Υποβολή παρατηρήσεων της Homo Digitalis στο πλαίσιο της δημόσιας διαβούλευσης για το Εθνικό Στρατηγικό Σχέδιο Οδικής Ασφάλειας Ελλάδα 2030

Αθήνα, 9 Ιουνίου 2022

Η Συντακτική Ομάδα: Καλλιόπη Τερζίδου, Κλαίρη Γραμμένου, Αιμιλία Γιβροπούλου, Ιωάννης Κροντήρης, Φωτεινή Μπαλαδήμα.

Ζητήματα που προκύπτουν από τη χρήση νέων τεχνολογιών για την οδική ασφάλεια

1. **Επεξεργασία προσωπικών δεδομένων**

Το Εθνικό Στρατηγικό Σχέδιο Οδικής Ασφάλειας περιλαμβάνει τη χρήση νέων τεχνολογιών, συμπεριλαμβανομένων των καμερών επιτήρησης, τηλεματικής, ειδικών αισθητήρων, και μέσων κοινωνικής δικτύωσης. Οι συγκεκριμένες τεχνολογίες θα συλλέγουν και θα επεξεργάζονται, μεταξύ άλλων, δεδομένα προσωπικού χαρακτήρα και επομένως θα πρέπει να συμμορφώνονται με τους σχετικούς κανονισμούς (βλ. Γενικός Κανονισμός Προσωπικών Δεδομένων, στο εξής: ΓΚΠΔ, καθώς και την Οδηγία 2010/40/ΕΕ περί πλαισίου ανάπτυξης των Συστημάτων Ευφυών Μεταφορών στον τομέα των οδικών μεταφορών και των διεπαφών με άλλους τρόπους μεταφοράς).

Συγκεκριμένα, οι αναφερόμενες τεχνολογίες συλλέγουν δεδομένα τα οποία μπορούν να ταυτοποιήσουν άμεσα ή έμμεσα τον οδηγό ή τους επιβάτες του αυτοκινήτου (Άρθρο 4 σημείο 1 ΓΚΠΔ). Άμεση ταυτοποίηση είναι δυνατή μέσω της επεξεργασίας δεδομένων, όπως του ονόματος, της εικόνας, ή του αριθμού διπλώματος οδήγησης. Έμμεση ταυτοποίηση μπορεί να γίνει μέσω της συλλογής ή επεξεργασίας δεδομένων, όπως δεδομένα σχετικά με τον τρόπο οδήγησης, τη διανυθείσα απόσταση, ή δεδομένα σχετικά με τη φθορά των μερών του οχήματος. Τα δεδομένα αυτά μπορούν αν διασταυρωθούν με δεδομένα όπως ο αριθμός της πινακίδας του αυτοκινήτου και εμμέσως να οδηγήσουν στην ταυτοποίηση του υποκειμένου επεξεργασίας. Επίσης, παρουσιάζεται πιθανή η επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα (Άρθρο 9 παρ. 1 ΓΚΠΔ), όπως βιομετρικά δεδομένα μέσω των ειδικών αισθητήρων, και άλλων ιδιαίτερων κατηγοριών δεδομένων, όπως δεδομένα θέσης (που μπορεί να συνεπάγεται την αποκάλυψη ευαίσθητων πληροφοριών, όπως εθνικότητα ή θρησκεία) και δεδομένα σχετικά με (τροχαία) αδικήματα. Ειδικά για αυτές τις κατηγορίες προσωπικών δεδομένων πρέπει να εφαρμόζονται οι εγγυήσεις των άρθρων 9 και 10 του ΓΚΠΔ, δηλαδή επεξεργασία με ειδική νόμιμη βάση .

Πέρα από τη συλλογή των προσωπικών δεδομένων, η επεξεργασία τους μπορεί να συνίσταται και σε περαιτέρω ενέργειες (Άρθρο 4 παρ. 2 ΓΚΠΔ), όπως η καταχώριση και αποθήκευση προσωπικών

δεδομένων εντός του οχήματος, η μετάδοση σε συσκευές που συνδέονται με το αυτοκίνητο, όπως τα έξυπνα τηλέφωνα, ή η διαβίβαση σε οντότητες, συμπεριλαμβανομένων των κατασκευαστών οχημάτων, διαχειριστών υποδομής, ασφαλιστικών εταιρειών, και επισκευαστών αυτοκινήτων. Για να είναι σύννομη η επεξεργασία των προσωπικών δεδομένων, πρέπει να βασίζεται σε κάποια νόμιμη βάση (Άρθρο 6 ΓΚΠΔ). Κατά κανόνα, η επεξεργασία πρέπει να γίνεται με την έγκυρη και ενημερωμένη συγκατάθεση του υποκειμένου επεξεργασίας ως προς, μεταξύ άλλων, την αποθήκευση και διαβίβαση των δεδομένων στου κατασκευαστές των οχημάτων και τις δημόσιες υπηρεσίες. Η συγκατάθεση πρέπει να δίνεται χωριστά, για συγκεκριμένους σκοπούς και δεν μπορεί να συνδέεται, παραδείγματος χάριν, με τη σύμβαση αγοράς ή μίσθωσης νέου αυτοκινήτου (άρθρο 7, παρ. 4 ΓΚΠΔ). Η συγκατάθεση πρέπει να μπορεί να ανακαλείται εξίσου εύκολα όπως παρέχεται.

Επιπλέον, η επεξεργασία δεδομένων πρέπει να γίνεται για συγκεκριμένους σκοπούς, να περιορίζεται στο αναγκαίο μέτρο ανάλογα με τους προσδιορισμένους σκοπούς, και να διασφαλίζεται η ακρίβεια των δεδομένων. Τα δεδομένα πρέπει να επικαιροποιούνται, να αποθηκεύονται για συγκεκριμένο χρονικό διάστημα, και να διασφαλίζεται η ακεραιότητα και εμπιστευτικότητα τους κατά την επεξεργασία (Άρθρο 5 ΓΚΠΔ). Οι συγκεκριμένες αρχές πρέπει να εφαρμόζονται πάραυτα σε περιπτώσεις συλλογής προσωπικών δεδομένων από τους ειδικούς αισθητήρες και επεξεργασίας τους μέσω μεθόδων τεχνητής νοημοσύνης, όπως η μηχανική μάθηση, όπου ενέχει ο κίνδυνος υπερβολικής συλλογής δεδομένων για την εκπαίδευση του αλγορίθμου και την ακρίβεια των προβλέψεων του.

Σημαντική είναι η αρχή ελαχιστοποίησης (Άρθρο 5.1.γ ΓΚΠΔ) όσον αφορά την αξιοποίηση δεδομένων από ειδικούς αισθητήρες επί της της οδού, επί των οχημάτων και επί των έξυπνων κινητών τηλεφώνων καθώς και από την ανάλυση εικόνας βίντεο, τα μέσα κοινωνικής δικτύωσης και την τηλεματική, όπως αναφέρεται στη σελίδα 60 του Σχεδίου. Θα πρέπει να υπάρχει ο ακριβής προσδιορισμός της ανάγκης αξιοποίησης δεδομένων, για παράδειγμα, από τα μέσα κοινωνικής δικτύωσης. Ποιός είναι ο σκοπός της αξιοποίησης των εν λόγω δεδομένων; Είναι η επεξεργασία τους αναγκαία;

Επίσης, στο μέτρο που υπάρχει συνδεσιμότητα των οχημάτων με εξωτερικά δίκτυα και συστήματα, η ασφάλεια των προσωπικών δεδομένων κατά τη διάρκεια της επεξεργασίας τους πρέπει να διασφαλίζεται από ενδεχόμενες κυβερνοεπιθέσεις μέσω εκμετάλλευσης των τρωτών σημείων τους. Τέλος, οι ανωτέρω εγγυήσεις πρέπει να διασφαλίζονται ήδη από τον σχεδιασμό των εφαρμοσμένων τεχνολογιών και εξ ορισμού (Άρθρο 25 ΓΚΔΠ).

Το Εθνικό Στρατηγικό Σχέδιο Οδικής Ασφάλειας προβλέπει τη συλλογή δεδομένων με τεχνολογίες τηλεματικής. Οι Τεχνολογίες αυτές συλλέγουν και επεξεργάζονται βιομετρικά δεδομένα για τα οποία είναι απαραίτητη η ειδική νόμιμη βάση υπό τον έλεγχο της επίσημης αρχής. Βάσει τα ανωτέρω και ενώ ο Κανονισμός περί Τεχνητής Νοημοσύνης βρίσκεται υπό συζήτηση, πρέπει να ληφθεί υπόψιν πως τέτοιες τεχνολογίες συνιστούν τεχνολογίες υψηλού κινδύνου. Για τον λόγο αυτό υπάρχει η ανάγκη ειδικής μεταχείρισης και η εφαρμογή περαιτέρω μέτρων προστασίας.

Για την καλύτερη προστασία των προσωπικών δεδομένων κατά την επεξεργασία τους, είναι δυνατή η εφαρμογή ορισμένων πρακτικών, όπως η τοπική επεξεργασία των δεδομένων που επιτρέπει τα

υποκείμενα επεξεργασίας να έχουν τον πλήρη έλεγχο των προσωπικών τους δεδομένων. Επιπρόσθετα, η ανωνυμοποίηση των δεδομένων επιτρέπει την επεξεργασία τους χωρίς περιορισμούς αφού παύουν να οδηγούν στην ταυτοποίηση των υποκειμένων και άρα δεν χαρακτηρίζονται πλέον ως προσωπικά (Άρθρο 4 σημείο 5 ΓΚΠΔ). Σε περίπτωση ανωνυμοποίησης, ο υπεύθυνος επεξεργασίας θα πρέπει να εφαρμόσει τεχνικές οι οποίες εγγυώνται την ελαχιστοποίηση της πιθανότητας να υπάρξει εκ νέου ταυτοποίηση των δεδομένων. Η Homo Digitalis αναγνωρίζει την τεχνική ανωνυμοποίησης διαφορικής ιδιωτικότητας (differential privacy) ως την τεχνική που παρέχει αυτές τις εγγυήσεις στο βέλτιστο βαθμό.

Τέλος, πρέπει να διενεργούνται εκτιμήσεις αντικτύπου όταν ο κίνδυνος της ασφάλειας των συστημάτων και άρα των δεδομένων που επεξεργάζονται εκτιμάται υψηλός (Άρθρα 35 και 36 ΓΚΠΔ).

2. Χρήση συστημάτων τεχνητής νοημοσύνης

Στο μέτρο που χρησιμοποιούνται συστήματα τεχνητής νοημοσύνης, όπως συστήματα μηχανικής εκμάθησης για την μετατροπή δεδομένων σε χρήσιμους δείκτες, οι ακόλουθες αρχές πρέπει να τηρούνται κατά τον σχεδιασμό, χρήση, και επανασχεδιασμό τους:

- Σεβασμός της ανθρώπινης αυτονομίας
- Πρόληψη βλάβης
- Δικαιοσύνη
- Επεξηγησιμότητα

Για την τήρηση αυτών των αρχών, οι εξής απαιτήσεις πρέπει να εφαρμόζονται:

- Ανθρώπινη παρέμβαση και εποπτεία: Συμπεριλαμβανομένων των θεμελιωδών δικαιωμάτων, της ανθρώπινης παρέμβασης και της ανθρώπινης εποπτείας·
- Τεχνική στιβαρότητα και ασφάλεια: Συμπεριλαμβανομένων της ανθεκτικότητας σε επιθέσεις και της προστασίας, του εφεδρικού σχεδίου και της γενικής ασφάλειας, της ακρίβειας, της αξιοπιστίας και της αναπαραγωγιμότητας·
- Ιδιωτική ζωή και διακυβέρνηση των δεδομένων: Συμπεριλαμβανομένων του σεβασμού της ιδιωτικής ζωής, της ποιότητας και της ακεραιότητας των δεδομένων και της πρόσβασης στα δεδομένα·
- Διαφάνεια: Συμπεριλαμβανομένης της ανιχνευσιμότητας, της επεξηγησιμότητας και της επικοινωνίας·
- Πολυμορφία, απαγόρευση των διακρίσεων και δικαιοσύνη: Συμπεριλαμβανομένων της αποφυγής της αθέμιτης μεροληψίας, της προσβασιμότητας και του καθολικού σχεδιασμού και της συμμετοχής των ενδιαφερόμενων μερών·
- Κοινωνική και περιβαλλοντική ευημερία: Συμπεριλαμβανομένων της βιωσιμότητας και της φιλικότητας προς το περιβάλλον, των κοινωνικών επιπτώσεων, της κοινωνίας και της δημοκρατίας·
- Λογοδοσία: Συμπεριλαμβανομένων της ελεγξιμότητας, της ελαχιστοποίησης και της γνωστοποίησης των αρνητικών επιπτώσεων, των αντισταθμιστικών ρυθμίσεων και της

έννομης προστασίας.

Ειδικότερα όσον αφορά στις τεχνολογίες τηλεματικής που συλλέγουν και επεξεργάζονται βιομετρικά δεδομένα με σκοπό την παρακολούθηση της συμπεριφοράς και κατάστασης του οδηγού, αυτές οφείλουν να περιορίζονται στη συλλογή των απολύτως αναγκαίων δεδομένων και να χρησιμοποιούνται σε περιορισμένες, συγκεκριμένες καταστάσεις. Ο Κανονισμός περί Τεχνητής Νοημοσύνης βρίσκεται υπό συζήτηση σε ευρωπαϊκό επίπεδο. Οφείλουμε να λάβουμε υπόψη πως τέτοιες τεχνολογίες ενδέχεται να χαρακτηριστούν ως τεχνολογίες "υψηλού κινδύνου" με αποτέλεσμα να χρήζουν ειδικής και προσεκτικής μεταχείρισης εξαιτίας του κινδύνου που φέρουν όσον αφορά στα εσφαλμένα αποτελέσματα και λειτουργίες που διακινδυνεύουν την ακεραιότητα του οδηγού.

Πηγές

1. Κατευθυντήριες γραμμές 01/2020 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των συνδεδεμένων οχημάτων και των εφαρμογών που σχετίζονται με την κινητικότητα (https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_el.pdf)
2. Automating Society Report 2020, Εξελίξεις στην Ελλάδα (https://automatingsociety.algorithmwatch.org/report2020/greece/)
3. Autonomous Vehicles: Data Protection and Ethical Considerations (https://dl.acm.org/doi/abs/10.1145/3385958.3430481)
4. Ασφάλεια στον κυβερνοχώρο και ανθεκτικότητα των έξυπνων αυτοκινήτων· (https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars)
5. Ψήφισμα σχετικά με την προστασία δεδομένων σε αυτοματοποιημένα και συνδεδεμένα οχήματα (https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf)
6. Κατευθυντήριες γραμμές δεοντολογίας για αξιόπιστη τεχνητή νοημοσύνη, Ομάδα εμπειρογνωμόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη, 2018 (https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_EL.pdf)
7. Ethics guidelines for trustworthy AI (https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai)