ΣΧΟΛΙΑΣΜΟΣ ΤΗΣ ΑΠΟΦΑΣΗΣ C-162/22 ΤΟΥ ΔΙΚΑΣΤΗΡΙΟΥ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ (ΔΕΕ) – ΑΠΑΓΟΡΕΥΣΗ ΧΡΗΣΗΣ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΕΡΕΥΝΩΝ ΣΧΕΤΙΚΩΝ ΜΕ ΤΗ ΔΙΑΦΘΟΡΑ ΣΤΟΝ ΔΗΜΟΣΙΟ ΤΟΜΕΑ

Θεόδωρος Ρέντζιος
Υπ. Δρ. Παντείου Πανεπιστημίου
Υπότροφος Ernst & Young Greece

ΠΕΡΙΛΗΨΗ

Η απόφαση της 7ης Σεπτεμβρίου 2023 στην υπόθεση C-162/22 (*Lietuvos Respublikos generalinė prokuratūra*) προστίθεται στον μακρύ κατάλογο αποφάσεων του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ) σχετικά με το πεδίο εφαρμογής της υποχρέωσης των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών να διατηρούν δεδομένα κίνησης και θέσης, η οποία απορρέει από το άρθρο 15 παράγραφος 1 της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[1], (Οδηγία ePrivacy). Η εν λόγω διάταξη επιτρέπει στα κράτη μέλη να θεσπίζουν νομοθετικά μέτρα που περιορίζουν θεμελιώδη δικαιώματα, όπως το δικαίωμα στην προστασία των προσωπικών δεδομένων και του απορρήτου των επικοινωνιών, ενώ απαιτεί από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών να

[1] 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, όπως τροποποιήθηκε με την Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009 (Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ 2002, L 201, σελ. 37).

διατηρούν δεδομένα προερχόμενα από ηλεκτρονικές επικοινωνίες για την επιδίωξη των στόχων δημοσίου συμφέροντος που απαριθμούνται στην Οδηγία, συμπεριλαμβανομένης της δίωξης σοβαρών ποινικών αδικημάτων.

Στη σχολιαζόμενη απόφαση, το ΔΕΕ έκρινε ότι το άρθρο 15 παρ. 1 της προρρηθείσας Οδηγίας, ερμηνευόμενο υπό το πρίσμα των άρθρων 7 (σεβασμός του απορρήτου των επικοινωνιών), 8 (προστασία των δεδομένων προσωπικού χαρακτήρα), 11 (ελευθερία της έκφρασης) και 52 παρ. 1 (περιορισμοί στην άσκηση των δικαιωμάτων και ελευθεριών υπό την επιφύλαξη της αρχής της αναλογικότητας) του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ΧΘΔΕ), έχει την έννοια ότι δεν επιτρέπει να χρησιμοποιούνται, στο πλαίσιο ερευνών για υπηρεσιακά παραπτώματα συνδεόμενα με διαφθορά, δεδομένα προσωπικού χαρακτήρα σχετικά με ηλεκτρονικές επικοινωνίες τα οποία διατηρήθηκαν, κατ' εφαρμογή νομοθετικού μέτρου, από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών και τα οποία εν συνεχεία τέθηκαν στη διάθεση των αρμόδιων αρχών, κατ' εφαρμογή του ίδιου αυτού μέτρου, για την καταπολέμηση της σοβαρής εγκληματικότητας.

Ι. ΑΝΑΛΥΣΗ ΤΗΣ ΑΠΟΦΑΣΗΣ

1. ΤΑ ΠΡΑΓΜΑΤΙΚΑ ΠΕΡΙΣΤΑΤΙΚΑ

Στο πλαίσιο της διαδικασίας που οδήγησε στο προδικαστικό ερώτημα, υποβλήθηκε αίτηση ακύρωσης απόφασης της Γενικής Εισαγγελίας της Λιθουανίας, με την οποία η τελευταία έπαυσε από τα καθήκοντά του εισαγγελέα, ο οποίος υπηρετούσε σε περιφερειακή εισαγγελία της χώρας. Η εν λόγω διοικητική κύρωση του επιβλήθηκε διότι φέρεται να παρέσχε παρανόμως πληροφορίες σε έναν ύποπτο και στον δικηγόρο του στο πλαίσιο ανάκρισης που διενεργούσε. Το υπηρεσιακό παράπτωμα που προσάπτεται στον εισαγγελέα και οδήγησε στην επιβολή της προαναφερθείσας κύρωσης στοιχειοθετήθηκε βάσει δεδομένων που είχαν διατηρηθεί από παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών.

Σημειώνεται, επίσης, ότι με εισαγγελική παραγγελία είχε διαταχθεί η παρακολούθηση και η καταγραφή πληροφοριών που διαβιβάστηκαν μέσω δικτύων ηλεκτρονικών επικοινωνιών και αφορούσαν στον δικηγόρο και τον εντολέα του, στους οποίους φέρεται ο προσφεύγων εισαγγελέας να είχε παράσχει πληροφορίες. Ωστόσο, αφ' ης στιγμής λαμβάνονται τα εν λόγω δεδομένα, αυτά χρησιμοποιήθηκαν εν προκειμένω για διοικητική διαδικασία άλλη από την ποινική διαδικασία, στο πλαίσιο της οποίας διατάχθηκε η παρακολούθηση των επικοινωνιών και η σχετική διατήρηση και διαβίβαση των δεδομένων.

2. ΤΟ ΠΡΟΔΙΚΑΣΤΙΚΟ ΕΡΩΤΗΜΑ

Στη σχολιαζόμενη υπόθεση τέθηκε το ερώτημα κατά πόσον τα δεδομένα που διατηρούν και διαθέτουν οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών για τη δίωξη ποινικών αδικημάτων θα μπορούσαν επίσης να χρησιμοποιηθούν σε πειθαρχικές-διοικητικές διαδικασίες σχετικές με τη

διερεύνηση παράβασης καθήκοντος, δεδομένου ότι, σύμφωνα με το άρθρο 19 παρ. 1 περ. 5 του λιθουανικού νόμου περί πληροφοριών ποινικού ενδιαφέροντος, οι πληροφορίες που προέρχονται από ανακριτικές πράξεις που αφορούν σε πράξη με χαρακτηριστικά αδικήματος συνδεόμενου με διαφθορά μπορούν να αποχαρακτηριστούν, με τη σύμφωνη γνώμη της εισαγγελικής αρχής, και να χρησιμοποιηθούν στο πλαίσιο έρευνας για πειθαρχικά ή υπηρεσιακά παραπτώματα.

Στο πλαίσιο αυτό, ο προσφεύγων σταχυολόγησε δύο βασικά ζητήματα: *Πρώτον*, την πρόσβαση σε δεδομένα που διατηρούν οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών για σκοπούς άλλους από την καταπολέμηση της σοβαρής εγκληματικότητας και την αποτροπή σοβαρών απειλών κατά της δημόσιας ασφάλειας και *δεύτερον*, τη χρήση των δεδομένων αυτών, μετά την απόκτηση της εν λόγω πρόσβασης, για τη διερεύνηση υπηρεσιακών παραπτωμάτων. Έτσι, υποστήριξε ότι η χρήση δεδομένων που καθιστούν δυνατή την ταυτοποίηση της πηγής και του προορισμού μιας τηλεφωνικής επικοινωνίας από το σταθερό ή το κινητό τηλέφωνο ενός υπόπτου σε υποθέσεις που αφορούν υπηρεσιακά παραπτώματα και όχι σε ποινικές υποθέσεις ή σε υποθέσεις που τελούν σε άμεση σχέση με τη διάπραξη σοβαρών ποινικών αδικημάτων συνιστά αδικαιολόγητη επέμβαση στα θεμελιώδη δικαιώματα που κατοχυρώνονται στο ενωσιακό δίκαιο.

Στην παρούσα υπόθεση, το Ανώτατο Διοικητικό Δικαστήριο της Λιθουανίας[2], ενώπιον του οποίου ασκήθηκε έφεση, ζητεί, κατ' ουσίαν να διευκρινιστεί από το ΔΕΕ εάν συνάδει προς την Οδηγία ePrivacy η χρήση, στο πλαίσιο πειθαρχικών-διοικητικών ερευνών σχετικών με υπηρεσιακά παραπτώματα συνδεόμενα με διαφθορά, δεδομένων προσωπικού χαρακτήρα, τα οποία αφενός σχετίζονται με ηλεκτρονικές επικοινωνίες και αφετέρου διατηρήθηκαν, κατ' εφαρμογή νομοθετικού μέτρου, από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, ενώ εν συνεχεία τέθηκαν στη διάθεση των αρμόδιων αρχών, κατ' εφαρμογή του ίδιου αυτού μέτρου, για την καταπολέμηση της σοβαρής εγκληματικότητας.

Επισημαίνεται ότι, εν προκειμένω, δεν διερευνάται ούτε αμφισβητείται η πρόσβαση στα δεδομένα per se, η οποία, εξάλλου, έλαβε πράγματι χώρα με σκοπό τη δίωξη σοβαρής εγκληματικότητας στο πλαίσιο ποινικής έρευνας και με την αντίστοιχη άδεια, αλλά η χρήση των δεδομένων που αποκτήθηκαν, τα οποία φαίνεται ότι ελήφθησαν υπόψη και χρησιμοποιήθηκαν για την επιβολή πειθαρχικών-διοικητικών μέτρων σχετιζόμενα με υπηρεσιακά παραπτώματα.

3. ΟΡΙΣΜΕΝΕΣ ΠΡΟΚΑΤΑΡΚΤΙΚΕΣ ΣΚΕΨΕΙΣ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΥΠΟΧΡΕΩΣΗ ΔΙΑΤΗΡΗΣΗΣ (ΑΔΙΑΚΡΙΤΩΣ) ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΚΙΝΗΣΗΣ ΚΑΙ ΘΕΣΗΣ

Η υπό κρίση απόφαση ακολουθεί το ευρέως συζητούμενο τόσο στη θεωρία όσο και στη νομολογία ζήτημα σχετικά με την υποχρέωση που επιβάλλεται στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών να διατηρούν δεδομένα κίνησης και θέσης για ορισμένο χρονικό διάστημα. Μερικές από αυτές τις διαπιστώσεις θα παρουσιαστούν συνοπτικά, καθώς αποτέλεσαν τη βάση για τα ερωτήματα του αιτούντος δικαστηρίου και την απόφαση του ΔΕΕ.

[2] Lietuvos vyriausiasis administracinis teismas.

Στις συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12[3], το ΔΕΕ κήρυξε άκυρη την Οδηγία 2006/24/ΕΚ[4], λόγω της επέμβασής της στα θεμελιώδη δικαιώματα που προστατεύονται από τον ΧΘΔΕ[5]. Το σκεπτικό του ΔΕΕ για την απόφασή του συνίστατο στο ότι η επέμβαση που επέτρεπε η Οδηγία δεν περιοριζόταν στο απολύτως αναγκαίο μέτρο[6]. Επιπλέον, η Οδηγία δεν περιείχε σαφείς και ακριβείς κανόνες σχετικά με το πεδίο εφαρμογής του μέτρου, ούτε επέβαλε ελάχιστες εγγυήσεις για την πρόσβαση ή χρήση των δεδομένων. Περαιτέρω, η Οδηγία ίσχυε για όλα τα μέσα ηλεκτρονικής επικοινωνίας και δεν περιοριζόταν σε δεδομένα που αφορούσαν συγκεκριμένη χρονική περίοδο και γεωγραφική περιοχή ή ορισμένο κύκλο προσώπων[7]. Επιπρόσθετα, δεν υπήρχε αντικειμενικό κριτήριο για να καθοριστεί πότε θα πρέπει να επιτρέπεται η πρόσβαση στα δεδομένα, καθώς η Οδηγία αναφερόταν απλώς με γενικό τρόπο στη σοβαρή εγκληματικότητα, όπως αυτή ορίζεται από κάθε κράτος μέλος[8]. Το ΔΕΕ τόνισε επίσης ότι απουσίαζαν ουσιαστικές και τυπικές προϋποθέσεις σχετικά με την πρόσβαση των αρμόδιων εθνικών αρχών[9]. Παράλληλα, το Δικαστήριο υπογράμμισε ότι η Οδηγία δεν καθόριζε αντικειμενικό κριτήριο για τον περιορισμό του αριθμού των προσώπων που επιτρέπεται να έχουν πρόσβαση σε δεδομένα[10] και για τον καθορισμό της περιόδου διατήρησης των δεδομένων[11].

Μετά την ακύρωση από το ΔΕΕ το 2014 της Οδηγίας 2006/24/ΕΚ, πολυάριθμα νομοθετικά μέτρα των κρατών μελών που ενσωμάτωσαν την προρρηθείσα Οδηγία έχουν αμφισβητηθεί[12], καθώς επιβάλλουν στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών την υποχρέωση να διατηρούν τα δεδομένα κίνησης (πηγή και προορισμός της επικοινωνίας, τύπος τερματικού που χρησιμοποιήθηκε, ταυτότητα των χρηστών που συμμετείχαν στην επικοινωνία και διευθύνσεις IP) και τα δεδομένα θέσης όλων των ηλεκτρονικών επικοινωνιών που πραγματοποιούνται από

[3] Βλ. ΔΕΕ, C-293/12 και C-594/12 (συνεκδ.), *Digital Rights Ireland Ltd κ.ά.*

[4] Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2006, για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ.

[5] Βλ. ΔΕΕ, C-293/12 και C-594/12 (συνεκδ.), ό.π., σκ. 68 επ.

[6] Βλ. ibidem, σκ. 65.

[7] Βλ. ibidem, σκ. 56 και 59.

[8] Βλ. ibidem, σκ. 60.

[9] Βλ. ibidem, σκ. 61.

[10] Βλ. ibidem, σκ. 62.

[11] Βλ. ibidem, σκ. 64.

[12] Για παράδειγμα, στη χώρα μας η ακυρωθείσα από το ΔΕΕ Οδηγία μεταφέρθηκε στην ελληνική έννομη τάξη με τον ν. 3917/2011, ο οποίος εξακολουθεί να ισχύει και ο οποίος δεν μπορεί να κριθεί ως αντισυνταγματικός. Βλ. περαιτέρω, Ι. Ιγγλεζάκης, *Υποχρεωτική διατήρηση δεδομένων: Ακύρωση της οδηγίας 2006/24 από το ΔΕΕ*, 22.11.2014, διαθέσιμο στο link (τελευταία πρόσβαση 25.11.2023).

όλους τους χρήστες υπηρεσιών ηλεκτρονικών επικοινωνιών για συγκεκριμένο χρονικό διάστημα[13]. Αυτός ο τύπος υποχρέωσης θα μπορούσε, κατ' αρχήν, να χαρακτηριστεί ως γενική και αδιάκριτη διατήρηση περιορισμένης μόνο χρονικής διάρκειας και να συνιστά παράνομη επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν δικαιολογείται από λόγους δημοσίου συμφέροντος.

Στις συνεκδικασθείσες υποθέσεις C-203/15 and C-698/15[14] το ΔΕΕ εξέτασε αν είναι επιτρεπτή εθνική ρύθμιση που υποχρεώνει τους ιδιωτικούς παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών να διατηρούν δεδομένα που εμπίπτουν στην Οδηγία ePrivacy[15]. Το Δικαστήριο διαπίστωσε ότι ο γενικός κανόνας του άρθρου 5 παρ. 1 της Οδηγίας, ο οποίος διασφαλίζει το απόρρητο των επικοινωνιών, μπορεί να παρεκκλίνει σύμφωνα με το άρθρο 15 παρ. 1[16]. Ωστόσο, σύμφωνα με το Δικαστήριο, το άρθρο 15 παρ. 1 πρέπει να ερμηνεύεται στενά, καθώς ρυθμίζει εξαντλητικά τον κατάλογο των σκοπών[17], ενώ οι επιβαλλόμενοι περιορισμοί πρέπει να είναι οι απολύτως αναγκαίοι[18]. Επιπλέον, το Δικαστήριο κατέστησε σαφές ότι τα αποθηκευμένα δεδομένα κίνησης και θέσης επιτρέπουν εκτεταμένα συμπεράσματα για την ιδιωτική ζωή των ατόμων[19], επομένως, η πρόσβαση θα πρέπει να επιτρέπεται μόνο για την καταπολέμηση σοβαρής εγκληματικότητας[20].

Επιπρόσθετα, το ΔΕΕ τόνισε ότι η απεριόριστη διατήρηση δεδομένων χωρίς καθορισμένα όρια είναι απαράδεκτη. Για τον λόγο αυτό πρέπει να προσδιορίζονται οι κατηγορίες των αποθηκευμένων δεδομένων, οι συσκευές και τα πρόσωπα που αυτά αφορούν, καθώς και η διάρκεια της αποθήκευσής τους[21]. Το Δικαστήριο συνέχισε αναφέροντας ότι τα κράτη μέλη πρέπει να παρέχουν επαρκείς εγγυήσεις για την αποτροπή της κατάχρησης των δεδομένων[22] και ότι η εθνική ρύθμιση πρέπει να είναι σαφής και ακριβής όσον αφορά το πεδίο εφαρμογής ενός μέτρου διατήρησης δεδομένων. Στο πλαίσιο αυτό, πρέπει να υπάρχει αντικειμενικό κριτήριο που να δημιουργεί σύνδεση μεταξύ των προς διατήρηση δεδομένων και του επιδιωκόμενου σκοπού. Σε μια ειδική περίπτωση, η πρόσβαση στα δεδομένα θα μπορούσε να δικαιολογηθεί εάν υπήρχαν αντικειμενικές προσδοκίες ότι τα δεδομένα θα μπορούσαν να συμβάλουν στην επίτευξη του σκοπού. Μια τέτοια ειδική κατάσταση θα μπορούσε να αντιπροσωπεύεται από τα ζωτικά συμφέροντα του κράτους, όπως η καταπολέμηση της σοβαρής εγκληματικότητας ή οι σοβαρές απειλές

[13] Ο ελληνικός ν. 3917/2011 προβλέπει τη διατήρηση των ως άνω τηλεπικοινωνιακών δεδομένων για διάστημα δώδεκα μηνών (άρθρο 6) και με σκοπό τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων (άρθρο 1).

[14] Βλ. ΔΕΕ, C-203/15 και C-698/15 (συνεκδ.), *Tele2 Sverige και Watson κ.ά.*

[15] Βλ. ibidem, σκ. 69 επ.

[16] Βλ. ibidem, σκ. 89 επ.

[17] Βλ. ibidem, σκ. 96.

[18] Βλ. ibidem, σκ. 98 επ.

[19] Βλ. ibidem, σκ. 102.

[20] Βλ. ibidem, σκ. 106 επ.

[21] Βλ. ibidem, σκ. 109.

[22] Βλ. ibidem, σκ. 110 επ.

για τη δημόσια ασφάλεια, ενώ η πρόσβαση στα δεδομένα πρέπει να επιτρέπεται από δικαστήριο ή ανεξάρτητη αρχή[23].

Όπως είναι λογικό, δεν αναπαράγεται εν προκειμένω όλη η νομολογία του ΔΕΕ που έχει εξετάσει τη σχετική υποχρέωση και τα όριά της. Η σχολιαζόμενη απόφαση περιέχει στο σκεπτικό της μια σύντομη περίληψη των πολυάριθμων αποφάσεων που προσθέτουν νέες αποχρώσεις στην υποχρέωση διατήρησης των δεδομένων κίνησης και θέσης και οι οποίες, κατ' αρχήν, φαίνεται να αποκλείουν την αδιάκριτη διατήρηση αυτών[24]. Σε κάθε περίπτωση και στο μέτρο που συνιστά επέμβαση στα θεμελιώδη δικαιώματα, η υποχρέωση διατήρησης πρέπει να υπόκειται σε αυστηρό καθεστώς εγγυήσεων και να ερμηνεύεται στενά, καθώς αποτελεί εξαίρεση, η οποία πρέπει να δικαιολογείται για λόγους δημοσίου συμφέροντος και σύμφωνα με την αρχή της αναλογικότητας[25].

4. Η ΑΠΟΦΑΣΗ: Η ΔΙΩΞΗ ΓΙΑ ΜΗ ΣΟΒΑΡΑ ΕΓΚΛΗΜΑΤΑ Η ΓΙΑ ΠΕΙΘΑΡΧΙΚΕΣ-ΔΙΟΙΚΗΤΙΚΕΣ ΠΑΡΑΒΑΣΕΙΣ ΔΕΝ ΔΙΚΑΙΟΛΟΓΕΙ ΕΠΕΜΒΑΣΗ ΣΤΑ ΘΕΜΕΛΙΩΔΗ ΔΙΚΑΙΩΜΑΤΑ

Στη νέα αυτή απόφαση της 7ης Σεπτεμβρίου 2023, το ΔΕΕ ολοκληρώνει τη θεωρία του σχετικά με την υποχρέωση διατήρησης των δεδομένων κίνησης και των δεδομένων θέσης στο πλαίσιο παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών. Εν προκειμένω, το ΔΕΕ, επικαλούμενο αφενός προηγούμενη νομολογία του[26], αφετέρου την αρχή της αναλογικότητας, τονίζει ότι μόνον η καταπολέμηση της σοβαρής εγκληματικότητας και η πρόληψη σοβαρών απειλών κατά της δημόσιας ασφάλειας δύνανται να δικαιολογήσουν σοβαρές επεμβάσεις στα θεμελιώδη δικαιώματα που κατοχυρώνονται στα άρθρα 7 και 8 του ΧΘΔΕ, όπως αυτές τις οποίες συνεπάγεται η διατήρηση των δεδομένων κίνησης και των δεδομένων θέσης[27]. Ως εκ τούτου, οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών υποχρεούνται να διατηρούν και να διαβιβάζουν δεδομένα κίνησης και θέσης στις αρμόδιες αρχές μόνο για την καταπολέμηση της σοβαρής εγκληματικότητας[28].

Από την απόφαση και τη νομολογία που παρατίθεται σε αυτήν προκύπτουν τα ακόλουθα: *Πρώτον*, στην ιεράρχηση των σκοπών δημοσίου συμφέροντος που απαριθμούνται στο άρθρο 15 παρ. 1 της Οδηγίας ePrivacy, σύμφωνα με την αρχή της αναλογικότητας, η σημασία του σκοπού διαφύλαξης της εθνικής ασφάλειας (αποκλειστική αρμοδιότητα κάθε κράτους μέλους) υπερτερεί της περιωπής των άλλων σκοπών, ιδίως των σκοπών καταπολέμησης της εγκληματικότητας εν γένει, συμπεριλαμβανομένης της σοβαρής εγκληματικότητας, και της πρόληψης μη σοβαρών

[23] Βλ. ibidem, σκ. 120 επ

[24] Βλ. ΔΕΕ, C-511/18,C-512/18 και C-520/18 (συνεκδ.), *La Quadrature du Net κ.ά.*, σκ. 110· ΔΕΕ, C-746/18, *Prokuratuur*, σκ. 33 και 35· ΔΕΕ, C-793/19 και C-794/19, *SpaceNet και Telekom Deutschland*, σκ. 74 και 131 και εκεί παρατιθέμενη νομολογία.

[25] Βλ. ΔΕΕ, C-140/20, *Commissioner of An Garda Síochána κ.ά.*, σκ. 40.

[26] Βλ. ΔΕΕ, C-746/18, ό.π., σκ. 33 και 35.

[27] Βλ. ΔΕΕ, C-162/22, *Lietuvos Respublikos generalinė prokuratūra,* σκ. 36.

[28] Βλ. ibidem, σκ. 37.

απειλών κατά της δημόσιας ασφάλειας[29]. *Δεύτερον*, ο σκοπός διαφύλαξης της εθνικής ασφάλειας μπορεί, αντιστοίχως, να δικαιολογήσει μέτρα που συνεπάγονται σοβαρότερες επεμβάσεις στα θεμελιώδη δικαιώματα από εκείνα που θα μπορούσαν να δικαιολογηθούν από τους άλλους αυτούς σκοπούς[30]. *Τρίτον*, ο σκοπός της πρόληψης, διερεύνησης, ανίχνευσης και δίωξης ποινικών αδικημάτων εν γένει μπορεί να δικαιολογήσει μη σοβαρές επεμβάσεις στα θεμελιώδη δικαιώματα[31].

Τέταρτον, η πρόσβαση και η χρήση των δεδομένων κίνησης και θέσης που διατηρούν οι πάροχοι, σύμφωνα με μέτρο που θεσπίστηκε δυνάμει του άρθρου 15 παρ. 1 της Οδηγίας ePrivacy, μπορεί, κατ' αρχήν, να δικαιολογείται μόνο από τον σκοπό δημοσίου συμφέροντος για τον οποίο οι εν λόγω πάροχοι διατάχθηκαν να διατηρήσουν τα εν λόγω δεδομένα· ειδάλλως, μόνο αν η σημασία του σκοπού που επιδιώκεται με την πρόσβαση είναι μεγαλύτερη από εκείνη του σκοπού που δικαιολογεί τη διατήρηση[32]. *Πέμπτον*, το ίδιο ισχύει και για άλλες πιθανές χρήσεις των διατηρούμενων δεδομένων: Αφ' ης στιγμής διατηρήθηκαν και διαβιβάσθηκαν στις αρμόδιες αρχές για την καταπολέμηση της σοβαρής εγκληματικότητας, τα δεδομένα αυτά δεν δύνανται να διαβιβαστούν σε άλλες αρχές ή να χρησιμοποιηθούν για άλλους σκοπούς, συμπεριλαμβανομένης της καταπολέμησης της διαφθοράς που σχετίζεται με την παράβαση (υπηρεσιακού) καθήκοντος. Αυτοί οι άλλοι σκοποί είναι λιγότερο σημαντικοί στην ιεραρχία των σκοπών δημοσίου συμφέροντος από την καταπολέμηση της σοβαρής εγκληματικότητας και την πρόληψη σοβαρών απειλών για τη δημόσια ασφάλεια. Σε μια τέτοια περίπτωση, η πρόσβαση στα διατηρούμενα δεδομένα θα ήταν αντίθετη προς την ιεράρχηση των σκοπών δημοσίου συμφέροντος που αναφέρθηκαν προηγουμένως[33]. Ως εκ τούτου, η καταπολέμηση της σοβαρής εγκληματικότητας και η πρόληψη σοβαρών απειλών κατά της δημόσιας ασφάλειας θεωρείται μικρότερης σημασίας από τη διαφύλαξη της εθνικής ασφάλειας, αλλά μεγαλύτερης σημασίας από εκείνη της εν γένει καταπολέμησης των ποινικών αδικημάτων[34].

Τέλος, οι πειθαρχικές διαδικασίες που αφορούν σε παραπτώματα που σχετίζονται με διαφθορά στην υπηρεσία θα μπορούσαν να συνδέονται με την προστασία της δημόσιας ασφάλειας, αν και αυτό θα απαιτούσε την απόδειξη της ύπαρξης σοβαρής απειλής για τη δημόσια ασφάλεια[35]. Ωστόσο, υπό το πρίσμα του άρθρου 15 παρ. 1 της Οδηγίας ePrivacy, ο περιορισμός των θεμελιωδών δικαιωμάτων που απορρέει από τη διατήρηση των δεδομένων κίνησης και θέσης δικαιολογείται μόνο στο πλαίσιο ποινικής διαδικασίας και όχι στο πλαίσιο πειθαρχικής διαδικασίας,

[29] Βλ. ΔΕΕ, C-140/20, ό.π., σκ. 99.

[30] Βλ. ibidem, σκ. 57 και εκεί παρατιθέμενη νομολογία.

[31] Βλ. Ibidem, σκ. 59 και εκεί παρατιθέμενη νομολογία.

[32] Βλ. ibidem, σκ. 98 και εκεί παρατιθέμενη νομολογία.

[33] Βλ. ibidem, σκ. 99 και ΔΕΕ, C-162/22, ό.π., σκ. 41.

[34] Βλ. ΔΕΕ, C-162/22, ό.π., σκ. 35-36.

[35] Βλ. ΔΕΕ, C-162/22, σκ. 42.

όσο σημαντικός και αν είναι ο ρόλος που διαδραματίζουν οι διαδικασίες αυτές για την καταπολέμηση της σοβαρής εγκληματικότητας[36].

Με βάση τα ανωτέρω, το ΔΕΕ επισημαίνει ότι τα σχετικά νομοθετικά μέτρα των κρατών μελών δύνανται να προβλέπουν[37]: *Πρώτον*, στοχευμένη διατήρηση των δεδομένων κίνησης και των δεδομένων θέσης, η οποία πρέπει να οριοθετείται βάσει αντικειμενικών στοιχείων που δεν εισάγουν δυσμενείς διακρίσεις, ανάλογα με τις κατηγορίες των προσώπων στα οποία αφορούν τα δεδομένα ή με γεωγραφικά κριτήρια, μόνο για το χρονικό διάστημα που είναι απολύτως αναγκαίο, με δυνατότητα, όμως, παράτασής του· *δεύτερον*, γενική και χωρίς διάκριση διατήρηση των διευθύνσεων IP που έχουν αποδοθεί στην πηγή μιας σύνδεσης, για χρονική περίοδο περιοριζόμενη στο απολύτως αναγκαίο· *τρίτον*, γενική και χωρίς διάκριση διατήρηση των δεδομένων σχετικά με την ταυτότητα των χρηστών μέσων ηλεκτρονικών επικοινωνιών και *τέταρτον* τη δυνατότητα να διατάσσονται οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών, μέσω απόφασης της αρμόδιας αρχής υποκείμενης σε αποτελεσματικό δικαστικό έλεγχο, να προβαίνουν για ορισμένο χρονικό διάστημα στην κατεπείγουσα διατήρηση των δεδομένων κίνησης και των δεδομένων θέσης που διαθέτουν οι εν λόγω πάροχοι υπηρεσιών.

Λαμβανομένων υπόψη των προεκτεθέντων, το ΔΕΕ κατέληξε στο συμπέρασμα ότι το άρθρο 15 παρ. 1 της Οδηγίας ePrivacy δεν επιτρέπει να χρησιμοποιούνται στο πλαίσιο ερευνών για υπηρεσιακά παραπτώματα συνδεόμενα με διαφθορά δεδομένα προσωπικού χαρακτήρα σχετικά με ηλεκτρονικές επικοινωνίες, τα οποία διατηρήθηκαν, κατ' εφαρμογή νομοθετικού μέτρου θεσπισθέντος δυνάμει της ανωτέρω διάταξης, από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών και τα οποία εν συνεχεία τέθηκαν στη διάθεση των αρμόδιων αρχών κατ' εφαρμογή του ίδιου αυτού μέτρου για την καταπολέμηση της σοβαρής εγκληματικότητας[38].

ΙΙ. ΣΥΜΠΕΡΑΣΜΑΤΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ

Η περιωπή της σχολιαζόμενης απόφασης του ΔΕΕ συνίσταται στο γεγονός ότι δημιουργεί σημαντικό προηγούμενο σχετικά με τη χρήση δεδομένων ηλεκτρονικών επικοινωνιών σε έρευνες διαφθοράς στον δημόσιο τομέα, καθώς είναι δεδομένο ότι θα έχει εκτεταμένες συνέπειες για τον τρόπο με τον οποίο μπορούν να χρησιμοποιηθούν προσωπικά δεδομένα σε σχετικές διοικητικές έρευνες.

Επιπλέον, μολονότι οι προηγούμενες αποφάσεις του ΔΕΕ υποστήριξαν σαφώς την ανάγκη απόλυτης προστασίας της ιδιωτικής ζωής, εντούτοις οι επόμενες αποφάσεις του εξειδίκευσαν και σχετικοποίησαν τις προϋποθέσεις για τη διατήρηση των δεδομένων προσωπικού χαρακτήρα. Η σχολιαζόμενη απόφαση, ωστόσο, αποτρέπει την περαιτέρω άμβλυνση των απαιτήσεων, καθώς η ερμηνεία που δίδεται στο άρθρο 15 παρ. 1 της Οδηγίας ePrivacy σχετικά με την πρόσβαση σε δεδομένα κίνησης και θέσης περιορίζεται στη διερεύνηση σοβαρών εγκλημάτων.

[36] Βλ. ibidem, σκ. 43.

[37] Βλ. ΔΕΕ, C-162/22, ό.π., σκ. 31.

[38] Ibidem, σκ. 44.

Τα δεδομένα κίνησης και θέσης μπορεί να περιλαμβάνουν πληροφορίες για ευαίσθητους τομείς, όπως ο σεξουαλικός προσανατολισμός, τα πολιτικά φρονήματα, οι θρησκευτικές, φιλοσοφικές, κοινωνικές ή άλλες πεποιθήσεις και η κατάσταση της υγείας, με τα δεδομένα αυτά να απολαμβάνουν ειδικής προστασίας βάσει του δικαίου της Ένωσης. Επιπλέον, τα εν λόγω δεδομένα είναι δυνατό να οδηγήσουν σε ακριβή συμπεράσματα σχετικά με την ιδιωτική ζωή, όταν συνδυάζονται (π.χ. προφίλ προσωπικότητας). Από την άποψη του σεβασμού της ιδιωτικής ζωής, οι πληροφορίες αυτές είναι εξίσου ευαίσθητες με το περιεχόμενο της επικοινωνίας. Υπό αυτό το πρίσμα, ο περιορισμός της πρόσβασης σε δεδομένα για τη δίωξη σοβαρών εγκλημάτων είναι, καταρχήν, ευπρόσδεκτος.

Παρόλα αυτά, εξακολουθούν να υπάρχουν ανοικτά ερωτήματα όσον αφορά τα όρια και τις προϋποθέσεις της εθνικής νομοθεσίας που επιτρέπει τη διατήρηση τηλεπικοινωνιακών δεδομένων και τη χρήση τους για σκοπούς επιβολής του νόμου εντός του πλαισίου που έχει καθορίσει το ΔΕΕ. Το Δικαστήριο τονίζει (και πάλι) ότι η αποθήκευση δεδομένων κίνησης και θέσης συνεπάγεται σοβαρή επέμβαση στα θεμελιώδη δικαιώματα του σεβασμού της ιδιωτικής και οικογενειακής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα. Η διευκρίνιση, όμως, του ζητήματος σχετικά με τη μεταγενέστερη χρήση των αποθηκευμένων δεδομένων στη σχολιαζόμενη υπόθεση προκαλεί περαιτέρω ερωτήματα: Πώς, λοιπόν, ορίζεται η «καταπολέμηση της σοβαρής εγκληματικότητας»; Πώς εφαρμόζεται το κριτήριο της «ιεράρχησης των σκοπών» σε άλλες περιπτώσεις; Τι γίνεται με τη χρήση των διατηρηθέντων δεδομένων που χρησιμοποιήθηκαν αρχικά για την προστασία της δημόσιας ασφάλειας και στη συνέχεια διαβιβάστηκαν για την καταπολέμηση σοβαρής εγκληματικότητας (και αντίστροφα);

Τα ζητήματα αυτά, όπως και η έννοια της εθνικής ασφάλειας, εξακολουθούν να ρυθμίζονται αποκλειστικά από τα κράτη μέλη, με αποτέλεσμα να ελλοχεύει ο κίνδυνος τόσο για ευρεία ερμηνεία, όσο και για κατακερματισμό του ενωσιακού δικαίου στην πράξη, ελλείψει της απαιτούμενης ομοιομορφίας. Είναι σαφές ότι η επιλογή του ενωσιακού νομοθέτη να ρυθμίσει το κρίσιμο αυτό ζήτημα με Οδηγία και όχι με Κανονισμό δημιουργεί προβλήματα ενιαίας εφαρμογής της χρήσης και διατήρησης δεδομένων θέσης και κίνησης. Έτσι, η Επιτροπή, αντιλαμβανόμενη ότι η προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων είναι θεμελιώδης για τη δημοκρατική λήψη αποφάσεων και προϋπόθεση για την άσκηση άλλων θεμελιωδών δικαιωμάτων, ανέλαβε το 2017 σχετική νομοθετική πρωτοβουλία, με την πρόταση θέσπισης Κανονισμού για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες[39], ο οποίος θα αντικαθιστά την Οδηγία ePrivacy και θα ευθυγραμμίζεται με τις αρχές και τις επιταγές του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ), αποτελώντας lex specialis αυτού. Δυστυχώς, όμως, η μεγάλη καθυστέρηση στην υιοθέτησή του δημιουργεί εύλογες αμφιβολίες για το κατά πόσο τελικά το κείμενο είναι εφικτό να εγκριθεί. ❑

[39] Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες) COM(2017) 10 τελικό.