Η Προστασία Προσωπικών Δεδομένων στην Ψηφιακή Εποχή

Ανάλυση του GDPR και η Εφαρμογή του στην Ελλάδα

Μάθημα: Δίκαιο Πληροφορικής
Συγγραφέας: Φοιτητής/τρια
Φεβρουάριος 2026

Πίνακας Περιεχομένων

1. Εισαγωγή

Η προστασία των προσωπικών δεδομένων αποτελεί ένα από τα κορυφαία νομικά ζητήματα της σύγχρονης ψηφιακής εποχής. Η εκθετική αύξηση της συλλογής, επεξεργασίας και αποθήκευσης δεδομένων από δημόσιους και ιδιωτικούς φορείς έχει δημιουργήσει ένα περιβάλλον στο οποίο η ιδιωτικότητα των πολιτών απειλείται σε πρωτόγνωρο βαθμό (Solove, 2008).

Η Ευρωπαϊκή Ένωση αντέδρασε με την υιοθέτηση του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR - Κανονισμός 2016/679), ο οποίος τέθηκε σε εφαρμογή τον Μάιο 2018 και αποτελεί το πιο φιλόδοξο νομοθετικό πλαίσιο προστασίας προσωπικών δεδομένων παγκοσμίως (Voigt & von dem Bussche, 2017). Στην Ελλάδα, ο Ν. 4624/2019 ενσωμάτωσε τον Κανονισμό στο εθνικό δίκαιο.

Η παρούσα εργασία εξετάζει τις βασικές αρχές και μηχανισμούς του GDPR, αναλύει ζητήματα πρακτικής εφαρμογής στην ελληνική έννομη τάξη, και αξιολογεί τις προκλήσεις που προκύπτουν από τις αναδυόμενες τεχνολογίες τεχνητής νοημοσύνης.

2. Θεωρητικό Πλαίσιο

2.1 Η Έννοια των Προσωπικών Δεδομένων

Σύμφωνα με το άρθρο 4 παρ. 1 του GDPR, ως προσωπικά δεδομένα ορίζεται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (υποκείμενο δεδομένων). Ο ορισμός είναι ευρύτατος, καλύπτοντας όχι μόνο παραδοσιακά στοιχεία ταυτότητας αλλά και

ψηφιακά αναγνωριστικά, δεδομένα τοποθεσίας, cookies και μεταδεδομένα επικοινωνιών (Bygrave, 2014).

Ιδιαίτερη κατηγορία αποτελούν τα ευαίσθητα δεδομένα (άρθρο 9 GDPR), που περιλαμβάνουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκευτικές πεποιθήσεις, βιομετρικά δεδομένα, δεδομένα υγείας και σεξουαλικό προσανατολισμό. Η επεξεργασία αυτών των δεδομένων κατ' αρχήν απαγορεύεται, με αυστηρά περιορισμένες εξαιρέσεις.

2.2 Ο Γενικός Κανονισμός (GDPR)

Ο GDPR εισήγαγε μια σειρά θεμελιωδών αρχών για την επεξεργασία δεδομένων: νομιμότητα, αντικειμενικότητα και διαφάνεια, περιορισμός σκοπού, ελαχιστοποίηση δεδομένων, ακρίβεια, περιορισμός αποθήκευσης, ακεραιότητα και εμπιστευτικότητα, και λογοδοσία (άρθρο 5). Αυτές οι αρχές αποτελούν τον πυρήνα κάθε νόμιμης επεξεργασίας δεδομένων.

Βασική καινοτομία του Κανονισμού αποτελεί η αρχή της λογοδοσίας (accountability), η οποία μεταθέτει το βάρος απόδειξης στον υπεύθυνο επεξεργασίας. Επιπλέον, ο GDPR εισήγαγε το δικαίωμα στη φορητότητα δεδομένων (data portability), το δικαίωμα στη λήθη (right to erasure), και την υποχρέωση γνωστοποίησης παραβιάσεων εντός 72 ωρών (Kuner et al., 2020).

Τα πρόστιμα του GDPR είναι τα υψηλότερα σε διεθνές επίπεδο: έως 20 εκατομμύρια ευρώ ή 4% του παγκόσμιου ετήσιου κύκλου εργασιών. Χαρακτηριστικά, η Meta (Facebook) τιμωρήθηκε με πρόστιμο 1,2 δισ. ευρώ το 2023 από την ιρλανδική DPC.

2.3 Εφαρμογή στην Ελλάδα — Ν. 4624/2019

Ο Ν. 4624/2019 αποτελεί τον εθνικό εφαρμοστικό νόμο του GDPR στην Ελλάδα. Ο νόμος ρυθμίζει ειδικότερα ζητήματα όπως η ηλικία συναίνεσης παιδιών (15 έτη), η επεξεργασία δεδομένων για δημοσιογραφικούς σκοπούς, και η λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

Η ΑΠΔΠΧ αποτελεί ανεξάρτητη αρχή με αρμοδιότητα εποπτείας και επιβολής του GDPR στη χώρα. Κατά την περίοδο 2019-2025, η Αρχή έχει εκδώσει πληθώρα αποφάσεων, με αξιοσημείωτα πρόστιμα σε τηλεπικοινωνιακές εταιρείες, τράπεζες και δημόσιους φορείς (Ιγγλεζάκης, 2022).

3. Ανάλυση Βασικών Ζητημάτων

Ένα από τα κεντρικά ζητήματα εφαρμογής του GDPR αφορά τη νομική βάση επεξεργασίας. Το άρθρο 6 προβλέπει έξι νομικές βάσεις: συναίνεση, εκτέλεση σύμβασης, έννομη υποχρέωση, ζωτικό συμφέρον, δημόσιο συμφέρον και έννομο συμφέρον. Στην πράξη, η επιλογή κατάλληλης νομικής βάσης αποτελεί συχνά πηγή σύγχυσης και λαθών (Irene Kamara & De Hert, 2018).

Ιδιαίτερα σημαντικό ζήτημα αποτελεί η συγκατάθεση. Ο GDPR απαιτεί η συγκατάθεση να είναι ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει. Τα cookie banners που εμφανίζονται σε ιστοσελίδες αποτελούν χαρακτηριστικό παράδειγμα, όπου η πρακτική εφαρμογή συχνά υστερεί σε σχέση με τις νομικές απαιτήσεις. Η πρακτική των dark patterns — σχεδιαστικών τεχνικών που οδηγούν τον χρήστη σε αποδοχή — έχει αποτελέσει αντικείμενο κριτικής και επιβολής κυρώσεων.

Η ανάπτυξη τεχνολογιών τεχνητής νοημοσύνης δημιουργεί νέες προκλήσεις. Τα συστήματα AI απαιτούν μεγάλους όγκους δεδομένων για εκπαίδευση, θέτοντας ζητήματα σχετικά με τον σκοπό επεξεργασίας, τη διαφάνεια αλγορίθμων και την αυτοματοποιημένη λήψη αποφάσεων (άρθρο 22 GDPR). Ο AI Act (2024) της ΕΕ επιχειρεί να αντιμετωπίσει αυτά τα ζητήματα, αλλά η αλληλεπίδρασή του με τον GDPR παραμένει υπό διαμόρφωση.

4. Νομολογία και Πρακτική Εφαρμογή

Η νομολογία του ΔΕΕ και των εθνικών εποπτικών αρχών έχει διαμορφώσει σημαντικά τη ερμηνεία του GDPR. Η απόφαση Schrems II (C-311/18) κατέστησε άκυρο το Privacy Shield, επηρεάζοντας δραματικά τις διατλαντικές μεταφορές δεδομένων. Στην Ελλάδα, η ΑΠΔΠΧ επέβαλε πρόστιμο 150.000 ευρώ σε τηλεπικοινωνιακή εταιρεία για παράνομη αποστολή marketing μηνυμάτων χωρίς συγκατάθεση.

Ενδιαφέρον παρουσιάζουν οι αποφάσεις που αφορούν τη χρήση AI στην αξιολόγηση πιστοληπτικής ικανότητας (SCHUFA, C-634/21), όπου το ΔΕΕ αναγνώρισε ότι η αυτοματοποιημένη βαθμολόγηση αποτελεί αυτοματοποιημένη λήψη απόφασης κατά την έννοια του άρθρου 22.

Στο ελληνικό πεδίο, η ΑΠΔΠΧ εξέδωσε κατευθυντήριες γραμμές για τη χρήση cookies (Απόφαση 25/2023), τη βιντεοεπιτήρηση σε χώρους εργασίας, και τη νόμιμη παρακολούθηση ηλεκτρονικών επικοινωνιών εργαζομένων, διαμορφώνοντας σταδιακά ένα πιο σαφές πλαίσιο εφαρμογής.

5. Συμπεράσματα — Προτάσεις

Ο GDPR αποτελεί αναμφίβολα ένα ορόσημο στην προστασία των προσωπικών δεδομένων σε παγκόσμιο επίπεδο. Η εφαρμογή του στην Ελλάδα, μέσω του Ν. 4624/2019, έχει σημειώσει αξιοσημείωτη πρόοδο, αν και εξακολουθούν να υπάρχουν σημαντικές προκλήσεις, ιδίως στον δημόσιο τομέα και τις μικρομεσαίες επιχειρήσεις.

Η ανάπτυξη τεχνολογιών τεχνητής νοημοσύνης αναμένεται να αυξήσει τις προκλήσεις, καθιστώντας αναγκαία τη συνεχή επικαιροποίηση του νομοθετικού πλαισίου. Η αλληλεπίδραση GDPR και AI Act θα αποτελέσει κρίσιμο πεδίο εξέλιξης τα επόμενα χρόνια.

Προτείνεται η ενίσχυση της ΑΠΔΠΧ με πρόσθετους πόρους, η συστηματική εκπαίδευση επιχειρήσεων και δημόσιων φορέων, και η ανάπτυξη εξειδικευμένης καθοδήγησης για τις αναδυόμενες τεχνολογίες.

Βιβλιογραφία

Bygrave, L.A. (2014). Data Privacy Law: An International Perspective. Oxford University Press.

Ιγγλεζάκης, Ι. (2022). Δίκαιο Πληροφορικής (5η εκδ.). Σάκκουλας.

Kamara, I. & De Hert, P. (2018). Data Protection Certification Mechanisms. In EU General Data Protection Regulation. Springer.

Kuner, C. et al. (2020). The EU General Data Protection Regulation: A Commentary. Oxford University Press.

Solove, D.J. (2008). Understanding Privacy. Harvard University Press.

Voigt, P. & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer.