.

Υπενθυμίζουμε ακόμα ότι, οι απαιτήσεις του GDPR ισχύουν για κάθε κράτος μέλος της Ευρωπαϊκής Ένωσης, με στόχο τη δημιουργία πιο συνεκτικής προστασίας των καταναλωτικών και προσωπικών δεδομένων σε όλα τα κράτη μέλη της ΕΕ. Μία από τις βασικές απαιτήσεις προστασίας της ιδιωτικής ζωής και προστασίας στοιχείων του GDPR είναι η απαίτηση από ορισμένες εταιρείες (ανάλογα με το μέγεθος τους) να διορίσουν έναν υπεύθυνο προστασίας δεδομένων για να επιβλέπουν τη συμμόρφωση τους με το GDPR. Με άλλα λόγια, το GDPR ορίζει ένα βασικό σύνολο προτύπων για εταιρείες που χειρίζονται τα στοιχεία των πολιτών της ΕΕ για την καλύτερη διασφάλιση της επεξεργασίας και της κυκλοφορίας των προσωπικών στοιχείων των πολιτών.

Τα ακόλουθα είναι μερικά από τα κεφάλαια και τα άρθρα του GDPR που έχουν το μεγαλύτερο αντίκτυπο:

Άρθρα 17 και 18 - Τα άρθρα 17 και 18 του GDPR παρέχουν στα υποκείμενα των δεδομένων μεγαλύτερο έλεγχο των προσωπικών στοιχείων που υποβάλλονται σε επεξεργασία αυτόματα. Το αποτέλεσμα είναι ότι τα πρόσωπα στα οποία αναφέρονται τα δεδομένα είναι δυνατόν να μεταφέρουν ευκολότερα τα προσωπικά τους στοιχεία μεταξύ των παρόχων υπηρεσιών («δικαίωμα μεταφοράς») και είναι δυνατόν να ζητήσουν από τον υπεύθυνο επεξεργασίας να διαγράψει τα προσωπικά τους στοιχεία υπό ορισμένες συνθήκες («δικαίωμα στη λήθη»).

Άρθρα 23 και 30 - Τα άρθρα 23 και 30 απαιτούν από τις εταιρείες να εφαρμόζουν εύλογα μέτρα προστασίας των προσωπικών δεδομένων των καταναλωτών και της ιδιωτικής τους ζωής έναντι της απώλειας ή της έκθεσης.

[87] Πρόκειται για μία συγκεκριμένη προσέγγιση στον τομέα της πληροφορικής που απαιτεί την εφαρμογή κατάλληλων τεχνικών που να διασφαλίζουν την προστασία των προσωπικών δεδομένων ήδη από το σχεδιασμό και την ανάπτυξη των λογισμικών Πρβλ. P. Hustinx, «Privacy by Design: Delivering the Promises», *Identity in the Information Society*, v. 3 (2), 2010, σ. 253–255

Άρθρα 31 και 32 – Η υποχρέωση κοινοποίησης της παραβίασης δεδομένων διαδραματίζει σημαντικό ρόλο στο κείμενο του GDPR. Ειδικότερα, το άρθρο 31 ορίζει ότι οι ελεγκτές πρέπει να ενημερώνουν τις αρχές εποπτείας για παραβίαση προσωπικών δεδομένων εντός 72 ωρών από την εκμάθηση της παραβίασης και πρέπει να παρέχουν συγκεκριμένες λεπτομέρειες της παραβίασης, όπως η φύση της παραβίασης. Περαιτέρω, το άρθρο 32 απαιτεί από τους υπεύθυνους επεξεργασίας δεδομένων να ειδοποιούν τα υποκείμενα όσο το δυνατόν συντομότερα ακόμη και όταν υπάρχουν απλώς ενδείξεις για παραβιάσεις που εκθέτουν τα δικαιώματά τους και τις ελευθερίες τους σε υψηλό κίνδυνο.

Άρθρα 33 και 33α - Τα άρθρα 33 και 33α απαιτούν από τις εταιρείες να εκτελούν αξιολογήσεις των επιπτώσεων στην προστασία δεδομένων για τον εντοπισμό των κινδύνων για τα δεδομένα των υποκειμένων και για την αξιολόγηση της συμμόρφωσης στον GDPR.

Άρθρο 35 - Το άρθρο 35 απαιτεί ορισμένες εταιρείες να διορίζουν αξιωματούχους προστασίας δεδομένων. Συγκεκριμένα, κάθε εταιρεία που επεξεργάζεται δεδομένα που αποκαλύπτουν τα γενετικά στοιχεία ενός ατόμου, την υγεία, τη φυλετική ή εθνοτική καταγωγή, τις θρησκευτικές πεποιθήσεις κλπ. Υποχρεούται επίσης να ορίσει υπεύθυνο προστασίας δεδομένων.

Άρθρα 36 και 37 - Τα άρθρα 36 και 37 περιγράφουν τη θέση του υπευθύνου προστασίας δεδομένων και τις αρμοδιότητές του όσον αφορά τη διασφάλιση της συμμόρφωσης με το GDPR, καθώς και την υποβολή εκθέσεων στις εποπτικές αρχές και τα πρόσωπα στα οποία αναφέρονται τα δεδομένα.

Άρθρο 45 - Το άρθρο 45 επεκτείνει τις απαιτήσεις προστασίας των δεδομένων σε διεθνείς εταιρείες που συλλέγουν ή επεξεργάζονται προσωπικά στοιχεία των πολιτών της ΕΕ, υποβάλλοντάς τους στις ίδιες απαιτήσεις και κυρώσεις με τις εταιρείες που εδρεύουν εντός της ΕΕ.

Άρθρο 79 - Το άρθρο 79 περιγράφει τις κυρώσεις για τη μη συμμόρφωση με το GDPR, η οποία μπορεί να φτάσει έως και το 4% του συνολικού ετήσιου εισοδήματος της εταιρείας, ανάλογα βέβαια με τη φύση της παραβίασης.

Στο σημείο αυτό κρίνεται σκόπιμο να παρατεθούν συνοπτικά ορισμένα στοιχεία που είναι κοινά ανάμεσα στο GDPR και την Οδηγία 95/46/ΕΚ προκειμένου να αναδειχθούν οι αρκετές ομοιότητες τους:

1) Αναγνώριση της σημασίας προστασίας των προσωπικών δεδομένων και της ελεύθερης κυκλοφορίας τους.

2) Υποχρέωση εφαρμογής των διατάξεων στον ιδιωτικό και στο δημόσιο κλάδο.

3) Υποχρέωση εφαρμογής των διατάξεων από υπεύθυνους επεξεργασίας οι οποίοι είναι εγκατεστημένοι στην Ένωση[88].

4) Εξαίρεση από το πεδίο εφαρμογής των δραστηριοτήτων εκείνων με αυστηρά προσωπικό χαρακτήρα.

5) Εφαρμογή των υποχρεώσεων σε αυτοματοποιημένη, μερικώς αυτοματοποιημένη ή μη αυτοματοποιημένη επεξεργασία.

6) Συγκεκριμένος ορισμός της έννοιας των προσωπικών δεδομένων[89].

7) Πλαίσιο προστασίας των ευαίσθητων δεδομένων[90].

8) Προϋπόθεση για ύπαρξη νομικής βάσης για την επεξεργασία δεδομένων, η οποία τις περισσότερες φορές καλύπτεται από τη συγκατάθεση του υποκειμένου των δεδομένων.

9) Τήρηση της αρχής της αναλογικότητας.

10) Αναφορά στον κίνδυνο από την επεξεργασία και τη φύση των στοιχείων που απολαύουν προστασίας[91].

11) Ομάδα προστασίας των προσώπων έναντι της επεξεργασίας στοιχείων προσωπικού χαρακτήρα (γνωστή και ως «Ομάδα του άρθρου 29» ή «η Ομάδα»)[92].

12) Δικαίωμα πρόσβασης του Υποκειμένου στα στοιχεία του που τηρούνται.

13) Δικαίωμα των υποκειμένων στη λήθη[93].

---

[88] Ωστόσο πρέπει να σημειωθεί ότι ο Κανονισμός καταλαμβάνει και υπεύθυνους επεξεργασίας/ εκτελούντες την επεξεργασία, μη εγκατεστημένους στην ΕΕ εφόσον η επεξεργασία εκτελείται στην Ένωση. Επίσης, η Οδηγία δεν κάνει αναφορά στους εκτελούντες την επεξεργασία, σε αντίθεση με τον Κανονισμό που τους περιλαμβάνει ρητή αναφορά.

[89] Ο Κανονισμός διευρύνει τον ορισμό, προσθέτοντας τα δεδομένα τοποθεσίας.

[90] Στην περίπτωση του Κανονισμού η έννοια διευρύνεται με την προσθήκη των γενετικών και βιομετρικών δεδομένων.

[91] Παρότι η έννοια του κινδύνου αναφέρεται και στην Οδηγία, στον Κανονισμό μεταβάλλεται σε καθοριστικό παράγοντα αντιμετώπισης των ακολουθούμενων πρακτικών και μέτρων ασφαλείας

[92] Προβλέπεται στο άρθρο 29 της Οδηγίας και επαναλαμβάνεται στον Κανονισμό. Η ομάδα εργασίας του άρθρου 29 ήταν η ανεξάρτητη ευρωπαϊκή ομάδα εργασίας που χειριζόταν θέματα σχετικά με την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα βάσει της Οδηγίας 95/46/ΕΚ έως και τις 25 Μαΐου 2018 (έναρξη ισχύος του GDPR).

[93] Πρέπει να σημειωθεί ότι το δικαίωμα αυτό ενισχύεται και εξειδικεύεται με τον Κανονισμό καθώς η Οδηγία δεν περιλάμβανε σαφή προσδιορισμό του τρόπου άσκησης του δικαιώματος στη λήθη σε σχέση με τα φυσικά αρχεία

14) Υποχρεώσεις τήρησης διαδικασιών διαφάνειας και λογοδοσίας, καθώς και υποχρέωσης ενημέρωσης των υποκειμένων και λήψης μέτρων ασφαλείας.

15) Παροχή διακριτικής ευχέρειας των κρατών μελών να υιοθετήσουν συγκεκριμένα μέτρα για τη ρύθμιση ορισμένων ζητημάτων[94].

16) Πρόβλεψη προστασίας δικαιωμάτων έναντι κατάρτισης προφίλ τους από τους υπεύθυνους επεξεργασίας.

4.3: Η έναρξη της εφαρμογής του Κανονισμού

Η εφαρμογή του Γενικού Κανονισμού για την Προστασία Προσωπικών Δεδομένων (GDPR) ξεκίνησε επίσημα την 25η Μαΐου 2018, οδηγώντας στην κατάργηση της Οδηγίας 95/46/ΕΚ η οποία ως την ημερομηνία εκείνη αποτελούσε το βασικό ευρωπαϊκό νομοθέτημα για την προστασία των δεδομένων προσωπικού χαρακτήρα.

Όπως προαναφέρθηκε, ο Κανονισμός αποτέλεσε αντικείμενο έντονων διαβουλεύσεων και ενδεικτικό είναι το γεγονός ότι η Ευρωπαϊκή Επιτροπή επεσήμανε την ανάγκη τροποποίησης της Οδηγίας ήδη από τον Ιανουάριο του 2012, το Ευρωπαϊκό Κοινοβούλιο υπερψήφισε το σχέδιο Κανονισμού τον Μάρτιο του 2014 και η τελική συμφωνία μεταξύ του Κοινοβουλίου, της Επιτροπής και του Συμβουλίου επήλθε τον Δεκέμβριο του 2015.

Στον παρακάτω πίνακα παρουσιάζονται συνοπτικά οι βασικότερες έννοιες του Κανονισμού προς διευκόλυνση του αναγνώστη:

Οι βασικότερες έννοιες του Κανονισμού (με βάση το άρθρο 4 του Κανονισμού)	
Προσωπικά Στοιχεία ή Στοιχεία Προσωπικού Χαρακτήρα	Κάθε πληροφορία που αφορά ταυτοποιημένο, ή ταυτοποιήσιμο, φυσικό πρόσωπο
Υποκείμενο των Στοιχείων	Αφορά το φυσικό πρόσωπο του οποίου η ταυτότητα είναι δυνατόν να εξακριβωθεί, άμεσα ή έμμεσα.
Επεξεργασία στοιχείων	Κάθε πράξη που αφορά προσωπικά στοιχεία
Διασυνοριακή επεξεργασία	Αφορά στην επεξεργασία στοιχείων προσωπικού α) διάφορων εγκαταστάσεων σε περισσότερα του ενός κράτη μέλη β) μίας εγκατάστασης υπευθύνου

[94] Ο βαθμός της προβλεπόμενης διακριτικής ευχέρειας διατηρείται και στον Κανονισμό, φυσικά σε μικρότερο βαθμό από ό,τι συμβαίνει στην περίπτωση της Οδηγίας

Υπεύθυνος Επεξεργασίας Στοιχείων	Το φυσικό, ή νομικό, πρόσωπο, ή δημόσια αρχή / υπηρεσία, που καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας των στοιχείων προσωπικού χαρακτήρα.
Εκτελών την Επεξεργασία	Το φυσικό, ή νομικό, πρόσωπο, ή δημόσια αρχή / υπηρεσία, που επεξεργάζεται στοιχεία προσωπικού χαρακτήρα για λογαριασμό του Υπευθύνου Επεξεργασίας.
Αποδέκτης στοιχείων	Το φυσικό, ή νομικό, πρόσωπο, ή δημόσια αρχή / υπηρεσία / άλλος φορέας, στον οποίο κοινολογούνται τα στοιχεία προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι.
Υπεύθυνος Προστασίας Στοιχείων	Ορίζεται από τον Υπεύθυνο Επεξεργασίας και τον Εκτελούντα την Επεξεργασία και συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία στοιχείων προσωπικού χαρακτήρα. Αποτελεί το πρόσωπο επικοινωνίας τόσο με τα υποκείμενα των στοιχείων όσο και με την εποπτική Αρχή.
Εκτίμηση Αντικτύπου σχετικά με την προστασία στοιχείων	Όταν ένα είδος επεξεργασίας δεδομένων, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο Υπεύθυνος Επεξεργασίας οφείλει να διενεργήσει, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία προσωπικών δεδομένων.
Συγκατάθεση Υποκειμένου	Κάθε ένδειξη βούλησης (ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει), με την οποία το υποκείμενο των στοιχείων εκδηλώνει

	ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα στοιχεία προσωπικού χαρακτήρα που το αφορούν.
Παραβίαση Στοιχείων Προσωπικού Χαρακτήρα	Παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας αποκάλυψη ή πρόσβαση στοιχείων προσωπικού χαρακτήρα, τα οποία διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.
Εποπτική Αρχή Προστασίας Στοιχείων	Πρόκειται για την ανεξάρτητη δημόσια Αρχή, καθ' ύλην αρμόδια για την εποπτεία εφαρμογής του Κανονισμού. Ο Κανονισμός ενθαρρύνει την επικοινωνία και συνεργασία μεταξύ των διάφορων Αρχών, ώστε να διασφαλίζεται ομοιογένεια στην αντιμετώπιση υποθέσεων διευρωπαϊκού ενδιαφέροντος και ασφάλεια δικαίου.
Επικεφαλής Εποπτική Αρχή	Ορίζεται η Αρχή του κράτους-μέλους όπου βρίσκεται η «κύρια εγκατάσταση» του Υπευθύνου Επεξεργασίας.
Ενδιαφερόμενη Εποπτική Αρχή	Ορίζεται η Αρχή, την οποία αφορά η επεξεργασία στοιχείων προσωπικού χαρακτήρα, όταν: α) ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι εγκατεστημένος στο έδαφος του κράτους μέλους της εν λόγω εποπτικής αρχής, β) τα υποκείμενα των στοιχείων που διαμένουν στο κράτος μέλος της εν λόγω εποπτικής αρχής επηρεάζονται ή ενδέχεται να επηρεαστούν ουσιωδώς από την επεξεργασία, ή γ) έχει υποβληθεί καταγγελία στην εν λόγω εποπτική αρχή.

Κύρια Εγκατάσταση	Για τον Υπεύθυνο Επεξεργασίας: Σε περίπτωση που έχει εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, πρόκειται για τον τόπο της κεντρικής του διοίκησης στην ΕΕ. Ωστόσο, εάν οι αποφάσεις, όσον αφορά στους σκοπούς και τα μέσα της επεξεργασίας στοιχείων προσωπικού χαρακτήρα, λαμβάνονται σε άλλη εγκατάστασή του στην ΕΕ, και η εγκατάσταση αυτή έχει την εξουσία εφαρμογής των αποφάσεων αυτών, τότε πρόκειται για την εγκατάσταση στην οποία έλαβε αυτές τις αποφάσεις.
Ευρωπαϊκό Συμβούλιο Προστασίας Στοιχείων	Απαρτίζεται από τον προϊστάμενο μίας εποπτικής Αρχής κάθε κράτους μέλους και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων. Έχει ως στόχο να συμβάλλει στη συνεκτική εφαρμογή του Κανονισμού σε ολόκληρη την ΕΕ.
Μηχανισμός Συνεκτικότητας	Ο μηχανισμός με βάση τον οποίο οι εποπτικές Αρχές συνεργάζονται μεταξύ τους, με κύριο στόχο τη συνεκτική εφαρμογή του Κανονισμού στο σύνολο της ΕΕ[95].
Κατάρτιση Προφίλ	Περιλαμβάνει οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας στοιχείων προσωπικού χαρακτήρα που συνίσταται στη χρήση στοιχείων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου
Ψευδωνυμοποίηση	αφορά την επεξεργασία στοιχείων προσωπικού χαρακτήρα κατά τρόπο ώστε τα στοιχεία να μην είναι σε θέση να αποδοθούν σε καθορισμένο υποκείμενο των στοιχείων χωρίς τη χρήση συμπληρωματικών

[95] Στα άρθρα 64 έως και 67 αναφέρονται προβλέψεις για το ρόλο του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, την επίλυση διαφορών μεταξύ των εποπτικών Αρχών, τις επείγουσες διαδικασίες και την ανταλλαγή απόψεων.

	πληροφοριών, αν τα εν λόγω στοιχεία διατηρούνται χώρια και ανήκουν σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν είναι δυνατόν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

Περαιτέρω για την ευχερέστερη κατανόηση των σημαντικότερων ημερομηνιών-σταθμών για την έναρξη της ισχύος του Κανονισμού παρατίθεται ο κατωτέρω πίνακας:

Βασικές ημερομηνίες έως την έναρξη εφαρμογής του Κανονισμού[96]

24/10/1995	Θεσπίζεται η Οδηγία 95/46/ΕΚ.
25/01/2012	Η Ευρωπαϊκή Επιτροπή τονίζει την ανάγκη τροποποίησης της Οδηγίας.
07/03/2012	Το Ευρωπαϊκό Συμβούλιο Προστασίας Στοιχείων κοινοποιεί γνώμη επί της προτεινόμενης (από την Επιτροπή) τροποποίησης της Οδηγίας.
23/03/2012	Το "Article 29 Working Party" κοινοποιεί γνώμη επί της προτεινόμενης (από την Επιτροπή) τροποποίησης της Οδηγίας.
05/10/2012	Το "Article 29 Working Party" κοινοποιεί περαιτέρω σχόλια επί της προτεινόμενης (από την Επιτροπή) τροποποίησης της Οδηγίας.
12/03/2014	Το Ευρωπαϊκό Κοινοβούλιο υπερψηφίζει το σχέδιο Κανονισμού.
15/06/2015	Το Συμβούλιο καταλήγει σε μια γενική προσέγγιση επί του το σχεδίου Κανονισμού.
27/07/2015	Το Ευρωπαϊκό Συμβούλιο Προστασίας Στοιχείων κοινοποιεί συστάσεις προς την Επιτροπή σύνταξης του τελικού κειμένου του Κανονισμού
15/12/2015	Επέρχεται τελική συμφωνία μεταξύ του Κοινοβουλίου, της Επιτροπής και του Συμβουλίου
02/02/2016	Το "Article 29 Working Party" κοινοποιεί το χρονοδιάγραμμα υλοποίησης του Κανονισμού
24/05/2016	Δημοσιεύεται ο Κανονισμός
10/01/2017	Η Ευρωπαϊκή Επιτροπή προτείνει δύο νέους Κανονισμούς αναφορικά α) με την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες και β) τους κανονισμούς προστασίας στοιχείων που ισχύουν για τα θεσμικά όργανα της ΕΕ που ευθυγραμμίζουν τους ισχύοντες κανόνες με το Γενικό Κανονισμό
06/05/2018	υλοποίηση της Οδηγίας ΕΕ/2016/680 για την προστασία των φυσικών προσώπων από αρμόδιες αρχές για τους σκοπούς της πρόληψης, ή δίωξης ποινικών αδικημάτων
25/05/2018	Έναρξη εφαρμογής του Κανονισμού 2016/679

[96] Βλ. European data protection supervisor, (2018), «The History of the General Data Protection Regulation», Διαθέσιμο σε: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation

4.4: Πεδίο Ισχύος

Ο κανονισμός εφαρμόζεται εάν ο υπεύθυνος επεξεργασίας δεδομένων (ένας οργανισμός που συλλέγει δεδομένα από κάτοικους της ΕΕ) ή ο μεταποιητής (ένας οργανισμός που επεξεργάζεται δεδομένα για λογαριασμό υπεύθυνου επεξεργασίας δεδομένων, όπως οι πάροχοι υπηρεσιών) ή το πρόσωπο στο οποίο αναφέρονται τα δεδομένα (πρόσωπο) βρίσκονται στην ΕΕ. Υπό ορισμένες συνθήκες, ο κανονισμός εφαρμόζεται επίσης σε οργανισμούς που εδρεύουν εκτός ΕΕ, εάν συλλέγουν ή επεξεργάζονται προσωπικά δεδομένα ατόμων που βρίσκονται εντός της ΕΕ. Ο κανονισμός δεν εφαρμόζεται στην επεξεργασία δεδομένων από ένα πρόσωπο για «καθαρά προσωπική ή οικιακή δραστηριότητα και συνεπώς χωρίς σύνδεση με επαγγελματική ή εμπορική δραστηριότητα».

Ο κανονισμός δεν έχει σκοπό να εφαρμόζεται στην επεξεργασία προσωπικών δεδομένων για δραστηριότητες εθνικής ασφάλειας ή για επιβολή του νόμου στην ΕΕ. Ωστόσο, οι βιομηχανικές ομάδες που ανησυχούν για την αντιμετώπιση ενδεχόμενης σύγκρουσης νόμων αμφισβήτησαν εάν θα μπορούσε να γίνει επίκληση του άρθρου 48 του GDPR προκειμένου να αποφευχθεί η επιβολή από έναν υπεύθυνο επεξεργασίας δεδομένων ενός νόμου τρίτης χώρας της συμμόρφωσης με μια έννομη τάξη από την επιβολή του νόμου, δικαστικές ή εθνικές αρχές ασφαλείας να αποκαλύπτουν στις αρχές αυτές τα προσωπικά δεδομένα ενός προσώπου της ΕΕ, ανεξάρτητα από το εάν τα δεδομένα διαμένουν εντός ή εκτός της ΕΕ.

Περαιτέρω, το άρθρο 48 ορίζει ότι οποιαδήποτε απόφαση δικαστηρίου και οποιαδήποτε απόφαση διοικητικής αρχής τρίτης χώρας που απαιτεί από τον υπεύθυνο επεξεργασίας ή τον μεταποιητή να μεταβιβάσει ή να αποκαλύψει προσωπικά δεδομένα δεν μπορεί να αναγνωριστεί ή να εκτελεστεί με οποιονδήποτε τρόπο εκτός εάν βασίζεται σε διεθνή συμφωνία, μια συνθήκη αμοιβαίας δικαστικής συνδρομής που ισχύει μεταξύ της αιτούσας τρίτης χώρας (εκτός ΕΕ) και της ΕΕ ή ενός κράτους μέλους[97].

Η δέσμη μεταρρυθμίσεων για την προστασία των δεδομένων περιλαμβάνει επίσης ξεχωριστή Οδηγία για την προστασία των δεδομένων για τον τομέα της αστυνομίας και της ποινικής δικαιοσύνης, η οποία προβλέπει κανόνες για την ανταλλαγή προσωπικών δεδομένων σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο.

Συνεπώς με τον GDPR θα ισχύει ένα ενιαίο σύνολο κανόνων για όλα τα κράτη μέλη της ΕΕ. Κάθε κράτος μέλος θα συστήσει ανεξάρτητη εποπτική αρχή για την εξέταση και διερεύνηση καταγγελιών, την επιβολή κυρώσεων σε διοικητικά αδικήματα κλπ.

4.5: Νομιμοποιητική βάση της επεξεργασίας των δεδομένων

[97] Βλ. Για μία ενδιαφέρουσα ανάλυση της λειτουργίας του συγκεκριμένου άρθρου Πρβλ. Μ. Σκόνδρα, «USA Cloud Act: ο αντι-GDPR των Ηνωμένων Πολιτειών Αμερικής», 15/07/2019, LawSpot, Διαθέσιμο σε: https://www.lawspot.gr/nomika-blogs/magdalini_skondra/usa-cloud-act-o-anti-gdpr-ton-inomenon-politeion-amerikis

Εκτός εάν ένα υποκείμενο των δεδομένων έχει παράσχει ενημερωμένη συγκατάθεση για την επεξεργασία δεδομένων για έναν ή περισσότερους σκοπούς, τα προσωπικά δεδομένα δεν υποβάλλονται σε επεξεργασία, εκτός εάν υπάρχει τουλάχιστον μία νομική βάση για να γίνει κάτι τέτοιο. Σύμφωνα με το άρθρο 6, οι νόμιμοι σκοποί είναι:

(α) Εάν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων.

(β) Να εκπληρώνει συμβατικές υποχρεώσεις με πρόσωπο στο οποίο αναφέρονται τα δεδομένα ή για καθήκοντα κατόπιν αιτήσεως ενός προσώπου στο οποίο αναφέρονται τα δεδομένα και το οποίο βρίσκεται στη διαδικασία σύναψης μιας σύμβασης.

(γ) Να συμμορφώνεται με τις νομικές υποχρεώσεις του υπεύθυνου επεξεργασίας δεδομένων.

(δ) Να προστατεύει τα ζωτικά συμφέροντα του υποκειμένου των δεδομένων ή άλλου ατόμου.

(ε) Να εκτελεί καθήκον δημοσίου συμφέροντος ή δημόσιας εξουσίας·

Συνεπώς, οι νομιμοποιητικοί λόγοι της επεξεργασίας των προσωπικών δεδομένων απαριθμούνται περιοριστικά και εξίσου στενά πρέπει να ερμηνεύονται.

Εάν η συναίνεση χρησιμοποιείται ως νόμιμη βάση για τη μεταβίβαση, η συγκατάθεση πρέπει να είναι ρητή για τα δεδομένα που συλλέγονται και για τα δεδομένα που χρησιμοποιούνται (άρθρο 7, όπως ορίζεται στο άρθρο 4). Μια ηλεκτρονική φόρμα που έχει επιλογές συναίνεσης διαρθρωμένες από προεπιλογή παραβιάζουν τον GDPR, καθώς η συγκατάθεση δεν επιβεβαιώνεται με σαφήνεια από τον χρήστη. Επιπλέον, πολλοί τύποι επεξεργασίας δεν μπορούν να «συνδυαστούν» μαζί σε ένα μόνο μήνυμα επιβεβαίωσης, καθώς αυτό δεν είναι συγκεκριμένο για κάθε χρήση δεδομένων και οι ατομικές άδειες δεν δίδονται ελεύθερα.

Τα πρόσωπα στα οποία αναφέρονται τα δεδομένα πρέπει να έχουν τη δυνατότητα να αποσύρουν τη συναίνεση αυτή ανά πάσα στιγμή και η διαδικασία δεν πρέπει να είναι δυσκολότερη από ό, τι η διαδικασία παροχής της συγκατάθεσης.

Περαιτέρω, ο υπεύθυνος επεξεργασίας δεν μπορεί να αρνηθεί την παροχή υπηρεσιών σε χρήστες που αρνούνται τη συγκατάθεσή τους στην επεξεργασία που δεν είναι απολύτως απαραίτητη για τη χρήση της υπηρεσίας. (Άρθρο 7 παράγραφος 4) Η συγκατάθεση για τα παιδιά, που ορίζονται στον κανονισμό ως ηλικίας κάτω των 16 ετών (αν και με την επιλογή των κρατών μελών να φτάνουν μόνο σε ηλικία 13 ετών (άρθρο 8 παράγραφος 1) πρέπει να παρέχεται από τον γονέα ή τον κηδεμόνα του παιδιού και να επαληθεύεται (άρθρο 8).

4.6: Ευθύνη και λογοδοσία

Για να είναι σε θέση να αποδείξει τη συμμόρφωσή του με το GDPR, ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να εφαρμόσει μέτρα τα οποία πληρούν τις αρχές της προστασίας δεδομένων τόσο από το σχεδιασμό όσο και από προεπιλογή. Η προστασία δεδομένων από το σχεδιασμό και

από προεπιλογή (άρθρο 25) απαιτεί να σχεδιάζονται μέτρα προστασίας δεδομένων για την ανάπτυξη επιχειρηματικών διαδικασιών για προϊόντα και υπηρεσίες.

Τα μέτρα αυτά περιλαμβάνουν ψευδώνυμα προσωπικών δεδομένων από τον υπεύθυνο επεξεργασίας, το συντομότερο δυνατό (αιτιολογική σκέψη 78). Είναι ευθύνη του υπεύθυνου επεξεργασίας δεδομένων να εφαρμόζει αποτελεσματικά μέτρα και να είναι σε θέση να αποδείξει τη συμμόρφωση των δραστηριοτήτων επεξεργασίας, ακόμη και αν η επεξεργασία διεξάγεται από έναν επεξεργαστή δεδομένων για λογαριασμό του υπεύθυνου επεξεργασίας (αιτιολογική σκέψη 74).

Όταν συλλέγονται δεδομένα, τα πρόσωπα στα οποία αναφέρονται τα δεδομένα πρέπει να ενημερώνονται σαφώς σχετικά με την έκταση της συλλογής δεδομένων, τη νομική βάση για την επεξεργασία των προσωπικών δεδομένων, τον χρόνο διατήρησης των δεδομένων, τη μεταφορά δεδομένων σε τρίτους ή και εκτός της ΕΕ, και οποιαδήποτε αυτοματοποιημένη διαδικασία λήψης αποφάσεων που γίνεται με αποκλειστικό αλγόριθμο.

Τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται για τα δικαιώματά τους στο πλαίσιο του GDPR, συμπεριλαμβανομένου του δικαιώματός τους να ανακαλούν τη συγκατάθεσή τους[98] για την επεξεργασία δεδομένων ανά πάσα στιγμή, το δικαίωμά τους να βλέπουν τα προσωπικά τους δεδομένα και να έχουν πρόσβαση σε μια επισκόπηση του τρόπου με τον οποίο μεταποιούνται, αντίγραφο των αποθηκευμένων δεδομένων, το δικαίωμα διαγραφής δεδομένων υπό ορισμένες συνθήκες, το δικαίωμα αμφισβήτησης τυχόν αυτόματης λήψης αποφάσεων που έγινε με αποκλειστικό αλγόριθμο και το δικαίωμα υποβολής καταγγελιών στην Αρχή Προστασίας Δεδομένων.

Ως εκ τούτου, στο πρόσωπο στο οποίο αναφέρονται τα δεδομένα πρέπει επίσης να παρέχονται στοιχεία επαφής για τον υπεύθυνο επεξεργασίας δεδομένων και τον αρμόδιο υπάλληλο προστασίας δεδομένων, κατά περίπτωση. Οι εκτιμήσεις επιπτώσεων για την προστασία δεδομένων (άρθρο 35) πρέπει να διεξάγονται όταν προκύπτουν ειδικοί κίνδυνοι στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Απαιτείται εκτίμηση κινδύνου και μετριασμός και απαιτείται προηγούμενη έγκριση των αρχών προστασίας δεδομένων για τους υψηλούς κινδύνους.

4.7: Προστασία δεδομένων κατά το σχεδιασμό

Η προστασία δεδομένων από το σχεδιασμό και από προεπιλογή (άρθρο 25) απαιτεί την προστασία των δεδομένων να σχεδιάζεται για την ανάπτυξη επιχειρηματικών διαδικασιών για προϊόντα και υπηρεσίες. Ως εκ τούτου, οι ρυθμίσεις προστασίας της ιδιωτικής ζωής πρέπει να οριστούν σε υψηλό επίπεδο από προεπιλογή και να ληφθούν τεχνικά και διαδικαστικά μέτρα από τον υπεύθυνο επεξεργασίας για να εξασφαλιστεί ότι η επεξεργασία, καθ' όλη τη διάρκεια του κύκλου ζωής της επεξεργασίας, συμμορφώνεται με τον κανονισμό.

[98] Βλ. άρθρο 7 παρ. 3 του Κανονισμού

Οι ελεγκτές θα πρέπει επίσης να εφαρμόζουν μηχανισμούς που θα διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα δεν θα υποβάλλονται σε επεξεργασία, εκτός εάν αυτό είναι απαραίτητο για κάθε συγκεκριμένο σκοπό.

Μια έκθεση του Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών της Ευρωπαϊκής Ένωσης εξηγεί τι πρέπει να γίνει για την επίτευξη της προστασίας της ιδιωτικής ζωής και των δεδομένων εξ ορισμού. Διευκρινίζει ότι οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης πρέπει να εκτελούνται τοπικά και όχι μέσω απομακρυσμένης υπηρεσίας, διότι και τα δύο κλειδιά και τα δεδομένα πρέπει να παραμείνουν στην εξουσία του ιδιοκτήτη των δεδομένων, προκειμένου να επιτευχθεί ιδιωτικότητα.

4.7.1: Ψευδωνυμοποίηση

Το GDPR ορίζει την ψευδωνυμοποίηση[99] ως μία διαδικασία που απαιτείται όταν αποθηκεύονται δεδομένα (ως εναλλακτική λύση στην άλλη επιλογή της πλήρους ανωνυμίας δεδομένων) για τη μετατροπή των προσωπικών δεδομένων με τέτοιο τρόπο ώστε τα προκύπτοντα δεδομένα να μην μπορούν να αποδοθούν σε συγκεκριμένα υποκείμενα χωρίς τη χρήση πρόσθετων πληροφοριών.

Ένα παράδειγμα είναι η κρυπτογράφηση, η οποία καθιστά τα αρχικά δεδομένα ακατανόητα και η διαδικασία δεν μπορεί να αντιστραφεί χωρίς πρόσβαση στο σωστό κλειδί αποκρυπτογράφησης. Το GDPR απαιτεί να διατηρούνται ξεχωριστά οι πρόσθετες πληροφορίες (όπως το κλειδί αποκρυπτογράφησης) ξεχωριστά από τα ψευδονομισμένα δεδομένα.

Ένα άλλο παράδειγμα ψευδωνυμοποίησης είναι το tokenisation, το οποίο είναι μια μη μαθηματική προσέγγιση για την προστασία δεδομένων σε κατάσταση ηρεμίας που αντικαθιστά ευαίσθητα δεδομένα με μη ευαίσθητα υποκατάστατα, που αναφέρονται ως μάρκες. Ενώ οι μάρκες δεν έχουν εξωτερικό ή εκμεταλλεύσιμο νόημα ή αξία, επιτρέπουν την πλήρη ή μερική ορατότητα συγκεκριμένων δεδομένων για επεξεργασία και ανάλυση ενώ οι ευαίσθητες πληροφορίες παραμένουν κρυμμένες.

Η σηματοδότηση δεν μεταβάλλει τον τύπο ή τη διάρκεια των δεδομένων, πράγμα που σημαίνει ότι μπορεί να γίνει επεξεργασία από παλαιότερα συστήματα όπως βάσεις δεδομένων που μπορεί να είναι ευαίσθητα στο μήκος και τον τύπο δεδομένων. Αυτό απαιτεί επίσης πολύ λιγότερους υπολογιστικούς πόρους για επεξεργασία και λιγότερο χώρο αποθήκευσης σε βάσεις δεδομένων από τα παραδοσιακά κρυπτογραφημένα δεδομένα.

Συνιστάται η ψευδωνυμοποίηση για τη μείωση των κινδύνων για τα ενδιαφερόμενα πρόσωπα στα οποία αναφέρονται τα δεδομένα καθώς και για να βοηθηθούν οι ελεγκτές και οι μεταποιητές να εκπληρώσουν τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων (αιτιολογική σκέψη 28).

[99] Για περισσότερα στοιχεία σχετικά με τη λειτουργία της ψευδωνυμοποίησης Πρβλ. τη μελέτη του Κ. Λιμνιώτη, «Η ψευδωνυμοποίησηστον Γενικό Κανονισμό Προστασίας Δεδομένων», Αρχή Προστασίας Προσωπικών Δεδομένων, 2018, Διαθέσιμο σε: https://www.enisa.europa.eu/events/personal-data-security/pseydonymization

4.8: Αντίκτυπος του νέου Κανονισμού

Παρά το γεγονός ότι βάσει του Κανονισμού οι εταιρείες και οι ιστότοποι είχαν δύο χρόνια για να προετοιμαστούν κατάλληλα ώστε να συμμορφωθούν στις νέες ρυθμίσεις (ας θυμηθούμε ότι ο Κανονισμός ψηφίστηκε το 2016 και ετέθη σε ισχύ από το Μαϊο του 2018), πολλές εταιρείες με παγκόσμια παρουσία άλλαξαν τις πολιτικές απορρήτου αμέσως πριν από την υλοποίηση του GDPR και μάλιστα απέστειλαν απευθείας μηνύματα ηλεκτρονικού ταχυδρομείου και άλλες ειδοποιήσεις σχετικά με τις αλλαγές στις οποίες προέβησαν.

Αυτό επικρίθηκε έντονα καθώς οδήγησε σε έναν τεράστιο αριθμό επικοινωνιών, ενώ οι εμπειρογνώμονες σημείωσαν ότι ορισμένα μηνύματα εξ' αυτών δήλωναν εσφαλμένα ότι έπρεπε να ληφθεί νέα συγκατάθεση για την επεξεργασία δεδομένων όταν τεθεί σε ισχύ ο GDPR (στην πραγματικότητα οποιαδήποτε προηγούμενη συναίνεση για επεξεργασία είναι έγκυρη εφόσον πληροί τις απαιτήσεις του νέου κανονισμού).

Περαιτέρω, οι απάτες του λεγόμενου «ηλεκτρονικού ψαρέματος» έκαναν επίσης την εμφάνιση τους, με τη χρήση ψεύτικων μηνυμάτων ηλεκτρονικού ταχυδρομείου που σχετίζονται με τον GDPR και υποστηρίχθηκε επίσης ότι ορισμένα από αυτά τα μηνύματα ειδοποιήσεων απορρήτου ενδέχεται να απεστάλησαν κατά παράβαση των νόμων κατά του spam[100]. Ειδικότερα, τον Μάρτιο του 2019, ένας πάροχος λογισμικού συμμόρφωσης διαπίστωσε ότι πολλοί ιστότοποι που λειτουργούν από κυβερνήσεις των κρατών μελών της ΕΕ περιείχαν ενσωματωμένη παρακολούθηση από παρόχους τεχνολογίας διαφημίσεων[101].

Σύμφωνα με σχετικές έρευνες[102] που πραγματοποιηθηκαν πρόσφατα, περίπου 25% των τρωτών σημείων του λογισμικού έχουν επιπτώσεις που δυνητικά παραβιάζουν τον GDPR. Δεδομένου ότι το άρθρο 33 υπογραμμίζει τις παραβιάσεις και όχι τα σφάλματα, οι εμπειρογνώμονες ασφάλειας συμβουλεύουν τις εταιρείες να επενδύουν σε διαδικασίες και δυνατότητες για τον εντοπισμό τρωτών σημείων πριν μπορέσουν να αξιοποιηθούν από κακόβουλα λογισμικά, συμπεριλαμβανομένων των διαδικασιών κοινοποίησης τρωτών σημείων συντονισμού[103].

---

[100] Βλ. K. Afifi-Sabet, «Scammers are using GDPR email alerts to conduct phishing attacks», IT PRO, 3/5/2018, Διαθέσιμο σε: https://www.itpro.co.uk/general-data-protection-regulation-gdpr/31058/scammers-are-using-gdpr-email-alerts-to-conduct

[101] Βλ. «EU citizens being tracked on sensitive government websites», Financial Times, 18/3/2019, Διαθέσιμο σε: https://www.ft.com/content/6dbacf74-471b-11e9-b168-96a37d002cd3

[102] Βλ. «What Percentage of Your Software Vulnerabilities Have GDPR Implications?», HackerOne, 16/1/2018, Διαθέσιμο σε: https://www.hackerone.com/sites/default/files/2018-01/GDPR%20Implications-ebook.pdf

[103] Βλ. «The Data Protection Officer (DPO): Everything You Need to Know», Cranium and HackerOne, 20/3/2018, Διαθέσιμο σε: https://www.slideshare.net/hacker0x01/everything-you-need-to-know-about-the-data-protection-officer-role

Από την ημερομηνία έναρξης ισχύος του Κανονισμού, ορισμένοι διεθνείς ιστότοποι άρχισαν να μπλοκάρουν πλήρως τους χρήστες της ΕΕ (συμπεριλαμβανομένων των Instapaper[104], Unroll.me, και εφημερίδων της Tribune Publishing, όπως τις Chicago Tribune και Los Angeles Times) με περιορισμένη λειτουργικότητα ή και απαγόρευσαν τις διαφημίσεις, προκειμένου να απομακρύνουν τα κενά ασφαλείας τους[105].

Ορισμένες εταιρείες, όπως η Klout και διάφορα ηλεκτρονικά βιντεοπαιχνίδια, έπαψαν να λειτουργούν εξ ολοκλήρου κατηγορώντας τον GDPR «ως επιβάρυνση για τη συνέχιση των δραστηριοτήτων τους[106]». Ο όγκος των πωλήσεων διαδικτυακών διαφημίσεων στην Ευρώπη μειώθηκε κατά 25-40% στις 25 Μαΐου 2018 λόγω του Κανονισμού[107].

Το Facebook και οι θυγατρικές εταιρείες WhatsApp και Instagram, καθώς και το Google LLC, μηνύθηκαν από τον μη κερδοσκοπικό οργανισμό NOYB του Max Schrems λίγες μόνο ώρες μετά τα μεσάνυχτα της 25ης Μαΐου του 2018 για τη χρήση της «καταναγκαστικής συγκατάθεσης». Πιο συγκεκριμένα, ο Schrems ισχυρίζεται ότι και οι δύο εταιρείες παραβίασαν το άρθρο 7 παράγραφος 4 του Κανονισμού, επειδή δεν παρουσίασαν δικαιώματα εξαίρεσης για τη συναίνεση όσον αφορά την επεξεργασία δεδομένων σε εξατομικευμένη βάση και επειδή απαίτησαν από τους χρήστες να συναινούν σε όλες τις δραστηριότητες επεξεργασίας δεδομένων (συμπεριλαμβανομένων και εκείνων που δεν είναι απολύτως απαραίτητες) ή που απαγορεύεται να χρησιμοποιούν τις υπηρεσίες[108].

Τέλος, στις 3 Απριλίου 2019, στη Google επιβλήθηκε πρόστιμο ύψους 44 εκατομμυρίων δολλαρίων για μη συμμόρφωση με τον GDPR. Το CNIL, το γραφείο προστασίας των δεδομένων της Γαλλίας, έκρινε ότι η Google ήταν ένοχη για παραβίαση των κανόνων περί απορρήτου της ΕΕ παραλείποντας να αποκτήσει επαρκή συναίνεση από τους χρήστες σχετικά με τα δεδομένα που χρησιμοποιούνται για εξατομικευμένη διαφήμιση. Η ρυθμιστική αρχή διαπίστωσε επίσης ότι η Google δεν παρείχε σαφείς και εύκολα προσβάσιμες πληροφορίες στους καταναλωτές σχετικά με τη συλλογή δεδομένων και τη διατήρηση δεδομένων.

4.9: Συμπεράσματα

[104] Βλ. «Instapaper is temporarily shutting off access for European users due to GDPR», The Verge, 24/5/2018. Διαθέσιμο σε: https://www.theverge.com/2018/5/23/17387146/instapaper-gdpr-europe-access-shut-down-privacy-changes

[105] Βλ. J. Waterson, 24/5/2018, «Sites block users, shut down activities and flood inboxes as GDPR rules loom», The Guardian, Διαθέσιμο σε: https://www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect

[106] Βλ. B. Chen, 23/5/2018, «Getting a Flood of G.D.P.R.-Related Privacy Policy Updates? Read Them», The New York Times, Διαθέσιμο σε: https://www.nytimes.com/2018/05/23/technology/personaltech/what-you-should-look-for-europe-data-law.html

[107] Βλ. «GDPR mayhem: Programmatic ad buying plummets in Europe», 25/5/2018, Digiday, Διαθέσιμο σε: https://digiday.com/media/gdpr-mayhem-programmatic-ad-buying-plummets-europe/

[108] Βλ. «Facebook and Google hit with $8.8 billion in lawsuits on day one of GDPR», The Verge, 25/5/2018, Διαθέσιμο σε: https://www.theverge.com/2018/5/25/17393766/facebook-google-gdpr-lawsuit-max-schrems-europe

Από την ανάλυση που προηγήθηκε διαπιστώνεται ότι ο Κανονισμός Προστασίας Προσωπικών Δεδομένων σε μεγάλο βαθμό «συστηματοποιεί» και συγκεντρώνει σε ένα ενιαίο και συνεκτικό θεσμικό κείμενο τις ρυθμίσεις που παλαιότερα υπήρχαν και είχαν προκύψει για την προστασία των προσωπικών δεδομένων. Είναι γεγονός ότι ο Κανονισμός εμπλουτίζει σημαντικά τον κατάλογο των δικαιωμάτων του υποκειμένου των δεδομένων και προσθέτει και σημαντικές εγγυήσεις για τη διασφάλιση της προστασίας τους κατοχυρώνοντας αφ' ενός ως ρητή αρμοδιότητα των εθνικών ανεξαρτήτων αρχών την παρακολούθηση της εφαρμογής του Κανονισμού και αφ' ετέρου με τη σύσταση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων που αντικατέστησε την ομάδα εργασίας.

Ωστόσο υπάρχουν και αρκετά σημεία του Κανονισμού στα οποία έχει ασκηθεί κριτική. Ειδικότερα, ο τομέας της συγκατάθεσης του GDPR έχει ορισμένες συνέπειες για τις επιχειρήσεις που καταγράφουν τις τηλεφωνικές κλήσεις. Μια τυπική αποποίηση ευθυνών δεν θεωρείται επαρκής για την απόκτηση της συναίνεσης για την καταγραφή κλήσεων. Επιπλέον, όταν ξεκινά η εγγραφή, αν ο καλών αποσύρει τη συγκατάθεσή του, τότε πρέπει να σταματήσει μια εγγραφή που είχε αρχίσει και να διασφαλιστεί ότι η εγγραφή δεν θα αποθηκευτεί. Οι ανησυχίες επαληθεύθηκαν σε μια έκθεση που κατέθεσε η δικηγορική εταιρεία Baker & McKenzie όπου διαπίστωσε ότι περίπου το 70% των ερωτηθέντων πιστεύουν ότι οι οργανώσεις θα πρέπει να επενδύσουν πρόσθετο προϋπολογισμό/προσπάθεια για να συμμορφωθούν με τη συγκατάθεση, τη χαρτογράφηση δεδομένων και τις προβλέψεις για τη διασυνοριακή μεταφορά δεδομένων βάσει του GDPR.

Πάντως, η δέσμη μέτρων για την προστασία δεδομένων που εγκρίθηκε τον Μάιο του 2016 αποσκοπεί να καταστήσει την Ευρώπη κατάλληλη για την ψηφιακή εποχή. Ο Κανονισμός αποτελεί ουσιαστικό βήμα για την ενίσχυση των θεμελιωδών δικαιωμάτων των ατόμων στην ψηφιακή εποχή και τη διευκόλυνση των επιχειρήσεων, αποσαφηνίζοντας τους κανόνες για τις επιχειρήσεις και τους δημόσιους φορείς στην ενιαία ψηφιακή αγορά. Ένας ενιαίος νόμος θα εξαλείψει επίσης τον σημερινό κατακερματισμό των διαφόρων εθνικών συστημάτων και την περιττή διοικητική επιβάρυνση.

Η Οδηγία προστατεύει το θεμελιώδες δικαίωμα των πολιτών στην προστασία των δεδομένων όποτε τα προσωπικά δεδομένα χρησιμοποιούνται από τις αρχές επιβολής του νόμου για σκοπούς επιβολής του νόμου. Ειδικότερα, θα εξασφαλίσει ότι τα προσωπικά δεδομένα των θυμάτων, των μαρτύρων και των υπόπτων εγκλήματος θα προστατεύονται δεόντως και θα διευκολύνουν τη διασυνοριακή συνεργασία για την καταπολέμηση του εγκλήματος και της τρομοκρατίας. Οι χώρες της ΕΕ έχουν συστήσει εθνικούς φορείς υπεύθυνους για την προστασία των δεδομένων προσωπικού χαρακτήρα σύμφωνα με με το άρθρο 8 παράγραφος 3 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ.

Από τις 25 Μαΐου 2018, η ομάδα εργασίας του άρθρου 29[109] θα αντικατασταθεί από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB). Το EDPB έχει την ιδιότητα του οργάνου της ΕΕ με νομική προσωπικότητα και διαθέτει ανεξάρτητη γραμματεία.

[109] Η ομάδα εργασίας του άρθρου 29 ήταν η ανεξάρτητη ευρωπαϊκή ομάδα εργασίας που χειριζόταν θέματα σχετικά με την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα έως τις 25 Μαΐου 2018 (έναρξη ισχύος του ΓΚΠΔ).

Ο κανονισμός 2018/1725 ορίζει τους κανόνες που εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα θεσμικά όργανα, τους οργανισμούς, τα γραφεία και τους οργανισμούς της Ευρωπαϊκής Ένωσης. Ευθυγραμμίζεται με τον γενικό κανονισμό για την προστασία των δεδομένων και την Οδηγία για την επιβολή της νομοθεσίας για την προστασία των δεδομένων. Η αίτηση τέθηκε σε εφαρμογή στις 11 Δεκεμβρίου 2018.

Ο κανονισμός 2018/1725 θέσπισε έναν ευρωπαίο επόπτη προστασίας δεδομένων (ΕΕΠΔ). Ο ΕΕΠΔ είναι ανεξάρτητο όργανο της ΕΕ που είναι υπεύθυνο για την παρακολούθηση της εφαρμογής των κανόνων προστασίας δεδομένων στα ευρωπαϊκά θεσμικά όργανα και για τη διερεύνηση καταγγελιών. Η Ευρωπαϊκή Επιτροπή όρισε έναν υπεύθυνο προστασίας δεδομένων ο οποίος είναι υπεύθυνος για την παρακολούθηση και την εφαρμογή των κανόνων προστασίας δεδομένων στην Ευρωπαϊκή Επιτροπή. Ο υπεύθυνος προστασίας δεδομένων διασφαλίζει ανεξάρτητα την εσωτερική εφαρμογή των κανόνων προστασίας δεδομένων σε συνεργασία με τον ευρωπαίο επόπτη προστασίας δεδομένων.

Σε αυτό το σημείο, η θέσπιση του Γενικού Κανονισμού Προστασίας Στοιχείων θεωρείται ιδιαίτερα σημαντική εξέλιξη, καθώς αναπτύσσει τη λογική της αυτορρύθμισης στους υπεύθυνους επεξεργασίας, μειώνοντας σημαντικά των όγκο των υποθέσεων που θα καταλήγουν στην Αρχή. Βέβαια, ο νέος Κανονισμός θέτει στην Αρχή ιδιαίτερες απαιτήσεις προετοιμασίας και ετοιμότητας εντός αυστηρών χρονικών προθεσμιών.

Το συνολικό κόστος για τις επιχειρήσεις της ΕΕ εκτιμάται σε περίπου 200 δισ. ευρώ, ενώ για τις αμερικανικές εταιρείες η εκτίμηση είναι 41,7 δισ. δολάρια. Έχει υποστηριχθεί επίσης ότι οι μικρότερες επιχειρήσεις ενδέχεται να μην έχουν τους οικονομικούς πόρους για να συμμορφωθούν επαρκώς με το GDPR, σε αντίθεση με τις μεγαλύτερες διεθνείς εταιρείες τεχνολογίας (όπως το Facebook και το Google). Η έλλειψη γνώσης και κατανόησης των κανονισμών υπήρξε επίσης λόγος άσκησης κριτικής. Ένα αντεπιχείρημα ήταν ότι οι εταιρείες ενημερώθηκαν για τις αλλαγές αυτές δύο χρόνια πριν από την έναρξη ισχύος τους και, ως εκ τούτου, έπρεπε να είχαν αρκετό χρόνο για να προετοιμαστούν. Επομένως, τίθεται το ζήτημα εάν οι προβλέψεις του Κανονισμού για τη συμμόρφωση των εταιρειών ευνοούν τους επιχειρηματικούς κολοσσούς που έχουν την οικονομική δυνατότητα να συμμορφωθούν στις προβλέψεις του εις βάρος των μικρότερων εταιρειών.

Κεφάλαιο 5: Ο ρόλος των εποπτικών αρχών

Εξέχουσα σημασία για την αποτελεσματική εφαρμογή του Γενικού Κανονισμού Προστασίας των Προσωπικών Δεδομένων κατέχουν και οι προβλέψεις του για τη λειτουργία, το καθεστώς και τις αρμοδιότητες των Εποπτικών Αρχών, οι οποίες εξετάζονται στο παρόν κεφάλαιο. Πιο συγκεκριμένα, στο πρώτο υποκεφάλαιο αναλύονται τα άρθρα 51-59 του Κανονισμού που αφορούν τις Ανεξάρτητες Εποπτικές Αρχές, στο δεύτερο υποκεφάλαιο εξετάζεται η Αρχή Προστασίας Προσωπικών Δεδομένων, ενώ στο τρίτο υποκεφάλαιο μελετάται το Ευρωπαϊκό Συμβούλιο Προστασίας Προσωπικών Δεδομένων, ως μία σημαντική καινοτομία του GDPR.

5.1: Οι προβλέψεις του Κανονισμού σχετικά με τις εποπτικές αρχές

Για τη συστηματική ερμηνεία του Κανονισμού κρίνεται αρχικώς αναγκαίο να διευκρινιστεί ότι τα άρθρα 51-59 που ρυθμίζουν τις Ανεξάρτητες Εποπτικές Αρχές ανευρίσκονται στο Κεφάλαιο 6 του GDPR το οποίο επιμερίζεται σε δύο τμήματα. Το πρώτο τμήμα τιτλοφορείται ως «Ανεξάρτητο Καθεστώς» και περιέχει τα άρθρα 51-54, ενώ το δεύτερο τμήμα τιτλοφορείται ως «Αρμοδιότητα, καθήκοντα και εξουσίες» και περιέχει τα άρθρα 55-59.

Πιο συγκεκριμένα, στο άρθρο 51 παρ. 1[110] κατοχυρώνεται η υποχρέωση όλων των κρατών μελών να διασφαλίζουν ότι μία ή περισσότερες ανεξάρτητες δημόσιες αρχές επιφορτίζονται με την παρακολούθηση της εφαρμογής του παρόντος κανονισμού, με σκοπό την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας τη διευκόλυνση της ελεύθερης κυκλοφορίας δεδομένων προσωπικού χαρακτήρα στην Ένωση («εποπτική αρχή»). Τα σημαντικά στοιχεία της παρούσας ρύθμισης είναι δύο.

Εν πρώτοις, το άρθρο κατοχυρώνει πλέον ως ρητή αρμοδιότητα των εποπτικών αρχών να παρακολουθούν την τήρηση του παρόντος κανονισμού. Επομένως, γίνεται αντιληπτό και με τον πιο αναντίρρητο τρόπο πως ο Γενικός Κανονισμός «αντικαθιστά» όλες τις προηγούμενες ευρωπαϊκές και γενικότερα υπερνομοθετικές πράξεις που διασφάλιζαν την προστασία των προσωπικών δεδομένων. Αυτό θα καταστεί φανερό κυρίως παρακάτω (Βλ. υποκεφάλαιο 6.4) όπου εξετάζονται συγκριτικά γνωμοδοτήσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, καθώς όπως θα αποδειχθεί πριν τη θέσπιση του GDPR η Αρχή επικαλούταν πληθώρα νομικών κειμένων για να στηρίξει τη γνωμοδοτική της αρμοδιότητα. Περαιτέρω, σημαντική είναι η πρόβλεψη του Κανονισμού για τη δυνατότητα ύπαρξης περισσότερων της μίας εποπτικής αρχής σε κάθε κράτος μέλος.

Περαιτέρω, στην παράγραφο 2 ο Κανονισμός κατοχυρώνει την υποχρέωση των εποπτικών αρχών για συνεργασία μεταξύ τους αλλά και με την Επιτροπή προκειμένου να διασφαλιστεί η συνεκτική εφαρμογή του, ενώ στην παράγραφο 3 ορίζεται η υποχρέωση κάθε κράτους μέλους να ορίζει την

[110] Πρβλ. το κείμενο του Κανονισμού στην ιστοσελίδα: https://www.lawspot.gr/nomikes-plirofories/nomothesia/genikos-kanonismos-gia-tin-prostasia-dedomenon?lspt_context=gdpr

εποπτική αρχή που θα την εκπροσωπεί στο Συμβούλιο Προστασίας Δεδομένων. Έπειτα, στο άρθρο 52 του Κανονισμού στις πρώτες 2 παραγράφους κατοχυρώνονται οι εγγυήσεις αμεροληψίας των επιπτικών αρχών και μάλιστα στην παράγραφο 3 τονίζεται ότι τα μέλη κάθε εποπτικής αρχής απέχουν από κάθε πράξη ασυμβίβαστη προς τα καθήκοντά τους και δεν ασκούν κανένα ασυμβίβαστο επάγγελμα.

Στην παράγραφο 4 θεσπίζεται η υποχρέωση κάθε κράτους μέλους να διασφαλίζει ότι κάθε εποπτική αρχή διαθέτει τους απαραίτητους ανθρώπινους και οικονομικούς πόρους, καθώς και τις απαραίτητες υποδομές και εγκαταστάσεις για την εκτέλεση των καθηκόντων τους. Αντίστοιχες είναι οι διατάξεις και των επόμενων παραγράφων, καθώς εξασφαλίζεται ότι κάθε εποπτική αρχή διαθέτει τους δικούς της υπαλλήλους και γενικώς έχει το δικαίωμα της αυτοδιοίκησης, αλλά κατοχυρώνεται παράλληλα και η υποχρέωση οικονομικού ελέγχου της αρχής που να μην επηρεάζει την ανεξαρτησία της.

Όπως είναι λογικό αυτές οι προβλέψεις δημιουργούν σημαντικά ερμηνευτικά προβλήματα και δεν μπορούν να θεωρηθούν επαρκείς για τη διασφάλιση της αμεροληψίας των αρχών. Και τούτο διότι ο τρόπος λειτουργίας των ανεξάρτητων διοικητικών αρχών διαφέρει από κράτος σε κράτος και εν πολλοίς ρυθμίζεται από τα εθνικά συντάγματα των κρατών μελών (πχ τρόπος επιλογής της ηγεσίας). Ουσιαστικά δηλαδή στο σημείο αυτό ο Κανονισμός δεν πρωτοτυπεί ιδιαίτερα, αλλά αντίθετα επαναλαμβάνει τις θεσμικές εγγυήσεις που ούτως ή άλλως υφίστανται για τις ανεξάρτητες αρχές (λειτουργική και οργανική ανεξαρτησίας, αυτοδιοίκηση, οικονομική αυτοτέλεια κτλ.). Είναι μάλιστα απορίας άξιον με ποιό ένδικό βοήθημα δύνανται να ελεγχθούν τα κράτη μέλη αν δεν συμμορφώνονται προς τις συγκεκριμένες ρυθμίσεις.

Επιπροσθέτως, στο άρθρο 53 ορίζονται οι προϋποθέσεις διορισμού ενός μέλους της εποτπικής αρχής που περιλαμβάνουν τη διαφανή διαδικασία διορισμού τους από το Κοινοβούλιο, την Κυβέρνηση, ή τον Αρχηγό του κράτους, τα απαραίτητα προσόντα, δεξιότητες και εμπειρία για την άσκηση αυτών των καθηκόντων καθώς και τις αυστηρές προϋποθέσεις παύσης ενός μέλους της Αρχής.

Τέλος, στο άρθρο 54 κατοχυρώνεται η υποχρέωση των κρατών-μελών να προβλέπει διά νόμου τη σύσταση της εποπτικής αρχής, τα προσόντα και τις προϋποθέσεις επιλεξιμότητας των μελών, τη διάρκεια της θητείας των μελών, τις υποχρεώσεις και απαγορεύσεις που ισχύουν για αυτά, καθώς και τη δέσμευση τους από το επαγγελματικό απόρρητο. Και σε αυτή την περίπτωση οι προβλέψεις του Κανονισμού κρίνονται επουσιώδεις, διότι σε μεγάλο βαθμό σε όλα κράτη μέλη έχουν συσταθεί ήδη εποπτικές αρχές με διαφορετικό συστατικό νόμο λόγω του Κανονισμού 46/2001[111].

Έπειτα, στο άρθρο 55 ορίζονται οι αρμοδιότητες κάθε εποπτικής αρχής που περιλαμβάνουν την παρακολούθηση εφαρμογής του παρόντα Κανονισμού και μάλιστα στην παράγραφο 3 τονίζεται ότι οι εποπτικές αρχές δεν είναι αρμόδιες να ελέγχουν πράξεις που διενεργούνται από δικαστήρια στο

[111] Βλ. Λ. Μήτρου, «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων», Εκδ. Σάκκουλα, 2017, σ. 78

πλαίσιο της δικαιοδοτικής τους αρμοδιότητας. Περαιτέρω, στο επόμενο άρθρο ορίζονται οι κανόνες που διέπουν τη διασυνοριακή πράξη μεταβίβασης προσωπικών δεδομένων, διασφαλίζοντας την αρμοδιότητα της επικεφαλής αρχής, ενώ στα άρθρο 57 και 58 απαριθμούνται τα καθήκοντα των εποπτικών αρχών που περιλαμβάνουν την παρακολούθηση και εφαρμογή του Κανονισμού, την προώθηση της ευαισθητοποίησης του κοινού και την κατανόηση των κινδύνων για τα προσωπικά δεδομένα, το καθήκον να συμβουλεύουν/γνωμοδοτούν το εθνικό κοινοβούλιο, την κυβέρνηση και άλλα όργανα του κράτους για θέματα που σχετίζονται με τα προσωπικά δεδομένα, την προώθηση της ευαισθητοποίησης των υπεύθυνων επεξεργασίας σχετικά με τις υποχρεώσεις τους, τον χειρισμό καταγγελιών που υποβάλλονται από υποκείμενο δεδομένων, η συνεργασία με άλλες εποπτικές αρχές και η εκπόνηση ερευνών σχετικά με την εφαρμογή του Κανονισμού.

Στο σημείο αυτό παρατηρείται ότι κατοχυρώνεται ένας εκτενής κατάλογος υποχρεώσεων/αρμοδιοτήτων για τις εποπτικές αρχές[112]. Τέλος, στο άρθρο 59 κατοχυρώνεται η υποχρέωση των εποπτικών αρχών να καταρτίζουν ετήσιες εκθέσεις των δραστηριοτήτων τους που υποβάλλονται στο εθνικό κοινοβούλιο, στην κυβέρνηση και στις άλλες αρχές των κρατών μελών.

5.2: Η Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Η Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι συνταγματικώς κατοχυρωμένη[113] ανεξάρτητη διοικητική αρχή η οποία ιδρύθηκε[114] με το νόμο 2472/1997 «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, με τον οποίο όπως προαναφέρθηκε ενσωματώθηκε στην ελληνική έννομη τάξη η ευρωπαϊκή Οδηγία 95/46/ΕΚ. Σύμφωνα με την παράγραφο 1 του άρθρου 20 του ιδρυτικού της νόμου 2472/1997 η Αρχή εξυπηρετείται από Γραμματεία που λειτουργεί σε επίπεδο Διεύθυνσης και αποτελείται από τα τμήματα Ελεγκτών, Επικοινωνίας και Διοικητικών και Οικονομικών Υποθέσεων. Η Αρχή, είναι ουσιαστικά το θεμέλιο του συστήματος επάνω στο οποίο οικοδομείται ο μηχανισμός τήρησης και εφαρμογής του Νόμου, έχει δε ευρύτατες αρμοδιότητες, τις οποίες θα μπορούσε κανείς να διακρίνει σε: α) εποπτικές-ελεγκτικές, β) αποφασιστικές-κυρωτικές και γ) νομοθετικές-γνωμοδοτικές[115].
Παρατηρείται λοιπόν ότι η σύσταση εποπτικής αρχής στην Ελλάδα είχε ήδη λάβει χώρα από την ενσωμάτωση της Οδηγίας 95/46/ΕΚ.

---

[112] Βλ. Λ. Κοτσαλή, «Γενικός Κανονισμός Προστασίας Δεδομένων», Εκδ. Νομική Βιβλιοθήκη, 2018, σ. 198

[113] Σύμφωνα με το άρθρο 9Α Σ. «η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει». Ουσιαστικά το Σύνταγμα επιβεβαίωσε το ρυθμιστικό σχήμα που είχε ήδη εισαγάγει τρία χρόνια πριν ο Ν. 2472/97. Η Αρχή Προστασίας Προσωπικών Δεδομένων είναι μία από τις πέντε Ανεξάρτητες Αρχές που περιεβλήθησαν με συνταγματική περιωπή με την συνταγματική αναθεώρηση του 2001 . Κατά συνέπεια δεν μπορεί να καταργηθεί ή να τροποποιηθεί, όσον αφορά στο συνταγματικά προσδιορισμένο θεσμικό της περιεχόμενο με νόμο. Αυτό μπορεί να συμβεί μόνο με συνταγματική αναθεώρηση. Βλ. αναλυτικά Κ. Δελούκα-Ιγγλέση, Νομικά Θέματα Ηλεκτρονικού Εμπορίου, ό.π., σ. 317 επ.

[114] Πρβλ. για το κείμενο του νόμου σε: http://www.nurs.uoa.gr/fileadmin/nurs.uoa.gr/uploads/Nomothesia_Nosilefton/Nomoi/Nomos_2472_FEK_501997.pdf Η λειτουργία της Αρχής ξεκίνησε στις 10 Νοεμβρίου 1997.

[115] Βλ. Κ. Δελούκα-Ιγγλέση, Νομικά Θέματα Ηλεκτρονικού Εμπορίου, ό.π., σ. 319.

Σημειωτέον επίσης ότι στη χώρα δεν λειτουργεί άλλη ανεξάρτητη εποπτική αρχή με τον ίδιο σκοπό. Επομένως παρατηρείται ότι προκύπτουν ιδιαίτερα προβλήματα καθώς ο νέος Κανονισμός θέτει συγκεκριμένα πλαίσια λειτουργίας σε εποπτικές αρχές που έχουν ήδη συσταθεί με εθνικούς νόμους και λειτουργούν εδώ και αρκετά χρόνια με ένα τελείως διαφορετικό καθεστώς.

5.3: Ευρωπαϊκό Συμβούλιο Προστασίας Προσωπικών Δεδομένων

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων έχει την ιδιότητα του οργάνου της ΕΕ με νομική προσωπικότητα και διαθέτει ανεξάρτητη γραμματεία, διοικητική και οικονομική αυτοτέλεια. Πιο συγκεκριμένα, ο κανονισμός 2018/1725 ορίζει τους κανόνες που εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα θεσμικά όργανα, τους οργανισμούς, τα γραφεία και τους οργανισμούς της Ευρωπαϊκής Ένωσης. Ευθυγραμμίζεται με τον γενικό κανονισμό για την προστασία των δεδομένων και την Οδηγία για την επιβολή της νομοθεσίας για την προστασία των δεδομένων.

Ο κανονισμός 2018/1725 θέσπισε έναν Ευρωπαίο Επόπτη Προστασίας Δεδομένων. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων είναι ανεξάρτητο όργανο της ΕΕ που είναι υπεύθυνο για την παρακολούθηση της εφαρμογής των κανόνων προστασίας δεδομένων στα ευρωπαϊκά θεσμικά όργανα και για τη διερεύνηση καταγγελιών. Η Ευρωπαϊκή Επιτροπή όρισε έναν υπεύθυνο προστασίας δεδομένων ο οποίος είναι υπεύθυνος για την παρακολούθηση και την εφαρμογή των κανόνων προστασίας δεδομένων στην Ευρωπαϊκή Επιτροπή. Ο υπεύθυνος προστασίας δεδομένων διασφαλίζει ανεξάρτητα την εσωτερική εφαρμογή των κανόνων προστασίας δεδομένων σε συνεργασία με τον ευρωπαίο επόπτη προστασίας δεδομένων.

Στην ετήσια έκθεση της Αρχής για το έτος 2015 (Φ.Ε.Κ. Α΄ 3682/15-11-2016) είναι εμφανές ο αυξημένος όγκος υποθέσεων που διαχειρίζεται, για παράδειγμα ο αριθμός των προσφυγών, ερωτημάτων, αιτήσεων ανήλθε στις 2076, ενώ οι γνωστοποιήσεις για την τήρηση αρχείων προσωπικών στοιχείων έφτασε τις 1244. Πιο αναλυτικά, στον τομέα της υγείας την 31η Δεκεμβρίου του 2015 εκκρεμούσαν 99 υποθέσεις προσφυγών και καταγγελιών, ενώ οι εισερχόμενες υποθέσεις ερωτημάτων ήταν 190, οι διεκπεραιωμένες 207 και οι εκκρεμείς 355.

Αντίστοιχα, στην ετήσια έκθεση της Αρχής για το έτος 2016, διατυπώνεται ότι η Αρχή διεκπεραίωσε συνολικά 3.105 υποθέσεις προσφυγών/καταγγελιών, ερωτημάτων και γνωστοποιήσεων, 39 % περισσότερες από το 2015 και εξέδωσε 8 γνωμοδοτήσεις. Σε αυτό το σημείο, η θέσπιση του Γενικού Κανονισμού Προστασίας Στοιχείων θεωρείται ιδιαίτερα σημαντική εξέλιξη, καθώς αναπτύσσει τη λογική της αυτορρύθμισης στους υπεύθυνους επεξεργασίας, μειώνοντας σημαντικά των όγκο των υποθέσεων που θα καταλήγουν στην Αρχή[116]. Βέβαια, ο νέος Κανονισμός θέτει στην Αρχή ιδιαίτερες απαιτήσεις προετοιμασίας και ετοιμότητας εντός αυστηρών χρονικών προθεσμιών[117].

[116] Βλ. «Ένας χρόνος GDPR: Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων εξέδωσε έρευνα-απολογισμό και βίντεο», 23/05/2019, Lawspot, Διαθέσιμο σε: https://www.lawspot.gr/nomika-nea/enas-hronos-gdpr-eyropaiko-symvoylio-prostasias-dedomenon-exedose-ereyna-apologismo-kai

[117] Βλ. Ετήσια έκθεση Α.Π.Δ.Π.Χ. 2016(Φ.Ε.Κ. Β΄ 4105/23-11-2017)

5.4: Υπεύθυνος προστασίας δεδομένων

Εάν η επεξεργασία πραγματοποιείται από δημόσια αρχή (εκτός από τα δικαστήρια ή τις ανεξάρτητες δικαστικές αρχές όταν ασκούν τα δικαστικά τους καθήκοντα) ή εάν οι εργασίες επεξεργασίας συνεπάγονται τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα ή εάν η επεξεργασία σε μεγάλη κλίμακα ειδικών κατηγοριών δεδομένων και δεδομένων προσωπικού χαρακτήρα σχετικά με τις ποινικές καταδίκες και αξιόποινες πράξεις (άρθρα 9 και 10), πρέπει να ορίζεται ένας υπεύθυνος προστασίας δεδομένων (ΥΠΔ) -ένα πρόσωπο με εξειδικευμένες γνώσεις σχετικά με το δίκαιο και τις πρακτικές προστασίας δεδομένων- χειριστή ή μεταποιητή για την παρακολούθηση της εσωτερικής συμμόρφωσής τους με τον κανονισμό.

Ένας καθορισμένος ΥΠΔ μπορεί να είναι σημερινό μέλος του προσωπικού του υπεύθυνου επεξεργασίας ή του μεταποιητή ή ο ρόλος αυτός μπορεί να ανατεθεί σε εξωτερικό πρόσωπο ή οργανισμό μέσω σύμβασης παροχής υπηρεσιών. Σε κάθε περίπτωση, ο φορέας επεξεργασίας πρέπει να διασφαλίζει ότι δεν υπάρχει σύγκρουση συμφερόντων σε άλλους ρόλους ή συμφέροντα που μπορεί να κατέχει ένας ΥΠΔ. Τα στοιχεία επικοινωνίας για τον ΥΠΔ πρέπει να δημοσιεύονται από τον οργανισμό επεξεργασίας (για παράδειγμα, σε ανακοίνωση προστασίας δεδομένων) και να καταχωρούνται στην εποπτική αρχή.

Ο ΥΠΔ είναι παρόμοιος με έναν υπεύθυνο συμμόρφωσης και αναμένεται επίσης να είναι ικανός να διαχειρίζεται τις διαδικασίες πληροφορικής, την ασφάλεια των δεδομένων (συμπεριλαμβανομένης της αντιμετώπισης κυβερνοαπελευθερώσεων) και άλλων κρίσιμων ζητημάτων συνέχισης των δραστηριοτήτων γύρω από την εκμετάλλευση και την επεξεργασία προσωπικών και ευαίσθητων δεδομένων.

Το απαιτούμενο σύνολο δεξιοτήτων εκτείνεται πέρα από την κατανόηση της συμμόρφωσης με τους νόμους και τους κανονισμούς περί προστασίας δεδομένων, ο ΥΠΔ πρέπει να διατηρεί ένα απόθεμα ζωντανών δεδομένων για όλα τα δεδομένα που συλλέγονται και αποθηκεύονται για λογαριασμό του οργανισμού. Περισσότερες λεπτομέρειες σχετικά με τη λειτουργία και τον ρόλο του υπεύθυνου προστασίας δεδομένων δόθηκαν στις 13 Δεκεμβρίου 2016 (αναθεωρημένες στις 5 Απριλίου 2017) σε έγγραφο κατευθυντηρίων γραμμών.

Οι οργανισμοί που εδρεύουν εκτός ΕΕ πρέπει επίσης να διορίσουν ένα πρόσωπο με έδρα την ΕΕ ως εκπρόσωπο και σημείο επαφής για τις υποχρεώσεις τους στο πλαίσιο του GDPR (άρθρο 27). Αυτός είναι ένας ξεχωριστός ρόλος από έναν ΥΠΔ, παρόλο που υπάρχουν αλληλεπικαλύψεις στις ευθύνες που υποδηλώνουν ότι αυτός ο ρόλος μπορεί να διατεθεί και από τον ορισθέντα ΥΠΔ.

5.5: Εκπρόσωπος της ΕΕ

Ένας εκπρόσωπος της ΕΕ είναι εντολοδόχος ή «πρεσβευτής» της ΕΕ που είναι εγκατεστημένος εκτός ΕΕ (υπεύθυνος επεξεργασίας δεδομένων ή επεξεργαστής δεδομένων) και υπόκειται στον γενικό

κανονισμό για την προστασία των δεδομένων (GDPR) της ΕΕ. Ένα φυσικό (ατομικό) ή (εταιρικό) πρόσωπο μπορεί να διαδραματίσει το ρόλο του εκπροσώπου της ΕΕ.

Ο εκπρόσωπος της ΕΕ είναι υπεύθυνος επικοινωνίας του ελεγκτή ή του μεταποιητή έναντι του ευρωπαίου επόπτη προστασίας δεδομένων και των προσώπων στα οποία αναφέρονται τα δεδομένα, σε όλα τα θέματα που σχετίζονται με τη μεταποίηση, προκειμένου να διασφαλιστεί η συμμόρφωση με τον GDPR. Σκοπός αυτής της εκπροσώπησης είναι να δοθεί η δυνατότητα στις ευρωπαϊκές εποπτικές αρχές προστασίας δεδομένων να διασφαλίσουν τη συμμόρφωση με το GDPR, ελέγχοντας ή επιβλέποντας τις δραστηριότητες των μη κοινοτικών μονάδων που υπόκεινται στο GDPR μέσω των αντίστοιχων αντιπροσώπων τους στην ΕΕ.

Όπως αναφέρθηκε προηγουμένως, μόνο οι μη ευρωπαϊκές εγκαταστάσεις που υπόκεινται στο GDPR είναι υποχρεωμένες να ορίζουν έναν εκπρόσωπο της ΕΕ. Αξίζει να επαναληφθεί το γεγονός ότι μια εγκατάσταση εκτός ΕΕ υπόκειται στο GDPR εάν αναλαμβάνει τακτικά μία από τις ακόλουθες δραστηριότητες: α) την προσφορά αγαθών ή υπηρεσιών, ανεξάρτητα από το αν απαιτείται πληρωμή του προσώπου στο οποίο αναφέρονται τα δεδομένα, στα υποκείμενα των δεδομένων στην ΕΕ · και / ή β) την παρακολούθηση της συμπεριφοράς των προσώπων στα οποία αναφέρονται τα δεδομένα στην ΕΕ, όσον αφορά τη συμπεριφορά τους εντός της ΕΕ.

Η διάταξη αυτή αφορά κάθε εταιρεία που προσφέρει προϊόντα ή υπηρεσίες σε απευθείας σύνδεση σε πελάτες της ΕΕ ή χρησιμοποιεί cookies ή παρόμοιες τεχνολογίες για την παρακολούθηση των υποκειμένων των δεδομένων της ΕΕ. Οι εγκαταστάσεις αυτές πρέπει να συμμορφώνονται με το GDPR και, ως εκ τούτου, υποχρεούνται να ορίσουν έναν εκπρόσωπο της ΕΕ.

Εντούτοις, μια εγκατάσταση εκτός ΕΕ απαλλάσσεται από τον ορισμό ενός εκπροσώπου της ΕΕ όταν η επεξεργασία είναι απλώς περιστασιακή και δεν περιλαμβάνει, σε μεγάλη κλίμακα, επεξεργασία ειδικών κατηγοριών δεδομένων όπως αναφέρεται στο άρθρο 9 παράγραφος 1 της GDPR ή επεξεργασία προσωπικών δεδομένων σχετικά με τις ποινικές καταδίκες και τα αδικήματα που αναφέρονται στο άρθρο 10 της GDPR και η επεξεργασία αυτή είναι απίθανο να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, λαμβάνοντας υπόψη τη φύση, το πλαίσιο, το πεδίο εφαρμογής και τους σκοπούς της επεξεργασίας. Οι εξωκοινοτικές δημόσιες αρχές και φορείς εξαιρούνται εξίσου.

Εάν μια ξένη εταιρεία που υπόκειται στο GDPR αρνείται να ορίσει εκπρόσωπο της ΕΕ όπως απαιτείται, ο πρώτος παραβιάζει το GDPR και διατρέχει τον κίνδυνο να επιβληθεί διοικητικό πρόστιμο ύψους μέχρι 10 εκατομμυρίων ευρώ (10 000 000 ευρώ) σε 2% του συνολικού ετήσιου κύκλου εργασιών της εταιρείας σε παγκόσμιο επίπεδο κατά το προηγούμενο οικονομικό έτος, όποια από τις δύο είναι υψηλότερη.

Η άγνοια του GDPR δεν θα αποτελούσε δικαιολογία και ο εκ προθέσεως ή η αμέλεια (εκ προθέσεως τύφλωση) χαρακτήρα της παράβασης (αδυναμία ορισμού αντιπροσώπου της ΕΕ) μπορεί μάλλον να αποτελέσει επιβαρυντικούς παράγοντες. Γι’ αυτούς ακριβώς τους λόγους, οι περισσότερες ξένες εταιρείες βρίσκονται σε βιασύνη για να ορίσουν τους αντίστοιχους αντιπροσώπους τους στην ΕΕ, ενώ εξειδικευμένες εταιρείες με προστασία δεδομένων από την ΕΕ έχουν διευκολύνει τα πράγματα.

Όπως οι αρχηγοί κρατών ορίζουν τους πρεσβευτές τους με επιστολές αξιοπιστίας, η εγκατάσταση εκτός ΕΕ πρέπει να εκδώσει έγγραφο δεόντως υπογεγραμμένο (επιστολή διαπίστευσης) που ορίζει ένα συγκεκριμένο άτομο ή εταιρεία ως εκπρόσωπό της στην ΕΕ. Η εν λόγω ονομασία μπορεί να γίνει μόνο γραπτώς (GDPR άρθρο 27). Ορισμένες εταιρείες προστασίας δεδομένων με έδρα την ΕΕ διαθέτουν ήδη σχέδια επιστολών διαπίστευσης, τα οποία απλώς διαβιβάζουν στις ενδιαφερόμενες εταιρείες για να υπογράψουν και να στείλουν ταχυδρομικώς.

5.6: Συμπεράσματα

Αναντίρρητα οι προβλέψεις του Κανονισμού αναφορικά με τις εποπτικές αρχές είναι ιδιαιτέρως σημαντικές καθώς αποτελούν τις θεσμικές εγγυήσεις για την αποτελεσματική εφαρμογή του περιεχομένου του. Ο Κανονισμός αλλάζει αρκετά στοιχεία σχετικά με τη λειτουργία των εποπτικών αρχών θεσπίζοντας σειρά εγγυήσεων λειτουργικής και οργανικής ανεξαρτησίας, όπως επί παραδείγματι οι συγκεκριμένες προϋποθέσεις επιλογής και διαφανούς διορισμού των μελών της (διορισμός από το εθνικό κοινοβούλιο, τον αρχηγό του κράτους, της κυβέρνησης ή από ανεξάρτητη αρχή έμπειρων και ειδικώς καταρτισμένων μελών), αυτοδιοίκηση, οικονομική αυτοτέλεια και παράλληλα υποχρέωση των εθνικών κυβερνήσεων να ενισχύουν οικονομικά και να παράσχουν την κατάλληλη υποδομή στις Αρχές για να εκτελούν τα καθήκοντα τους.

Σίγουρα οι συγκεκριμένες εγγυήσεις κρίνονται επαρκείς, ιδίως συνερμηνεύομενες με το ασυμβίβαστο των μελών των εποπτικών αρχών. Προκύπτουν ωστόσο τα εξής ζητήματα. Εν πρώτοις, όπως αποδείχθηκε και από το υποκεφάλαιο 5.2 οι περισσότερες εθνικές εποπτικές αρχές έχουν ήδη συσταθεί παλαιότερα με το εσωτερικό δίκαιο που ενσωμάτωσε τις παλαιότερες Οδηγίες. Επομένως, είναι απορίας άξιον πόσο εύκολο είναι να αλλάξει ο τρόπος λειτουργίας εποπτικών αρχών που ήδη λειτουργούν εδώ και πολλά χρόνια με διαφορετικό καθεστώς που προβλεπόταν σε αποκλίνοντες εθνικούς νόμους μεταξύ των κρατών μελών. Και δευτερευόντως προκύπτει το ζήτημα του πώς μπορούν να ελεγχθούν οι εθνικές κυβερνήσεις όσον αφορά τις υποχρεώσεις τους έναντι των εποπτικών αρχών (δηλαδή το σεβασμό των προαναφερθέντων εγγυήσεων, την επαρκή οικονομική ενίσχυση τους κτλ.). Εξάλλου, η οικονομική ενίσχυση και οι παροχές των εθνικών κρατών προς τις ανεξάρτητες αρχές εξαρτάται από την οικονομική τους δυνατότητα και από την ουσιαστική τους εκτίμηση. Επομένως να συγκεκριμένα ζητήματα δεν μπορούν να ελεγχθούν. Πάντως, η σύσταση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων είναι ιδιαιτέρως σημαντική.

Κεφάλαιο 6: Υποθέσεις Εκμετάλλευσης Προσωπικών Δεδομένων

Στο συγκεκριμένο κεφάλαιο επιδιώκεται αρχικώς να διερευνηθεί η έννοια της στοχευμένης διαφήμισης, καθώς και να εξεταστούν συγκεκριμένες υποθέσεις εκμετάλλευσης προσωπικών δεδομένων που απασχόλησαν την επικαιρότητα. Ειδικότερα, στο πρώτο υποκεφάλαιο αναλύεται η στοχευμένη διαφήμιση, στο δεύτερο υποκεφάλαιο εξετάζεται η υπόθεση «διάρρευσης» προσωπικών δεδομένων Facebook-Cambrige Analytica, ενώ στο τρίτο υποκεφάλαιο παρουσιάζεται η υπόθεση διάρρευσης προσωπικών δεδομένων από την Google+.

6.1: Στοχευμένη Διαφήμιση

Η στοχευμένη διαφήμιση αποτελεί μία μορφή διαδικτυακής διαφήμισης η οποία στοχεύει σε συγκεκριμένο αποδέκτη, με συγκεκριμένα προσωπικά χαρακτηριστικά ανάλογα με το προϊόν η το πρόσωπο που η διαφήμιση προβάλλει[118]. Αυτά τα χαρακτηριστικά μπορούν να είναι είτε δημογραφικά που να βασίζονται στη φυλή, στην οικονομική επιφάνεια, στο φύλο, στην ηλικία, στο μορφωτικό επίπεδο και στο επάγγελμα, είτε ψυχογραφικά και να βασίζονται στις αξίες, στην προσωπικότητα, στη νοοτροπία, στις απόψεις και στα ενδιαφέροντα του καταναλωτή[119].

Το «προσωποποιημένο, one-to-one μάρκετινγκ» έχει τη δυνατότητα να δώσει στον πελάτη την εντύπωση ότι ολόκληρη η επιχείρηση είναι προσαρμοσμένη στις προσωπικές του ανάγκες και προτιμήσεις, ως εκ τούτου τα στοιχεία που μόλις προαναφέραμε αποδεικνύονται χρυσοφόρα. Είναι προφανές ότι η αποτελεσματικότητα στην προσέγγιση του πελάτη στην περίπτωση της στοχευμένης διαφήμισης είναι ευθέως ανάλογη με γνώσεις σχετικές με τις ατομικές ανάγκες, τις συνήθειες και τις προτιμήσεις του καταναλωτή[120].

Επιπροσθέτως, μπορούν να βασίζονται στη γενικότερη συμπεριφορά-δραστηριότητα του καταναλωτή, δηλαδή στο ιστορικό περιήγησης στο διαδίκτυο ή στις διαδικτυακές αγορές. Βάσει λοιπόν της λειτουργίας της στοχευμένης διαφήμισης, η διαφήμιση ενός προϊόντος θα εμφανιστεί σε χρήστες που βάσει των ανωτέρω στοιχείων κρίνεται ότι ενδέχεται να ενδιαφέρονται περισσότερο για αυτό και όχι σε χρήστες που κρίνεται ότι δεν έχουν κάποιο ενδιαφέρον για αυτό. Είναι προφανές ότι με αυτό τον τρόπο μειώνεται δραστικά το κόστος της διαφήμισης[121]. Λόγω της προαναφερθείσας αποτελεσματικότητας και του χαμηλότερου κόστους, η στοχευμένη διαδικτυακή διαφήμιση αντικαθιστά προοδευτικά τις παραδοσιακές μορφές διαφήμισης στις εφημερίδες, στην τηλεόραση και στο ραδιόφωνο[122].

---

[118] Βλ. J. Plummer & S. Rappaport, «The Online Advertising Playbook: Proven Strategies and Tested Tactics from the Advertising Research Foundation», Εκδ. John Wiley & Sons, 2007, σ. 26

[119] Βλ. B. Jansen & K. Moore, «Evaluating the performance of demographic targeting using gender in sponsored search», *Information Processing & Management* (περιοδικό), τεύχος 49 (1), 2013, σ. 286–302

[120] Βλ. Κ. Δελούκα-Ιγγλέση, ό.π., σ. 271

[121] Βλ. G. Iyer & D. Soberman, «The Targeting of Advertising», *Marketing Science* (περιοδικό), τεύχος 24 (3), 2005, σ. 461–476

[122] Βλ. P. Johnson, «Targeted advertising and advertising avoidance», *The RAND Journal of Economics* (περιοδικό) τεύχος 44 (1), 2013, σ. 128–144

Είναι προφανές ότι για τους σκοπούς της στοχευμένης διαφήμισης απαιτούνται εξ ορισμού «αρχεία» διευθύνσεων πραγματικών και δυνητικών καταναλωτών, καθώς αυτές αποτελούν τη βάση της επικοινωνίας μεταξύ επιχείρησης και πελάτη. Η συλλογή αυτή των διευθύνσεων μπορεί να γίνεται βεβαίως απευθείας από τα άτομα, τα οποία ενδέχεται να συναινούν προς αυτό, μπορεί όμως να γίνεται και εν αγνοία τους, π.χ. από τις ιστοσελίδες κοινωνικής δικτύωσης, τις ομάδες συζητήσεων κ.ά. είτε με τη χρήση διαφόρων τεχνικών «εξόρυξης» που στηρίζονται π.χ. στις επισκέψεις των χρηστών στους διάφορους ιστοχώρους, ή ακόμα και από hacking σε ιδιωτικές βάσεις δεδομένων. Ποτέ άλλοτε η συμπεριφορά και οι συνήθειες των ατόμων δεν καταγράφονταν τόσο συστηματικά, η προσπάθεια να επεκταθεί η χρήση των συγκεντρωνούμενων προσωπικών δεδομένων δεν ήταν πιο επίμονη και η εμπορευματοποίηση των προσωπικών πληροφοριών δυνητικών καταναλωτών τόσο εκτεταμένη, αφού οι πληροφορίες συλλέγονται, μεταφέρονται και «αξιοποιούνται» μέσα σε ελάχιστο χρόνο και με ελάχιστο κόστος[123].

6.1.1: Είδη στοχευμένης διαφήμισης

Οι διαδικτυακές υπηρεσίες δημιουργούν συνεχώς νέες επιχειρηματικές δραστηριότητες και ευκαιρίες αύξησης των εσόδων των εταιρειών που δραστηριοποιούνται στον τομέα του Διαδικτύου. Πιο συγκεκριμένα, οι εταιρείες αναπτύσσουν ταχέως τεχνολογικές δυνατότητες που τους επιτρέπουν να συλλέγουν πληροφορίες σχετικά με τους χρήστες του διαδικτύου. Μέσω της παρακολούθησης των ιστοσελίδων που επισκέπτονται οι χρήστες, οι πάροχοι υπηρεσιών διαδικτύου μπορούν να προβάλουν απευθείας διαφημίσεις που σχετίζονται με τις προτιμήσεις του καταναλωτή. Οι περισσότεροι από τους ιστοτόπους χρησιμοποιούν τεχνολογικά μέσα παρακολούθησης της διαδικτυακής δραστηριότητας των χρηστών[124] τα οποία αναλύονται κατωτέρω.

Μηχανές αναζήτησης

Η μηχανή αναζήτησης της Google αποτελεί σημαντικό μέσο για τη στοχευμένη διαφήμιση, καθώς χρησιμοποιείται για την προσέγγιση του κοινού-στόχου. Ειδικότερα, το επαναληπτικό μάρκετινγκ της Google είναι ένας τύπος στοχευμένης διαφήμισης, όπου οι ιστότοποι χρησιμοποιούν τις διευθύνσεις IP των ηλεκτρονικών υπολογιστών που έχουν επισκεφτεί τους ιστότοπούς τους προκειμένου να επαναφέρει τη διαφήμισή τους στο χρήστη που είχε προηγουμένως επισκεφτεί τον συγκεκριμένο ιστότοπο. Μέσω αυτής της λειτουργίας, οι μηχανές αναζήτησης συμβάλλουν στη βελτίωση της στοχευμένης διαφήμισης, καθώς οι διαφημίσεις μπορούν να συμπεριλάβουν τα προϊόντα ή τις υπηρεσίες για τα οποία οι χρήστες-καταναλωτές έχουν προβάλλει ενδιαφέρον μέσω των διαδικτυακών τους αναζητήσεων.

Το Google Adwords έχει διαφορετικές πλατφόρμες για τον τρόπο προβολής των διαφημίσεων. Ειδικότερα, το Δίκτυο αναζήτησης εμφανίζει τις διαφημίσεις σε άλλους ιστότοπους Google, όπως

---

[123] Βλ. Κ. Δελούκα-Ιγγλέση, ό.π., σ. 271

[124] Βλ. C. Schlee, «Targeted Advertising Technologies in the ICT Space: A Use Case Driven Analysis», *Springer Science & Business Media*, 2013, σ. 14 επ.

στους Χάρτες (Google Maps) και σε εκατοντάδες άλλους ιστότοπους συνεργατών αναζήτησης εκτός της Google, οι οποίοι εμφανίζουν διαφημίσεις του AdWords που ταιριάζουν με τα αποτελέσματα αναζήτησης. Το Δίκτυο εμφάνισης περιλαμβάνει μια συλλογή ιστοτόπων της Google (όπως το Google Finance, το Gmail, το Blogger και το YouTube), τους ιστοτόπους συνεργατών και τις εφαρμογές για κινητά που εμφανίζουν διαφημίσεις του AdWords που ταιριάζουν με το περιεχόμενο μιας συγκεκριμένης σελίδας. Τα είδη των διαφημιστικών δικτύων μπορούν να είναι ιδιαιτέρως επωφελή για τους στόχους των εταιρειών.

Για παράδειγμα, το δίκτυο αναζήτησης μπορεί να ωφελήσει μια εταιρεία που επιδιώκει να προσελκύσει καταναλωτές που αναζητούν ένα συγκεκριμένο προϊόν ή υπηρεσία. Άλλοι τρόποι με τους οποίους μπορούν να στοχεύσουν οι διαφημιστικές καμπάνιες είναι να χρησιμοποιήσουν το ιστορικό αναζήτησης. Επί παραδείγματι, εάν ο χρήστης αναζητήσει στυλό σε μια μηχανή αναζήτησης όπως το Google, οι διαφημίσεις για στυλό θα εμφανιστούν στο πάνω μέρος της ιστοσελίδας.

Η Google χρησιμοποιεί το δίκτυο εμφάνισης για να παρακολουθεί τί βλέπουν οι χρήστες και να συλλέγει πληροφορίες σχετικά με αυτές. Όταν ένας χρήστης μεταβεί σε έναν ιστότοπο που χρησιμοποιεί το δίκτυο εμφάνισης Google, θα στείλει ένα μήνυμα στην Google το οποίο περιλαμβάνει πληροφορίες σχετικά με το χρήστη, όπως αυτά που αναζήτησε, την τοποθεσία του, τη διεύθυνση IP και στη συνέχεια δημιουργείται ένα προφίλ επιτρέποντας στη Google να προωθεί συγκεκριμένες διαφημίσεις στον χρήστη ανάλογα με τις προτιμήσεις του.

Έτσι, εάν ένας χρήστης επισκέπτεται συχνά ιστοτόπους διαφημιστικών εταιρειών, οι οποίες πωλούν διαφημιστικά στυλό, η Google θα συλλέξει δεδομένα του χρήστη, όπως η ηλικία, το φύλο, την τοποθεσία και άλλες δημογραφικές πληροφορίες, καθώς και πληροφορίες σχετικά με τους ιστοτόπους που επισκέφθηκαν. Στη συνέχεια, η Google προβάλλει διαφημίσεις σε ιστοτόπους που σχετίζονται με τη συγκεκριμένη κατηγορία διαφημιστικών προϊόντων[125]. Αυτοί οι τύποι διαφημίσεων καλούνται επίσης διαφημίσεις συμπεριφοράς, καθώς παρακολουθούν τη «διαδικτυακή» συμπεριφορά του χρήστη στον ιστότοπο και εμφανίζουν διαφημίσεις βάσει προηγούμενων σελίδων ή όρων αναζήτησης του.

Στόχευση Μέσων Κοινωνικής Δικτύωσης

Τα δίκτυα κοινωνικής δικτύωσης δεν συνιστούν απλώς ένα κανάλι επικοινωνίας αλλά και ένα εξόχως εύφορο πεδίο διαφήμισης. Η στοχευμένη διαφήμιση τροφοδοτείται καθοριστικά και από το γεγονός ότι οι χρήστες, δημοσιεύοντας το «προφίλ» τους, κοινοποιούν σημαντικές πληροφορίες για τα ενδιαφέροντά τους, τα hobbies τους, οι προτιμήσεις που εκφράζονται σε διαδικτυακό περιεχόμενο με το πάτημα του πλήκτρου «Μου αρέσει!» στον ιστοχώρο κοινωνικής δικτύωσης facebook, κ.ο.κ. Το πλήθος των πληροφοριών αυτών, σε συνδυασμό με τις τεράστιες δυνατότητες διαδραστικότητας

[125] Βλ. J. Thomas, «Programming, filtering, adblocking: advertising and media automation», *Media International Australia* (περιοδικά), τεύχος 166 (1), 2017, σ. 34–43

και διάδοσης του διαφημιστικού μηνύματος, χρησιμοποιούνται ως εκ τούτου ευρύτατα από τις πάσης φύσεως επιχειρήσεις για διαφημιστικούς σκοπούς[126].

Στο σημείο αυτό θα πρέπει να επισημάνουμε ότι οι ιστότοποι κοινωνικής δικτύωσης προσφέρουν υπηρεσίες δικτύωσης δωρεάν στους χρήστες, ενόσω η βασική πηγή εσόδων τους δεν είναι άλλη από τις διαφημιστικές καταχωρήσεις. Άρα, ας μην εξαπατώμεθα: τίποτε δεν είναι δωρεάν στο Διαδίκτυο. Το νόμισμα με το οποίο πληρώνουν οι χρήστες, πολλές φορές μάλιστα χωρίς καν να το γνωρίζουν, είναι «τα προσωπικά τους δεδομένα»[127].

Η στόχευση των μέσων κοινωνικής δικτύωσης είναι μια μορφή στοχεύμενης διαφήμισης, η οποία χρησιμοποιεί γενικά χαρακτηριστικά στόχευσης όπως η γεωγραφική θέση, η διαδικτυακή συμπεριφορά και η κοινωνικο-ψυχογραφική στόχευση και συγκεντρώνει πληροφορίες που έχουν δώσει οι καταναλωτές σε κάθε πλατφόρμα μέσων κοινωνικής δικτύωσης. Διερευνώντας το ιστορικό των χρηστών στα μέσα κοινωνικής δικτύωσης, χρήστες που έχουν εκδηλώσει ενδιαφέρον για συγκεκριμένα αντικείμενα θα τους εμφανιστεί αυτόματα η διαφήμιση ορισμένων προϊόντων ή υπηρεσιών.

Για παράδειγμα στο Facebook, εάν ένας χρήστης έχει κάνει like σε σελίδες ένδυσης, θα λαμβάνει διαφημίσεις βάσει αυτών των σελίδων και της τοποθεσίας τους. Αυτό επιτρέπει στις διαφημιζόμενες ετερείες να στοχεύουν σε πολύ συγκεκριμένους καταναλωτές βάσει της τοποθεσίας τους και των ενδιαφερόντων τους. Τα μέσα κοινωνικής δικτύωσης δημιουργούν αυτοματοποιημένα προφίλ του καταναλωτή βάσει των προτιμήσεων του.

Επί παραδείγματι, το Facebook επιτρέπει στις διαφημιζόμενες εταιρείες να «στοχεύουν» χρησιμοποιώντας ευρεία χαρακτηριστικά όπως το φύλο, η ηλικία και η τοποθεσία. Επιπλέον, επιτρέπουν πιο περιορισμένη στόχευση με βάση τα δημογραφικά στοιχεία, τη «διαδικτυακή» συμπεριφορά και τα ενδιαφέροντα[128].

Η διαφήμιση προσλήψεων του Facebook προσφέρει ευρύτερη και οικονομικά αποδοτικότερη έρευνα σε σχέση με τη διαφήμιση στις εφημερίδες. Για παράδειγμα, η στρατολόγηση χρηστών για συμμετοχή σε έρευνα σχετικά με τους καπνιστές πραγματοποιήθηκε από τις Ηνωμένες Πολιτείες το 2015. Η εταιρεία «εντόπισε» τους καπνιστές μέσω των διαδικτυακών τους προφίλ, όπως η τοποθεσία και η ηλικία. Έτσι συγκέντρωσε 56.621 συμμετέχοντες για την έρευνα.

Το 1,97% των χρηστών έκανε κλικ στη διαφήμιση με κόστος 1,51 δολλάρια ανά έρευνα, ενώ το 37,7% των συμμετεχόντων ολοκλήρωσε την έρευνα. Επίσης, για τη «στρατολόγηση» των χρηστών χρειάστηκε λιγότερος χρόνος καθώς η εταιρεία είχε ήδη συλλέξει τις πληροφορίες μέσω του

[126] Βλ. Κ. Δελούκα-Ιγγλέση, ό.π., σ. 277

[127] Ibid, σ. 277

[128] Βλ. L. Carter-Harris & S. Rawl, «Beyond Traditional Newspaper Advertisement: Leveraging Facebook-Targeted Advertisement to Recruit Long-Term Smokers for Research», *Journal of Medical Internet Research*, τεύχος 18 (6), 2016, σ. 117

Facebook. Στον αντίποδα, η εφημερίδα «στρατολόγησε» 30 συμμετέχοντες σε διαφήμιση 3 ημερών, αλλά μόνο 10 από τους 30 συμμετέχοντες ολοκλήρωσαν την έρευνα. Το κόστος για την στρατολόγηση ήταν 40,80 δολλάρια ανά μία ολοκληρωμένη έρευνα. Επίσης, η διαφήμιση της εφημερίδας χρειαζόταν να ζητήσει το όνομα, την ηλικία και το επάγγελμα των ανθρώπων μέσω επιπρόσθετων ερευνών, οι οποίες δεν απαιτούνταν στην έρευνα μέσω του Facebook. Αντίστοιχα, η διαφήμιση στο Facebook είχει πολύ χαμηλότερο κόστος και σαφώς ήταν λιγότερο χρονοβόρα[129].

Κινητές συσκευές

Ήδη από τις αρχές της δεκαετίας του 2000, η διαφήμιση ήταν διαδεδομένη στα κινητά τηλέφωνα. Η συγκεκριμένη μορφή στοχευμένης διαφήμισης βασίζεται σε κινητές συσκευές και παρέχει περισσότερες πληροφορίες σχετικά με τον καταναλωτή, όχι μόνο για τα ενδιαφέροντά τους, αλλά και για τις πληροφορίες σχετικά με την τοποθεσία και τον χρόνο τους. Αυτό επιτρέπει στους διαφημιζόμενους να παράγουν διαφημίσεις που θα μπορούσαν να ικανοποιήσουν το πρόγραμμά τους σε ένα διαρκώς μεταβαλλόμενο περιβάλλον.

Τεχνική στόχευση

Η τεχνική στόχευση σχετίζεται με την κατάσταση του λογισμικού του χρήστη. Η διαφήμιση δηλαδή μεταβάλλεται ανάλογα με το διαθέσιμο εύρος ζώνης του χρήστη. Επί παραδείγματι αν ο χρήστης βρίσκεται στο κινητό τηλέφωνο που έχει περιορισμένη σύνδεση, το σύστημα παράδοσης διαφημίσεων θα εμφανίσει μια έκδοση της διαφήμισης μικρότερη για την ταχύτερη μεταφορά δεδομένων.

Τα διευθυντικά διαφημιστικά συστήματα προβάλλουν διαφημίσεις απευθείας βάσει δημογραφικών, ψυχογραφικών ή συμπεριφορικών χαρακτηριστικών που σχετίζονται με τους καταναλωτές που εκτίθενται στη διαφήμιση. Αυτά τα συστήματα είναι πάντοτε ψηφιακά και πρέπει να εξυπηρετεί τη διαφήμιση (αποκωδικοποιητής, δικτυακός τόπος ή ψηφιακό σήμα) και πρέπει να είναι ικανό να προβάλει μια διαφήμιση ανεξάρτητα από οποιαδήποτε άλλα τελικά σημεία βάσει ειδικών χαρακτηριστικών του καταναλωτή κατά τη στιγμή της προβολής της διαφήμισης. Επομένως, τα διευθυντικά διαφημιστικά συστήματα χρησιμοποιούν τα γνωρίσματα των καταναλωτών που συνδέονται με τα τελικά σημεία ως βάση για την επιλογή και την προβολή διαφημίσεων[130].

Γεωγραφική στόχευση

[129] Βλ. L. Carter-Harris & S. Rawl, όπ. π., σ. 123

[130] Βλ. D. Taylor & D. Strutton, «Friends, fans, and followers: do ads work on social networks?», *Journal of Advertising Research*, τεύχος 51 (1), 2011, σ. 258–275

Αυτός ο τύπος διαφήμισης περιλαμβάνει τη στόχευση διαφόρων χρηστών με βάση τη γεωγραφική τους θέση. Οι διευθύνσεις IP μπορούν να αποκαλύπτουν την τοποθεσία ενός χρήστη και συνήθως μπορούν να μεταφέρουν την τοποθεσία μέσω ταχυδρομικών κωδικών[131]. Οι τοποθεσίες αποθηκεύονται στη συνέχεια σε στατικά προφίλ και έτσι οι διαφημιζόμενες εταιρείες μπορούν εύκολα να στοχεύσουν αυτά τα άτομα με βάση τη γεωγραφική τους θέση. Μια υπηρεσία βάσει τοποθεσίας (LBS) είναι μια υπηρεσία κινητής πληροφορίας που επιτρέπει την χωρική και χρονική μετάδοση δεδομένων και μπορεί να χρησιμοποιηθεί προς όφελος της διαφημιζόμενης εταιρείας[132]. Αυτά τα δεδομένα μπορούν να αξιοποιηθούν από εφαρμογές στη συσκευή που επιτρέπουν την πρόσβαση στις πληροφορίες τοποθεσίας[133]. Αυτός ο τύπος στοχευμένης διαφήμισης επικεντρώνεται στο στοιχείο της τοποθεσίας ο οποίος για παράδειγμα δηλώνεται όταν ένας χρήστης κάνει check in σε μέρη για φαγητό, κοντινά καταστήματα κλπ. Όπως είναι προσφανές η συγκεκριμένη μορφή στοχευμένης διαφήμισης μπορεί να δημιουργήσει προβλήματα με το απόρρητο του χρήστη[134].

Στόχευση συμπεριφοράς

Η στόχευση της συμπεριφοράς επικεντρώνεται γύρω από τη δραστηριότητα και τις ενέργειες των χρηστών στο διαδίκτυο[135]. Οι πληροφορίες από ιστοσελίδες περιήγησης μπορούν να συλλεχθούν από την επεξεργασία δεδομένων, η οποία βρίσκει μοτίβα στο ιστορικό αναζήτησης χρηστών. Οι διαφημιζόμενες εταρείες που χρησιμοποιούν αυτή τη μέθοδο πιστεύουν ότι παράγει διαφημίσεις που θα είναι πιο σχετικές με τα ενδιαφέροντα των χρηστών, οδηγώντας έτσι τους καταναλωτές να επηρεάζονται περισσότερο από αυτές[136]. Έτσι αν ένας καταναλωτής αναζητούσε συχνά τιμές αεροπορικών εισιτηρίων, το σύστημα στόχευσης θα άρχιζε να εμφανίζει σχετικές διαφημίσεις σε μη σχετιζόμενους ιστοτόπους, όπως για παράδειγμα στο Facebook. Το πλεονέκτημά του συστήματος είναι ότι μπορεί να στοχεύει τα συμφέροντα του χρήστη, αντί να στοχεύει σε ομάδες ανθρώπων των οποίων τα συμφέροντα μπορεί να ποικίλουν.

---

[131] Βλ. C. Schlee, «Targeted Advertising Technologies in the ICT Space: A Use Case Driven Analysis», Springer Science & Business Media, 2013

[132] Βλ. S. Dhar & U. Varshney, «Challenges and business models for mobile location-based services and advertising», *Communications of the ACM*, τεύχος 54 (5), 2011, σ. 121–128

[133] Βλ. L. Peterson & R. Groot, «Location-Based Advertising: The Key to Unlocking the Most Value in the Mobile Advertising and Location-Based Services Markets», 2009

[134] Βλ. K. Li, «Building a targeted mobile advertising system for location-based services», Decision Support Systems, 2012, σ. 1–8

[135] Βλ. J. Krumm, «Ubiquitous advertising: The killer application for the 21st century», IEEE Pervasive Computing, 2010, σ. 66–73

[136] Βλ. J. Yan & Z. Chen, «How much can behavioral targeting help online advertising?», σε: *Proceedings of the 18th international conference on World Wide Web*, 2009, σ. 261–270

Όταν κάποιος χρήστης επισκέπτεται έναν ιστότοπο, οι σελίδες που επισκέπτεται, ο χρόνος που βλέπει κάθε σελίδα, οι αναζητήσεις που πραγματοποιούν και τα πράγματα με τα οποία αλληλεπιδρούν επιτρέπουν στους ιστοτόπους να συλλέγουν αυτά τα δεδομένα και να δημιουργούν ένα «προφίλ» που να συνδέεται με το πρόγραμμα περιήγησης αυτού του χρήστη. Ως αποτέλεσμα, οι διαφημιζόμενες εταιρείες μπορούν να χρησιμοποιήσουν αυτά τα δεδομένα για να δημιουργήσουν και να προσελκύσουν χρήστες που έχουν παρόμοια προφίλ.

Όταν οι επισκέπτες επιστρέφουν σε έναν συγκεκριμένο ιστότοπο ή σε ένα δίκτυο ιστοτόπων, αυτά τα προφίλ μπορούν να χρησιμοποιηθούν για να επιτρέψουν στους διαφημιζόμενους να τοποθετήσουν τις διαφημίσεις και τα μηνύματά τους στο διαδίκτυο μπροστά σε αυτούς τους χρήστες που παρουσιάζουν μεγαλύτερο ενδιαφέρον και επιθυμία για τα προϊόντα και τις υπηρεσίες που διαφημίζονται. Για τους ανωτέρω λόγους η στοχευμένη συμπεριφορά έχει αναδειχθεί ως μία από τις κύριες τεχνολογίες που χρησιμοποιούνται για την αύξηση της αποδοτικότητας και των κερδών του ψηφιακού μάρκετινγκ και των διαφημίσεων, καθώς οι πάροχοι πολυμέσων είναι σε θέση να εμφανίζουν σε χρήστες πολύ σχετικές διαφημίσεις. Σχετικά με τη θεωρία ότι κατάλληλα στοχευμένες διαφημίσεις και μηνύματα θα προσελκύσουν μεγαλύτερο ενδιαφέρον για τους καταναλωτές, οι εκδότες μπορούν να χρεώνουν ένα ασφάλιστρο για διαφημίσεις με στοχοθετημένες συμπεριφορές και οι έμποροι μπορούν να επιτύχουν. Το μάρκετινγκ συμπεριφοράς μπορεί να χρησιμοποιηθεί μόνο του ή σε συνδυασμό με άλλες μορφές στόχευσης. Πολλοί επαγγελματίες ορίζουν τη διαδικασία αυτή και ως «στόχευση κοινού».

Δίκτυο

Τα διαφημιστικά δίκτυα χρησιμοποιούν τη στοχευμένη συμπεριφορά με διαφορετικό τρόπο από τους μεμονωμένους ιστοτόπους. Ειδικότερα, δεδομένου ότι εξυπηρετούν πολλές διαφημίσεις σε πολλούς διαφορετικούς ιστοτόπους, είναι σε θέση να δημιουργήσουν μια εικόνα για την πιθανή δημογραφική σύνθεση των χρηστών του διαδικτύου. Τα δεδομένα από μια επίσκεψη σε έναν ιστότοπο μπορούν να σταλούν σε πολλές διαφορετικές εταιρείες, συμπεριλαμβανομένων των θυγατρικών της Microsoft και της Google, του Facebook, του Yahoo, πολλών ιστότοπων καταγραφής επισκεψιμότητας και μικρότερων εταιρειών διαφημίσεων.

Αυτά τα δεδομένα μπορούν μερικές φορές να αποστέλλονται σε περισσότερους από 100 ιστοτόπους και να μοιράζονται σε επιχειρηματικούς εταίρους, διαφημιζόμενους και άλλα τρίτα μέρη για επιχειρηματικούς σκοπούς. Τα δεδομένα συλλέγονται με τη χρήση cookies, web beacons και παρόμοιων τεχνολογιών ή και λογισμικού προβολής διαφημίσεων, για την αυτόματη συλλογή πληροφοριών σχετικά με τους χρήστες του ιστοτόπου και τη δραστηριότητα του χρήστη. Ορισμένοι διακομιστές καταγράφουν ακόμη και τη σελίδα που παραπέμπουν τους χρήστες, τους ιστοτόπους που επισκέπτονται μετά από αυτές, τις διαφημίσεις που βλέπουν και τις διαφημίσεις στις οποίες κάνουν κλικ.

Αυτά τα δεδομένα συλλέγονται χωρίς να επισυνάπτονται τα ονόματα, η διεύθυνση, η διεύθυνση ηλεκτρονικού ταχυδρομείου ή ο αριθμός τηλεφώνου, αλλά μπορεί να περιλαμβάνει πληροφορίες

αναγνώρισης συσκευών όπως η διεύθυνση IP, η διεύθυνση MAC, το cookie ή άλλο μοναδικό αλφαριθμητικό αναγνωριστικό συγκεκριμένης συσκευής του υπολογιστή, μπορεί να δημιουργήσει αναγνωριστικά επισκεπτών για να προχωρήσει μαζί με τα δεδομένα. Τα cookie χρησιμοποιούνται για τον έλεγχο των εμφανιζόμενων διαφημίσεων και για την παρακολούθηση της δραστηριότητας περιήγησης και των μοτίβων χρήσης σε ιστοτόπους. Αυτά τα δεδομένα χρησιμοποιούνται από τις εταιρείες για να συναγάγουν την ηλικία, το φύλο και τα ενδεχόμενα ενδιαφέροντα των αγορών, έτσι ώστε να μπορούν να κάνουν προσαρμοσμένες διαφημίσεις στις οποίες θα ήταν πιο πιθανό να επιλεγούν από τους χρήστες.

Επί παραδείγματι ένας χρήστης που εισέρχεται σε ιστότοπους ποδοσφαίρου, επιχειρηματικούς ιστότοπους και ιστότοπους μόδας λογικό είναι να υποτεθεί ότι είναι άνδρας. Οι δημογραφικές αναλύσεις των επιμέρους τοποθεσιών που παρέχονται είτε εσωτερικά (έρευνες χρηστών) είτε εξωτερικά (Comscore\netratings) επιτρέπουν στα δίκτυα να επιλέγουν ακροατήρια και όχι ιστότοπους[137]. Παρόλο που τα διαφημιστικά δίκτυα χρησιμοποιήθηκαν για την πώληση αυτού του προϊόντος, αυτό βασίστηκε στην επιλογή των ιστοτόπων όπου υπήρχαν τα ακροατήρια.

6.1.2: Προστασία προσωπικών δεδομένων

Με βάση όσα αναφέρθηκαν δεν μπορεί να χωρέσει ασφαλώς καμία αμφιβολία ότι με τις αυξημένες δυνατότητες που προσφέρονται για την επεξεργασία και αξιοποίηση προσωπικών δεδομένων από την ανάπτυξη των νέων τεχνολογιών, απειλείται σοβαρά η ιδιωτικότητα και ο πληροφοριακός αυτοπροσδιορισμός των ατόμων, τόσο ως πολιτών μιας δημοκρατικά οργανωμένης Πολιτείας όσο και υπό την ιδιότητά τους ως καταναλωτών. Στο περιβάλλον του διαδικτύου κάθε πτυχή της ιδιωτικής ζωής των ατόμων γίνεται εξαιρετικά εύκολα προσπελάσιμη από οποιονδήποτε ενδιαφερόμενο και είναι διαθέσιμη για κάθε χρήση και επεξεργασία, επιτρέποντας την παραγωγή μιας ανάγλυφης εικόνας κάθε ατόμου[138].

Ετσι, πολλοί χρήστες του διαδικτύου και ομάδες υπεράσπισης ανησυχούν για θέματα ιδιωτικότητας σχετικά με αυτό το είδος στόχευσης. Αυτή είναι μια διαμάχη που η βιομηχανία στόχευσης συμπεριφοράς προσπαθεί να περιορίσει μέσω της εκπαίδευσης, της υπεράσπισης και των περιορισμών των προϊόντων, προκειμένου να διατηρήσει όλες τις πληροφορίες ή να λάβει άδεια από τους τελικούς χρήστες. Χαρακτηριστικό παράδειγμα αποτελεί η δημιουργία κινουμένων σχεδίων AOL το 2008 για να εξηγήσει στους χρήστες ότι οι προηγούμενες ενέργειές τους μπορεί να καθορίσουν το περιεχόμενο των διαφημίσεων που βλέπουν μελλοντικά[139].

Οι Καναδοί ακαδημαϊκοί στο Πανεπιστήμιο της Οτάβα Καναδικής Πολιτικής Διαδικτύου και Κλινικής Δημοσίου Ενδιαφέροντος ζήτησαν πρόσφατα από τον ομοσπονδιακό Επίτροπο για την προστασία της ιδιωτικής ζωής να διερευνήσει τη διαδικτυακή προβολή των χρηστών του Διαδικτύου για στοχευμένη διαφήμιση.

---

[137] Βλ. R. Singel, «Online Tracking Firm Settles Suit Over Undeletable Cookies», Wired, 2010

[138] Βλ. Κ. Δελούκα-Ιγγλέση, ό.π., σ. 284

[139] Βλ. L. Story, «AOL Brings Out the Penguins to Explain Ad Targeting», *The New York Times*, 2008

Η Ευρωπαϊκή Επιτροπή έχει επίσης εκφράσει ορισμένες ανησυχίες σχετικά με τη συλλογή δεδομένων σε απευθείας σύνδεση (προσωπικά δεδομένα), τη διαμόρφωση προφίλ και τη στοχευμένη συμπεριφορά και επιδιώκει την επιβολή των υφιστάμενων κανονισμών.

Τον Οκτώβριο του 2009 αναφέρθηκε ότι πρόσφατη έρευνα που πραγματοποιήθηκε από το Πανεπιστήμιο της Πενσυλβανίας και το Κέντρο Δικαιοσύνης και Τεχνολογίας του Μπέρκλεϊ διαπίστωσε ότι η μεγάλη πλειοψηφία των χρηστών του διαδικτύου των ΗΠΑ απέρριψε τη χρήση της συμπεριφοριστικής διαφήμισης[140]. Αρκετές ερευνητικές προσπάθειες από ακαδημαϊκούς έδειξαν ότι δεδομένα που υποτίθεται ότι είναι ανώνυμα μπορούν να χρησιμοποιηθούν για τον εντοπισμό πραγματικών ατόμων[141].

Τον Δεκέμβριο του 2010, η εταιρεία Quantcast συμφώνησε να πληρώσει 2,4 εκατομμύρια δολάρια για τον διακανονισμό μιας αγωγής για τη χρήση των cookies που αφορούσε την παρακολούθηση των καταναλωτών. Η συγκεκριμένη κατηγορία cookies, τα οποία βρίσκονταν σε συνεργαζόμενους ιστότοπους, όπως το MTV, το Hulu και το ESPN, εξακολουθούσαν να παρακολουθούν τον χρήστη ακόμη και αν είχε διαγραφεί.

Άλλες χρήσεις μιας τέτοιας τεχνολογίας περιλαμβάνουν το Facebook και τη χρήση του Facebook Beacon για τον εντοπισμό των χρηστών στο διαδίκτυο, για πιο στοχευμένη διαφήμιση[142]. Οι μηχανισμοί εντοπισμού χωρίς τη συγκατάθεση των καταναλωτών γενικεύονται. Ωστόσο, η παρακολούθηση της συμπεριφοράς των καταναλωτών στο διαδίκτυο ή στις κινητές συσκευές είναι το κλειδί για την ψηφιακή διαφήμιση, η οποία είναι η οικονομική «ραχοκοκαλιά» του μεγαλύτερου μέρους του Διαδικτύου.

Τον Μάρτιο του 2011 αναφέρθηκε ότι η βιομηχανία διαφημίσεων μέσω διαδικτύου θα αρχίσει να συνεργάζεται με το Συμβούλιο Γραφείων Επιχειρήσεων για να ξεκινήσει την «αστυνόμευση» ως μέρος του προγράμματός της για την παρακολούθηση και τη ρύθμιση του τρόπου με τον οποίο οι εμπορικές εταιρείες παρακολουθούν τους καταναλωτές στο διαδίκτυο.

Η στοχευμένη διαφήμιση έχει προκαλέσει αντιπαραθέσεις, ιδιαίτερα όσον αφορά τα δικαιώματα και τις πολιτικές απορρήτου. Με τη στοχοθέτηση της συμπεριφοράς, η οποία εστιάζεται σε συγκεκριμένες ενέργειες των χρηστών, όπως το ιστορικό ιστότοπου, το ιστορικό περιήγησης και η συμπεριφορά αγοράς, αυτό δημιουργεί ανησυχίες στους χρήστες ότι όλη η δραστηριότητα τους παρακολουθείται.

---

[140] Βλ. «US web users reject behavioral advertising, study finds», Διαθέσιμο σε: https://www.pinsentmasons.com/out-law/news/us-web-users-reject-behavioural-advertising-study-finds

[141] Βλ. Z. Zorz, «Is it possible for data to be both anonymous and useful?», Help Net Security, 2009

[142] Βλ. B. Kendall, «Facebook's Settlement on 'Beacon' Service Survives Challenge», *Wall Street Journal*, 2015

Μια έρευνα που διεξήχθη στις Ηνωμένες Πολιτείες[143] από το Pew Internet & American Life Projectbetween 20 Ιανουαρίου και 19 Φεβρουαρίου 2012 αποκάλυψε ότι οι περισσότεροι Αμερικανοί δεν τάσσονται υπέρ της στοχευμένης διαφήμισης, θεωρώντας την ως «εισβολή» στην ιδιωτικότητα. Πράγματι, το 68% των ερωτηθέντων δήλωσε ότι δεν συμφωνεί με τη στοχευμένη διαφήμιση επειδή δεν τους αρέσει να παρακολουθούνται και να αναλύεται η ηλεκτρονική τους συμπεριφορά.

Ένα άλλο ζήτημα είναι η έλλειψη «νέων» διαφημίσεων αγαθών ή υπηρεσιών. Δεδομένου ότι όλες οι διαφημίσεις είναι προσαρμοσμένες ώστε να βασίζονται στις προτιμήσεις των χρηστών, δεν θα εισαχθούν διαφορετικά προϊόντα στον καταναλωτή. Ως εκ τούτου, στην περίπτωση αυτή ο καταναλωτής δεν εκτίθενται σε κάτι νέο.

Οι διαφημιζόμενες εταιρείες συγκεντρώνουν τους πόρους τους στον καταναλωτή, κάτι που μπορεί να αποδειχθεί πολύ αποτελεσματικό[144]. Οι καταναλωτές μπορούν να έχουν ανησυχίες σχετικά με διαφημίσεις που στοχεύουν σε αυτές, οι οποίες είναι κατά βάση πολύ προσωπικές για άνεση, αισθάνεται την ανάγκη ελέγχου των δικών τους δεδομένων[145].

Η προστασία της ιδιωτικής ζωής είναι ένα περίπλοκο ζήτημα λόγω του είδους των προστατευόμενων πληροφοριών για τους χρήστες και του αριθμού των ενδιαφερομένων μερών. Τα τρία κύρια μέρη που συμμετέχουν στην ηλεκτρονική διαφήμιση είναι ο διαφημιζόμενος, ο χρήστης και το δίκτυο.

6.2: Η υπόθεση Facebook-Cambrige Analytica

Το σκάνδαλο δεδομένων Facebook-Cambridge Analytica είναι ένα μεγάλο πολιτικό σκάνδαλο στις που έλαβε χώρα στις αρχές του 2018, όταν αποκαλύφθηκε ότι η Cambridge Analytica[146] είχε συλλέξει τα προσωπικά δεδομένα εκατομμυρίων ατόμων από τα προφίλ του Facebook χωρίς τη συγκατάθεσή τους και τα χρησιμοποίησε για σκοπούς πολιτικής χειραγώγησης. Έχει χαρακτηριστεί ως μία κρίσιμη καμπή για την κατανόηση της αξίας των προσωπικών δεδομένων και οδήγησε στην τεράστια πτώση

[143] Είναι αξιοσημείωτο ότι στις ΗΠΑ δεν υπάρχει κάποιος ομοσπονδιακός νόμος που να ρυθμίζει το ζήτημα της επεξεργασίας και χρήσης των προσωπικών δεδομένων. Ωστόσο, υπάρχει πληθώρα νομοθετικών κειμένων, ομοσπονδιακών αλλά και πολιτειακών, που περιλαμβάνουν ρυθμίσεις αφορώσες στην προστασία των προσωπικών δεδομένων. Ετσι, διάφορες κυβερνητικές αρχές έχουν αναπτύξει την έννοια των best practices οι οποίες, αν και δεν αποτελούν παραδοσιακό δίκαιο, προσομοιάζουν στην ευρωπαϊκή έννοια της εναρμόνισης.

[144] Βλ. A. Goldfarb & C. Tucker, («Online advertising, behavioral targeting, and privacy», Communications of the ACM, τεύχος 5 (5), 2011, σ. 25–27

[145] Βλ. C. Tucker, «Social networks, personalized advertising, and privacy controls», *Journal of Marketing Research*, τεύχος 51 (5), 2014, σ. 546–562

[146] Η Cambrige Analytica είναι πολιτική συμβουλευτική εταιρεία που κατά τη διάρκεια των προεκλογικών αγώνων μετέρχεται μεθόδους παραβίασης, διαβίβασης και ανάλυσης προσωπικών δεδομένων μέσω του διαδικτύου.

της τιμής των μετοχών του Facebook, καθιστώντας αναγκαία την αυστηρότερη ρύθμιση της χρήσης των δεδομένων από τις εταιρείες τεχνολογίας.

Η παράνομη συγκομιδή δεδομένων προσωπικού χαρακτήρα από την Cambridge Analytica αναφέρθηκε για πρώτη φορά τον Δεκέμβριο του 2015 από τον Χάρι Νταβιέ, δημοσιογράφο της Guardian. Πιο συγκεκριμένα, ο δημοσιογράφος κατήγγειλε ότι η Cambridge Analytica εργαζόταν για λογαριασμό του γερουσιαστή των Ηνωμένων Πολιτειών Ted Cruz, χρησιμοποιώντας δεδομένα που συλλέχθησαν από λογαριασμούς του Facebook εκατομμυρίων ανθρώπων χωρίς τη συγκατάθεσή τους.

Το Facebook αρνήθηκε να σχολιάσει την καταγγελία, σχολιάζοντας απλώς ότι το διερευνούσε. Περαιτέρω αναφορές κατέθεσαν η Hanse Grasseger και ο Mikael Krogerus τον Δεκέμβριο 2016, η Carole Cadwalla στην Guardian το Φεβρουάριο του 2017 και ο Mattathias Schwartz στο Intercept το Μάρτιος 2017. Το Facebook αρνήθηκε να σχολιάσει τις συγκεκριμένες καταγγελίες.

Το σκάνδαλο τελικά ξέσπασε τον Μάρτιο του 2018 με την εμφάνιση ενός καταγγελλόμενου, πρώην υπαλλήλου της Cambridge Analytica, Κρίστοφερ Ουίλι. Κατ' ουσίαν αποτελούσε το πρόσωπο πίσω από ένα άρθρο του 2017 στο The Observer του Cadwalladr, με τίτλο «Η μεγάλη βρετανική ληστεία του Brexit».

Οι τρεις οργανώσεις ειδήσεων που δημοσιεύθηκαν ταυτόχρονα στις 17 Μαρτίου 2018, προκάλεσαν μια τεράστια δημόσια κατακραυγή. Η τιμή της μετοχής του Facebook σημείωσε τεράστια πτώση σε λίγες μόνο ημέρες και οι πολιτικοί στις ΗΠΑ και στο Ηνωμένο Βασίλειο ζήτησαν εξηγήσεις από τον CEO της Facebook Mark Zuckerberg. Το σκάνδαλο τελικά τον οδήγησε να συμφωνήσει να καταθέσει μπροστά στο Κογκρέσο των Ηνωμένων Πολιτειών.

Το σκάνδαλο ήταν σημαντικό για την υποκίνηση δημόσιας συζήτησης αναφορικά με τα δεοντολογικά πρότυπα για τις εταιρείες των μέσων κοινωνικής δικτύωσης, των πολιτικών συμβουλευτικών εταιρειών και των πολιτικών. Οι συνήγοροι των χρηστών ζήτησαν μεγαλύτερη προστασία στα μέσα κοινωνικής δικτύωσης και για το δικαίωμα στην προστασία της ιδιωτικής ζωής, καθώς και περιορισμό της παραπληροφόρησης και της προπαγάνδας.

Ο Aleksandr Kogan, ένας επιστήμονας δεδομένων στο Πανεπιστήμιο του Cambridge, ανέπτυξε μια εφαρμογή που ονομάζεται «This Is Your Digital Life[147]», παρείχε δε τη συγκεκριμένη εφαρμογή στην Cambridge Analytica[148]. Η Cambridge Analytica με τη σειρά της διαμόρφωσε μια ενημερωμένη διαδικασία συναίνεσης για έρευνα στην οποία εκατοντάδες χιλιάδες χρήστες του Facebook θα συμφωνούσαν να ολοκληρώσουν μόνο για ακαδημαϊκή χρήση.

[147] Βλ. A. Hern, «How to check whether Facebook shared your data with Cambridge Analytica», The Guardian, 2018

[148] Βλ. E. Graham-Harrison, «Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach», the Guardian, 2018

Ωστόσο, ο σχεδιασμός του Facebook επέτρεψε σε αυτή την εφαρμογή όχι μόνο να συλλέξει τα προσωπικά στοιχεία των ατόμων που συμφώνησαν να πραγματοποιήσουν την έρευνα, αλλά και τις προσωπικές πληροφορίες όλων των ανθρώπων στο κοινωνικό δίκτυο του Facebook. Με αυτόν τον τρόπο η Cambridge Analytica απέκτησε δεδομένα από εκατομμύρια χρήστες του Facebook.

Οι New York Times ανέφεραν ότι το σύνολο των δεδομένων περιελάμβανε πληροφορίες για 50 εκατομμύρια χρήστες του Facebook[149]. Το Facebook επιβεβαίωσε αργότερα ότι είχε στην πραγματικότητα δεδομένα για έως και 87 εκατομμύρια χρήστες[150], με 70,6 εκατομμύρια από αυτούς να είναι από τις Ηνωμένες Πολιτείες.

Στα πλαίσια των Ηνωμένων Πολιτειών, το Facebook εκτιμά ότι η Καλιφόρνια ήταν το πιο επηρεασμένο κράτος των Η.Π.Α., με 6,7 εκατομμύρια χρήστες, ενώ το Τέξας με 5,6 εκατομμύρια και η Φλόριντα με 4,3 εκατομμύρια. Αντίθετα, η Cambridge Analytica ισχυρίστηκε ότι συνέλεξε μόνο 30 εκατομμύρια προφίλ χρηστών του Facebook[151].

Το Facebook έστειλε ένα μήνυμα στους χρήστες των οποίων τα δεδομένα είχαν υποκλαπεί, αναφέροντας ότι οι πληροφορίες πιθανότατα περιελάμβαναν το δημόσιο προφίλ, τις σελίδες που τους αρέσουν, τα γενέθλια και την τοποθεσία τους[152]. Μερικοί από τους χρήστες της εφαρμογής έδωσαν στην εφαρμογή την άδεια να αποκτήσει πρόσβαση στη ροή ειδήσεων, το χρονοδιάγραμμά της και τα μηνύματά της.

Τα δεδομένα ήταν αρκετά λεπτομερή ώστε η Cambridge Analytica να δημιουργήσει ψυχογραφικά προφίλ των υποκειμένων των δεδομένων. Τα δεδομένα περιελάμβαναν επίσης τις ιδεολογικές θέσεις κάθε ατόμου. Για μια πολιτική εκστρατεία τα δεδομένα ήταν αρκετά λεπτομερή ώστε να δημιουργήσουν ένα προφίλ που πρότεινε το είδος της διαφήμισης που θα ήταν πιο αποτελεσματικό να πείσει ένα συγκεκριμένο άτομο σε μια συγκεκριμένη τοποθεσία για κάποια πολιτική εκδήλωση.

6.2.1: Κατάθεση στο Κογκρέσο

Κατά τη διάρκεια της κατάθεσης του ενώπιον του Κογκρέσου στις 10 Απριλίου 2018, ο Mark Zuckerberg δήλωσε ότι ήταν προσωπικό του λάθος ότι δεν έκανε αρκετά για να αποτρέψει το τη βλάβη του Facebook. Μάλιστα, κατά τη διάρκεια της κατάθεσης, ο Mark Zuckerberg ζήτησε δημοσίως συγγνώμη για την παραβίαση προσωπικών δεδομένων.

---

[149] Βλ. M. Rosenberg, «How Trump Consultants Exploited the Facebook Data of Millions», The New York Times, 2018

[150] Βλ. H. Kozlowska, «The Cambridge Analytica scandal affected 87 million people, Facebook says», Quartz, 2018

[151] Βλ. R. Nieva, «Most Facebook users hit by Cambridge Analytica scandal are Californians», CNET, 2018

[152] Βλ. M. Coulter, «Find out if your Facebook data was shared with Cambridge Analytica», Evening Standard, 2018

Ο Ζούκερμπεργκ δήλωσε ότι το 2013 ο ερευνητής Aleksandr Kogan από το Πανεπιστήμιο του Κέιμπριτζ είχε δημιουργήσει μια εφαρμογή-κουίζ προσωπικότητας, η οποία ελήφθη από 300.000 άτομα. Η εφαρμογή ήταν στη συνέχεια ανακτούσε πληροφορίες από το Facebook, συμπεριλαμβανομένων των φίλων των χρηστών.

Στην πραγματικότητα μόλις το 2015 ο Zuckerberg έμαθε ότι οι πληροφορίες αυτών των χρηστών αποσπάστηκαν από την Cambridge Analytica. Η Cambridge Analytica κλήθηκε στη συνέχεια να αφαιρέσει όλα τα δεδομένα.

6.3: Η υπόθεση διάρρευσης προσωπικών δεδομένων από την Google+

Η δεύτερη υπόθεση διάρρευσης προσωπικών δεδομένων που θα μας απασχολήσει στο παρόν υποκεφάλαιο είναι αυτή από το κοινωνικό δίκτυο της Google+. Πιο συγκεκριμένα, τον Απρίλιο του 2019 το κοινωνικό δίκτυο της Google+ σταμάτησε τη λειτουργία του με απόφαση της μητρικής εταιρείας της Google, Alphabet Inc. Ο επίσημος λόγος που προέβαλε η εταιρεία για το κλείσιμο του δικτύου ήταν η χαμηλή του χρήση, καθώς και οι δυσκολίες διατήρησης ενός πετυχημένου προϊόντος που να ανταποκρίνεται στις προσδοκίες των χρηστών[153].

Είναι πράγματι γεγονός πως η Google+ υπήρξε μία ακόμη αποτυχημένη απόπειρα της εταιρείας να δημιουργήσει ένα κοινωνικό δίκτυο ικανό να ανταγωνιστεί το Facebook, καθώς ελάχιστοι χρήστες χρησιμοποιούσαν το Google+. Ωστόσο ο πραγματικός λόγος για το κλείσιμο της Google+ ήταν το βαρύτατο πλήγμα που είχε δεχθεί η φήμη του λόγω της μεγάλης διαρροής προσωπικών δεδομένων που αφορούσε τους λογαριασμούς πολλών χρηστών (ο αριθμός τους ανήλθε στους 500.000) και που συντελέστηκε τον Μάρτιο του 2018[154].

Το σημαντικότερο ωστόσο στοιχείο είναι ότι η εταιρεία γνωστοποίησε το συγκεκριμένο πρόβλημα έξι μήνες αργότερα επικαλούμενο, ως δικαιολογία για αυτή τη μεγάλη χρονική καθυστέρηση, ότι δεν είχε επαρκείς ενδείξεις για κακόβουλη χρήση των προσωπικών δεδομένων. Ωστόσο, όπως έγινε γνωστό από δημοσίευμα της αμερικανικής εφημερίδας Wall Street General[155] η Google σκόπιμα απέφυγε την αποκάλυψη του προβλήματος στο κοινό νωρίτερα, προκειμένου να αποφύγει τον επακόλουθο αυστηρό ρυθμιστικό έλεγχο που θα της επιβάλλονταν.

---

[153] Βλ. «Τέλος από σήμερα για το Google+ το μέσο κοινωνικής δικτύωσης που ατύχησε», 2/4/2019, news247, Διαθέσιμο σε: https://www.news247.gr/technologia/google-telos-meso-koinonikis-diktyosis-atychise.6708676.amp.html

[154] Βλ. «Η Google διέρρευσε προσωπικά δεδομένα χρηστών της με λογαριασμούς στο Google+», 8/10/2018, Η Καθημερινή, Διαθέσιμο σε: https://www.kathimerini.gr/988767/article/epikairothta/kosmos/h-google-dierreyse-proswpika-dedomena-xrhstwn-ths-me-logariasmoys-sto-google

[155] Βλ. Google to Accelerate Closure of Google+ Social Network After Finding New Software Bug, 10/12/2018, Wall Street General, Διαθέσιμο σε: https://www.google.com/amp/s/www.wsj.com/amp/articles/google-to-accelerate-closure-of-google-social-network-1544465975

Περαιτέρω, στο δημοσίευμα αναφέρθηκε ότι το ελάττωμα της Google+ θα μπορούσε να είχε πάρει μεγαλύτερες διαστάσεις, επιτρέποντας σε 438 εξωτερικές εφαρμογές να αποκτήσουν πρόσβαση σε ονόματα χρηστών, διευθύνσεις ηλεκτρονικού ταχυδρομείου, επαγγέλματα, φύλο και ηλικία χωρίς την άδεια του υποκειμένου. Όπως αποκαλύφθηκε στην πορεία, την περίοδο μεταξύ του 2015-2018 ένα ελάττωμα στο σύστημα ασφαλείας της Google+ επέτρεπε σε εξωτερικούς επεξεργαστές (μέσω bugs) να αποκτούν εύκολα πρόσβαση στα προσωπικά προφίλ των χρηστών του δικτύου[156], αλλά και των διαδικτυακών φίλων τους.

Αξίζει στο σημείο αυτό, για την εναργέστερη κατανόηση της στάσης της Google, να αναφερθεί όσα η ίδια δήλωσε μέσω της ετήσιας αναφοράς της για το 2018, στην οποία μεταξύ άλλων αναφέρθηκε στην ανάγκη για συνεχή προσαρμοστικότητα στους κανονιστικούς ελέγχους που πραγματοποιούνται, όπως επίσης και στις συνεχώς εναλλασσόμενες συμπεριφορές των καταναλωτών προς τα δεδομένα τους, διευκρινίζοντας ότι οι νέες αλλαγές στην ιδιωτικότητα των δεδομένων, οι νέες πολιτικές στην ψηφιακή διαφήμιση και τα bugs του λογισμικού τα οποία προκαλούν διάρρευσης των προσωπικών πληροφοριών των χρηστών μπορούν να βλάψουν την επιχείρηση και τις δραστηριότητες της[157].

Από τα ανωτέρω στοιχεία της υπόθεσης συνάγονται κρίσιμα συμπεράσματα. Εν πρώτοις, αποκαλύπτεται πόσο εύκολο είναι να αποκτηθεί πρόσβαση σε προσωπικά δεδομένα ακόμα και σε εφαρμογές με χαμηλή χρήση, όπου η εφαρμογή επαρκών συστημάτων ασφαλείας είναι αρκετά πιο εύκολη από ότι σε εφαρμογές με μεγαλύτερη χρήση. Δευτερευόντως, αναδεικνύεται η εγκληματική αδιαφορία των εταιρειών κολοσσών για την προστασία των προσωπικών δεδομένων, αλλά και η βασική τους ανησυχία για το κατά πόσο το κανονιστικό πλαίσιο ρύθμισης της επεξεργασίας δεδομένων πλήττει την εμπορική τους δραστηριότητα και τα οικονομικά τους συμφέροντα (Βλ. την ανωτέρω αναφορά της Google).

Και τέλος αποδεικνύει ότι ακόμη και ο Γενικός Κανονισμός αποτέλεσε αντικείμενο καταδολίευσης ήδη πριν καν τεθεί σε εφαρμογή. Και τούτο διότι ο GDPR ετέθη σε ισχύ δύο χρόνια αργότερα προκειμένου να δοθεί επαρκής χρόνος στους επιχειρηματικούς κολοσσούς να προσαρμόσουν κατάλληλα τα σύστημα προστασίας στις προβλέψεις του. Αντ' αυτού όμως όπως είδαμε ανωτέρω η Google+ είχε τη δυνατότητα να αποκρύψει τη διάρρευση των προσωπικών δεδομένων από τους χρήστες και να αποφύγει τις αυστηρές κυρώσεις και ελέγχους που προέβλεπε ο Κανονισμός, προβαίνοντας στις απαιτούμενες αλλαγές μόλις λίγους μήνες πριν τη θέση του σε ισχύ.

---

[156] Βλ. Kate O' Flaherty, 9/10/2018, «Google+ Security Bug -- What Happened, Who Was Impacted And How To Delete Your Account», Forbes, Διαθέσιμο σε: https://www.forbes.com/sites/kateoflahertyuk/2018/10/09/google-plus-breach-what-happened-who-was-impacted-and-how-to-delete-your-account/amp/

[157] Βλ. «Η Google προειδοποιεί πως οι αλλαγές στην ιδιωτικότητα των προσωπικών δεδομένων θα μπορούσαν να αποτελέσουν πλήγμα για την εταιρία», 6/2/2019, ired.gr, Διαθέσιμο σε: https://www.ired.gr/blog/item/7391-i-google-proeidopoiei-pos-oi-allages-stin-idiotikotita-ton-prosopikon-dedomenon-tha-mporousan-na-apotelesoun-pligma-gia-tin-etairia.html

6.4: Παραδείγματα Γνωμοδοτήσεων της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Σε αυτό το υποκεφάλαιο θα επιχειρηθεί η συγκριτική εξέταση γνωμοδοτήσεων[158] της Αρχής Προστασίας Προσωπικών Δεδομένων πριν και μετά τη θέση σε ισχύ του νέου Κανονισμού, προκειμένου να αναδειχθεί κατά πόσο ο GDPR επηρέασε το υφιστάμενο κανονιστικό πλαίσιο προστασίας των προσωπικών δεδομένων.

Η πρώτη γνωμοδότηση της Αρχής που θα εξεταστεί είναι είναι η γνωμοδότηση υπ'αριθμόν 1/2017 στην οποία η Αρχή Προστασίας Προσωπικών Δεδομένων κλήθηκε να γνωμοδοτήσει αναφορικά με τη γνωστοποίηση επεξεργασίας προσωπικών δεδομένων στο πλαίσιο του νέου Ενιαίου Αυτόματου Συστήματος Συλλογής Κομίστρου για τις εταιρείες του Ομίλου ΟΑΣΑ (Ηλεκτρονικό Εισιτήριο). Στην προκειμένη γνωμοδότηση η Αρχή Προστασίας Προσωπικών Δεδομένων αρχικώς διευκρίνισε πως η γνωμοδοτική της αρμοδιότητα δεν περιορίζεται μόνο στην περίπτωση που υπάρχει συγκεκριμένο σχέδιο νόμου, αλλά υπό το πρίσμα του άρθρου 28 της Οδηγίας 95/46/ΕΚ, αλλά ενδείκνυται να αναζητείται η έγκαιρη αναζήτηση της Αρχής ήδη κατά τον προγραμματισμό λήψης ή αναθεώρησης υφιστάμενων κανονιστικών ρυθμίσεων ή διοικητικών μέτρων, καθώς και κατά το σχεδιασμό συγκεκριμένων συστημάτων που ενέχουν επεξεργασία προσωπικών δεδομένων[159].

Εν συνεχεία, η γνωμοδότηση χρησιμοποιεί τους νομικούς ορισμούς των προσωπικών δεδομένων, του υποκειμένου των δεδομένων και της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα όπως αυτοί εκτίθενται στο νομό 2472/1997 (ο οποίος ουσιαστικά ενσωμάτωσε το περιεχόμενο της Οδηγίας 95/46/ΕΚ). Επιπροσθέτως, στη σκέψη 3 της γνωμοδότησης της Αρχής αναφέρεται ότι από τις διατάξεις του νόμου 2472/1997 συνάγεται ότι στις θεμελιώδεις αρχές προστασίας των προσωπικών δεδομένων συγκαταλέγονται ιδίως η θεμελίωση της επεξεργασίας των δεδομένων στο νόμο, η αρχή του σκοπού (καθορισμένος, σαφής και νόμιμος σκοπός), η αρχή της αναλογικότητας της επεξεργασίας, η κατοχύρωση των δικαιωμάτων των υποκειμένων των δεδομένων και η ανάθεση του ελέγχου τήρησης των παραπάνω κανόνων σε ανεξάρτητη αρχή, ως θεσμική εγγύηση του δικαιώματος στην προστασία των προσωπικών δεδομένων.

Μάλιστα, η Αρχή διευκρινίζει ότι οι ανωτέρω αρχές είναι θεμελιώδεις διότι κατοχυρώνονται σε υπερνομοθετικά κείμενα (όπως_πχ το άρθρο 9Α του Συντάγματος, η ΕΣΔΑ (άρθρο 8), ο Χάρτης Θεμελιωδών Δικαιωμάτων (άρθρο 8), η Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης (άρθρο 6), η σύμβαση 108 του Συμβουλίου της Ευρώπης, η Σύμβαση για την εφαρμογή της συμφωνίας Σένγκεν κτλ). Βάσει των ανωτέρω λοιπόν η Αρχή μπόρεσε εν προκειμένω να ασκήσει ικανοποιητικά τη γνωμοδοτική της αρμοδιότητα στην προκειμένη περίπτωση, τονίζοντας επαρκώς τους κινδύνους που εγκυμονούσε ο προτεινόμενος σχεδιασμός του Ηλεκτρονικού Εισιτηρίου, δηλαδή ο υπέρμετρος

[158] Πρβλ. άρθρο 19 παρ. 1 ν. 2472/1997: «Η Αρχή Προστασίας Προσωπικών Δεδομένων γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα»

[159] Πρβλ. υπ' αριθμόν 168/2009 έγγραφο της Ομάδας Εργασίας του άρθρου 29 της Οδηγίας 95/46/ΕΚ, Το μέλλον προστασίας των προσωπικών δεδομένων, σ. 91 επ.

περιορισμός της ελεύθερης μετακίνησης (που αποτελεί έκφανση της ελευθερίας ανάπτυξης της προσωπικότητας και της προσωπικής ελευθερίας) σε δυσανάλογο βαθμό με τους θεμιτούς, διαφανείς και νόμιμους σκοπούς της επεξεργασίας (Σημειώνεται εδώ ότι με το προτεινόμενο ηλεκτρονικό εισιτήριο, ο υπεύθυνος επεξεργασίας του ΟΑΣΑ μπορούσε, εφόσον αυτό ζητούνταν από δημόσια αρχή, να καταγράφει τις διαδρομές που πραγματοποιεί συγκεκριμένο πρόσωπο).

Η επόμενη γνωμοδότηση της Αρχής που θα εξεταστεί είναι η υπ' αριθμόν 3/2018, η οποία πραγματοποιήθηκε μετά τη θέση σε ισχύ του νέου Γενικού Κανονισμού, και αφορούσε τη νομοθετική ρύθμιση για τη δημοσιοποίηση οικονομικών στοιχείων από τις δηλώσεις περιουσιακών καταστάσεων πολιτικών προσώπων και δικαστικών λειτουργών στο διαδίκτυο για το Πόθεν Έσχες[160]. Και στη συγκεκριμένη γνωμοδότηση, η Αρχή στηρίχθηκε στις προβλέψεις του νόμου 2472/1997 προκειμένου να υποστηρίξει τη γνωμοδοτική της αρμοδιότητα.

Το σημαντικό είναι ότι στο τέλος της γνωμοδότησης γίνεται λόγος και για το ζήτημα που προκύπτει αναφορικά με τη συμφωνία του περιεχομένου της ρύθμισης του άρθρου 3 παράγραφος 26 του νόμου με τις διατάξεις του νέου Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων, στο βαθμό που δεν καθορίζεται ρητώς ο ανώτατος χρόνος διατήρησης των δεδομένων, ούτε παρέχονται ειδικά και συγκεκριμένα κριτήρια για τον προσδιορισμό του[161].

Η τελευταία γνωμοδότηση της Αρχής που θα μας απασχολήσει σε αυτό το υποκεφάλαιο είναι η υπ' αριθμόν 1/2019 στην οποία η Αρχή της Προστασίας των Προσωπικών Δεδομένων κλήθηκε να γνωμοδοτήσει επί του προωθούμενου σχεδίου νόμου με τίτλο: «Δοκιμασία προσόντων και συμπεριφοράς υποψήφιων οδηγών και οδηγών για τη χορήγηση αδειών οδήγησης οχημάτων, άλλες διατάξεις για τις άδειες οδήγησης και λοιπές διατάξεις», καθώς καθιερώνει νέες διαδικασίες, οι οποίες προβλέπουν μεταξύ άλλων τη διαμόρφωση νέου συστήματος εποπτείας και ελέγχου των εκπαιδευτών, των διενεργούντων τις θεωρητικές εξετάσεις και των εξεταστών δοκιμασιών προσόντων και συμπεριφοράς, πέραν των άλλων, με καταγραφή, μέσω οπτικοακουστικών μέσων, της θεωρητικής εξέτασης και της δοκιμασίας προσόντων και συμπεριφοράς αλλά και αξιοποίηση του καταγραφέντος υλικού κατά την αξιολόγηση των εκπαιδευτών και των εξεταστών.

Στη σκέψη 1 της γνωμοδότησης, η Αρχή θεμελιώνει την γνωμοδοτική της αρμοδιότητα να συμβουλεύει το εθνικό κοινοβούλιο, την κυβέρνηση και άλλα όργανα και οργανισμούς για νομοθετικά και διοικητικά μέτρα που σχετίζονται με την προστασία των δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας των προσωπικών τους δεδομένων στο άρθρο 57 παρ. 1 γ' του Κανονισμού, σε συνδυασμό με το άρθρο 19 παρ. 1. θ' του ν. 2472/1997. Περαιτέρω στη σκέψη 3 της γνωμοδότησης η Αρχή επικαλείται το άρθρο 6 παρ. 1 του Κανονισμού, την παράγραφο 3, καθώς και το άρθρο 9 παρ. 1 για να διευκρινίσει τη νομική βάση που πρέπει να υπάρχει αναφορικά με το σκοπό της επεξεργασίας και τη γενική απαγόρευση επεξεργασίας δεδομένων που αφορούν στην υγεία των υποκειμένων.

[160] Βλ. ΦΕΚ Α' 186/2018

[161] Βλ. Αρχή Προστασίας Προσωπικών Δεδομένων, Γνωμοδότηση 3/2018, 13/11/2018

Μάλιστα, στη σκέψη 4 παρατηρείται ότι πλέον η Αρχή αντλεί τους νομικούς ορισμούς της επεξεργασίας δεδομένων, του υπεύθυνου επεξεργασίας και του εκτελούντος την υπηρεσία από το νέο Γενικό Κανονισμό, ενώ στις σκέψεις 5 και 6 η Αρχή επικαλείται το άρθρο 5 για τις αρχές που πρέπει να διέπουν την επεξεργασία (νομιμότητα, αντικειμενικότητα και διαφάνεια, περιορισμός του σκοπού, ελαχιστοποίηση των δεδομένων, ακρίβεια, περιορισμός της περιόδου αποθήκευσης, ακεραιότητα και εμπιστευτικότητα και λογοδοσία), καθώς και το άρθρο 25 για τη ρητή υποχρέωση προστασίας των προσωπικών δεδομένων αντίστοιχα.

Αυτό λοιπόν που συνάγεται από την εξέταση των ανωτέρω γνωμοδοτήσεων είναι ότι πράγματι η θέσπιση του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων, επηρέασε σημαντικά τις γνωμοδοτήσεις της Αρχής Προστασίας των Προσωπικών Δεδομένων. Και τούτο διότι ενώ το σκεπτικό των γνωμοδοτήσεων της Αρχής πριν το 2018 στηρίζονταν σχεδόν αποκλειστικά στις προβλέψεις του ν. 2472/1997, με τον οποίο ενσωματώθηκε η θεμελιώδης Οδηγία 95/46/ΕΚ στην εσωτερική έννομη τάξη, οι γνωμοδοτήσεις της Αρχής μετά το 2018 εδράζονται αποκλειστικά στον πληρέστερο GDPR.

Από αυτή την άποψη λοιπόν ο νέος Γενικός Κανονισμός κατόρθωσε να είναι πιο πλήρης εν αντιθέσει με τα προηγούμενα ευρωπαϊκά νομοθετήματα, συγκεντρώνοντας ουσιαστικά σε ένα ενιαίο νομικό κείμενο τις περισσότερες ρυθμίσεις σχετικά με την προστασία των προσωπικών δεδομένων, που παλαιότερα βρίσκονταν διάσπαρτοι σε διάφορα διεθνή και ευρωπαϊκά νομοθετήματα (Επί παραδείγματι είναι ενδεικτικό ότι ενώ πριν από το 2018 η Αρχή στήριζε τη γνωμοδοτική της αρμοδιότητα και τις θεμελιώδεις αρχές της επεξεργασίας προσωπικών δεδομένων σε πληθώρα υπερνομοθετικών κειμένων (Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης, Χάρτης Θεμελιωδών Δικαιωμάτων, ΕΣΔΑ, Σύμβαση για την Εφαρμογή της Συμφωνίας Σένγκεν) πλέον επικαλείται απλώς τις προβλέψεις του πληρέστερου Γενικού Κανονισμού για όλα τα θέματα που αφορούν τις γνωμοδοτήσεις της. Παρατηρώντας ωστόσο καλύτερα τις αλλαγές που έχουν συντελεστεί, γίνεται εύκολα αντιληπτό ότι ο νέος Κανονισμός δεν διαφέρει κάτι το καινούργιο στο κανονιστικό πλαίσιο της προστασίας των δεδομένων, αλλά απλώς συστηματοποιεί ρυθμίσεις που είτε υπήρχαν διάσπαρτες σε παλαιότερες υπερνομοθετικές πράξεις, είτε είχαν προκύψει από τη διαπλαστική ερμηνεία των Αρχών και των Δικαστηρίων.

6.5: Συμπεράσματα

Η αλματώδης τεχνολογική ανάπτυξη των εφαρμογών του διαδικτύου και πρωτίστως των μέσων κοινωνικής δικτύωσης έχει δημιουργήσει πολλαπλούς κινδύνους για την εκμετάλλευση των προσωπικών δεδομένων ιδίως μέσω της στοχευμένης διαφήμισης από τους επιχειρηματικούς κολοσσούς. Η ανεπαρκής προστασία των δεδομένων από τις εφαρμογές και ορισμένες άλλες αθέμιτες τεχνικές (πχ οι λεγόμενοι bugs που εισβάλλουν στα συστήματα ασφαλείας) υποκλέπτουν με μεγάλη ευκολία προσωπικά δεδομένα που χρησιμοποιούνται για εμπορικούς αλλά και πολιτικούς σκοπούς. Όπως επίσης αναδείχθηκε στο πρώτο υποκεφάλαιο η στοχευμένη διαφήμιση είναι ιδιαιτέρως αποτελεσματική και οικονομική, διότι «στοχεύει» σε συγκεκριμένα πρόσωπα που είναι πιο πιθανό να ενδιαφέρονται για το διαφημιζόμενο προϊόν ή πρόσωπο. Ιδιαιτέρως αποκαλυπτικές υπήρξαν και οι εξετασθείσες υποθέσεις υποκλοπής προσωπκών δεδομένων. Στην

περίπτωση της υπόθεσης Facebook-Cambrige Analytica αποδείχθηκε πόσο εύκολο είναι να χρησιμοποιηθούν τα προσωπικά δεδομένα για πολιτικούς σκοπούς και καμπάνιες. Οι επιπτώσεις ήταν ιδιαιτέρως σημαντικές για την Facebook η οποία υποχρεώθηκε να συμμορφωθεί με τις διατάξεις του νέου τότε Γενικού Κανονισμού. Ωστόσο, η δεύτερη υπόθεση (διάρρευση προσωπικών δεδομένων από την Google+, αποκαλύπτει με πόσο μεγάλη ευκολία μπορεί ένας επιχειρηματικός κολοσσός να αποκρύψει από το κοινό τη διαρροή προσωπικών δεδομένων, προκειμένου να αποφύγει τις αυστηρές επιπτώσεις του Γενικού Κανονισμού.

Κεφάλαιο 7: Τελικά Συμπεράσματα

Στη συγκεκριμένη εργασία επιχειρήθηκε μία κριτική προσέγγιση του νέου Κανονισμού για την προστασία των προσωπικών δεδομένων. Η δομή της ήταν τέτοια ούτως ώστε να διασφαλίζεται η συνεκτική και λογική της διάρθρωση για την εξαγωγή σημαντικών συμπερασμάτων σχετικά με τον νέο Κανονισμό. Ειδικότερα, στο πρώτο κεφάλαιο αναδείχθηκε ότι οι σημαντικότερες έννοιες της θεματικής της εργασίας είναι πρωτίστως η έννοια και ο νομικός ορισμός των προσωπικών δεδομένων, της επεξεργασίας τους, καθώς και του υπεύθυνου επεξεργασίας.

Όπως αναδείχθηκε ανωτέρω η ευρωπαϊκή και εθνική έννομη τάξη (με τον εφαρμοστικό νόμο 2472/1997) είχε συγκεκριμενοποιήσει επαρκώς το περιεχόμενο αυτών των εννοιών, υιοθετώντας ως επί το πλείστον ευρείς ορισμούς που να περιλαμβάνουν οποιαδήποτε μορφή πληροφορίας που μπορεί να συνδεθεί με την ταυτότητα συγκεκριμένου προσώπου. Περαιτέρω, αποδείχθηκε ότι το δικαίωμα προστασίας των προσωπικών δεδομένων έχει σημαντικά ερείσματα στο πρωτογενές ενωσιακό δίκαιο, αποκαλύφθηκε ωστόσο και μία συγκεκριμένη ιδιαιτερότητα του δικαιώματος η οποία σχετίζεται με το γεγονός ότι η κατοχύρωση του χρονικά ακολούθησε της «νομοθετικής συγκεκριμενοποίησης» και κατοχύρωσης του στο παράγωγο ενωσιακό δίκαιο.

Έπειτα, στο δεύτερο κεφάλαιο, αποδείχθηκε πως η ρύθμιση της προστασίας των προσωπικών δεδομένων πριν την ψήφιση του νέου κανονισμού στηρίχθηκε σε πολυάριθμες ατελείς ευρωπαϊκές νομοθετικές πράξεις, ενδεικτικό στοιχείο του πολυκερματισμού που επικρατούσε επί χρόνια στο ευρωπαϊκό νομικό πλαίσιο προστασίας των προσωπικών δεδομένων.

Αναμφισβήτητα, τα σημαντικότερα νομοθετικά κείμενα ήταν η Οδηγία 95/46/ΕΚ, που έδωσε τους βασικούς νομικούς ορισμούς των προσωπικών δεδομένων, της επεξεργασίας και του φορέα επεξεργασίας, καθώς και ο Κανονισμός 45/2001 που συνέστησε την Ευρωπαίο Επόπτη Προστασίας Προσωπικών Δεδομένων. Αυτό που αποδείχθηκε από την ανωτέρω ανάλυση είναι η ιδιαιτερότητα και ο δυναμικός χαρακτήρας του δικαιώματος της πληροφοριακής αυτοδιάθεσης, στοιχεία που δυσχεραίνουν την επαρκή ρύθμιση του.

Ο δυναμικός χαρακτήρας οφείλεται στο γεγονός ότι η προστασία των δεδομένων συναρτάται με τη διαρκώς μεταβαλλόμενη και ταχύτατη τεχνολογική εξέλιξη, η οποία καθιστά σε σύντομο χρονικό διάστημα τη νομική της ρύθμιση παρωχημένη. Περαιτέρω, βασικό εμπόδιο στην επαρκή ρύθμιση της προστασίας των δεδομένων αποτέλεσε η άνιση τεχνολογική εξέλιξη μεταξύ των χωρών της ΕΕ και αντιστοίχως η ασύμμετρη ανάπτυξη του νομικού «οπλοστασίου» των κρατών για την προστασία του δικαιώματος. Χαρακτηριστικό παράδειγμα επιβεβαίωσης του ανωτέρω ισχυρισμού αποτελεί η προσπάθεια της Ένωσης ήδη από τα μέσα της δεκαετίας του 1990 να ρυθμίσει το ζήτημα σε επίπεδο Οδηγίας και αργότερα σε επίπεδο Κανονισμού.

Επιπλέον όπως φάνηκε στο δεύτερο κεφάλαιο, οι πρώτες κανονιστικές ρυθμίσεις καταγράφονται σε διεθνές επίπεδο, διότι η ανταλλαγή και διαβίβαση πληροφοριών από χώρα σε χώρα, ήταν ένα χαρακτηριστικό των νέων τεχνολογικών, οικονομικών και γεωπολιτικών εξελίξεων που οδήγησαν σε

παγκοσμιοποίηση της πληροφορίας. Ο σεβασμός της ιδιωτικής και οικογενειακής ζωής κατοχυρώνεται για πρώτη φορά σε διεθνές νομικό κείμενο στις 10 Δεκεμβρίου του 1948 με την «Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του Οργανισμού Ηνωμένων Εθνών (Ο.Η.Ε.)» .

Το άρθρο 12 της ως άνω Διακήρυξης όριζε ότι «Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Ο καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους». Η Οικουμενική Διακήρυξη αποτέλεσε την απαρχή για τη θέσπιση πράξεων για τα ανθρώπινα δικαιώματα στην Ευρώπη.

Έπειτα ακολούθησε η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου στη Ρώμη (Ε.Σ.Δ.Α.) το 1950, για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών, η οποία τέθηκε σε ισχύ το 1953. Το δικαίωμα στην προστασία της ιδιωτικής ζωής κατοχυρώθηκε στο άρθρο 8 Ε.Σ.Δ.Α., το οποίο εγγυάται το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας και καθορίζει τις προϋποθέσεις υπό τις οποίες επιτρέπονται οι περιορισμοί του εν λόγω δικαιώματος. Περαιτέρω, με το άρθρο 19 της παραπάνω σύμβασης ιδρύθηκε στο Στρασβούργο της Γαλλίας το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου (Ε.Δ.Δ.Α.) που λειτουργεί από το 1959, με σκοπό να διασφαλίζει την τήρηση των υποχρεώσεων του υπέχουν από την Ε.Σ.Δ.Α. όλα τα συμβαλλόμενα μέρη. Επομένως σε ένα μεγάλο μέρος το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου «διέπλασε» με τη νομολογία του το δικαίωμα στην προστασία της ιδιωτικής ζωής.

Σημαντικό ρόλο στην κατοχύρωση του δικαιώματος της προστασίας της ιδιωτικής ζωής διαδραμάτισε επίσης η απόφαση 2450/19.12.1968 της Γ.Σ. των Ηνωμένων Εθνών, η οποία διατύπωνε τα ζητήματα καταπάτησης των ανθρωπίνων δικαιωμάτων από την ανάπτυξη της επιστήμης και της τεχνολογίας και ειδικότερα από τη χρήση των ηλεκτρονικών μέσων. Επιπροσθέτως, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α.) εξέδωσε το 1980 τις «Κατευθυντήριες Αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών δεδομένων», οι οποίες περιελάμβαναν την αρχή της περιορισμένης συγκέντρωσης και συλλογής των δεδομένων, την αρχή της ποιότητας των δεδομένων, την αρχή του προσδιορισμένου σκοπού, την αρχή της περιορισμένης χρήσης των προσωπικών δεδομένων, την αρχή μέτρων ασφαλείας των προσωπικών δεδομένων, την αρχή της διαφάνειας, την αρχή της συμμετοχής του ατόμου και τέλος την αρχή της ευθύνης. Οι συγκεκριμένες αρχές αποτέλεσαν τη βάση των μεταγενέστερων ευρωπαϊκών νομοθετημάτων σχετικά με την προστασία των δεδομένων.

Ακολούθησε το 1981 η Σύμβαση 108 του Συμβουλίου της Ευρώπης (άρθρο 6) για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία καθόρισε τις θεμελιώδεις αρχές της προστασίας των δεδομένων προσωπικού χαρακτήρα. Είχε ως στόχο να εξασφαλίσει σε κάθε άτομο, ανεξάρτητα από την ιθαγένεια ή την κατοικία, την προστασία της ιδιωτικής του ζωής κατά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Επίσης, θεσπίζει το δικαίωμα του καθενός να έχει πρόσβαση στα δεδομένα που τον αφορούν και να διεκδικήσει τη διόρθωση ή τη διαγραφή των δεδομένων αυτών, εφόσον έχουν υποστεί παράνομη επεξεργασία. Η Σύμβαση αυτή αποτέλεσε τη νομοθετική αρχή, ώστε αρκετές χώρες προέβησαν στη ψήφιση ειδικών νόμων, ενώ άλλες τροποποίησαν την υπάρχουσα νομοθεσία προκειμένου να

θεσπίσουν ένα ολοκληρωμένο νομοθετικό πλαίσιο. Όλα τα κράτη μέλη της ΕΕ έχουν κυρώσει τη Σύμβαση 108.

Η ελεύθερη κυκλοφορία προσώπων, αγαθών, κεφαλαίων και υπηρεσιών εντός της εσωτερικής αγοράς της ΕΕ απαιτούσε την ελεύθερη ροή δεδομένων, υπό την προϋπόθεση ότι τα κράτη μέλη θα μπορούσαν να βασιστούν σε ένα ενιαίο θεσμικό πλαίσιο προστασίας των δεδομένων. Έτσι, τα θεσμικά όργανα της ΕΕ οδηγήθηκαν στην έκδοση της Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων. Η Οδηγία είχε ως σκοπό να καταστήσει ισότιμο σε όλα τα κράτη μέλη το επίπεδο προστασίας των δικαιωμάτων και των ελευθεριών των προσώπων, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Για αυτό και μέσω αυτής θεσπίστηκαν γενικοί κανονισμοί περί της νομιμότητας επεξεργασίας δεδομένων προσωπικού χαρακτήρα, οι οποίοι καθορίζουν τα δικαιώματα των προσώπων που αφορούν τα δεδομένα και προβλέπουν τη σύσταση εθνικών ανεξάρτητων εποπτικών αρχών. Επιπρόσθετα, όριζε τον τρόπο με τον οποίο επιτρέπεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα, δηλαδή μόνο εφόσον έχει δοθεί η ρητή συγκατάθεση του ατόμου στο οποίο αναφέρονται τα δεδομένα προς επεξεργασία και έχει ενημερωθεί εκ των προτέρων για την επεξεργασία τους.

Η ραγδαία εξέλιξη της ψηφιακής τεχνολογίας και ιδιαίτερα η ταχύτατη ανάπτυξη των τηλεπικοινωνιακών δικτύων απαίτησε την έκδοση της Οδηγίας 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 για την προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα. Έπειτα ακολούθησε ο Κανονισμός (ΕΚ) 45/2001 σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Περαιτέρω, ο Κανονισμός (ΕΚ) 45/2001, προέβλεψε τη σύσταση μίας ανεξάρτητης εποπτικής αρχής («Ευρωπαίος Επόπτης Προστασίας Δεδομένων») με αρμοδιότητα να εξασφαλίζει ότι τα όργανα και οι οργανισμοί της ΕΕ τηρούν τις υποχρεώσεις τους ως προς την προστασία των δεδομένων. Ορισμένα από τα καθήκοντα του Ε.Ε.Π.Δ. είναι η εποπτεία, η γνωμοδότηση και η συνεργασία.

Επιπροσθέτως, δημιουργήθηκε η ομάδα εργασίας του άρθρου 29 που ήταν ένα ανεξάρτητο συμβουλευτικό όργανο για την προστασία των δεδομένων και της ιδιωτικής ζωής, βάσει του άρθρου 29 της Οδηγίας 95/46/ΕΚ. Η Οδηγία 97/66/ΕΚ αντικαταστάθηκε από την Οδηγία 2002/58/ΕΚ 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.

Έπειτα ακολούθησε η Οδηγία 2006/24/ΕΚ για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών, η οποία τροποποίησε την Οδηγία 2002/58/ΕΚ και

τελικώς κηρύχθηκε άκυρη από το Ευρωπαϊκό Δικαστήριο στις 8 Απριλίου 2014 επειδή ήταν σε μεγάλο βαθμό ασύμβατη με την ιδιωτική ζωή κ αι τ ην προστασία των δεδομένων.

Επιπρόσθετα, η Οδηγία 2009/136/ΕΚ (ωστόσο μετέπειτα καταργηθείσα) συμπλήρωσε την Οδηγία 2002/58/ΕΚ, εξειδικεύοντας ορισμένες διατάξεις σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τελικά το 2013 εκδόθηκε ο Κανονισμός ΕΕ 611/2013 σχετικά με τα εφαρμοστέα μέτρα για την κοινοποίηση παραβιάσεων προσωπικών δεδομένων βάσει της Οδηγίας 2002/58/ΕΚ.

Το γεγονός ότι οι αρχικές Συνθήκες δεν περιείχαν καμιά αναφορά στα ανθρώπινα δικαιώματα, ανάγκασε την ΕΕ το 2000 να προβεί στη διακήρυξη του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Ο Χάρτης ενσωμάτωσε τα ατομικά, πολιτικά, οικονομικά και κοινωνικά δικαιώματα των Ευρωπαίων πολιτών σε μια σύνθεση κοινών συνταγματικών παραδόσεων και κοινών διεθνών υποχρεώσεων των κρατών μελών. Συναφώς, δεν εγγυάται μόνο το σεβασμό της ιδιωτικής και κοινωνικής ζωής (άρθρο 7), αλλά κατοχυρώνει και το δικαίωμα στην προστασία των δεδομένων (άρθρο 8).

Ο Χάρτης κατέστη νομικά δεσμευτικός ως πρωτογενές ενωσιακό δίκαιο με την έναρξη της Συνθήκης της Λισαβόνας την 1η Δεκεμβρίου του 2009. Πιο συγκεκριμένα, στο άρθρο 16 της Συνθήκης οριοθετήθηκε το θεσμικό πλαίσιο, σύμφωνα με το οποίο δόθηκε σε κάθε πολίτη το δικαίωμα της προστασίας των προσωπικών δεδομένων του, ενώ ταυτόχρονα καθορίστηκε το νομικό πλαίσιο θέσπισης κανονισμών για την προστασία των δεδομένων σε όλες τις δραστηριότητες που σχετίζονται με την υλοποίηση του δικαίου της ΕΕ.

Εν συνεχεία στο κεφάλαιο 3 αποδείχθηκε ότι οι βασικότερες εξελίξεις που οδήγησαν στον GDPR υπήρξαν η ραγδαία τεχνολογική ανάπτυξη, η επέκταση των ηλεκτρονικών συναλλαγών, η επέκταση της χρήσης των μέσων κοινωνικής δικτύωσης, καθώς και η ανάγκη για «σύγκλιση» των των εθνικών νόμων των κρατών μελών που έως τότε ρύθμιζαν την προστασία των προσωπικών δεδομένων. Περαιτέρω, στο κεφάλαιο 4 από την ανάλυση του Γενικού Κανονισμού αναδείχθηκε πως ο Κανονισμός Προστασίας Προσωπικών Δεδομένων σε μεγάλο βαθμό «συστηματοποιεί» και συγκεντρώνει σε ένα ενιαίο και συνεκτικό θεσμικό κείμενο τις ρυθμίσεις που παλαιότερα υπήρχαν και είχαν προκύψει για την προστασία των προσωπικών δεδομένων.

Πιο συγκεκριμένα, ο Κανονισμός εμπλουτίζει σημαντικά τον κατάλογο των δικαιωμάτων του υποκειμένου των δεδομένων και προσθέτει και σημαντικές εγγυήσεις για τη διασφάλιση της προστασίας τους κατοχυρώνοντας αφ’ ενός ως ρητή αρμοδιότητα των εθνικών ανεξαρτήτων αρχών την παρακολούθηση της εφαρμογής του Κανονισμού και αφ’ ετέρου με τη σύσταση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων που αντικατέστησε την ομάδα εργασίας.

Ωστόσο υπάρχουν και αρκετά σημεία του Κανονισμού στα οποία έχει ασκηθεί κριτική. Ειδικότερα, ο τομέας της συγκατάθεσης του GDPR έχει ορισμένες συνέπειες για τις επιχειρήσεις που καταγράφουν τις τηλεφωνικές κλήσεις. Μια τυπική αποποίηση ευθυνών δεν θεωρείται επαρκής για την απόκτηση της συναίνεσης για την καταγραφή κλήσεων. Επιπλέον, όταν ξεκινά η εγγραφή, αν ο

καλών αποσύρει τη συγκατάθεσή του, τότε πρέπει να σταματήσει μια εγγραφή που είχε αρχίσει και να διασφαλιστεί ότι η εγγραφή δεν θα αποθηκευτεί.

Επιπλέον, το συνολικό κόστος για τις επιχειρήσεις της ΕΕ εκτιμάται σε περίπου 200 δισ. ευρώ, ενώ για τις αμερικανικές εταιρείες η εκτίμηση είναι 41,7 δισ. δολάρια. Έχει υποστηριχθεί επίσης ότι οι μικρότερες επιχειρήσεις ενδέχεται να μην έχουν τους οικονομικούς πόρους για να συμμορφωθούν επαρκώς με το GDPR, σε αντίθεση με τις μεγαλύτερες διεθνείς εταιρείες τεχνολογίας (όπως το Facebook και το Google). Η έλλειψη γνώσης και κατανόησης των κανονισμών υπήρξε επίσης λόγος άσκησης κριτικής. Επομένως, βασικός λόγος άσκησης κριτικής είναι ότι οι προβλέψεις του Κανονισμού φαίνεται να ευνοούν τις επιχειρήσεις με μεγαλύτερη οικονομική επιφάνεια. Ένα αντεπιχείρημα πάντως στην ανωτέρω κριτική είναι ότι οι εταιρείες ενημερώθηκαν για τις αλλαγές αυτές δύο χρόνια πριν από την έναρξη ισχύος τους και, ως εκ τούτου, είχαν αρκετό χρόνο για να προετοιμαστούν.

Επιπροσθέτως, στο κεφάλαιο 5 αποδείχθηκε πως οι προβλέψεις για τις εποπτικές αρχές είναι ιδιαιτέρως σημαντικές καθώς αποτελούν τις θεσμικές εγγυήσεις για την αποτελεσματική εφαρμογή του περιεχομένου του. Ο Κανονισμός αλλάζει αρκετά στοιχεία σχετικά με τη λειτουργία των εποπτικών αρχών θεσπίζοντας σειρά εγγυήσεων λειτουργικής και οργανικής ανεξαρτησίας, όπως επί παραδείγματι οι συγκεκριμένες προϋποθέσεις επιλογής και διαφανούς διορισμού των μελών της (διορισμός από το εθνικό κοινοβούλιο, τον αρχηγό του κράτους, της κυβέρνησης ή από ανεξάρτητη αρχή έμπειρων και ειδικώς καταρτισμένων μελών), αυτοδιοίκηση, οικονομική αυτοτέλεια και παράλληλα υποχρέωση των εθνικών κυβερνήσεων να ενισχύουν οικονομικά και να παράσχουν την κατάλληλη υποδομή στις Αρχές για να εκτελούν τα καθήκοντα τους.

Σίγουρα οι συγκεκριμένες εγγυήσεις κρίνονται επαρκείς, ιδίως συνερμηνεύομενες με το ασυμβίβαστο των μελών των εποπτικών αρχών. Προκύπτουν ωστόσο σοβαρά ζητήματα. Εν πρώτοις, όπως αποδείχθηκε και από το υποκεφάλαιο 5.2, οι περισσότερες εθνικές εποπτικές αρχές έχουν ήδη συσταθεί παλαιότερα με το εσωτερικό δίκαιο που ενσωμάτωσε τις παλαιότερες Οδηγίες. Επομένως, είναι απορίας άξιον πόσο εύκολο είναι να αλλάξει ο τρόπος λειτουργίας εποπτικών αρχών που ήδη λειτουργούν εδώ και πολλά χρόνια με διαφορετικό καθεστώς που προβλεπόταν σε «αποκλίνοντες» εθνικούς νόμους μεταξύ των κρατών μελών.

Και δευτερευόντως προκύπτει το ζήτημα του πώς μπορούν να ελεγχθούν οι εθνικές κυβερνήσεις όσον αφορά τις υποχρεώσεις τους έναντι των εποπτικών αρχών (δηλαδή το σεβασμό των προαναφερθέντων εγγυήσεων, την επαρκή οικονομική ενίσχυση τους κτλ.). Εξάλλου, η οικονομική ενίσχυση και οι παροχές των εθνικών κρατών προς τις ανεξάρτητες αρχές εξαρτάται από την οικονομική τους δυνατότητα και από την ουσιαστική τους εκτίμηση. Επομένως να συγκεκριμένα ζητήματα δεν μπορούν να ελεγχθούν. Πάντως, η σύσταση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων είναι ιδιαιτέρως σημαντική.

Τέλος, στο κεφάλαιο 6 αναδείχθηκε ότι η αλματώδης τεχνολογική ανάπτυξη των εφαρμογών του διαδικτύου και πρωτίστως των μέσων κοινωνικής δικτύωσης έχει δημιουργήσει πολλαπλούς

κινδύνους για την εκμετάλλευση των προσωπικών δεδομένων μέσω της στοχευμένης διαφήμισης από τους επιχειρηματικούς κολοσσούς. Η ανεπαρκής προστασία των δεδομένων από τις εφαρμογές και ορισμένες άλλες αθέμιτες τεχνικές (πχ οι λεγόμενοι bugs που εισβάλλουν στα συστήματα ασφαλείας) υποκλέπτουν με μεγάλη ευκολία προσωπικά δεδομένα που χρησιμοποιούνται για εμπορικούς αλλά και πολιτικούς σκοπούς.

Όπως επίσης αναδείχθηκε στο πρώτο υποκεφάλαιο, η στοχευμένη διαφήμιση είναι ιδιαιτέρως αποτελεσματική και οικονομική, διότι «στοχεύει» σε συγκεκριμένα πρόσωπα που είναι πιο πιθανό να ενδιαφέρονται για το διαφημιζόμενο προϊόν ή πρόσωπο. Ιδιαιτέρως αποκαλυπτικές υπήρξαν οι εξετασθείσες υποθέσεις υποκλοπής προσωπικών δεδομένων. Στην περίπτωση της υπόθεσης Facebook-Cambrige Analytica αποδείχθηκε πόσο εύκολο είναι να χρησιμοποιηθούν τα προσωπικά δεδομένα για πολιτικούς σκοπούς και καμπάνιες.

Οι επιπτώσεις ήταν ιδιαιτέρως σημαντικές για την Facebook, η οποία υποχρεώθηκε να συμμορφωθεί με τις διατάξεις του νέου Γενικού Κανονισμού. Ωστόσο, η δεύτερη υπόθεση (διάρρευση προσωπικών δεδομένων από την Google+), αποκαλύπτει με πόσο μεγάλη ευκολία μπορεί ένας επιχειρηματικός κολοσσός να αποκρύψει από το κοινό τη διαρροή προσωπικών δεδομένων, προκειμένου να αποφύγει τις αυστηρές επιπτώσεις του Γενικού Κανονισμού. Το Ευρωπαϊκό Κοινοβούλιο περιλαμβάνει πολύ σημαντικούς καινοτόμους κανόνες που θα εφαρμοστούν σε ολόκληρη την Ευρωπαϊκή Ένωση και θα επηρεάσουν άμεσα κάθε κράτος μέλος.

Όπως αποκαλύφθηκε, οι πρακτικές και κοινωνικές επιπτώσεις του GDPR είναι πολύ σημαντικές, καθώς αποτελούν ενιαίο και ενημερωμένο σύνολο κανόνων που εφαρμόζονται σε ολόκληρη την ΕΕ και για όλη την επεξεργασία δεδομένων των ευρωπαίων πολιτών. Βασικός στόχος του υπήρξε η αποτροπή του κατακερματισμού της αγοράς της ΕΕ και η διευκόλυνση της διασυνοριακής επιχειρηματικής δραστηριότητας, της ελεύθερης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα καθώς και της διασφάλισης των θεμελιωδών δικαιωμάτων και ελευθεριών των ευρωπαίων πολιτών.

Είναι προφανές ότι ζητήματα προσωπικών δεδομένων μπορεί να προκύψουν σε όλες τις επιχειρηματικές δραστηριότητες και σε όλες τις πτυχές της ζωής εν γένει, δεδομένου ότι οι πληροφορίες από τις οποίες είναι δυνατός ο εντοπισμός φυσικών προσώπων μπορούν να βρεθούν σχεδόν παντού. Επομένως, αποδεικνύεται πόσο σημαντική είναι η ρύθμιση της προστασίας των προσωπικών δεδομένων.

Στην ελληνική έννομη τάξη, το κύριο σύνολο κανόνων προστασίας δεδομένων αποτελείται από τον Ν. 2474/1997, ο οποίος εναρμόνισε την ελληνική νομοθεσία με την Οδηγία 95/46/ΕΚ. Ο νόμος αυτός καθόριζε τις υποχρεώσεις των προσώπων που επεξεργάζονται τα προσωπικά δεδομένα και τα αντίστοιχα δικαιώματα εκείνων στους οποίους αφορά η επεξεργασία των δεδομένων (υποκείμενα δεδομένων). Ο ίδιος νόμος προέβλεπε επίσης την ίδρυση της Ελληνικής Αρχής Προστασίας Δεδομένων και αρμοδιοτήτων της.

Επιπλέον, όταν πρόκειται για ειδικές περιπτώσεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ενδέχεται να ισχύουν και άλλοι νόμοι: π.χ. Νόμος 3471/2006 για την προστασία των προσωπικών δεδομένων σε σχέση με τις ηλεκτρονικές επικοινωνίες (βλ. Οδηγία 2002/58/ΕΚ), Ν. 3917/2011 σχετικά με τη διατήρηση δεδομένων που υφίστανται επεξεργασία στο πλαίσιο των δημόσιων ηλεκτρονικών επικοινωνιών (βλ. Οδηγία 2006/24/), το άρθρο 34 του Ν. 4002/2011 για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που διεξάγεται από την Επιτροπή Εποπτείας και Ελέγχου Παιχνιδιών στο πλαίσιο των κανονισμών για την Αγορά Τυχερών Παιχνιδιών κλπ.

Όπως αναδείχθηκε στο κεφάλαιο 4, οι υπεύθυνοι επεξεργασίας έχουν υποχρέωση λογοδοσίας στο πλαίσιο του GDPR. Αυτές περιλαμβάνουν την τήρηση αρχείων που μπορούν να παρασχεθούν στις εποπτικές αρχές κατόπιν αιτήματος. Οι ελεγκτές και οι επεξεργαστές μοιράζονται την ευθύνη για την ασφάλεια των προσωπικών δεδομένων και πρέπει να διασφαλίζουν τη συμμόρφωση με τους διεθνείς κανόνες μεταφοράς δεδομένων. Οι ελεγκτές υπόκεινται σε μεγάλα διοικητικά πρόστιμα αν δεν τηρούνται οι υποχρεώσεις τους και μπορούν να υποβληθούν σε αξιώσεις αποζημίωσης από ιδιώτες.

Είναι πολύ σημαντικό, όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα εντός πολυεθνικών οργανισμών (π.χ. με τη συμμετοχή ελεγκτών και μεταποιητών που βρίσκονται σε περισσότερες από μία χώρες), να εξεταστεί το σύνολο των εθνικών νομοθεσιών που ισχύουν. Σημειώνεται ότι, από την άποψη αυτή, ο ελληνικός νόμος είναι αρκετά αυστηρός, δεδομένου ότι υπερβαίνει τις απαιτήσεις της Οδηγίας 95/46 / ΕΚ.

Μέσα από την βιβλιογραφική και νομοθετική επισκόπηση, διαπιστώνει κανείς ότι υπάρχουν αρκετές προγενέστερες ή μεταγενέστερες ρυθμίσεις που αφορούν άμεσα ή έμμεσα την προστασία προσωπικών στοιχείων, όπως πχ τα άρθρα 57-59 του Αστικού Κώδικα για την προστασία της προσωπικότητας ή τα άρθρα για την προστασία της σφαίρας του απορρήτου (τα Άρθρα 248 και 370Α του Ποινικού Κώδικα), ο ν.2928/2001 (Φ.Ε.Κ. Α΄ 141) που αφορά την καταπολέμηση του οργανωμένου εγκλήματος, ο οποίος συμπεριλαμβάνει μεταξύ των άλλων και τις ρυθμίσεις που αφορούν την ανάλυση DNA για τη διαπίστωση της ταυτότητας υπόπτου για τέλεση ορισμένων εγκληματικών ενεργειών, καθώς και το Π.Δ. 131/2003 (Φ.Ε.Κ. Α΄ 116) που κυρώνει την Οδηγία 2000/31/ΕΚ για το ηλεκτρονικό εμπόριο.

Στόχος του νέου Κανονισμού είναι να προστατεύσει όλους τους πολίτες της ΕΕ από την ιδιωτική ζωή και τις παραβιάσεις των δεδομένων στο σύγχρονο κόσμο «της πληροφορίας». Μολονότι οι βασικές αρχές της προστασίας της ιδιωτικής ζωής εξακολουθούν να ισχύουν στην προηγούμενη Οδηγία, έχουν προταθεί πολλές αλλαγές στις ρυθμιστικές πολιτικές.

Ο νέος Κανονισμός καθιστά σαφή την εφαρμογή του. Ισχύει για την επεξεργασία προσωπικών στοιχείων από ελεγκτές και μεταποιητές στην ΕΕ, ανεξάρτητα από το εάν η επεξεργασία πραγματοποιείται στην ΕΕ ή όχι. Το GDPR ισχύει επίσης για την επεξεργασία δεδομένων προσωπικού χαρακτήρα των υποκειμένων στην ΕΕ από υπεύθυνο επεξεργασίας ή μεταποιητή που δεν είναι εγκατεστημένος στην ΕΕ, όπου οι δραστηριότητες αφορούν: προσφορά αγαθών ή υπηρεσιών σε πολίτες της ΕΕ (ανεξάρτητα από το αν απαιτείται πληρωμή) παρακολούθηση της συμπεριφοράς που λαμβάνει χώρα εντός της ΕΕ. Οι επιχειρήσεις εκτός ΕΕ που επεξεργάζονται τα στοιχεία των πολιτών της ΕΕ πρέπει επίσης να διορίσουν εκπρόσωπο στην ΕΕ.

Με το νέο Κανονισμό οι όροι για τη συγκατάθεση έχουν ενισχυθεί και οι εταιρείες δεν μπορούν πια να χρησιμοποιούν μακρούς, δυσανάγνωστους όρους ή συνθήκες γεμάτες νομικά-δυσνόητα στοιχεία. Η αίτηση συγκατάθεσης πρέπει να παρέχεται με κατανοητή και εύληπτη μορφή. Συναφώς, η συγκατάθεση πρέπει να είναι σαφής και διακριτή από άλλα θέματα και να παρέχεται με κατανοητή και εύκολα προσιτή μορφή, χρησιμοποιώντας σαφή και κατανοητή γλώσσα.

Αναντίρρητα, ο νέος Κανονισμός συμβάλλει σημαντικά στην ενίσχυση της προστασίας των προσωπικών δεδομένων των Ευρωπαίων πολιτών, ο οποίος άλλωστε ήταν και ο βασικός λόγος θέσπισης του. Ωστόσο το συγκεκριμένο νομοθέτημα έχει να αντιμετωπίσει σημαντικές προκλήσεις. Αρχικά, καλείται να αντικαταστήσει ένα νομικό πλαίσιο που όπως είχαμε τη δυνατότητα να διαπιστώσουμε σε αυτή την εργασία χαρακτηριζόταν από πολυκερματισμό (είναι ενδεικτική η πληθώρα ευρωπαϊκών Οδηγιών που προηγουμένως ρύθμιζε την προστασία των δεδομένων). Και δευτερευόντως, σημαντικότερες δυσχέρειες εντοπίζονται στη ρύθμιση της λειτουργίας και στην εκχώρηση αρμοδιοτήτων σε εθνικές εποπτικές αρχές που έχουν ήδη συσταθεί κατ' εφαρμογή των προηγούμενων ευρωπαϊκών νομοθετημάτων (πχ Οδηγία 95/46/ΕΚ, Κανονισμός 45/2001, καθ' ημάς ν. 2472/1997).

Μολονότι είναι πρόδηλη η επιδίωξη της ΕΕ να ενισχύσει την αποτελεσματικότητα και την αμεροληψία των εποπτικών αρχών (Βλ. Κεφ. 5), αναγνωρίζοντας το σημαντικό ρόλο που διαδραματίζουν στη διασφάλιση της προστασίας των προσωπικών δεδομένων, η εφαρμογή των σχετικών διατάξεων παραμένει ανέλεγκτη. Ειδικότερα, βασικές προϋποθέσεις της προσωπικής και λειτουργικής ανεξαρτησίας των μελών αλλά και της αποτελεσματικής λειτουργίας των εποπτικών αρχών, όπως η οικονομική ενίσχυση, οι κατάλληλες υλικοτεχικές υποδομές, η διοικητική και οικονομική αυτοτέλεια, καθώς και η αδιαφάνεια στη διαδικασία του διορισμού των μελών τους, παρά τις λεπτομερείς προβλέψεις του GDPR, παραμένουν υποθέσεις των κρατών μελών οι οποίες δεν μπορούν να ελεγχθούν επαρκώς από τα θεσμικά όργανα της ΕΕ. Αποδεικνύεται επομένως πως χωρίς την πρόβλεψη ικανοποιητικών διαδικασίων ελέγχου της συμμόρφωσης και των εθνών κρατών ως προς τις υποχρεώσεις που υπέχουν βάσει του νέου Κανονισμού, η αποτελεσματικότητα των διατάξεων του GDPR αναφορικά με τις εποπτικές αρχές θα είναι περιορισμένη.

Σε κάθε περίπτωση πάντως ο Κανονισμός περιέχει σημαντικότατες καινοτομίες που περιλαμβάνουν τη «συστηματοποίηση» των κανόνων που ρυθμίζουν την προστασία των προσωπικών δεδομένων, αυστηρότατες χρηματικές κυρώσεις σε περίπτωση παραβίασης των διατάξεων του από εταιρείες, τη σύσταση του Ευρωπαϊκού Συμβουλίου Προστασίας των Δεδομένων, τον εμπλουτισμό των δικαιωμάτων των υποκειμένων, καθώς και την υποχρέωση των εταιρειών για έγκαιρη γνωστοποίηση της διάρρευσης προσωπικών δεδομένων στα υποκείμενα των δεδομένων. Αξιόλογη θεματική ενότητα για περαιτέρω εμβάθυνση θα μπορούσε να αποτελέσει η διερεύνηση του κατά πόσον οι προβλέψεις του νέου Κανονισμού ωφελούν περισσότερο τους επιχειρηματικούς κολοσσούς εις βάρος των μικρών εταιρειών (πρόβλεψη υψηλών προστίμων, υψηλές-απλησίαστες προδιαγραφές σχεδιασμού της ασφάλειας του λογισμικού κτλ.).

Βιβλιογραφία

Ελληνόγλωσση:

- Αλεξανδροπούλου-Αιγυπτιάδου, Ε., «Προσωπικά Δεδομένα», Εκδ. Νομική Βιβλιοθήκη, 2016
- Βλαχόπουλος, Σ. (επιμ.), «Θεμελιώδη Δικαιώματα», Εκδ. Νομική Βιβλιοθήκη, 2016
- Δελούκα-Ιγγλέση, Κ., «Η προστασία του καταναλωτή από την άμεση διαφήμιση στο διαδίκτυο», ΔίΜΕΕ/2004
- Δελούκα-Ιγγλέση, Κ., «Νομικά Θέματα Ηλεκτρονικού Εμπορίου», Εκδ. Νομική Βιβλιοθήκη, 2015
- Δελούκα-Ιγγλέση, Κ., «Το ηλεκτρονικό εμπόριο στην Ευρωπαϊκή Ένωση και η Οδηγία 2000/31/ΕΚ σχετικά με ορισμένες πτυχές του ηλεκτρονικού εμπορίου στην εσωτερική αγορά», Μνήμη Μ. Μηνούδη (2004)
- Ευρωβαρόμετρο, Προστασία προσωπικών δεδομένων, Έρευνα 431, Στοιχεία 2015
- Ιγγλεζάκης Ι., Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του, εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη 2014.
- Ιγγλεζάκης Ι., Ευαίσθητα προσωπικά δεδομένα, εκδ. Σάκκουλα Αθήνα-Θεσσαλονίκη 2003
- Ιωακειμίδης, Π., «Η Συνθήκη της Λισαβόνας», Εκδ. Θεμέλιο, 2010
- Καρδασιάδου, Ζ., «Στον απόηχο της Οδηγίας 95/46/ΕΚ», Ευρωπαίων Πολιτεία, 2011
- Κοτσαλής, Λ. (επιμ.), «Γενικός Κανονισμός Προστασίας Δεδομένων», Εκδ. Νομική Βιβλιοθήκη, 2018
- Κοτσαλής, Λ., «Προσωπικά Δεδομένα», Εκδ. Νομική Βιβλιοθήκη, 2016
- Μήτρου, Λ., «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων», Εκδ. Σάκκουλα, 2017
- Παναγοπούλου-Κουτνατζή, Φ., «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016/ΕΕ», Εκδ. Σάκκουλα, 2017
- Τζώρτζη, Β., «Προστασία Δεδομένων Προσωπικού Χαρακτήρα», Εκδ. Νομική Βιβλιοθήκη, 2018
- Χριστοδούλου Κ., «Δίκαιο Προσωπικών Δεδομένων», εκδ. Νομική Βιβλιοθήκη 2013.

- Χριστοδούλου Κ., «Προς μια επανεξέταση της έννοιας της δικαιοπραξίας; Το παράδειγμα της συγκατάθεσης του υποκειμένου στην επεξεργασία των προσωπικών δεδομένων του», ΔiΜΕΕ 2005, σ. 357 επ.

Ξενόγλωσση:

- Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & security, 26(4)
- Almeida, L. D. A., & Baranauskas, M. C. C. (2010). Merging technical guidelines for accessible web content with universal design principles. Tech. Rep. IC-10-020.
- Anderson, B., Vance, T., Kirwan, B., Eargle, D., & Howard, S. (2014). Users aren't (necessarily) lazy: Using neurois to explain habituation to security warnings.
- Anderson, L., (2014): «The effects of interannual climate variability on the moraine record», σε: Geology, v. 42(1), 2014
- Balebako, R., Jung, J., Lu, W., Cranor, L. F., & Nguyen, C. (2013, July). Little brothers watching you: Raising awareness of data leaks on smartphones. In Proceedings of the Ninth Symposium on Usable Privacy and Security
- Bambauer, D. E., (2013) "Privacy versus Security," J. Crim. L. & Criminology, vol. 103, p. 667.
- Cormack, A. (2017). GDPR: What's your justification?. JISC community
- Coulter, M., «Find out if your Facebook data was shared with Cambridge Analytica», Evening Standard, 2018
- Cox III, E. P., Wogalter, M. S., Stokes, S. L., & Murff, E. J. T. (1997). Do product warnings increase safe behavior? A meta-analysis. Journal of Public Policy & Marketing, 16(2)
- Cranor, L. F. (2008). A framework for reasoning about the human in the loop
- Durkan, P., Durkin, M., & Gillen, J. (2003). Exploring efforts to engender on-line trust. International Journal of Entrepreneurial Behavior & Research, 9(3)
- Egelman, S., Cranor, L. F., & Hong, J. (2008, April). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems ACM

- Gantner, J., Demetz, L., & Maier, R. (2015, October). All You Need is Trust–An Analysis of Trust Measures Communicated by Cloud Providers. In OTM Confederated International Conferences" On the Move to Meaningful Internet Systems" Springer, Cham
- Graham-Harrison, E., «Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach», the Guardian, 2018
- Gritzalis, S., and Lambrinoudakis, C., (2008) “Privacy in the digital world,” in Encyclopedia of Internet Technologies and Applications. IGI Global
- Hern, «How to check whether Facebook shared your data with Cambridge Analytica», The Guardian, 2018
- Hunton & Williams, «The Proposed EU General Data Protection Regulation A guide for in-house lawyers», 2015
- Johnson, P., «Targeted advertising and advertising avoidance», The RAND Journal of Economics (περιοδικό) τεύχος 44 (1), 2013
- Kelley, P. G. (2009, April). Designing a privacy label: assisting consumer understanding of online privacy practices. In CHI'09 Extended Abstracts on Human Factors in Computing Systems ACM.
- Kendall, B., «Facebook's Settlement on 'Beacon' Service Survives Challenge», Wall Street Journal, 2015
- Kietzmann, J., «Social media? Get serious! Understanding the functional building blocks of social media», σε: Business Horizons, 54 (3), 2011
- Kozlowska, H., «The Cambridge Analytica scandal affected 87 million people, Facebook says», Quartz, 2018
- Kranenborg, H., Άρθρο 8, σε: S. Peers (επιμ.), «The EU Charter of Fundamental Rights, A Commentary», 2014
- Krumm, J., «Ubiquitous advertising: The killer application for the 21st century», IEEE Pervasive Computing, 2010
- Langhorne, A. L. (2014, June). Web privacy policies in higher education: How are content and design used to provide notice (or a lack thereof) to users?. In International Conference on Human Aspects of Information Security, Privacy, and Trust Springer, Cham.
- Lasswell, H. D. (1948). The structure and function of communication in society. The communication of ideas, 37

- Li, K., «Building a targeted mobile advertising system for location-based services», Decision Support Systems, 2012
- Louis, V., «Η κοινοτική έννομη τάξη», Εκδ. Επιτροπής των Ευρωπαϊκών Κοινοτήτων, 1981
- Nanda (επιμ.), P., «European Union law after Maastricht: a practical guide for lawyers outside the common market», Εκδ. Kluwer, 1996
- Nieva, R., «Most Facebook users hit by Cambridge Analytica scandal are Californians», CNET, 2018
- Reidenberg et al., J., «Ambiguity in Privacy Policies and the Impact of Regulation», σε: Journal of Legal Studies, v. 45, 2015
- Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., ... & Ramanath, R. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. Berkeley Tech. LJ
- Rosenberg, M., «How Trump Consultants Exploited the Facebook Data of Millions», The New York Times, 2018
- Schlee, C., «Targeted Advertising Technologies in the ICT Space: A Use Case Driven Analysis», Springer Science & Business Media, 2013
- Shannon, C. E. (2001). A mathematical theory of communication. Bell system technical journal, 27(3)
- Silic, M., Barlow, J., & Ormond, D. (2015). Warning! A comprehensive model of the effects of digital information security warning messages.
- Singel, R., «Online Tracking Firm Settles Suit Over Undeletable Cookies», Wired, 2010
- Skinner, G., Han, S., & Chang, E. (2005, July). A framework of privacy shield in organizational information systems. In International Conference on Mobile Business (ICMB'05) (pp. 647-650). IEEE.
- Story, L., «AOL Brings Out the Penguins to Explain Ad Targeting», The New York Times, 2008
- Thomas, J., «Programming, filtering, adblocking: advertising and media automation», Media International Australia (περιοδικά), τεύχος 166 (1), 2017
- Tucker, «Social networks, personalized advertising, and privacy controls», Journal of Marketing Research, τεύχος 51 (5), 2014
- Waldman, A. E., (2016) “Privacy, Notice and Design”

- Wogalter, M. and Mayhorn, C., (2017) “Warning design,” in Information Design: Research and Practice, A. Black, P. Luna, O. Lund, and S. Walker, Eds.
- Wogalter, M. S. (1998). Factors influencing the effectiveness of warnings. In Visual Information for everyday use CRC Press.
- Wogalter, M. S., DeJoy, D., & Laughery, K. R. (2005). Organizing theoretical framework: a consolidated communication-human information processing (C-HIP) model. In Warnings and risk communication CRC Press.
- Zorz, Z., «Is it possible for data to be both anonymous and useful?», Help Net Security, 2009

Διαδικτυακές πηγές:

- «Η Google προειδοποιεί πως οι αλλαγές στην ιδιωτικότητα των προσωπικών δεδομένων θα μπορούσαν να αποτελέσουν πλήγμα για την εταιρία», 6/2/2019, ired.gr, Διαθέσιμο σε: https://www.ired.gr/blog/item/7391-i-google-proeidopoiei-pos-oi-allages-stin-idiotikotita-ton-prosopikon-dedomenon-tha-mporousan-na-apotelesoun-pligma-gia-tin-etairia.html
- «Η Google διέρρευσε προσωπικά δεδομένα χρηστών της με λογαριασμούς στο Google+», 8/10/2018, Η Καθημερινή, Διαθέσιμο σε: https://www.kathimerini.gr/988767/article/epikairothta/kosmos/h-google-dierreyse-proswpika-dedomena-xrhstwn-ths-me-logariasmoys-sto-google
- «Τέλος από σήμερα για το Google+ το μέσο κοινωνικής δικτύωσης που ατύχησε», 2/4/2019, news247, Διαθέσιμο σε: https://www.news247.gr/technologia/google-telos-meso-koinonikis-diktyosis-atychise.6708676.amp.html
- C-131/12, Google Spain, 13 Μαϊού 2014, Διαθέσιμο σε: http://curia.europa.eu/juris/document/document.jsf;jsessionid=8B16E4B7657EA3BB00C0B34D0E9
- Case C-131/12, Ct.J.EU (Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González) Διαθέσιμο σε: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d543eebb46b73f4314b9d5db2974a717d8.e34KaxiLc3qMb40Rch0SaxuSbhn0?text=&docid=138782&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=396824
- Data Protection Network, (2017) “GDPR Data Retention Quick Guide,” https://www.dpnetwork.org.uk/gdpr-data-retention-guide/
- EU Parliament, (2018) “Home Page of EU GDPR,” https://www.eugdpr.org/

- Europa, Press Release Database, 2014, Διαθέσιμο σε: http://europa.eu/rapid/search.htm
- European data protection supervisor (2018) The History of the General Data Protection Regulation [online] available at: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation
- Google to Accelerate Closure of Google+ Social Network After Finding New Software Bug, 10/12/2018, Wall Street General, Διαθέσιμο σε: https://www.google.com/amp/s/www.wsj.com/amp/articles/google-to-accelerate-closure-of-google-social-network-1544465975
- Information Commissioner's Office, (2018) "Preparing for the General Data Protection Regulation (GDPR) - 12 Steps to Take Now, https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- Information Commissioner's Office, (2018) "Special Category Data," https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/?q=best+practice
- Intersoft Consulting, (2016) "Art. 6 GDPR Lawfulness of processing," https://gdpr-info.eu/art-6-gdpr/
- Karchimakis, E., «The Right to be Forgotten», Constitutionalism.gr, Διαθέσιμο σε: https://www.constitutionalism.gr/karchimakis-the-right-to-be-forgotten/
- O' Flaherty, K., 9/10/2018, «Google+ Security Bug -- What Happened, Who Was Impacted And How To Delete Your Account», Forbes, Διαθέσιμο σε: https://www.forbes.com/sites/kateoflahertyuk/2018/10/09/google-plus-breach-what-happened-who-was-impacted-and-how-to-delete-your-account/amp/
- The Organization for Economic Co-Operation and Development, «Guidelines on the Protection of Privacy and Transborder Flows of Personal Data», Διαθέσιμο σε: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
- Ενοποιημένη απόδοση της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:12012E/TXT
- Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, «Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης», Διαθέσιμο σε: http://www.europarl.europa.eu/charter/pdf/text_el.pdf