



## Συλλογή της Νομολογίας

ΠΡΟΤΑΣΕΙΣ ΤΟΥ ΓΕΝΙΚΟΥ ΕΙΣΑΓΓΕΛΕΑ  
MANUEL CAMPOS SÁNCHEZ-BORDONA  
της 15ης Ιανουαρίου 2020<sup>1</sup>

**Συνεκδικαζόμενες υποθέσεις C-511/18 και C-512/18**

**La Quadrature du Net,  
French Data Network,  
Fédération des fournisseurs d'accès à Internet associatifs,  
Igwam.net (C-511/18)  
κατά  
Premier ministre,  
Garde des Sceaux, ministre de la Justice,  
Ministre de l'Intérieur,  
Ministre des Armées**

[αίτηση του Conseil d'État (Συμβουλίου της Επικρατείας, Γαλλία)  
για την έκδοση προδικαστικής αποφάσεως]

«Προδικαστική παραπομπή – Επεξεργασία δεδομένων προσωπικού χαρακτήρα και προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών – Διαφύλαξη της εθνικής ασφάλειας και καταπολέμηση της τρομοκρατίας – Οδηγία 2002/58/EK – Πεδίο εφαρμογής – Άρθρο 1, παράγραφος 3 – Άρθρο 15, παράγραφος 3 – Άρθρο 4, παράγραφος 2, ΣΕΕ – Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης – Άρθρα 6, 7, 8, 11, 47 και 52, παράγραφος 1 – Γενική και χωρίς διάκριση διατήρηση των δεδομένων συνδέσεως καθώς και των δεδομένων που καθιστούν δυνατή την ταυτοποίηση των δημιουργών περιεχομένου – Συλλογή δεδομένων κίνησης και θέσης – Πρόσβαση στα δεδομένα»

1. Το Δικαστήριο έχει τηρήσει, κατά τα τελευταία έτη, πάγια νομολογιακή γραμμή όσον αφορά τη διατήρηση των δεδομένων προσωπικού χαρακτήρα και την πρόσβαση σε αυτά, με χαρακτηριστικά ορόσημα:

- την απόφαση της 8ης Απριλίου 2014, Digital Rights Ireland κ.λπ.<sup>2</sup>, με την οποία έκρινε ανίσχυρη την οδηγία 2006/24/EK<sup>3</sup> διότι επέτρεπε υπέρμετρη επέμβαση στα δικαιώματα που αναγνωρίζονται από τα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (στο εξής: Χάρτης).

<sup>1</sup> Γλώσσα του πρωτοτύπου: η ισπανική.

<sup>2</sup> Υποθέσεις C-293/12 και C-594/12 (στο εξής: απόφαση Digital Rights, EU:C:2014:238).

<sup>3</sup> Οδηγία 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/EK (EE 2006, L 105, σ. 54).

- την απόφαση της 21ης Δεκεμβρίου 2016, *Tele2 Sverige και Watson κ.λπ.*<sup>4</sup>, με την οποία ερμήνευσε το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58/ΕΚ<sup>5</sup>.
- την απόφαση της 2ας Οκτωβρίου 2018, *Ministerio Fiscal*<sup>6</sup>, με την οποία επιβεβαίωσε την ερμηνεία της ίδιας αυτής διάταξης της οδηγίας 2002/58.

2. Οι αποφάσεις αυτές (ιδίως, η δεύτερη) προβληματίζουν τις αρχές ορισμένων κρατών μελών, επειδή, κατά την άποψή τους, έχουν ως συνέπεια να τους στερούν ένα εργαλείο που θεωρούν αναγκαίο για την προστασία της εθνικής ασφάλειας και την καταπολέμηση της εγκληματικότητας και της τρομοκρατίας. Για τον λόγο αυτό, ορισμένα από αυτά τα κράτη μέλη υποστηρίζουν ότι η νομολογία αυτή πρέπει να μεταστραφεί ή να αποσαφηνιστεί.

3. Ορισμένα δικαστήρια των κρατών μελών διατύπωσαν τον ίδιο προβληματισμό σε τέσσερις προδικαστικές παραπομπές<sup>7</sup>, επί των οποίων αναπτύσσω τις προτάσεις μου σήμερα.

4. Οι τέσσερις υποθέσεις εγείρουν, καταρχάς, το ζήτημα της εφαρμογής της οδηγίας 2002/58 σε δραστηριότητες που σχετίζονται με την εθνική ασφάλεια και την καταπολέμηση της τρομοκρατίας. Εφόσον η ως άνω οδηγία έχει εφαρμογή στο πλαίσιο αυτό, θα πρέπει, ευθύς αμέσως, να αποσαφηνιστεί σε ποιον βαθμό τα κράτη μέλη δύνανται να περιορίζουν τα προστατευόμενα από αυτήν δικαιώματα στην ιδιωτική ζωή. Τέλος, θα πρέπει να εξεταστεί αν και κατά πόσον οι διάφορες εθνικές νομοθεσίες (η βρετανική<sup>8</sup>, η βελγική<sup>9</sup> και η γαλλική<sup>10</sup>) στον τομέα αυτόν συνάδουν με το δίκαιο της Ένωσης, όπως αυτό έχει ερμηνευθεί από το Δικαστήριο.

## I. Νομοθετικό πλαίσιο

### A. Δίκαιο της Ένωσης

#### 1. Οδηγία 2002/58

5. Κατά το άρθρο 1 («Πεδίο εφαρμογής και στόχος»):

«1. Η παρούσα οδηγία προβλέπει την εναρμόνιση των εθνικών διατάξεων οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, και ιδίως του δικαιώματος στην ιδιωτική ζωή και την εμπιστευτικότητα, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και να διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Κοινότητα.

[...]

4 Υποθέσεις C-203/15 και C-698/15 (στο εξής: απόφαση *Tele2 Sverige και Watson*, EU:C:2016:970).

5 Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ 2002, L 201, σ. 37).

6 Υπόθεση C-207/16 (στο εξής: *Ministerio Fiscal*, EU:C:2018:788).

7 Πέραν των δύο υπό κρίση υποθέσεων (C-511/18 και C-512/18), πρόκειται για τις υποθέσεις C-623/17, *Privacy International*, και C-520/18, *Ordre des barreaux francophones et germanophone* κ.λπ.

8 Υπόθεση *Privacy International*, C-623/17.

9 Υπόθεση *Ordre des barreaux francophones et germanophone* κ.λπ., C-520/18.

10 Υποθέσεις *La Quadrature du Net* κ.λπ., C-511/18 και C-512/18.

3. Η παρούσα οδηγία δεν εφαρμόζεται σε δραστηριότητες οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής της συνθήκης για την ίδρυση της Ευρωπαϊκής Κοινότητας, όπως οι δραστηριότητες που καλύπτονται από τους τίτλους V και VI της συνθήκης για την Ευρωπαϊκή Ένωση, και σε κάθε περίπτωση στις δραστηριότητες που αφορούν τη δημόσια ασφάλεια, την εθνική άμυνα, την ασφάλεια του κράτους (συμπεριλαμβανομένης της οικονομικής ευημερίας του κράτους εφόσον οι δραστηριότητες συνδέονται με θέματα ασφάλειας του κράτους) και στις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου.»

6. Το άρθρο 3 («Σχετικές υπηρεσίες») προβλέπει τα εξής:

«Η παρούσα οδηγία εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα επικοινωνιών στην Κοινότητα, περιλαμβανομένων των δημοσίων δικτύων επικοινωνιών που υποστηρίζουν συσκευές συλλογής δεδομένων και ταυτοποίησης.»

7. Η παράγραφος 1 του άρθρου 5 («Απόρρητο των επικοινωνιών») ορίζει τα εξής:

«Τα κράτη μέλη κατοχυρώνουν, μέσω της εθνικής νομοθεσίας, το απόρρητο των επικοινωνιών που διενεργούνται μέσω δημόσιου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης. Ειδικότερα, απαγορεύουν την ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεση των ενδιαφερομένων χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια, σύμφωνα με το άρθρο 15 παράγραφος 1. Η παρούσα παράγραφος δεν εμποδίζει την τεχνική αποθήκευση, η οποία είναι αναγκαία για τη διαβίβαση επικοινωνίας, με την επιφύλαξη της αρχής του απορρήτου.»

8. Το άρθρο 6 («Δεδομένα κίνησης») ορίζει τα εξής:

«1. Τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον πάροχο δημόσιου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, πρέπει να απαλείφονται ή να καθίστανται ανώνυμα όταν δεν είναι πλέον απαραίτητα για τον σκοπό της μετάδοσης μιας επικοινωνίας, με την επιφύλαξη των παραγράφων 2, 3 και 5 του παρόντος άρθρου και του άρθρου 15 παράγραφος 1.

2. Τα δεδομένα κίνησης που είναι απαραίτητα για τη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων μπορούν να υποβάλλονται σε επεξεργασία. Η επεξεργασία αυτή επιτρέπεται μόνον έως το τέλος της χρονικής περιόδου εντός της οποίας δύναται να αμφισβητείται νομίμως ο λογαριασμός ή να επιδιώκεται η πληρωμή.»

9. Το άρθρο 15 («Εφαρμογή ορισμένων διατάξεων της οδηγίας 95/46/ΕΚ <sup>[11]</sup>»), παράγραφος 1, αναφέρει τα εξής:

«Τα κράτη μέλη δύνανται να λαμβάνουν νομοθετικά μέτρα για να περιορίζουν τα δικαιώματα και τις υποχρεώσεις που προβλέπονται στα άρθρα 5 και 6, στο άρθρο 8 παράγραφοι 1 έως 4 και στο άρθρο 9 της παρούσας οδηγίας, εφόσον ο περιορισμός αυτός αποτελεί αναγκαίο, κατάλληλο και ανάλογο μέτρο σε μια δημοκρατική κοινωνία για τη διαφύλαξη της εθνικής ασφάλειας (δηλαδή της ασφάλειας του κράτους), της εθνικής άμυνας, της δημόσιας ασφάλειας, και για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων ή της άνευ αδείας χρησιμοποίησης του συστήματος ηλεκτρονικών επικοινωνιών, όπως προβλέπεται στο άρθρο 13 παράγραφος 1 της οδηγίας 95/46/ΕΚ. Για τον σκοπό αυτό, τα κράτη μέλη δύνανται, μεταξύ άλλων, να λαμβάνουν νομοθετικά

<sup>11</sup> Οδηγία 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).

μέτρα που θα προβλέπουν τη φύλαξη δεδομένων για ορισμένο χρονικό διάστημα για τους λόγους που αναφέρονται στην παρούσα παράγραφο. Όλα τα μέτρα που προβλέπονται στην παρούσα παράγραφο είναι σύμφωνα με τις γενικές αρχές του κοινοτικού δικαίου, συμπεριλαμβανομένων αυτών που αναφέρονται στο άρθρο 6 παράγραφοι 1 και 2 της συνθήκης για την Ευρωπαϊκή Ένωση.»

## 2. Οδηγία 2000/31/ΕΚ<sup>12</sup>

10. Το άρθρο 14 ορίζει τα εξής:

«1. Τα κράτη μέλη διασφαλίζουν ότι σε περίπτωση παροχής μιας υπηρεσίας της κοινωνίας της πληροφορίας η οποία συνίσταται στην αποθήκευση πληροφοριών παρεχομένων από έναν αποδέκτη υπηρεσίας, δεν υφίσταται ευθύνη του φορέα παροχής της υπηρεσίας για τις πληροφορίες που αποθηκεύονται μετά από αίτηση αποδέκτη της υπηρεσίας, υπό τον όρο ότι:

[...]

3. Το παρόν άρθρο δεν θίγει τη δυνατότητα δικαστικής ή διοικητικής αρχής, σύμφωνα με τα νομικά συστήματα των κρατών μελών, να απαιτούν από τον φορέα παροχής υπηρεσιών να προβεί στην παύση ή στην πρόληψη παράβασης, ούτε θίγει τη δυνατότητα των κρατών μελών να θεσπίζουν διαδικασίες για την απόσυρση των πληροφοριών ή την απενεργοποίηση της πρόσβασης σε αυτές.»

11. Κατά το άρθρο 15:

«1. Τα κράτη μέλη δεν επιβάλλουν στους φορείς παροχής υπηρεσιών, για την παροχή των υπηρεσιών που αναφέρονται στα άρθρα 12, 13 και 14, γενική υποχρέωση ελέγχου των πληροφοριών που μεταδίδουν ή αποθηκεύουν ούτε γενική υποχρέωση δραστηριότητας αναζήτησης γεγονότων ή περιστάσεων που δείχνουν ότι πρόκειται για παράνομες δραστηριότητες.

2. Τα κράτη μέλη δύνανται να υποχρεώσουν τους φορείς παροχής υπηρεσιών της κοινωνίας της πληροφορίας να ενημερώνουν πάραυτα τις αρμόδιες κρατικές αρχές για τυχόν υπόνοιες περί χορηγούμενων παρανόμων πληροφοριών ή δραστηριοτήτων που επιχειρούν αποδέκτες των υπηρεσιών τους ή να ανακοινώνουν στις αρμόδιες αρχές, κατ' αίτησή τους, πληροφορίες που διευκολύνουν την εντόπιση αποδεκτών των υπηρεσιών τους με τους οποίους έχουν συμφωνίες αποθήκευσης.

## 3. Κανονισμός (ΕΕ) 2016/679<sup>13</sup>

12. Κατά το άρθρο 2 («Ουσιαστικό πεδίο εφαρμογής»):

«1. Ο παρών κανονισμός εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης.

2. Ο παρών κανονισμός δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα:

α) στο πλαίσιο δραστηριότητας η οποία δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης,

12 Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8ης Ιουνίου 2000, για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά (οδηγία για το ηλεκτρονικό εμπόριο) (ΕΕ 2000, L 178, σ. 1).

13 Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ 2016, L 119, σ. 1).

- β) από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του κεφαλαίου 2 του τίτλου V της ΣΕΕ,
- γ) από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας,
- δ) από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια.

[...]»

13. Κατά το άρθρο 23, παράγραφος 1 («Περιορισμοί»):

«Το δίκαιο της Ένωσης ή του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία των δεδομένων μπορεί να περιορίζει μέσω νομοθετικού μέτρου το πεδίο εφαρμογής των υποχρεώσεων και των δικαιωμάτων που προβλέπονται στα άρθρα 12 έως 22 και στο άρθρο 34, καθώς και στο άρθρο 5, εφόσον οι διατάξεις του αντιστοιχούν στα δικαιώματα και τις υποχρεώσεις που προβλέπονται στα άρθρα 12 έως 22, όταν ένας τέτοιος περιορισμός σέβεται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών και συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση:

- α) της ασφάλειας του κράτους,
- β) της εθνικής άμυνας,
- γ) της δημόσιας ασφάλειας,
- δ) της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένης της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της πρόληψης αυτών,
- ε) άλλων σημαντικών στόχων γενικού δημόσιου συμφέροντος της Ένωσης ή κράτους μέλους, ιδίως σημαντικού οικονομικού ή χρηματοοικονομικού συμφέροντος της Ένωσης ή κράτους μέλους, συμπεριλαμβανομένων των νομισματικών, δημοσιονομικών και φορολογικών θεμάτων, της δημόσιας υγείας και της κοινωνικής ασφάλισης,
- στ) της προστασίας της ανεξαρτησίας της δικαιοσύνης και των δικαστικών διαδικασιών,
- ζ) της πρόληψης, της διερεύνησης, της ανίχνευσης και της δίωξης παραβάσεων δεοντολογίας σε νομοθετικά κατοχυρωμένα επαγγέλματα,
- η) της παρακολούθησης, της επιθεώρησης ή της κανονιστικής λειτουργίας που συνδέεται, έστω περιστασιακά, με την άσκηση δημόσιας εξουσίας στις περιπτώσεις που αναφέρονται στα στοιχεία α) έως ε) και ζ),
- θ) της προστασίας του υποκειμένου των δεδομένων ή των δικαιωμάτων και των ελευθεριών τρίτων,
- ι) της εκτέλεσης αστικών αξιώσεων.»

14. Το άρθρο 95 («Σχέση με την οδηγία 2002/58/ΕΚ») έχει ως εξής:

«Ο παρών κανονισμός δεν επιβάλλει πρόσθετες υποχρεώσεις σε φυσικά ή νομικά πρόσωπα σε σχέση με την επεξεργασία όσον αφορά την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό σε δημόσια δίκτυα επικοινωνίας στην Ένωση σε σχέση με θέματα τα οποία υπόκεινται στις ειδικές υποχρεώσεις με τον ίδιο στόχο που ορίζεται στην οδηγία 2002/58/ΕΚ.»

## **B. Εθνικό δίκαιο**

### **1. Code de la sécurité intérieure (κώδικας εσωτερικής ασφάλειας)**

15. Κατά το άρθρο L. 851-1:

«Υπό τις προϋποθέσεις του κεφαλαίου 1 του τίτλου II του παρόντος βιβλίου, μπορεί να επιτραπεί η συλλογή, από τους παρόχους ηλεκτρονικών επικοινωνιών και από τα πρόσωπα που μνημονεύονται στο άρθρο L. 34-1 του code des postes et des communications électroniques [(κώδικα περί ταχυδρομείων και ηλεκτρονικών επικοινωνιών)], καθώς και από τα πρόσωπα που αναφέρονται στο άρθρο 6, σημείο I, παράγραφοι 1 και 2, του loi n.º 2004-575 [...] pour la confiance dans l'économie numérique [(νόμου 2004-575 για την εμπιστοσύνη στην ψηφιακή οικονομία)], πληροφοριών ή εγγράφων που υποβάλλονται σε επεξεργασία ή διατηρούνται στο πλαίσιο των δικτύων τους ή των υπηρεσιών ηλεκτρονικής επικοινωνίας που παρέχουν, συμπεριλαμβανομένων των τεχνικών δεδομένων που σχετίζονται με την ταυτοποίηση των αριθμών εγγραφής ή συνδέσεως με υπηρεσίες παροχής ηλεκτρονικών επικοινωνιών, με την καταγραφή του συνόλου των αριθμών συνδρομητή ή συνδέσεως συγκεκριμένου προσώπου, με τον γεωγραφικό εντοπισμό του τερματικού εξοπλισμού που χρησιμοποιείται καθώς και με τις κλήσεις ενός συνδρομητή όσον αφορά τον κατάλογο των εισερχόμενων και εξερχόμενων κλήσεων, καθώς και τη διάρκεια και την ημερομηνία των συνδιαλέξεων [...]».

16. Στα άρθρα L. 851-2 και L. 851-4 ρυθμίζεται, για διαφορετικούς σκοπούς και σύμφωνα με διαφορετικές διαδικασίες, η σε πραγματικό χρόνο διοικητική πρόσβαση στα κατά τα ανωτέρω διατηρούμενα δεδομένα συνδέσεως.

17. Το άρθρο L. 851-2 επιτρέπει, για τους σκοπούς και μόνον της προλήψεως της τρομοκρατίας, τη συλλογή πληροφοριών ή εγγράφων που προβλέπονται στο άρθρο L. 851-1, από τα ίδια πρόσωπα. Η συλλογή αυτή, η οποία αφορά αποκλειστικώς ένα ή περισσότερα πρόσωπα που έχουν προηγουμένως χαρακτηριστεί ως ύποπτα για εμπλοκή σε τρομοκρατική απειλή, γίνεται σε πραγματικό χρόνο. Το ίδιο ισχύει όσον αφορά το άρθρο L. 851-4, το οποίο επιτρέπει τη διαβίβαση σε πραγματικό χρόνο από τους διαχειριστές μόνο τεχνικών δεδομένων για τον εντοπισμό του τερματικού εξοπλισμού<sup>14</sup>.

18. Το άρθρο L. 851-3 επιτρέπει να επιβληθεί στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών και στους τεχνικούς παρόχους «η εφαρμογή αυτοματοποιημένης επεξεργασίας στα δίκτυά τους με σκοπό, ανάλογα με τις παραμέτρους που καθορίζονται στην άδεια, τον εντοπισμό συνδέσεων που δύνανται να αποκαλύψουν τρομοκρατική απειλή»<sup>15</sup>.

19. Το άρθρο L. 851-5 ορίζει ότι, υπό συγκεκριμένες προϋποθέσεις, «μπορεί να επιτραπεί η χρήση τεχνικού μέσου που καθιστά δυνατό τον εντοπισμό σε πραγματικό χρόνο προσώπου, οχήματος ή αντικειμένου».

<sup>14</sup> Κατά το αιτούν δικαστήριο, οι μέθοδοι αυτές δεν δημιουργούν για τους παρόχους υπηρεσιών πρόσθετη υποχρέωση διατήρησης πέραν αυτής που απαιτείται για την τιμολόγηση των υπηρεσιών τους, τη διάθεσή τους στην αγορά και την παροχή υπηρεσιών προστιθέμενης αξίας.

<sup>15</sup> Κατά το αιτούν δικαστήριο, η μέθοδος αυτή, η οποία δεν επάγεται γενική και χωρίς διάκριση διατήρηση, σκοπεύει αποκλειστικώς στη συλλογή, για περιορισμένο χρονικό διάστημα, μεταξύ του συνόλου των υποβαλλόμενων σε επεξεργασία από τα πρόσωπα αυτά δεδομένων συνδέσεως, εκείνων των δεδομένων που θα μπορούσαν να συνδέονται με την εν λόγω σοβαρή παράβαση.

20. Κατά το άρθρο L. 851-6, παράγραφος I, είναι δυνατή, υπό συγκεκριμένες προϋποθέσεις, «η απευθείας συλλογή [...], μέσω συσκευής ή τεχνικού μέσου σύμφωνα με το άρθρο 226-3, παράγραφος 1, του code pénal [(ποινικού κώδικα)], τεχνικών δεδομένων συνδέσεως που καθιστούν δυνατή την ταυτοποίηση τερματικού εξοπλισμού ή του αριθμού συνδρομητή του χρήστη του, καθώς και των δεδομένων σχετικά με τον εντοπισμό του χρησιμοποιούμενου τερματικού εξοπλισμού».

## **2. Κώδικας περί ταχυδρομείων και ηλεκτρονικών επικοινωνιών**

21. Κατά το άρθρο L. 34-1, ως ίσχυε κατά τον χρόνο των πραγματικών περιστατικών:

«I. Το παρόν άρθρο εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο παροχής στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών· εφαρμόζεται ιδίως στα δίκτυα που υποστηρίζουν συσκευές συλλογής δεδομένων και ταυτοποίησης.

II. Με την επιφύλαξη των διατάξεων των παραγράφων III, IV, V και VI, οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών, και ιδίως τα πρόσωπα των οποίων η δραστηριότητα συνίσταται στην παροχή προσβάσεως σε υπηρεσίες ηλεκτρονικής επικοινωνίας προς το κοινό, πρέπει να απαλείφουν ή να καθιστούν ανώνυμα κάθε είδους δεδομένα κινήσεως.

Όποιος παρέχει στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών θεωρείται, τηρουμένων των διατάξεων του προηγούμενου εδαφίου, εσωτερικές διαδικασίες ώστε να απαντά στα αιτήματα των αρμόδιων αρχών.

Όποιος, στο πλαίσιο κύριας ή δευτερεύουσας επαγγελματικής δραστηριότητας, προσφέρει στο κοινό σύνδεση που καθιστά δυνατή ηλεκτρονική επικοινωνία μέσω της προσβάσεως σε δίκτυο, ακόμη και δωρεάν, υποχρεούται να τηρεί τις διατάξεις που εφαρμόζονται στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών δυνάμει του παρόντος άρθρου.

III. Για τη διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων ή την εκπλήρωση της υποχρεώσεως που ορίζεται στο άρθρο L. 336-3 του code de la propriété intellectuelle [(κώδικα διανοητικής ιδιοκτησίας)] ή για την αποτροπή επιθέσεων στα συστήματα αυτοματοποιημένης επεξεργασίας δεδομένων οι οποίες προβλέπονται και τιμωρούνται από τα άρθρα 323-1 έως 323-3-1 του ποινικού κώδικα και με μοναδικό σκοπό, εφόσον είναι αναγκαίο, τη διάθεσή τους στη δικαστική αρχή ή στην ανώτατη αρχή που προβλέπεται στο άρθρο L. 331-12 του κώδικα διανοητικής ιδιοκτησίας ή στην εθνική αρχή ασφαλείας των πληροφοριακών συστημάτων που προβλέπεται στο άρθρο L. 2321-1 του code de la défense [(κώδικα εθνικής άμυνας)], επιτρέπεται η αναβολή για μέγιστη διάρκεια ενός έτους των ενεργειών διαγραφής ή ανωνυμοποίησης ορισμένων κατηγοριών τεχνικών δεδομένων. Με διάταγμα υποκείμενο στη διαδικασία του Conseil d'État (Συμβουλίου Επικρατείας), εκδιδόμενο κατόπιν γνωμοδότησεως της Commission nationale de l'informatique et des libertés [(εθνικής επιτροπής πληροφορικής και ελευθεριών)], καθορίζονται, εντός των ορίων που προβλέπονται στην παράγραφο VI, οι κατηγορίες αυτές δεδομένων και η διάρκεια της διατηρήσεώς τους, ανάλογα με τη δραστηριότητα των παρόχων και τη φύση των επικοινωνιών, καθώς και ο τρόπος αντισταθμίσεως, κατά περίπτωση, των επιπλέον ειδικών και προσδιορισμένων πρόσθετων δαπανών για τις υπηρεσίες που παρασχέθηκαν από τους παρόχους κατόπιν αιτήματος του Δημοσίου.

[...]

VI. Τα δεδομένα που αποθηκεύονται και υποβάλλονται σε επεξεργασία υπό τους όρους των παραγράφων III, IV και V αφορούν αποκλειστικώς την ταυτοποίηση των χρηστών των παρεχόμενων από τους παρόχους, τα τεχνικά χαρακτηριστικά των παρεχόμενων επικοινωνιών και τον εντοπισμό του τερματικού εξοπλισμού.

Τα δεδομένα αυτά δεν επιτρέπεται να αφορούν το περιεχόμενο της επικοινωνίας ή των κάθε είδους πληροφοριών στις οποίες υπήρξε πρόσβαση στο πλαίσιο της παροχής των ως άνω υπηρεσιών επικοινωνίας.

Η διατήρηση και η επεξεργασία των δεδομένων πραγματοποιείται σύμφωνα με τις διατάξεις του νόμου 78-17, της 6ης Ιανουαρίου 1978, περί πληροφορικής, αρχείων και ελευθεριών.

Οι πάροχοι λαμβάνουν όλα τα μέτρα προς αποτροπή της χρήσεως των δεδομένων αυτών για σκοπούς άλλους από εκείνους που προβλέπονται στο παρόν άρθρο.»

22. Δυνάμει του άρθρου R. 10-13, παράγραφος I, του κώδικα περί ταχυδρομείων και ηλεκτρονικών επικοινωνιών, οι πάροχοι οφείλουν να διατηρούν, για τους σκοπούς της διερευνήσεως, της διαπιστώσεως και της διώξεως ποινικών αδικημάτων, τα ακόλουθα δεδομένα:

- «α) τις πληροφορίες που καθιστούν δυνατή την ταυτοποίηση του χρήστη·
- b) τα δεδομένα σχετικά με τον χρησιμοποιούμενο τερματικό εξοπλισμό επικοινωνίας·
- c) τα τεχνικά χαρακτηριστικά, καθώς επίσης και την ημερομηνία, την ώρα και τη διάρκεια εκάστης επικοινωνίας·
- d) τα δεδομένα σχετικά με τις ζητηθείσες ή χρησιμοποιηθείσες συμπληρωματικές υπηρεσίες και τους παρόχους τους·
- e) τα δεδομένα που καθιστούν δυνατή την ταυτοποίηση του ή των αποδεκτών της επικοινωνίας».

23. Σύμφωνα με την παράγραφο II του ίδιου άρθρου, στην περίπτωση της τηλεφωνίας, ο πάροχος οφείλει να διατηρεί, επιπλέον, τα δεδομένα που διευκολύνουν την ταυτοποίηση της προελεύσεως και της θέσεως της επικοινωνίας.

24. Κατά την παράγραφο III του ίδιου άρθρου, τα ως άνω δεδομένα πρέπει να διατηρούνται για ένα έτος από την ημερομηνία καταχωρίσεώς τους.

### **3. Loi n.º 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (νόμος 2004-575, της 21ης Ιουνίου 2004, για την εμπιστοσύνη στην ψηφιακή οικονομία)**

25. Το πρώτο εδάφιο της παραγράφου II του άρθρου 6 του νόμου 2004-575 ορίζει ότι τα πρόσωπα των οποίων η δραστηριότητα συνίσταται στην παροχή προσβάσεως σε υπηρεσίες ηλεκτρονικών επικοινωνιών προς το κοινό και τα φυσικά ή νομικά πρόσωπα τα οποία προβαίνουν, ακόμη και δωρεάν, με σκοπό να καθίστανται προσιτά στο κοινό μέσω υπηρεσιών ηλεκτρονικής επικοινωνίας προς το κοινό, σε αποθήκευση κάθε είδους σημάτων, κειμένου, εικόνων, ήχων ή μηνυμάτων που προέρχονται από τους αποδέκτες των υπηρεσιών αυτών, «φυλάσσουν και διατηρούν τα δεδομένα κατά τρόπο ώστε να καθίσταται δυνατή η ταυτοποίηση κάθε προσώπου που συνέβαλε στη δημιουργία του περιεχομένου ή μέρους του περιεχομένου των παρεχομένων από αυτά υπηρεσιών».

26. Το τρίτο εδάφιο της παραγράφου II του ίδιου άρθρου ορίζει ότι η δικαστική αρχή δύναται να αξιώνει από τα πρόσωπα αυτά την κοινοποίηση των δεδομένων του πρώτου εδαφίου.



27. Σύμφωνα με το τελευταίο εδάφιο της παραγράφου II, με διάταγμα υποκείμενο στη διαδικασία του Conseil d'État (Συμβουλίου της Επικρατείας) «ορίζονται τα κατά το πρώτο εδάφιο δεδομένα και καθορίζονται η διάρκεια και οι τρόποι διατηρήσεώς τους»<sup>16</sup>.

## II. Πραγματικά περιστατικά και προδικαστικά ερωτήματα

### A. Υπόθεση C-511/18

28. Η La Quadrature du Net, η French Data Network, η Igwan.net και η Fédération des fournisseurs d'accès à internet associatifs (στο εξής: προσφεύγουσες) ζήτησαν από το Conseil d'État (Συμβούλιο της Επικρατείας) την ακύρωση διαφόρων διαταγμάτων εφαρμογής ορισμένων διατάξεων του κώδικα εσωτερικής ασφάλειας<sup>17</sup>.

29. Οι αιτούσες υποστήριξαν, εν συνόψει, ότι τόσο τα προσβληθέντα διατάγματα όσο και οι διατάξεις αυτές του κώδικα εσωτερικής ασφάλειας προσέβαλλαν τα δικαιώματα σεβασμού της ιδιωτικής ζωής, προστασίας των δεδομένων προσωπικού χαρακτήρα και πραγματικής προσφυγής, όπως αυτά κατοχυρώνονται, αντιστοίχως, στα άρθρα 7, 8 και 47 του Χάρτη.

30. Υπό τις συνθήκες αυτές, το Conseil d'État (Συμβούλιο της Επικρατείας) υποβάλλει στο Δικαστήριο τα ακόλουθα προδικαστικά ερωτήματα:

«1) Πρέπει να γίνει δεκτό ότι η υποχρέωση γενικής και χωρίς διάκριση διατήρησης, η οποία επιβάλλεται στους παρόχους βάσει των επιτρεπτικών διατάξεων του άρθρου 15, παράγραφος 1, της οδηγίας [2002/58], συνιστά, στο πλαίσιο των συνεχιζόμενων σοβαρών απειλών για την εθνική ασφάλεια, και ιδίως λόγω του τρομοκρατικού κινδύνου, επέμβαση η οποία δικαιολογείται από το δικαίωμα στην ασφάλεια, που κατοχυρώνεται από το άρθρο 6 του Χάρτη [...], και από τις απαιτήσεις της εθνικής ασφάλειας για την οποία αποκλειστικώς υπεύθυνα είναι τα κράτη μέλη σύμφωνα με το άρθρο 4 [ΣΕΕ];

<sup>16</sup> Τα δεδομένα αυτά ορίστηκαν με το décret n.º 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (διάταγμα 2011-219, της 25ης Φεβρουαρίου 2011, σχετικά με τη διατήρηση των δεδομένων που επιτρέπουν την ταυτοποίηση όσων έχουν συμβάλει στη δημιουργία του προσφερόμενου ηλεκτρονικού περιεχομένου). Από το διάταγμα αυτό άξια μνείας είναι: 1) το άρθρο 1, παράγραφος 1, κατά το οποίο όσοι παρέχουν πρόσβαση σε υπηρεσίες ηλεκτρονικής επικοινωνίας οφείλουν να διατηρούν τα ακόλουθα δεδομένα: το αναγνωριστικό στοιχείο ταυτότητας της συνδέσεως, το χορηγηθέν στον συνδρομητή αναγνωριστικό στοιχείο ταυτότητας, το αναγνωριστικό στοιχείο ταυτότητας του χρησιμοποιηθέντος για τη σύνδεση τεμαχικού, την ημερομηνία και ώρα ενάρξεως και λήξεως της συνδέσεως, τα χαρακτηριστικά της γραμμής του συνδρομητή· β) το άρθρο 1, παράγραφος 2, δυνάμει του οποίου όσοι προβαίνουν, ακόμη και δωρεάν, με σκοπό να καθιστανται προσιτά στο κοινό μέσω υπηρεσιών ηλεκτρονικής επικοινωνίας προς το κοινό, σε αποθήκευση κάθε είδους σημάτων, κειμένων, εικόνων, ήχων ή μηνυμάτων που προέρχονται από τους αποδέκτες των υπηρεσιών αυτών οφείλουν να διατηρούν, για κάθε πράξη επικοινωνίας, τα ακόλουθα δεδομένα: το αναγνωριστικό στοιχείο ταυτότητας της συνδέσεως στην πηγή της επικοινωνίας, το αναγνωριστικό στοιχείο ταυτότητας που χορηγήθηκε στο αποτελούν το αντικείμενο της πράξεως περιεχόμενο, τα είδη πρωτοκόλλων που χρησιμοποιήθηκαν για τη σύνδεση με την υπηρεσία και για τη μεταφορά περιεχομένου, τη φύση της πράξεως, την ημερομηνία και την ώρα της πράξεως, το αναγνωριστικό στοιχείο ταυτότητας που χρησιμοποιήθηκε από τον διενεργούντα την πράξη· και γ) τέλος, το άρθρο 1, παράγραφος 3, το οποίο ορίζει ότι τα κατά τις δύο προηγούμενες παραγράφους πρόσωπα οφείλουν να διατηρούν τις ακόλουθες πληροφορίες οι οποίες παρέχονται από τον χρήστη κατά τη σύναψη συμβάσεως ή κατά τη δημιουργία λογαριασμού: το αναγνωριστικό στοιχείο ταυτότητας της συνδέσεως κατά τη δημιουργία του λογαριασμού· ονοματεπώνυμο ή επωνυμία· τις συναφείς ταχυδρομικές διευθύνσεις, τα χρησιμοποιούμενα ψευδώνυμα, τις συναφείς διευθύνσεις ηλεκτρονικού ταχυδρομείου ή λογαριασμού, τους αριθμούς τηλεφώνου, τον ενημερωμένο κωδικό προσβάσεως και τα στοιχεία που επιτρέπουν την επαλήθευση ή τροποποίησή του.

<sup>17</sup> Τα προσβληθέντα διατάγματα ήταν τα εξής: α) το décret n.º 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (διάταγμα 2015-1885, της 28ης Σεπτεμβρίου 2015, περί καθορισμού των εξειδικευμένων υπηρεσιών πληροφοριών)· β) το décret n.º 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (διάταγμα 2015-1211, της 1ης Οκτωβρίου 2015, περί ενδίκων διαφορών σχετικών με την εφαρμογή των μεθόδων συλλογής πληροφοριών που προϋποθέτουν τη χορήγηση αδείας και των αρχείων που άπτονται της κρατικής ασφάλειας)· γ) το décret n.º 2015-1639 du 11 décembre 2015 relatif à la désignation des services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure (διάταγμα 2015-1639, της 11ης Δεκεμβρίου 2015, περί καθορισμού των εξειδικευμένων υπηρεσιών πέραν των υπηρεσιών πληροφοριών, οι οποίες δύνανται να χρησιμοποιούν τις μεθόδους που αναφέρονται στον τίτλο V του βιβλίου VIII του κώδικα εσωτερικής ασφάλειας)· και δ) το décret n.º 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (διάταγμα 2016-67, της 29ης Ιανουαρίου 2016, περί των μεθόδων συλλογής πληροφοριών).

- 2) Έχει η οδηγία [2002/58], ερμηνευόμενη με γνώμονα τον Χάρτη [...], την έννοια ότι επιτρέπει νομοθετικά μέτρα, όπως τα μέτρα συλλογής σε πραγματικό χρόνο δεδομένων κυκλοφορίας και θέσης σχετικά με συγκεκριμένα πρόσωπα, τα οποία, αν και επηρεάζουν τα δικαιώματα και τις υποχρεώσεις των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών, δεν τους επιβάλλουν, εντούτοις, ειδική υποχρέωση διατηρήσεως των δεδομένων τους;
- 3) Έχει οδηγία [2002/58], ερμηνευόμενη με γνώμονα τον Χάρτη [...], την έννοια ότι εξαρτά σε όλες τις περιπτώσεις τη νομιμότητα της διαδικασίας συλλογής των δεδομένων συνδέσεως από απαίτηση ενημερώσεως των υποκειμένων των δεδομένων, όταν η ενημέρωση αυτή δεν δύναται πλέον να θέσει σε κίνδυνο τις έρευνες που διεξάγουν οι αρμόδιες αρχές ή όταν οι διαδικασίες αυτές μπορούν να θεωρηθούν σύννομες, λαμβανομένων υπόψη όλων των άλλων υφιστάμενων διαδικαστικών εγγυήσεων, δεδομένου ότι με αυτές διασφαλίζεται η αποτελεσματικότητα του δικαιώματος προσφυγής;»

## **B. Υπόθεση C-512/18**

31. Οι αιτούσες στην κύρια δίκη στην υπόθεση C-511/18, πλην της Iqwan.net, ζήτησαν επίσης από το Conseil d'État (Συμβούλιο της Επικρατείας) να ακυρώσει τη σιωπηρή απόρριψη της αιτήσεώς τους περί καταργήσεως του άρθρου R. 10-13 του code des postes et des communications électroniques (κώδικα ταχυδρομείων και ηλεκτρονικών επικοινωνιών) και του διατάγματος 2011-219, της 25ης Φεβρουαρίου 2011.

32. Κατά την άποψη των αιτουσών, οι προσβληθέντες κανόνες επιβάλλουν υποχρέωση διατηρήσεως των δεδομένων κινήσεως, θέσεως και συνδέσεως που, λόγω του γενικού χαρακτήρα της, συνιστά δυσανάλογη προσβολή των δικαιωμάτων σεβασμού της ιδιωτικής και οικογενειακής ζωής, προστασίας των δεδομένων προσωπικού χαρακτήρα και ελεύθερης εκφράσεως, τα οποία προστατεύονται από τα άρθρα 7, 8 και 11 του Χάρτη, κατά παράβαση του άρθρου 15, παράγραφος 1, της οδηγίας 2002/58.

33. Στο πλαίσιο της δίκης αυτής, το Conseil d'État (Συμβούλιο της Επικρατείας) υπέβαλε τα ακόλουθα προδικαστικά ερωτήματα:

- «1) Πρέπει να γίνει δεκτό ότι η υποχρέωση γενικής και χωρίς διάκριση διατηρήσεως, η οποία επιβάλλεται στους παρόχους βάσει των επιτρεπτικών διατάξεων του άρθρου 15, παράγραφος 1, της οδηγίας [2002/58] [...], συνιστά, λαμβανομένων ιδίως υπόψη των εγγυήσεων και ελέγχων που ισχύουν εν συνεχεία όσον αφορά τη συλλογή και τη χρήση των δεδομένων αυτών συνδέσεως, επέμβαση η οποία δικαιολογείται από το δικαίωμα στην ασφάλεια, που κατοχυρώνεται από το άρθρο 6 του Χάρτη [...], και από τις απαιτήσεις της εθνικής ασφάλειας για την οποία αποκλειστικώς υπεύθυνα είναι τα κράτη μέλη σύμφωνα με το άρθρο 4 [ΣΕΕ];
- 2) Έχουν οι διατάξεις της οδηγίας [2000/31] [...], ερμηνευόμενες με γνώμονα τα άρθρα 6, 7, 8 και 11, καθώς και το άρθρο 52, παράγραφος 1, του Χάρτη [...], την έννοια ότι επιτρέπουν σε κράτος να θεσπίσει εθνική ρύθμιση που επιβάλλει στα πρόσωπα των οποίων η δραστηριότητα συνίσταται στην παροχή προσβάσεως σε υπηρεσίες ηλεκτρονικών επικοινωνιών προς το κοινό και στα φυσικά ή νομικά πρόσωπα τα οποία προβαίνουν, ακόμη και δωρεάν, με σκοπό να καθίστανται προσιτά στο κοινό μέσω υπηρεσιών ηλεκτρονικής επικοινωνίας προς το κοινό, σε αποθήκευση κάθε είδους σημάτων, κειμένων, εικόνων, ήχων ή μηνυμάτων που προέρχονται από τους αποδέκτες των υπηρεσιών αυτών, την υποχρέωση να διατηρούν τα δεδομένα τα οποία καθιστούν δυνατή την ταυτοποίηση κάθε προσώπου που συνέβαλε στη δημιουργία του περιεχομένου ή μέρους του περιεχομένου των παρεχόμενων από αυτά υπηρεσιών, ούτως ώστε η δικαστική αρχή να δύναται, εφόσον είναι αναγκαίο, να ζητήσει την κοινοποίησή τους με σκοπό την εφαρμογή των κανόνων περί αστικής ή ποινικής ευθύνης;

### III. Διαδικασία ενώπιον του Δικαστηρίου και θέσεις των διαδίκων

34. Οι αιτήσεις προδικαστικής αποφάσεως περιήλθαν στο Δικαστήριο στις 3 Αυγούστου 2018.

35. Γραπτές παρατηρήσεις κατέθεσαν η La Quadrature du Net, η Fédération des fournisseurs d'accès à Internet associatifs, η French Data Network, η Γερμανική, η Βελγική, η Βρετανική, η Τσεχική, η Κυπριακή, η Δανική, η Ισπανική, η Εσθονική, η Γαλλική, η Ουγγρική, η Ιρλανδική, η Πολωνική και η Σουηδική Κυβέρνηση, καθώς και η Επιτροπή.

36. Στις 9 Σεπτεμβρίου 2019 διεξήχθη επ' ακροατηρίου συζήτηση από κοινού με τις υποθέσεις C-623/17, Privacy International, και C-520/18, Ordre des barreaux francophones et germanophone κ.λπ., στην οποία παρέστησαν οι διάδικοι των τεσσάρων προδικαστικών παραπομπών, οι προμνησθείσες κυβερνήσεις και αυτές των Κάτω Χωρών και της Νορβηγίας, καθώς και η Επιτροπή και ο Ευρωπαϊός Επόπτης Προστασίας Δεδομένων.

### IV. Ανάλυση

37. Τα ερωτήματα του Conseil d'État (Συμβουλίου της Επικρατείας) μπορούν να ομαδοποιηθούν σε τρία:

- πρώτον, εάν είναι συμβατή προς το δίκαιο της Ένωσης εθνική ρύθμιση η οποία επιβάλλει στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών την υποχρέωση γενικής και χωρίς διάκριση διατηρήσεως των δεδομένων συνδέσεως (πρώτο ερώτημα στην υπόθεση C-511/18 και στην υπόθεση C-512/18) και, ιδίως, των δεδομένων που καθιστούν δυνατή την ταυτοποίηση των δημιουργών του περιεχομένου που προσφέρουν οι εν λόγω πάροχοι (δεύτερο ερώτημα στην υπόθεση C-512/18).
- Δεύτερον, εάν η νομιμότητα των διαδικασιών συλλογής δεδομένων συνδέσεως εξαρτάται, σε κάθε περίπτωση, από την απαίτηση ενημερώσεως των υποκειμένων των δεδομένων, υπό τον όρο ότι δεν τίθενται σε κίνδυνο οι έρευνες (τρίτο ερώτημα στην υπόθεση C-511/18).
- Τρίτον, εάν η συλλογή σε πραγματικό χρόνο δεδομένων κινήσεως και θέσεως, χωρίς υποχρέωση διατηρήσεώς τους, είναι συμβατή –και υπό ποιες προϋποθέσεις– με την οδηγία 2002/58 (δεύτερο ερώτημα στην υπόθεση C-511/18).

38. Ζητείται να διαπιστωθεί, σε τελική ανάλυση, εάν είναι σύμφωνη με το δίκαιο της Ένωσης εθνική ρύθμιση η οποία επιβάλλει στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών δύο είδη υποχρεώσεων: α) αφενός, τη *συλλογή* ορισμένων δεδομένων, όχι όμως τη διατήρησή τους· β) αφετέρου, τη *διατήρηση* των δεδομένων συνδέσεως και αυτών που διευκολύνουν την ταυτοποίηση των δημιουργών του περιεχομένου των παρεχόμενων από τους παρόχους αυτούς υπηρεσιών.

39. Προηγουμένως θα πρέπει να εξεταστεί εάν, λόγω ακριβώς του πλαισίου<sup>18</sup> εντός του οποίου θεσπίστηκε η εθνική αυτή ρύθμιση (ήτοι, υπό συνθήκες ενδεχόμενης απειλής κατά της εθνικής ασφάλειας), έχει εφαρμογή η οδηγία 2002/58.

18 «[Σ]το πλαίσιο των συνεχιζόμενων σοβαρών απειλών για την εθνική ασφάλεια, και ιδίως λόγω του τρομοκρατικού κινδύνου», όπως αναφέρεται στο πρώτο ερώτημα της υποθέσεως C-511/18.

## A. Επί της δυνατότητας εφαρμογής της οδηγίας 2002/58

40. Το αιτούν δικαστήριο λαμβάνει ως δεδομένο ότι η επίμαχη ρύθμιση εμπίπτει στο πεδίο εφαρμογής της οδηγίας 2002/58. Αυτό προκύπτει, κατά την κρίση του, από την απόφαση *Tele2 Sverige* και *Watson* και επιβεβαιώθηκε με την απόφαση *Ministerio Fiscal*.

41. Αντιθέτως, ορισμένες από τις κυβερνήσεις που μετέχουν στη διαδικασία ισχυρίζονται ότι η επίμαχη ρύθμιση δεν εμπίπτει στο πεδίο εφαρμογής της εν λόγω οδηγίας. Προς στήριξη της θέσεώς τους, επικαλούνται, μεταξύ άλλων, την απόφαση της 30ής Μαΐου 2006, Κοινοβούλιο κατά Συμβουλίου και Επιτροπής<sup>19</sup>.

42. Συμφωνώ με το *Conseil d'État* (Συμβούλιο της Επικρατείας) ότι η απόφαση *Tele2 Sverige* και *Watson* έχει επιλύσει το ζήτημα αυτό, επιβεβαιώνοντας ότι η οδηγία 2002/58 έχει, κατ' αρχήν, εφαρμογή όταν οι πάροχοι των ηλεκτρονικών υπηρεσιών υποχρεούνται βάσει νόμου να διατηρούν τα δεδομένα των συνδρομητών τους και να επιτρέπουν στις δημόσιες αρχές την πρόσβαση σε αυτά. Αυτό ουδόλως αναιρείται από το γεγονός ότι οι υποχρεώσεις επιβάλλονται στους παρόχους για λόγους εθνικής ασφάλειας.

43. Οφείλω να αναφέρω, ήδη από το σημείο αυτό, ότι εάν υπήρχε δυσαρμονία μεταξύ της αποφάσεως *Tele2 Sverige* και *Watson* και των προηγούμενων αποφάσεων, υπερισχύουσα θα έπρεπε να θεωρηθεί η εν λόγω απόφαση δεδομένου ότι είναι μεταγενέστερη και έχει επιβεβαιωθεί με την απόφαση *Ministerio Fiscal*. Φρονώ, ωστόσο, ότι δεν υφίσταται τέτοιου είδους δυσαρμονία, όπως θα επιχειρήσω να εξηγήσω.

### 1. Απόφαση Κοινοβούλιο κατά Συμβουλίου και Επιτροπής

44. Οι υποθέσεις επί των οποίων εξεδόθη η απόφαση Κοινοβούλιο κατά Συμβουλίου και Επιτροπής αφορούσαν:

- τη συμφωνία μεταξύ της Ευρωπαϊκής Κοινότητας και των Ηνωμένων Πολιτειών της Αμερικής σχετικά με την επεξεργασία και τη διαβίβαση των δεδομένων PNR [Passenger Name Records (καταστάσεων με τα ονόματα των επιβατών)] από τους αερομεταφορείς προς τις αρχές των Ηνωμένων Πολιτειών<sup>20</sup>.
- την ικανοποιητική προστασία των δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται στον φάκελο των επιβατών ο οποίος διαβιβάζεται στις εν λόγω αρχές<sup>21</sup>.

45. Το Δικαστήριο κατέληξε στο συμπέρασμα ότι η διαβίβαση των δεδομένων αυτών αποτελούσε επεξεργασία η οποία είχε ως αντικείμενο τη δημόσια ασφάλεια και τις δραστηριότητες του κράτους στον ποινικό τομέα. Σύμφωνα με το άρθρο 3, παράγραφος 2, πρώτη περίπτωση, της οδηγίας 95/46, οι δύο αυτές επίμαχες αποφάσεις δεν ενέπιπταν στο πεδίο εφαρμογής της εν λόγω οδηγίας.

<sup>19</sup> Υποθέσεις C-317/04 και C-318/04 (στο εξής: Κοινοβούλιο κατά Συμβουλίου και Επιτροπής, EU:C:2006:346).

<sup>20</sup> Απόφαση 2004/496/EK του Συμβουλίου, της 17ης Μαΐου 2004, για τη σύναψη συμφωνίας μεταξύ της Ευρωπαϊκής Κοινότητας και των Ηνωμένων Πολιτειών της Αμερικής σχετικά με την επεξεργασία και τη διαβίβαση των καταστάσεων με τα ονόματα των επιβατών από τους αερομεταφορείς προς το Υπουργείο Εσωτερικής Ασφάλειας, Υπηρεσία Τελωνείων και Προστασίας των Συνόρων των Ηνωμένων Πολιτειών (EE 2004, L 183, σ. 83, και διορθωτικό EE 2005, L 255, σ. 168) (υπόθεση C-317/04).

<sup>21</sup> Απόφαση 2004/535/EK της Επιτροπής, της 14ης Μαΐου 2004, σχετικά με την ικανοποιητική προστασία των δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται στο φάκελο των επιβατών (Passenger Name Record) αεροπορικών μεταφορών ο οποίος διαβιβάζεται στο Bureau of Customs and Border Protection (Υπηρεσία Τελωνείων και Προστασίας των Συνόρων) των Ηνωμένων Πολιτειών της Αμερικής (EE 2004, L 235, σ. 11) (υπόθεση C-318/04).

46. Τα δεδομένα συλλέγονταν αρχικώς από τους αερομεταφορείς στο πλαίσιο δραστηριότητας –πώληση εισιτηρίων– η οποία ανήκε στη σφαίρα εφαρμογής του δικαίου της Ένωσης. Ωστόσο, η επεξεργασία τους, όπως προβλεπόταν στην επίμαχη απόφαση, «[δεν ήταν] αναγκαία για την παροχή των υπηρεσιών, αλλά [...] για την προάσπιση της δημόσιας ασφάλειας και για κατασταλτικούς σκοπούς»<sup>22</sup>.

47. Το Δικαστήριο υιοθέτησε κατ' αυτόν τον τρόπο μια τελεολογική προσέγγιση, λαμβάνοντας υπόψη τον σκοπό τον οποίον επεδίωκε η επεξεργασία των δεδομένων: στον βαθμό κατά τον οποίον η επεξεργασία αυτή σκοπούσε στην προστασία της δημόσιας ασφάλειας, έπρεπε να θεωρηθεί ότι εκφεύγει του πεδίου εφαρμογής της οδηγίας 95/46. Ωστόσο, ο σκοπός αυτός δεν ήταν το μοναδικό κρίσιμο κριτήριο<sup>23</sup>, λόγος για τον οποίον το Δικαστήριο υπογράμμισε ότι η επεξεργασία αυτή «εντάσσεται σε ένα πλαίσιο που έχουν δημιουργήσει οι δημόσιες αρχές σχετικά με τη δημόσια ασφάλεια»<sup>24</sup>.

48. Η απόφαση Κοινοβούλιο κατά Συμβουλίου και Επιτροπής καταδεικνύει, συνεπώς, τη διαφορά μεταξύ της ρήτρας εξαιρέσεως και των ρητρών περιορισμού που προβλέπει η οδηγία 95/46 (παρόμοιες με αυτές της οδηγίας 2002/58). Είναι, ωστόσο, αληθές ότι αμφότερες αναφέρονται σε παρόμοιους σκοπούς γενικού συμφέροντος, γεγονός που δημιουργεί κάποιου είδους σύγχυση ως προς το αντίστοιχο εύρος τους, όπως είχε επισημάνει τότε ο γενικός εισαγγελέας Υ. Βοτ<sup>25</sup>.

49. Στη σύγχυση αυτή οφείλεται ίσως η άποψη των κρατών μελών τα οποία τάσσονται υπέρ της μη εφαρμογής, στο πλαίσιο αυτό, της οδηγίας 2002/58. Κατά την άποψή τους, το συμφέρον της εθνικής ασφάλειας διασφαλίζεται μόνο μέσω της εξαιρέσεως του άρθρου 1, παράγραφος 3, της οδηγίας 2002/58. Είναι, ωστόσο, αληθές ότι το ίδιο αυτό συμφέρον εξυπηρετούν επίσης οι επιτρεπόμενοι από το άρθρο 15, παράγραφος 1, της εν λόγω οδηγίας περιορισμοί, μεταξύ των οποίων περιλαμβάνεται και ο σχετικός με την εθνική ασφάλεια. Το τελευταίο αυτό άρθρο θα ήταν περιττό εάν η κάθε είδους επίκληση της εθνικής ασφάλειας καθιστούσε ανεφάρμοστη την οδηγία 2002/58.

## 2. Απόφαση *Tele2 Sverige και Watson*

50. Με την απόφαση *Tele2 Sverige και Watson* εξετάστηκε εάν ορισμένα εθνικά καθεστώτα, τα οποία επέβαλλαν στους παρόχους προσβάσιμων στο κοινό υπηρεσιών ηλεκτρονικής επικοινωνίας γενική υποχρέωση διατηρήσεως των δεδομένων σχετικά με τις εν λόγω επικοινωνίες, ήταν συμβατά με το δίκαιο της Ένωσης. Οι περιπτώσεις ήταν, ως εκ τούτου, κατ' ουσίαν ταυτόσημες με αυτές που αποτελούν το αντικείμενο των υπό κρίση προδικαστικών παραπομπών.

22 Απόφαση Κοινοβούλιο κατά Συμβουλίου και Επιτροπής, σκέψη 57. Στη σκέψη 58, το Δικαστήριο επισημαίνει ότι το «γεγονός ότι τα δεδομένα [...] έχουν συλλεγεί από ιδιωτικούς φορείς για εμπορικούς σκοπούς και ότι οι φορείς αυτοί οργανώνουν τη διαβίβασή τους σε τρίτο κράτος» δεν σημαίνει ότι η διαβίβαση αυτή δεν αποτελεί μια από τις περιπτώσεις μη εφαρμογής της οδηγίας 95/46 οι οποίες απαριθμούνται στο άρθρο 3, παράγραφος 2, πρώτη περίπτωση, της τελευταίας, καθόσον «η διαβίβαση αυτή εντάσσεται σε ένα πλαίσιο που έχουν δημιουργήσει οι δημόσιες αρχές σχετικά με τη δημόσια ασφάλεια».

23 Ούτως θα επεσήμαινε, μεταγενέστερα, ο αιώνηστος γενικός εισαγγελέας Υ. Βοτ στις προτάσεις του στην υπόθεση Ιρλανδία κατά Κοινοβουλίου και Συμβουλίου (C-301/06, EU:C:2008:558). Υποστήριξε ότι η απόφαση Κοινοβούλιο κατά Συμβουλίου και Επιτροπής «δεν μπορεί να σημαίνει [...] ότι μόνον η εξέταση του σκοπού της επεξεργασίας των προσωπικών δεδομένων έχει σημασία για το αν θα περιληφθεί ή θα εξαιρεθεί η επεξεργασία αυτή από το πεδίο εφαρμογής του συστήματος προστασίας των δεδομένων που έθεσε σε εφαρμογή η οδηγία 95/46. Πρέπει επίσης να εξακριβωθεί το πλαίσιο του είδους δραστηριοτήτων στο οποίο πραγματοποιείται η επεξεργασία δεδομένων. Η επεξεργασία αυτή εξαιρείται από το κοινοτικό σύστημα προστασίας προσωπικών δεδομένων της οδηγίας 95/46 μόνο στις περιπτώσεις που πραγματοποιείται κατά την άσκηση των δραστηριοτήτων κρατών ή κρατικών αρχών και δεν αφορά τους τομείς δραστηριοτήτων των ιδιωτών, τούτο δε κατ' εφαρμογή του άρθρου 3, παράγραφος 2, πρώτη περίπτωση, της οδηγίας αυτής» (σημείο 122).

24 Απόφαση Κοινοβούλιο κατά Συμβουλίου και Επιτροπής, σκέψη 58. Η συμφωνία είχε ως κύριο σκοπό να απαιτηθεί από τους αερομεταφορείς επιβατών μεταξύ της Ένωσης και των Ηνωμένων Πολιτειών να παρέχουν στις αρχές των Ηνωμένων Πολιτειών ηλεκτρονική πρόσβαση στα στοιχεία PNR των φακέλων ονομάτων των επιβατών που τηρούνται στο πληροφοριακό τους σύστημα ελέγχου κρατήσεων και αναχωρήσεων. Η συμφωνία εγκαθίδρυε, επομένως, μια μορφή διεθνούς συνεργασίας μεταξύ της Ένωσης και των Ηνωμένων Πολιτειών για την καταπολέμηση της τρομοκρατίας και άλλων σοβαρών εγκλημάτων, επιχειρώντας να συμβιβάσει τον σκοπό αυτόν με την προστασία των δεδομένων προσωπικού χαρακτήρα των επιβατών. Στο πλαίσιο αυτό, η επιβαλλόμενη στους αερομεταφορείς υποχρέωση δεν διέφερε σημαντικά από την άμεση ανταλλαγή δεδομένων μεταξύ δημοσίων αρχών.

25 Προτάσεις του γενικού εισαγγελέα Υ. Βοτ στην υπόθεση Ιρλανδία κατά Κοινοβουλίου και Συμβουλίου (C-301/06, EU:C:2008:558, σημείο 127).

51. Ευρισκόμενο εκ νέου αντιμέτωπο με το ζήτημα της δυνατότητας εφαρμογής του δικαίου της Ένωσης –πλέον υπό το καθεστώς της οδηγίας 2002/58–, το Δικαστήριο επισήμανε κατ' αρχάς ότι «το πεδίο εφαρμογής της οδηγίας 2002/58 πρέπει να ερμηνεύεται λαμβάνοντας υπόψη, μεταξύ άλλων, τη γενική οικονομία της τελευταίας»<sup>26</sup>.

52. Υπό το πρίσμα αυτό, το Δικαστήριο επεσήμανε ότι, «[α]σφαλώς, τα νομοθετικά μέτρα που προβλέπονται στο άρθρο 15, παράγραφος 1, της οδηγίας 2002/58 αφορούν δραστηριότητες που ασκούνται από τα κράτη ή από τις κρατικές αρχές και δεν αφορούν τους τομείς δραστηριότητας των ιδιωτών [...] Επιπροσθέτως, οι σκοποί τους οποίους, βάσει της εν λόγω διατάξεως, πρέπει να επιδιώκουν τα μέτρα αυτά, ήτοι εν προκειμένω η διαφύλαξη της εθνικής ασφάλειας [...], αλληλοεπικαλύπτονται σε μεγάλο βαθμό με τους σκοπούς τους οποίους επιδιώκουν οι δραστηριότητες που περιλαμβάνονται στο άρθρο 1, παράγραφος 3, της εν λόγω οδηγίας»<sup>27</sup>.

53. Επομένως, ο σκοπός των μέτρων που, σύμφωνα με το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58, μπορούν να θεσπίζουν τα κράτη μέλη για τον περιορισμό του δικαιώματος στην ιδιωτική ζωή αλληλοεπικαλύπτεται (ως προς το σημείο αυτό) με αυτόν που, σύμφωνα με το άρθρο 1, παράγραφος 3, της οδηγίας, δικαιολογεί την εξαίρεση ορισμένων κρατικών δραστηριοτήτων από το καθεστώς της.

54. Ωστόσο, το Δικαστήριο έκρινε ότι, «λαμβανομένης υπόψη της γενικής οικονομίας της οδηγίας 2002/58», δεν μπορεί από την περίπτωση αυτή να «συναχθεί ότι τα νομοθετικά μέτρα στα οποία αναφέρεται το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58 αποκλείονται από το πεδίο εφαρμογής της εν λόγω οδηγίας, διαφορετικά η ως άνω διάταξη θα στερείτο πρακτικής αποτελεσματικότητας. Συγκεκριμένα, η ως άνω διάταξη προϋποθέτει κατ' ανάγκη ότι τα εθνικά μέτρα στα οποία αυτή αναφέρεται [...] εμπίπτουν στο πεδίο εφαρμογής της εν λόγω οδηγίας, δεδομένου ότι εξουσιοδοτεί ρητώς τα κράτη μέλη να λαμβάνουν τέτοια μέτρα μόνον υπό τους όρους που αυτή θεσπίζει»<sup>28</sup>.

55. Επιπλέον, οι επιτρεπόμενοι από το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58 περιορισμοί «διέπουν, για τους σκοπούς που ορίζονται στην εν λόγω διάταξη, τη δραστηριότητα των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών». Επομένως, το άρθρο αυτό, σε συνδυασμό με το άρθρο 3 της οδηγίας «έχει την έννοια ότι τα νομοθετικά αυτά μέτρα εμπίπτουν στο πεδίο εφαρμογής της εν λόγω οδηγίας»<sup>29</sup>.

56. Ως εκ τούτου, το Δικαστήριο υποστήριξε ότι στο πεδίο εφαρμογής της οδηγίας 2002/58 εμπίπτει τόσο το νομοθετικό μέτρο που επιβάλλει στους παρόχους «τη διατήρηση των δεδομένων κινήσεως και των δεδομένων θέσεως, δεδομένου ότι η εν λόγω δραστηριότητα συνεπάγεται, κατ' ανάγκη, την εκ μέρους τους επεξεργασία δεδομένων προσωπικού χαρακτήρα»<sup>30</sup> όσο και αυτό που διέπει την πρόσβαση των αρχών στα δεδομένα που διατηρούν οι εν λόγω πάροχοι<sup>31</sup>.

57. Η ερμηνεία της οδηγίας 2002/58 στην οποία προέβη το Δικαστήριο με την απόφαση *Tele2 Sverige* και *Watson* επαναλαμβάνεται στην απόφαση *Ministerio Fiscal*.

26 Απόφαση *Tele2 Sverige* και *Watson* (σκέψη 67).

27 Όπ.π. (σκέψη 72).

28 Όπ.π. (σκέψη 73).

29 Όπ.π. (σκέψη 74).

30 Όπ.π. (σκέψη 75).

31 Όπ.π. (σκέψη 76).

58. Θα μπορούσε να υποστηριχθεί ότι η απόφαση Tele2 Sverige και Watson συνιστά μεταστροφή της νομολογίας, κατά το μάλλον ή ήττον έμμεση, σε σχέση με την απόφαση Κοινοβούλιο κατά Συμβουλίου και Επιτροπής; Αυτό υποστηρίζει, παραδείγματος χάριν, η Ιρλανδική Κυβέρνηση, κατά την οποία μόνον η τελευταία είναι συμβατή με τη νομική βάση της οδηγίας 2002/58 και σέβεται το άρθρο 4, παράγραφος 2, ΣΕΕ<sup>32</sup>.

59. Η Γαλλική Κυβέρνηση, από την πλευρά της, εκτιμά ότι η αντίφαση θα μπορούσε να αποφευχθεί εάν ληφθεί υπόψη ότι η απόφαση Tele2 Sverige και Watson αναφέρεται στις δραστηριότητες των κρατών μελών στον τομέα του ποινικού δικαίου, ενώ η απόφαση Κοινοβούλιο κατά Συμβουλίου και Επιτροπής αφορά την ασφάλεια του κράτους και την εθνική άμυνα. Έτσι, κατά την άποψή της, η απόφαση Tele2 Sverige και Watson δεν έχει εφαρμογή στην υπό εξέταση περίπτωση, στην οποία θα πρέπει να ακολουθηθεί η λύση που υιοθετήθηκε με την απόφαση Κοινοβούλιο κατά Συμβουλίου και Επιτροπής<sup>33</sup>.

60. Όπως έχω ήδη αναφέρει, φρονώ ότι είναι δυνατή η ανεύρεση κάποιου τρόπου συγκερασμού των δύο αυτών αποφάσεων, διαφορετικού από αυτόν που υποστηρίζει η Γαλλική Κυβέρνηση. Δεν συμφωνώ με την τελευταία, καθόσον, κατά τη άποψή μου, οι εκτιμήσεις της αποφάσεως Tele2 Sverige και Watson, οι οποίες αναφέρονται ρητώς στην καταπολέμηση της τρομοκρατίας<sup>34</sup>, ισχύουν κατ' αναλογίαν για κάθε άλλου είδους απειλή κατά της εθνικής ασφάλειας (στις οποίες περιλαμβάνεται μεταξύ άλλων και η τρομοκρατία).

### ***3. Δυνατότητα συνδυαστικής ερμηνείας της αποφάσεως Κοινοβούλιο κατά Συμβουλίου και Επιτροπής και της αποφάσεως Tele2 Sverige και Watson***

61. Κατά τη γνώμη μου, με τις αποφάσεις Tele2 Sverige και Watson και Ministerio Fiscal, το Δικαστήριο έλαβε υπόψη τον λόγο υπάρξεως των ρητρών εξαιρέσεως και περιορισμού, καθώς και τη συστηματική σχέση μεταξύ των δύο αυτών ειδών ρητρών.

62. Εάν στην υπόθεση Κοινοβούλιο κατά Συμβουλίου και Επιτροπής το Δικαστήριο έκρινε ότι η επεξεργασία των δεδομένων δεν ενέπιπτε στο πεδίο εφαρμογής της οδηγίας 95/46, αυτό οφειλόταν, όπως έχω ήδη αναφέρει, στο γεγονός ότι, στο πλαίσιο της συνεργασίας μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών, ήτοι σε τυπική περίπτωση διεθνούς πλαισίου, έπρεπε να υπερισχύσει η κρατική διάσταση της δραστηριότητας έναντι του γεγονότος ότι η εν λόγω επεξεργασία είχε επίσης εμπορική ή ιδιωτική διάσταση. Ένα από τα τότε επίμαχα ζητήματα ήταν, ακριβώς, η κατάλληλη νομική βάση για την προσβληθείσα απόφαση.

63. Αντιθέτως, όσον αφορά τα εθνικά μέτρα που εξετάστηκαν με τις αποφάσεις Tele2 Sverige και Watson και Ministerio Fiscal, το Δικαστήριο τοποθέτησε σε πρώτο πλάνο την εσωτερική διάσταση της επεξεργασίας δεδομένων: το νομοθετικό πλαίσιο εντός του οποίου πραγματοποιούνταν η επεξεργασία αυτή ήταν αποκλειστικώς εθνικό, με αποτέλεσμα να απουσιάζει η εξωτερική διάσταση που χαρακτήριζε το αντικείμενο της αποφάσεως Κοινοβούλιο κατά Συμβουλίου και Επιτροπής.

64. Η διαφορετική βαρύτητα μεταξύ της διεθνούς και της εθνικής διαστάσεως (εμπορικής και ιδιωτικής) της επεξεργασίας δεδομένων είχε ως συνέπεια, στην πρώτη υπόθεση, να επιβληθεί η ρήτρα εξαιρέσεως από το πεδίο εφαρμογής του δικαίου της Ένωσης ως η πλέον κατάλληλη για την προστασία του γενικού συμφέροντος της εθνικής ασφάλειας. Στη δεύτερη, αντιθέτως, το ίδιο αυτό συμφέρον μπορούσε να εξυπηρετηθεί αποτελεσματικά μέσω της κατά το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58 ρήτρας περιορισμού.

32 Σημεία 15 και 16 των γραπτών παρατηρήσεων της Ιρλανδικής Κυβερνήσεως.

33 Σημεία 34 έως 50 των γραπτών παρατηρήσεων της Γαλλικής Κυβερνήσεως.

34 Απόφαση Tele2 Sverige και Watson (σκέψεις 103 και 119).

65. Θα μπορούσε να παρατηρηθεί και άλλη διαφορά, συνδεδεμένη με το διαφορετικό νομοθετικό πλαίσιο: έκαστη εκ των αποφάσεων αυτών επικεντρώθηκε στην ερμηνεία δύο άρθρων που, πέραν της φαινομενικής ομοιότητάς τους, δεν είναι ταυτόσημα.

66. Έτσι, η απόφαση Κοινοβούλιο κατά Συμβουλίου και Επιτροπής αφορούσε την ερμηνεία του άρθρου 3, παράγραφος 2, της οδηγίας 95/46, ενώ η απόφαση Tele2 Sverige και Watson την ερμηνεία του άρθρου 1, παράγραφος 3, της οδηγίας 2002/58. Η προσεκτική ανάγνωση των άρθρων αυτών καταδεικνύει μια επαρκή διαφορά προκειμένου να στηριχθεί η κρίση του Δικαστηρίου τόσο στη μία όσο και την άλλη υπόθεση.

67. Κατά το άρθρο 3, παράγραφος 2, της οδηγίας 95/46, «[ο]ι διατάξεις της παρούσας οδηγίας δεν εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα [...] η οποία πραγματοποιείται στο πλαίσιο δραστηριοτήτων που δεν εμπίπτουν στο πεδίο εφαρμογής του κοινοτικού δικαίου [...] και, εν πάση περιπτώσει, στην επεξεργασία δεδομένων που αφορά τη δημόσια ασφάλεια, την εθνική άμυνα, την ασφάλεια του κράτους (συμπεριλαμβανομένης και της οικονομικής ευημερίας του, εφόσον η επεξεργασία αυτή συνδέεται με θέματα ασφάλειας του κράτους) και τις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου»<sup>35</sup>.

68. Από την άλλη πλευρά, η οδηγία 2002/58, σύμφωνα με το άρθρο της 1, παράγραφος 3, «δεν εφαρμόζεται σε δραστηριότητες οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής της συνθήκης για την ίδρυση της Ευρωπαϊκής Κοινότητας [...], και σε κάθε περίπτωση στις δραστηριότητες που αφορούν τη δημόσια ασφάλεια, την εθνική άμυνα, την ασφάλεια του κράτους (συμπεριλαμβανομένης της οικονομικής ευημερίας του κράτους εφόσον οι δραστηριότητες συνδέονται με θέματα ασφάλειας του κράτους) και στις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου»<sup>36</sup>.

69. Ενώ το άρθρο 3, παράγραφος 2, της οδηγίας 95/46 εξαιρεί την επεξεργασία δεδομένων η οποία έχει ως αντικείμενο –καθ' ο μέρος ενδιαφέρει εν προκειμένω– την ασφάλεια του κράτους, το άρθρο 1, παράγραφος 3, της οδηγίας 2002/58 εξαιρεί τις δραστηριότητες οι οποίες αποσκοπούν στη διαφύλαξη –ομοίως καθ' ο μέρος ενδιαφέρει εν προκειμένω– της ασφάλειας του κράτους.

70. Η διαφορά δεν είναι αμελητέα. Η οδηγία 95/46 άφηνε εκτός του πεδίου εφαρμογής της μια δραστηριότητα (την «επεξεργασία δεδομένων προσωπικού χαρακτήρα») η οποία μπορεί να πραγματοποιηθεί από οιονδήποτε. Από τη δραστηριότητα αυτήν εξαιρούνταν ρητώς η επεξεργασία που, μεταξύ άλλων, είχε ως αντικείμενο την ασφάλεια του κράτους. Αντιθέτως, ήταν άνευ σημασίας η φύση του προσώπου ή φορέα που θα προέβαινε στην επεξεργασία των δεδομένων. Η προσέγγιση που υιοθετήθηκε για τον καθορισμό των εξαιρούμενων πράξεων ήταν, συνεπώς, τελεολογική ή βάσει του επιδιωκόμενου σκοπού, χωρίς διάκριση υποκειμένου.

71. Γίνεται, επομένως, κατανοητό ότι, στην υπόθεση Κοινοβούλιο κατά Συμβουλίου και Επιτροπής, το Δικαστήριο έλαβε κατά κύριο λόγο υπόψη τον σκοπό που επεδίωκε η επεξεργασία δεδομένων. Δεν ασκούσε επιρροή «το γεγονός ότι τα δεδομένα [...] έχουν συλλεχθεί από ιδιωτικούς φορείς για εμπορικούς σκοπούς και ότι οι φορείς αυτοί οργανώνουν τη διαβίβασή τους σε τρίτη χώρα», καθόσον κρίσιμο ήταν ότι «η διαβίβαση αυτή εντάσσεται σε ένα πλαίσιο που έχουν δημιουργήσει οι δημόσιες αρχές σχετικά με τη δημόσια ασφάλεια»<sup>37</sup>.

72. Αντιθέτως, «οι δραστηριότητες που έχουν ως αντικείμενο την ασφάλεια του κράτους» δεν εμπίπτουν στο εξετασθέν στην υπόθεση Tele2 Sverige και Watson πεδίο εφαρμογής της οδηγίας 2002/58 και δεν προσιδιάζουν σε κανένα άλλο υποκείμενο πλην του ίδιου του κράτους. Επιπλέον, δεν περιλαμβάνονται σε αυτές η νομοθετική ή ρυθμιστική λειτουργία του κράτους, αλλά αυστηρώς οι υλικές ενέργειες των δημοσίων αρχών.

<sup>35</sup> Η υπογράμμιση δική μου.

<sup>36</sup> Η υπογράμμιση δική μου.

<sup>37</sup> Απόφαση Κοινοβούλιο κατά Συμβουλίου και Επιτροπής (σκέψη 58).



73. Πράγματι, οι απαριθμούμενες στο άρθρο 1, παράγραφος 3, της οδηγίας 2002/58 *δραστηριότητες* «είναι, σε όλες τις περιπτώσεις, δραστηριότητες που ασκούνται από τα κράτη ή από τις κρατικές αρχές και δεν αφορούν τους τομείς δραστηριότητας των ιδιωτών»<sup>38</sup>. Εξάλλου, οι «δραστηριότητες» αυτές δεν μπορούν να είναι νομοθετικής φύσεως. Εάν ήταν έτσι, όλες οι διατάξεις που θεσπίζουν τα κράτη μέλη σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα θα εξέφευγαν του πεδίου εφαρμογής της οδηγίας 2002/58, εφόσον ως δικαιολογητικός λόγος προβαλλόταν η αναγκαιότητά τους για τη διαφύλαξη της ασφάλειας του κράτους.

74. Αφενός, αυτό θα έθιγε σε σημαντικό βαθμό την αποτελεσματικότητα της εν λόγω οδηγίας, καθόσον η απλή επίκληση μιας τόσο αφηρημένης νομικής έννοιας όπως αυτή της εθνικής ασφάλειας θα αρκούσε για να καταστήσει ανεφάρμοστες έναντι των κρατών μελών τις εγγυήσεις που ο νομοθέτης της Ένωσης έχει θεσπίσει για την προστασία των δεδομένων προσωπικού χαρακτήρα των πολιτών. Η προστασία αυτή είναι ανέφικτη χωρίς τη συνδρομή των κρατών μελών, διασφαλίζεται δε, ως προς τον πολίτη, και έναντι των εθνικών δημοσίων αρχών.

75. Αφετέρου, μια ερμηνεία του όρου «κρατικές δραστηριότητες» η οποία θα περιελάμβανε όσες συνίστανται στη θέσπιση νομικών κανόνων και διατάξεων θα καθιστούσε κενό περιεχομένου το άρθρο 15 της οδηγίας 2002/58, το οποίο εξουσιοδοτεί ακριβώς τα κράτη μέλη να λαμβάνουν –για λόγους προστασίας, μεταξύ άλλων, της εθνικής ασφάλειας– «νομοθετικά μέτρα» για να περιορίζουν ορισμένα δικαιώματα και υποχρεώσεις που προβλέπει η ίδια οδηγία<sup>39</sup>.

76. Όπως επισήμανε το Δικαστήριο στην υπόθεση *Tele2 Sverige και Watson*, «το πεδίο εφαρμογής της οδηγίας 2002/58 πρέπει να ερμηνεύεται λαμβάνοντας υπόψη, μεταξύ άλλων, τη γενική οικονομία της τελευταίας»<sup>40</sup>. Υπό το πρίσμα αυτό, η ερμηνεία του άρθρου 1, παράγραφος 3, και του άρθρου 15, παράγραφος 1, της οδηγίας 2002/58, η οποία τους προσδίδει περιεχόμενο χωρίς θίγει την αποτελεσματικότητά τους είναι εκείνη που εντοπίζει, στο πρώτο από τα άρθρα αυτά, μια καθ' ύλην εξαίρεση σχετικά με τις *δραστηριότητες* που αναπτύσσουν τα κράτη μέλη στον τομέα της εθνικής ασφάλειας (και στους αντίστοιχους τομείς) και, στο δεύτερο, μια εξουσιοδότηση για τη θέσπιση *νομοθετικών μέτρων* (ήτοι, κανόνων γενικής ισχύος) τα οποία, για τους σκοπούς της εθνικής ασφάλειας, διέπουν τις δραστηριότητες των προσώπων που υπόκεινται στο *imperium* των κρατών μελών, περιορίζοντας τα κατοχυρούμενα από την οδηγία 2002/58 δικαιώματα.

#### 4. Εξαίρεση της εθνικής ασφάλειας κατά την οδηγία 2002/58

77. Η εθνική ασφάλεια (ή η συνώνυμή της έκφραση «ασφάλεια του κράτους», όπως σημειώνει το άρθρο της 15, παράγραφος 1) αποτελεί αντικείμενο δύο ρυθμίσεων στην οδηγία 2002/58. Αφενός, αποτελεί λόγο *εξαίρεσης* (από το πεδίο εφαρμογής της οδηγίας αυτής) για όλες εκείνες τις δραστηριότητες των κρατών μελών που, ειδικώς, την «αφορούν». Αφετέρου, παρουσιάζεται ως λόγος *περιορισμού*, ο οποίος πρέπει να τίθεται σε εφαρμογή με νόμο, των προβλεπόμενων στην οδηγία 2002/58 δικαιωμάτων και υποχρεώσεων, ήτοι, έναντι δραστηριοτήτων ιδιωτικής ή εμπορικής φύσεως οι οποίες δεν εμπίπτουν στο πεδίο των δραστηριοτήτων δημοσίας αρχής<sup>41</sup>.

38 Απόφαση *Ministerio Fiscal* (σκέψη 32). Υπό την ίδια έννοια, απόφαση *Tele2 Sverige και Watson* (σκέψη 72).

39 Δυσχερώς, πράγματι, θα μπορούσε να υποστηριχθεί ότι το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58 επιτρέπει τον περιορισμό των κατά την οδηγία αυτή δικαιωμάτων και υποχρεώσεων σε ένα πεδίο που, όπως αυτό της εθνικής ασφάλειας, εκφεύγει, κατ' αρχήν, του πεδίου εφαρμογής της, δυνάμει του άρθρου 1, παράγραφος 3, της ίδιας της οδηγίας. Όπως έκρινε το Δικαστήριο με την απόφαση *Tele2 Sverige και Watson* (σκέψη 73), το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58 «προϋποθέτει κατ' ανάγκην ότι τα εθνικά μέτρα στα οποία αυτή αναφέρεται [...] εμπίπτουν στο πεδίο εφαρμογής της εν λόγω οδηγίας, δεδομένου ότι εξουσιοδοτεί ρητώς τα κράτη μέλη να λαμβάνουν τέτοια μέτρα μόνον υπό τους όρους που αυτή θεσπίζει».

40 Απόφαση *Tele2 Sverige και Watson* (σκέψη 67).

41 Όπως επισήμαινε, παρεμπιπτόντως, ο γενικός εισαγγελέας Η. Saugmandsgaard Øe στις προτάσεις του στην υπόθεση *Ministerio Fiscal* (C-207/16, EU:C:2018:300, σημείο 47), «δεν πρέπει να συγχέονται, αφενός, τα δεδομένα προσωπικού χαρακτήρα τα οποία υποβάλλονται *άμεσα* σε επεξεργασία στο πλαίσιο των δραστηριοτήτων –δημόσιας αρχής– του κράτους σε τομέα του ποινικού δικαίου και, αφετέρου, εκείνα που υποβάλλονται σε επεξεργασία στο πλαίσιο των –εμπορικού χαρακτήρα– δραστηριοτήτων παρόχου υπηρεσιών ηλεκτρονικών επικοινωνιών τα οποία χρησιμοποιούνται *εν συνεχεία* από τις αρμόδιες κρατικές αρχές».

78. Σε ποιες δραστηριότητες αναφέρεται το άρθρο 1, παράγραφος 3, της οδηγίας 2002/58; Κατά τη γνώμη μου, το ίδιο το Conseil d'État (Συμβούλιο της Επικρατείας) προσφέρει ένα πρώτης τάξεως παράδειγμα κατά την παράθεση των άρθρων L. 851-5 και L. 851-6 του κώδικα εσωτερικής ασφάλειας, κάνοντας λόγο για τις «μεθόδους συλλογής πληροφοριών που εφαρμόζονται απευθείας από το κράτος χωρίς να διέπουν τις δραστηριότητες των φορέων παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών, επιβάλλοντάς τους ειδικές υποχρεώσεις»<sup>42</sup>.

79. Φρονώ ότι εδώ βρίσκεται το κλειδί για τον προσδιορισμό του πεδίου εφαρμογής της εξαιρέσεως του άρθρου 1, παράγραφος 3, της οδηγίας 2002/58. Δεν εμπίπτουν στο καθεστώς του οι δραστηριότητες που έχουν ως σκοπό τη διαφύλαξη της εθνικής ασφάλειας και διεξάγονται από τις ίδιες τις δημόσιες αρχές, χωρίς τη συνδρομή ιδιωτών και χωρίς, ως εκ τούτου, να επιβάλλονται υποχρεώσεις στους τελευταίους όσον αφορά τη διαχείριση των επιχειρήσεών τους.

80. Ωστόσο, το φάσμα δραστηριοτήτων των δημοσίων αρχών που εξαιρούνται από το γενικό καθεστώς επεξεργασίας των δεδομένων προσωπικού χαρακτήρα πρέπει να ερμηνεύεται στενά. Συγκεκριμένα, η έννοια της εθνικής ασφάλειας, η αρμοδιότητα επί της οποίας ανήκει κατ' αποκλειστικότητα, σύμφωνα με το άρθρο 4, παράγραφος 2, ΣΕΕ, σε κάθε κράτος μέλος, δεν μπορεί να εκτείνεται σε άλλους τομείς, κατά το μάλλον ή ήττον συναφείς, του δημόσιου βίου.

81. Καθ' ο μέρος τα υπό κρίση προδικαστικά ερωτήματα αφορούν την εμπλοκή ιδιωτών (ήτοι, εκείνων που παρέχουν στους χρήστες υπηρεσίες ηλεκτρονικών επικοινωνιών) και όχι την απλή παρέμβαση των κρατικών αρχών, δεν χρειάζεται να επεκταθώ στην οριοθέτηση της εν στενή έννοια εθνικής ασφάλειας.

82. Φρονώ, ωστόσο, ότι ως κατευθυντήρια γραμμή μπορεί να χρησιμοποιηθεί το κριτήριο της αποφάσεως-πλαίσίου 2006/960/ΔΕΥ<sup>43</sup>, το άρθρο 2, στοιχείο α', της οποίας διακρίνει μεταξύ των εν ευρεία έννοια υπηρεσιών ασφαλείας –που περιλαμβάνουν την «εθνική αστυνομική, τελωνειακή ή άλλη αρχή στην οποία η εθνική νομοθεσία έχει αναθέσει να εντοπίζει, να προλαμβάνει και να διερευνά αξιόποινες πράξεις ή εγκληματικές δραστηριότητες καθώς και να ασκεί εξουσία και να λαμβάνει καταναγκαστικά μέτρα στα πλαίσια των δραστηριοτήτων αυτών»–, αφενός, και των «υπηρεσιών ή μονάδ[ων] που ασχολούνται ειδικά με θέματα εθνικής ασφάλειας», αφετέρου<sup>44</sup>.

83. Στην αιτιολογική σκέψη 11 της οδηγίας 2002/58 αναφέρεται ότι αυτή, «όπως και η οδηγία 95/46 [...] δεν υπεισέρχεται σε θέματα προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών που συνδέονται με δραστηριότητες οι οποίες δεν διέπονται από το [...] δίκαιο [της Ένωσης]». Επομένως, η οδηγία 2002/58 «δεν αλλάζει την υφιστάμενη ισορροπία ανάμεσα στο δικαίωμα του ατόμου στην ιδιωτική ζωή και τη δυνατότητα των κρατών μελών να θεσπίζουν μέτρα όπως αυτά που αναφέρονται στο άρθρο 15 παράγραφος 1 της παρούσας οδηγίας, εφόσον είναι αναγκαία για την προστασία [...] της ασφάλειας του κράτους [...]».

84. Υφίσταται, πράγματι, συνέχεια μεταξύ της οδηγίας 95/46 και της οδηγίας 2002/58 όσον αφορά τις αρμοδιότητες των κρατών μελών σε θέματα εθνικής ασφάλειας. Καμία εξ αυτών δεν έχει ως αντικείμενο την προστασία των θεμελιωδών δικαιωμάτων στον συγκεκριμένο αυτόν τομέα στον οποίο οι δραστηριότητες των κρατών μελών δεν «διέπονται από το δίκαιο [της Ένωσης]».

42 Σημεία 18 και 21 της αποφάσεως περί παραπομπής στην υπόθεση C-511/18.

43 Απόφαση πλαίσιο του Συμβουλίου, της 18ης Δεκεμβρίου 2016, για την απλούστευση της ανταλλαγής πληροφοριών και στοιχείων μεταξύ των αρχών επιβολής του νόμου των κρατών μελών της Ευρωπαϊκής Ένωσης (ΕΕ 2006, L 386, σ. 89).

44 Στο ίδιο πνεύμα, το άρθρο 1, παράγραφος 4, της αποφάσεως-πλαίσίου 2008/977/ΔΕΥ του Συμβουλίου, της 27ης Νοεμβρίου 2008, για την προστασία των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις (ΕΕ 2008, L 350, σ. 60), όριζε ότι «δεν θίγει τα ζωτικά συμφέροντα εθνικής ασφάλειας και τις ειδικές δραστηριότητες συλλογής πληροφοριών στον τομέα της εθνικής ασφάλειας».

85. Η «ισορροπία» στην οποία αναφέρεται η εν λόγω αιτιολογική σκέψη είναι απόρροια της ανάγκης σεβασμού των αρμοδιοτήτων των κρατών μελών σε θέματα ασφάλειας, όταν τις ασκούν *ευθέως και με ίδια μέσα*. Αντιθέτως, όταν, ακόμη και για τους ίδιους αυτούς λόγους εθνικής ασφάλειας, απαιτείται η συνδρομή ιδιωτών, στους οποίους επιβάλλονται ορισμένες υποχρεώσεις, το γεγονός αυτό σηματοδοτεί την είσοδο σε ένα πεδίο (την απαιτούμενη από τους ιδιωτικούς αυτούς φορείς προστασία της ιδιωτικής ζωής) το οποίο διέπεται από το δίκαιο της Ένωσης.

86. Τόσο η οδηγία 95/46 όσο και η οδηγία 2002/58 επιδιώκουν να επιτύχουν την ισορροπία αυτή επιτρέποντας τον περιορισμό των δικαιωμάτων των ιδιωτών δυνάμει νομοθετικών μέτρων που θεσπίζουν τα κράτη μέλη στο πλαίσιο των άρθρων τους 13, παράγραφος 1, και 15, παράγραφος 1, αντιστοίχως. Ουδεμία διαφορά υφίσταται ως προς το σημείο αυτό μεταξύ αμφοτέρων των οδηγιών.

87. Όσον αφορά τον κανονισμό 2016/679 ο οποίος διαμορφώνει (νέο) γενικό πλαίσιο για την προστασία των δεδομένων προσωπικού χαρακτήρα, το άρθρο του 2, παράγραφος 2, αναφέρει ότι δεν διέπει την «επεξεργασία δεδομένων προσωπικού χαρακτήρα» που πραγματοποιείται «από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του κεφαλαίου 2 του τίτλου V της ΣΕΕ».

88. Όπως στην οδηγία 95/46 όπου η επεξεργασία δεδομένων προσωπικού χαρακτήρα οριοθετούνταν μόνο βάσει του σκοπού της, ανεξαρτήτως του προσώπου που την πραγματοποιούσε, στον κανονισμό 2016/679 οι εξαιρούμενες κατηγορίες επεξεργασίας προσδιορίζονται τόσο από τον σκοπό τους όσο και από αυτούς που τις πραγματοποιούν: εξαιρείται η επεξεργασία που πραγματοποιείται από τα κράτη μέλη κατά την άσκηση *δραστηριότητας* που δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης (στοιχεία α' και β' της παραγράφου 2 του άρθρου 2) και εκείνη που εκτελείται από τις αρχές για τους σκοπούς της καταπολέμησης των ποινικών αδικημάτων και της προστασίας έναντι απειλών κατά της δημόσιας ασφάλειας<sup>45</sup>.

89. Ο καθορισμός των δραστηριοτήτων αυτών της δημόσιας εξουσίας πρέπει κατ' ανάγκην να είναι περιοριστικός, ειδάλλως η νομοθεσία της Ένωσης σε ζητήματα προστασίας της ιδιωτικής ζωής θα καθίστατο κενή περιεχομένου. Ο κανονισμός 2016/679 προβλέπει στο άρθρο του 23 –όπως το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58– τον περιορισμό, *μέσω νομοθετικών μέτρων*, των δικαιωμάτων και των υποχρεώσεων που θεσπίζει, όταν αυτό είναι αναγκαίο για τη διασφάλιση, μεταξύ άλλων σκοπών, της ασφάλειας του κράτους, της εθνικής άμυνας ή της δημόσιας ασφάλειας. Εκ νέου, εάν η προστασία των σκοπών αυτών αρκούσε για την εξαίρεση από το πεδίο εφαρμογής του κανονισμού 2016/679, θα ήταν περιττή η επίκληση της ασφάλειας του κράτους ως δικαιολογητικής βάσεως για τον περιορισμό, μέσω νομοθετικών μέτρων, των κατοχυρούμενων από τον κανονισμό αυτόν δικαιωμάτων.

90. Όπως συμβαίνει με την οδηγία 2002/58, δεν θα ήταν λογικό τα νομοθετικά μέτρα που προβλέπονται στο άρθρο 23 του κανονισμού 2016/679 (ο οποίος, επαναλαμβάνω, επιτρέπει κρατικής προελεύσεως περιορισμούς στα δικαιώματα ιδιωτικής ζωής για λόγους ασφάλειας του κράτους) να εμπίπτουν στο πεδίο εφαρμογής του τελευταίου και, ταυτοχρόνως, η προστασία της ασφάλειας του κράτους να καθιστά ανεφάρμοστο, άνευ ετέρου, τον ίδιον τον κανονισμό, πράγμα που θα σήμαινε ότι δεν αναγνωρίζεται κανενός είδους υποκειμενικό δικαίωμα.

<sup>45</sup> Ο κανονισμός 2016/679 εξαιρεί, πράγματι, από το πεδίο εφαρμογής του την επεξεργασία δεδομένων που πραγματοποιείται από τα κράτη μέλη κατά την άσκηση *δραστηριότητας* που δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης, καθώς και αυτήν που εκτελείται από τις αρχές για τους σκοπούς της προστασίας της δημόσιας ασφάλειας.

## **B. Επιβεβαίωση και δυνατότητες ανάπτυξεως της νομολογίας Tele2 Sverige και Watson**

91. Με τις προτάσεις μου στην υπόθεση C-520/18 προέβην σε επισταμένη ανάλυση<sup>46</sup> της νομολογίας του Δικαστηρίου στον τομέα αυτόν, κατόπιν της οποίας τάσσομαι υπέρ της επιβεβαίωσεως της, προτείνοντας ταυτοχρόνως συγκεκριμένη ερμηνευτική οδό για την αποσαφήνιση του περιεχομένου της.

92. Παραπέμπω στην ανάλυση αυτή, η οποία δεν χρήζει, κατά την άποψη μου, παραθέσεως εν προκειμένω για λόγους απλής οικονομίας. Οι παρατηρήσεις που πρόκειται να εκθέσω εν συνεχεία επί των προδικαστικών ερωτημάτων του Conseil d'Etat (Συμβουλίου της Επικρατείας) πρέπει, συνεπώς, να αναγνωστούν, λαμβανομένων ως δεδομένων των αντίστοιχων σημείων των προτάσεων στην υπόθεση C-520/18.

## **Γ. Απάντηση επί των προδικαστικών ερωτημάτων**

### **1. Ως προς την υποχρέωση διατηρήσεως των δεδομένων (πρώτο προδικαστικό ερώτημα στις υποθέσεις C-511/18 και C-512/18 και δεύτερο προδικαστικό ερώτημα στην υπόθεση C-512/18)**

93. Όσον αφορά την επιβαλλομένη στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών υποχρέωση διατηρήσεως των δεδομένων, το αιτούν δικαστήριο ζητεί συγκεκριμένα να μάθει:

- Εάν η υποχρέωση αυτή, που επιβάλλεται δυνάμει του άρθρου 15, παράγραφος 1, της οδηγίας 2002/58, συνιστά επέμβαση η οποία δικαιολογείται από το κατοχυρούμενο στο άρθρο 6 του Χάρτη «δικαίωμα στην ασφάλεια» και από τις απαιτήσεις εθνικής ασφάλειας (πρώτο ερώτημα στις υποθέσεις C-511/18 και C-512/18, καθώς και τρίτο ερώτημα της υποθέσεως C-511/18).
- Εάν η οδηγία 2000/31 επιτρέπει τη διατήρηση δεδομένων που καθιστούν δυνατή την ταυτοποίηση όσων έχουν συμβάλει στη δημιουργία των διαθέσιμων προς το κοινό ηλεκτρονικών περιεχομένων (δεύτερο ερώτημα στην υπόθεση C-512/18).

### **α) Προκαταρκτική παρατήρηση**

94. Το Conseil d'Etat (Συμβούλιο της Επικρατείας) αναφέρεται στα θεμελιώδη δικαιώματα που αναγνωρίζονται στα άρθρα 7 (σεβασμός της ιδιωτικής και οικογενειακής ζωής), 8 (προστασία των δεδομένων προσωπικού χαρακτήρα) και 11 (ελευθερία εκφράσεως και πληροφορήσεως) του Χάρτη. Αυτά είναι, πράγματι, τα δικαιώματα που, σύμφωνα με το Δικαστήριο, θα μπορούσαν να θιγούν από την υποχρέωση διατηρήσεως δεδομένων κινήσεως την οποία οι εθνικές αρχές επιβάλλουν στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών<sup>47</sup>.

95. Το αιτούν δικαστήριο αναφέρεται επίσης στο προστατευόμενο από το άρθρο 6 του Χάρτη δικαίωμα στην ασφάλεια. Το επικαλείται μάλλον ως παράγοντα που θα μπορούσε να νομιμοποιήσει την επιβολή της εν λόγω υποχρέωσεως και όχι ως δικαίωμα που ενδεχομένως προσβάλλεται.

96. Συμμερίζομαι την άποψη της Επιτροπής ότι η επίκληση του άρθρου 6 υπό τους όρους αυτούς θα μπορούσε να είναι παραπλανητική. Όπως η Επιτροπή, εκτιμώ ότι το άρθρο αυτό δεν πρέπει να ερμηνεύεται υπό την έννοια ότι είναι ικανό «να επιβάλλει στην Ένωση μια θετική υποχρέωση θεσπίσεως μέτρων για την προστασία των προσώπων έναντι εγκληματικών πράξεων»<sup>48</sup>.

<sup>46</sup> Σημεία 27 έως 68.

<sup>47</sup> Βλ. απόφαση Tele2 Sverige και Watson (σκέψη 92), με παράθεση, κατ' αναλογίαν, της αποφάσεως Digital Rights, σκέψεις 25 και 70.

<sup>48</sup> Σημείο 37 των γραπτών παρατηρήσεων της Επιτροπής.

97. Η ασφάλεια που κατοχυρώνεται από το εν λόγω άρθρο του Χάρτη δεν ταυτίζεται με τη δημόσια ασφάλεια. Ή, με άλλα λόγια, η σχέση της με την τελευταία είναι η ίδια με οποιοδήποτε άλλο θεμελιώδες δικαίωμα, στον βαθμό κατά τον οποίο η δημόσια ασφάλεια αποτελεί εκ των ων ουκ άνευ προϋπόθεση για την απόλαυση των θεμελιωδών δικαιωμάτων και ελευθεριών.

98. Όπως υπενθυμίζει η Επιτροπή, το άρθρο 6 του Χάρτη αντιστοιχεί στο άρθρο 5 της Ευρωπαϊκής Συμβάσεως για την Προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών (στο εξής: ΕΣΔΑ), όπως προκύπτει από τις επεξηγήσεις που τον συνοδεύουν. Από την ανάγνωση του άρθρου 5 της ΕΣΔΑ προκύπτει ότι η προστατευόμενη από αυτό «ασφάλεια» είναι αυστηρώς η προσωπική ασφάλεια, νοούμενη ως διασφάλιση του δικαιώματος στη φυσική ελευθερία έναντι της αυθαίρετης κρατήσεως ή φυλακίσεως. Σε τελική ανάλυση, πρόκειται για τη διασφάλιση ότι κανένας δεν μπορεί να στερηθεί της ελευθερίας του, εκτός από τις περιπτώσεις, υπό τις προϋποθέσεις και σύμφωνα με τις διαδικασίες που θεσπίζει ο νόμος.

99. Πρόκειται, συνεπώς, για *προσωπική ασφάλεια*, η οποία αφορά τις προϋποθέσεις υπό τις οποίες μπορεί να περισταλεί η φυσική ελευθερία των προσώπων<sup>49</sup> και όχι για *δημόσια ασφάλεια*, εγγενή στην ύπαρξη του κράτους, η οποία είναι απαραίτητη προϋπόθεση, σε μια ανεπτυγμένη κοινωνία, για την εναρμόνιση της ασκήσεως της δημόσιας εξουσίας με την απόλαυση των ατομικών δικαιωμάτων.

100. Ορισμένες κυβερνήσεις, ωστόσο, ζητούν να ληφθεί μάλλον υπόψη το δικαίωμα στην ασφάλεια υπό τη δεύτερη από τις έννοιες αυτές. Στην πραγματικότητα, το Δικαστήριο δεν το έχει αγνοήσει, τουναντίον, το έχει αναφέρει ρητώς στις αποφάσεις<sup>50</sup> και τις γνωμοδοτήσεις<sup>51</sup> του. Ουδέποτε παραγνώρισε τη σημασία των σκοπών γενικού συμφέροντος που συνίστανται στην προστασία της εθνικής ασφάλειας και της δημοσίας τάξεως<sup>52</sup>, στην καταπολέμηση της διεθνούς τρομοκρατίας για τη διατήρηση της διεθνούς ειρήνης και ασφάλειας και στην καταπολέμηση των σοβαρών αδικημάτων για τη διαφύλαξη της δημόσιας ασφάλειας<sup>53</sup>, που, ορθώς, είχε χαρακτηρίσει ως «πρωταρχικής σημασίας»<sup>54</sup>. Είχε επισημάνει δε ότι «η προστασία της δημόσιας ασφάλειας συμβάλλει επίσης στην προστασία των δικαιωμάτων και των ελευθεριών των τρίτων»<sup>55</sup>.

101. Θα μπορούσε να αξιοποιηθεί η ευκαιρία που παρέχουν οι προδικαστικές αυτές παραπομπές για να προταθεί με μεγαλύτερη σαφήνεια η αναζήτηση ισορροπίας μεταξύ του δικαιώματος στην ασφάλεια, αφενός, και του δικαιώματος στην ιδιωτική ζωή και του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα, αφετέρου. Θα αποφεύγονταν κατ' αυτόν τον τρόπο οι κριτικές ότι ευνοούνται τα δεύτερα εις βάρος του πρώτου.

102. Στην ισορροπία αυτή αναφέρονται, κατά την άποψή μου, η αιτιολογική σκέψη 11 και το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58, όταν κάνουν λόγο για απαιτήσεις αναγκαιότητας και αναλογικότητας των μέτρων *σε μια δημοκρατική κοινωνία*. Το δικαίωμα στην ασφάλεια, επαναλαμβάνω, είναι σύμφυτο με την ίδια την ύπαρξη και την επιβίωση μιας δημοκρατίας, γεγονός που δικαιολογεί την πλήρη συνεκτίμησή του στο πλαίσιο της αξιολογήσεως της αναλογικότητας. Με άλλα λόγια, εάν η διαφύλαξη της αρχής του απορρήτου των δεδομένων είναι πρωταρχικής σημασίας σε μια δημοκρατική κοινωνία, επ' ουδενί μπορεί να υποτιμάται η σημασία της ασφάλειάς της.

49 Την ερμηνεία αυτή δίδει το ΕΔΔΑ. Αντί όλων, απόφαση του ΕΔΔΑ της 5ης Ιουλίου 2016, Buzadji κατά Δημοκρατίας της Μολδαβίας (ECHR:2016:0705JUD002375507), στην παράγραφο 84 της οποίας αναφέρεται ότι ο βασικός σκοπός του αναγνωριζόμενου από το άρθρο 5 της ΕΣΔΑ δικαιώματος είναι η αποτροπή της αυθαίρετης ή αδικαιολόγητης στέρσεως της ατομικής ελευθερίας.

50 Απόφαση Digital Rights (σκέψη 42).

51 Γνωμοδότηση 1/15 (Συμφωνία PNR ΕΕ-Καναδάς), της 26ης Ιουλίου 2017 (στο εξής: γνωμοδότηση: 1/15, EU:C:2017:592, σκέψη 149 και εκεί μνημονευόμενη νομολογία).

52 Απόφαση της 15ης Φεβρουαρίου 2016, N. (C-601/15 PPU, EU:C:2016:84, σκέψη 53).

53 Απόφαση Digital Rights (σκέψη 42 και εκεί μνημονευόμενη νομολογία).

54 Όπ.π. (σκέψη 51).

55 Γνωμοδότηση 1/15 (σκέψη 149).

103. Το πλαίσιο των συνεχιζόμενων σοβαρών απειλών για την εθνική ασφάλεια και, ιδίως, ο κίνδυνος της τρομοκρατίας, πρέπει, συνεπώς, να λαμβάνονται υπόψη, σύμφωνα με όσα αναφέρονται στην τελευταία περίοδο της σκέψης 119 της αποφάσεως *Tele2 Sverige* και *Watson*. Ένα εθνικό σύστημα μπορεί να ανταποκρίνεται κατά τρόπο αναλογικό στη φύση και την ένταση των απειλών που αντιμετωπίζει, χωρίς η απάντηση αυτή να είναι υποχρεωτικώς ίδια με αυτήν άλλων κρατών μελών.

104. Πρέπει να προσθέσω, τέλος, ότι οι προηγούμενες παρατηρήσεις ουδόλως εμποδίζουν την εθνική νομοθεσία να προβλέπει, σε περιπτώσεις πραγματικά *έκτακτες*, οι οποίες χαρακτηρίζονται από επικείμενη απειλή ή από έκτακτο κίνδυνο που δικαιολογούν την επίσημη κήρυξη του κράτους μέλους σε κατάσταση ανάγκης, τη δυνατότητα επιβολής, για περιορισμένο χρονικό διάστημα, υποχρεώσεων διατήρησης δεδομένων τόσο ευρείων και γενικών όσο κρίνεται απαραίτητο<sup>56</sup>.

105. Κατά συνέπεια, το πρώτο ερώτημα αμφοτέρων των αιτήσεων προδικαστικής αποφάσεως θα πρέπει να αναδιατυπωθεί και να επικεντρωθεί, μάλλον, στη δυνατότητα δικαιολογήσεως της επεμβάσεως για λόγους εθνικής ασφάλειας. Το ζήτημα είναι, συνεπώς, αν η επιβαλλομένη στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών υποχρέωση συνάδει με το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58.

## **β) Εκτίμηση**

*1) Χαρακτηρισμός των εσωτερικών κανόνων, όπως αυτοί εκτίθενται στις δύο αιτήσεις προδικαστικής αποφάσεως, υπό το πρίσμα της νομολογίας του Δικαστηρίου*

106. Σύμφωνα με τις αποφάσεις περί παραπομπής, η επίμαχη στις διαφορές των κύριων δικών ρύθμιση επιβάλλει τη διατήρηση των δεδομένων:

- στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών και, ιδίως, σε αυτούς που παρέχουν πρόσβαση σε ηλεκτρονικές υπηρεσίες επικοινωνίας προς το κοινό· και
- στα φυσικά ή νομικά πρόσωπα τα οποία προβαίνουν, ακόμη και δωρεάν, με σκοπό να καθίστανται προσιτά στο κοινό με ηλεκτρονικό τρόπο, σε αποθήκευση κάθε είδους σημάτων, κειμένου, εικόνων, ήχων ή μηνυμάτων που προέρχονται από τους αποδέκτες των υπηρεσιών αυτών<sup>57</sup>.

107. Οι πάροχοι οφείλουν να διατηρούν, για διάστημα ενός έτους από την ημερομηνία καταχωρίσεώς τους, τις πληροφορίες που καθιστούν δυνατή την ταυτοποίηση του χρήστη, τα δεδομένα σχετικά με τον χρησιμοποιούμενο τερματικό εξοπλισμό επικοινωνίας, τα τεχνικά χαρακτηριστικά, την ημερομηνία, την ώρα και τη διάρκεια εκάστης κλήσεως, τα δεδομένα σχετικά με τις ζητηθείσες ή χρησιμοποιηθείσες συμπληρωματικές υπηρεσίες και τα πρόσωπα που τις παρέχουν, καθώς και τα δεδομένα που διευκολύνουν την ταυτοποίηση του αποδέκτη της επικοινωνίας και, στην περίπτωση των δραστηριοτήτων τηλεφωνίας, την προέλευση και τη θέση της επικοινωνίας<sup>58</sup>.

<sup>56</sup> Βλ. σημεία 105 έως 107 των προτάσεών μου στην υπόθεση C-520/18.

<sup>57</sup> Ούτως προκύπτει από το άρθρο L. 851-1 του κώδικα εσωτερικής ασφάλειας, το οποίο παραπέμπει στο άρθρο L. 34-1 του κώδικα περί ταχυδρομείων και ηλεκτρονικών επικοινωνιών και στο άρθρο 6 του νόμου 2004-575, για την εμπιστοσύνη στην ψηφιακή οικονομία.

<sup>58</sup> Ούτως ορίζει το άρθρο R. 10-13 του κώδικα περί ταχυδρομείων και ηλεκτρονικών επικοινωνιών.

108. Όσον αφορά, συγκεκριμένα, τις υπηρεσίες προσβάσεως στο Διαδίκτυο και τις υπηρεσίες αποθηκεύσεως, η εθνική νομοθεσία φαίνεται να απαιτεί τη διατήρηση των διευθύνσεων IP<sup>59</sup>, των κωδικών προσβάσεως και, εφόσον μεσολαβεί η σύναψη συμβάσεως ή η δημιουργία λογαριασμού με χρέωση, το είδος της πραγματοποιηθείσας πληρωμής, καθώς επίσης το αποδεικτικό της, το ποσό, την ημερομηνία και την ώρα της συναλλαγής<sup>60</sup>.

109. Η υποχρέωση αυτή διατηρήσεως επιβάλλεται για λόγους διερευνήσεως, διαπιστώσεως και διώξεως των ποινικών παραβάσεων<sup>61</sup>. Ήτοι, εν αντιθέσει –όπως πρόκειται να καταδειχθεί– προς ό,τι συμβαίνει με την υποχρέωση *συλλογής* δεδομένων κινήσεως και θέσεως, η υποχρέωση *διατηρήσεως* τους δεν έχει ως μοναδικό σκοπό την πρόληψη της τρομοκρατίας<sup>62</sup>.

110. Όσον αφορά τους όρους *προσβάσεως* στα διατηρούμενα δεδομένα, από τη δικογραφία προκύπτει ότι είτε εφαρμόζονται οι προβλεπόμενοι στο πλαίσιο του κοινού καθεστώτος (παρέμβαση της δικαστικής αρχής) είτε η πρόσβαση αυτή περιορίζεται σε ατομικώς προσδιοριζόμενους και εξουσιοδοτούμενους υπαλλήλους, κατόπιν άδειας που χορηγεί ο Πρωθυπουργός ύστερα από μη δεσμευτική γνωμοδότηση ανεξάρτητης διοικητικής αρχής<sup>63</sup>.

111. Ευχερώς διαπιστώνεται ότι, όπως επισήμανε η Επιτροπή<sup>64</sup>, τα δεδομένα των οποίων τη διατήρηση αξιώνουν οι εθνικοί κανόνες αντιστοιχούν, κατ' ουσίαν, σε αυτά που είχε εξετάσει το Δικαστήριο με τις αποφάσεις Digital Rights και Tele2 Sverige και Watson<sup>65</sup>. Όπως και τότε, τα δεδομένα αυτά αποτελούν αντικείμενο «γενικής και χωρίς διάκριση υποχρέωσης διατηρήσεως», όπως, ρητώς, επισημαίνει το Conseil d'État (Συμβούλιο της Επικρατείας) στην αρχή των προδικαστικών ερωτημάτων του.

112. Αν αυτό ισχύει, κάτι που, σε τελική ανάλυση, εναπόκειται στο αιτούν δικαστήριο να εκτιμήσει, δεν μπορεί παρά να συναχθεί ότι η επίμαχη εθνική ρύθμιση συνιστά «επέμβαση [...] στα θεμελιώδη δικαιώματα που κατοχυρώνουν τα άρθρα 7 και 8 του Χάρτη [η οποία] έχει τεράστιο εύρος και πρέπει να θεωρηθεί ως ιδιαίτερος σοβαρή»<sup>66</sup>.

113. Κανείς από τους μετέχοντες στη διαδικασία δεν αμφισβήτησε ότι μια ρύθμιση με αυτά τα χαρακτηριστικά συνιστά επέμβαση στα εν λόγω δικαιώματα. Δεν είναι επί του παρόντος αναγκαία η εξέταση του σημείου αυτού, ούτε καν για να υπομνησθεί ότι η προσβολή των δικαιωμάτων αυτών αναπόφευκτα υποσκάπτει τα ίδια τα θεμέλια μιας κοινωνίας η οποία επιδιώκει τον σεβασμό, μεταξύ άλλων αξιών, της προστατευόμενης από τον Χάρτη ιδιωτικής ζωής.

114. Η εφαρμογή της νομολογίας που καθιερώθηκε με την απόφαση Tele2 Sverige και Watson και επιβεβαιώθηκε με την απόφαση Ministerio Fiscal θα οδηγούσε αβίαστα στο συμπέρασμα ότι μια ρύθμιση όπως η επίμαχη εν προκειμένω «υπερβαίνει τα όρια του απολύτως αναγκαίου και δεν θα μπορούσε να θεωρηθεί δικαιολογημένη σε μια δημοκρατική κοινωνία όπως απαιτεί το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58, ερμηνευόμενο υπό το πρίσμα των άρθρων 7, 8 και 11 καθώς και του άρθρου 52, παράγραφος 1, του Χάρτη»<sup>67</sup>.

59 Εναπόκειται στο αιτούν δικαστήριο να επαληθεύσει το σημείο αυτό, σημείο ως προς το οποίο διατυπώθηκαν αποκλίνουσες θέσεις κατά την επ' ακροατηρίου συζήτηση.

60 Άρθρο 1 του διατάγματος 2011-219.

61 Άρθρο R. 10-13 του κώδικα περί ταχυδρομείων και ηλεκτρονικών επικοινωνιών.

62 Τόσο η La Quadrature du Net όσο και η Fédération des fournisseurs d'accès à Internet associatifs υπογραμμίζουν την ευρύτητα των σκοπών που επιδιώκει η διατήρηση, την εξουσία εκτιμήσεως που έχει παρασχεθεί στις αρχές, την έλλειψη αντικειμενικών κριτηρίων για τον καθορισμό τους και τη σημασία που αποδίδεται σε είδη εγκληματικότητας τα οποία δεν μπορούν να χαρακτηριστούν ως σοβαρά.

63 Της Commission nationale de contrôle des techniques de renseignement (εθνικής επιτροπής ελέγχου των μεθόδων συλλογής πληροφοριών). Βλ., συναφώς, σημεία 145 έως 148 των γραπτών παρατηρήσεων της Γαλλικής Κυβερνήσεως.

64 Σημείο 60 των γραπτών παρατηρήσεων της Επιτροπής.

65 Στην πραγματικότητα, είναι λίγο ευρύτερα, καθώς φαίνεται να περιλαμβάνουν επίσης, στην περίπτωση των υπηρεσιών προσβάσεως στο Διαδίκτυο, τη διατήρηση της διευθύνσεως IP ή των κωδικών προσβάσεως.

66 Απόφαση Tele2 Sverige και Watson (σκέψη 100).

67 Όπ.π. (σκέψη 107).

115. Πράγματι, όπως η εξετασθείσα με την απόφαση Tele2 Sverige και Watson ρύθμιση, έτσι και η υπό κρίση «καλύπτει κατά τρόπο γενικό όλους τους συνδρομητές και τους εγγεγραμμένους χρήστες και αφορά όλα τα μέσα ηλεκτρονικής επικοινωνίας καθώς και όλα τα δεδομένα κινήσεως [και] δεν προβλέπει καμία διαφοροποίηση, περιορισμό ή εξαίρεση σε σχέση προς τον επιδιωκόμενο σκοπό»<sup>68</sup>. Κατά συνέπεια, «εφαρμόζεται ακόμη και σε πρόσωπα για τα οποία ουδεμία ένδειξη υφίσταται από την οποία θα μπορούσε να προκύψει ότι η συμπεριφορά τους μπορεί να συνδέεται, έστω και κατά τρόπο έμμεσο ή απομεμακρυσμένο, με σοβαρές παραβάσεις», τούτο δε χωρίς να γίνεται δεκτή κανενός είδους εξαίρεση, «οπότε εφαρμόζεται ακόμη και σε πρόσωπα των οποίων οι επικοινωνίες εμπίπτουν, βάσει των κανόνων του εθνικού δικαίου, στο επαγγελματικό απόρρητο»<sup>69</sup>.

116. Εξάλλου, η επίμαχη ρύθμιση «δεν απαιτεί να υφίσταται σχέση μεταξύ των δεδομένων, των οποίων τη διατήρηση προβλέπει, και κάποιας απειλής για τη δημόσια ασφάλεια. Ιδίως, δεν περιορίζεται σε διατήρηση η οποία να αφορά είτε δεδομένα σχετικά με μια συγκεκριμένη χρονική περίοδο και/ή μια συγκεκριμένη γεωγραφική ζώνη και/ή έναν κύκλο προσώπων που θα μπορούσαν να είναι αναμειγμένοι, με τον έναν ή τον άλλο τρόπο, σε κάποια σοβαρή παράβαση είτε πρόσωπα που θα μπορούσαν, για άλλους λόγους, να συμβάλουν, μέσω της διατήρησης των δεδομένων που τους αφορούν, στην καταπολέμηση του εγκλήματος»<sup>70</sup>.

117. Εξ αυτού προκύπτει ότι η εν λόγω ρύθμιση «υπερβαίνει τα όρια του απολύτως αναγκαίου και δεν θα μπορούσε να θεωρηθεί δικαιολογημένη σε μια δημοκρατική κοινωνία όπως απαιτεί το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58, ερμηνευόμενο υπό το πρίσμα των άρθρων 7, 8 και 11 καθώς και του άρθρου 52, παράγραφος 1, του Χάρτη»<sup>71</sup>.

118. Το ανωτέρω ήταν αρκετό ώστε το Δικαστήριο να συναγάγει ότι οι αντίστοιχοι εθνικοί κανόνες δεν ήταν συμβατοί με το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58, στον βαθμό κατά τον οποίον προέβλεπαν, «προς τον σκοπό καταπολεμήσεως του εγκλήματος, [...] γενική και χωρίς διάκριση διατήρηση του συνόλου των δεδομένων κινήσεως και των δεδομένων θέσεως όλων των συνδρομητών και των εγγεγραμμένων χρηστών αφορώσα όλα τα μέσα ηλεκτρονικής επικοινωνίας»<sup>72</sup>.

119. Το ερώτημα που ανακύπτει πλέον είναι εάν η νομολογία του Δικαστηρίου σε θέματα διατήρησης δεδομένων προσωπικού χαρακτήρα μπορεί, εάν όχι να επανεξεταστεί, τουλάχιστον, να διαφοροποιηθεί όταν ο σκοπός τον οποίον επιτελεί αυτή η «γενική και χωρίς διάκριση» διατήρηση είναι η καταπολέμηση της τρομοκρατίας. Το πρώτο ερώτημα της υποθέσεως C-511/18 υποβάλλεται, ακριβώς, «στο πλαίσιο των συνεχιζόμενων σοβαρών απειλών για την εθνική ασφάλεια, ιδίως λόγω του κινδύνου τρομοκρατίας».

120. Ωστόσο, δοθέντος του *πραγματικού αυτού πλαισίου* εντός του οποίου επιβάλλεται η υποχρέωση διατήρησης των δεδομένων, είναι αληθές ότι το *νομοθετικό πλαίσιο* της δεν αφορά αποκλειστικώς και μόνον την τρομοκρατία. Το επίμαχο στο πλαίσιο της διαδικασίας ενώπιον του Conseil d'État (Συμβουλίου της Επικρατείας) καθεστώς διατήρησης και προσβάσεως στα δεδομένα συναρτά την εν λόγω υποχρέωση με τους σκοπούς της διερευνήσεως, της διαπιστώσεως και της διώξεως των ποινικών αδικημάτων γενικώς.

121. Εν πάση περιπτώσει, υπενθυμίζω ότι η καταπολέμηση της τρομοκρατίας δεν έμεινε στο περιθώριο της συλλογιστικής της αποφάσεως Tele2 Sverige και Watson, χωρίς, ωστόσο, το Δικαστήριο να κρίνει τότε ότι η εγκληματική αυτή μορφή καθιστούσε επιβεβλημένη διαφοροποίηση της κρίσης του<sup>73</sup>.

68 Όπ.π. (σκέψη 105).

69 Όπ.π.

70 Απόφαση Tele2 Sverige και Watson (σκέψη 106).

71 Όπ.π. (σκέψη 107).

72 Όπ.π. (σκέψη 112).

73 Όπ.π. (σκέψη 103).



122. Ως εκ τούτου, και κατ' αρχήν, φρονώ ότι το ερώτημα του αιτούντος δικαστηρίου, το οποίο επικεντρώνεται στην ιδιαιτερότητα της τρομοκρατικής απειλής, θα έπρεπε να απαντηθεί υπό την ίδια έννοια υπό την οποίαν απεφάνθη το Δικαστήριο με την απόφαση Tele2 Sverige και Watson.

123. Όπως υποστήριξα με τις προτάσεις μου στην υπόθεση Stichting Brein, «[η] απαίτηση περί ασφάλειας δικαίου επιβάλλει στα εθνικά δικαστήρια την υποχρέωση, εάν όχι απόλυτης εφαρμογής του stare decisis, τουλάχιστον συνεκτιμήσεως όσων, κατόπιν ωρίμου σκέψεως, τα ίδια έχουν κρίνει επί ορισμένου νομικού προβλήματος»<sup>74</sup>.

2) *Περιορισμένη διατήρηση δεδομένων έναντι απειλών κατά της ασφάλειας του κράτους, συμπεριλαμβανομένης της τρομοκρατικής.*

124. Θα ήταν, παρά ταύτα, δυνατή η διαφοροποίηση ή η συμπλήρωση της νομολογίας αυτής, υπό το πρίσμα των συνεπειών της για την καταπολέμηση της τρομοκρατίας ή για την προστασία του κράτους έναντι άλλων ανάλογων απειλών κατά της εθνικής ασφάλειας;

125. Έχω ήδη υπογραμμίσει ότι η απλή διατήρηση δεδομένων προσωπικού χαρακτήρα συνιστά επέμβαση στα δικαιώματα που κατοχυρώνονται από τα άρθρα 7, 8 και 11 του Χάρτη<sup>75</sup>. Ανεξαρτήτως του ότι, σε τελική ανάλυση, σκοπός της είναι να καταστήσει δυνατή την πρόσβαση, αναδρομική ή ταυτόχρονη, στα δεδομένα σε συγκεκριμένο χρονικό σημείο<sup>76</sup>, η απλή διατήρηση δεδομένων που βαίνει πέραν του απολύτως αναγκαίου για τη μετάδοση επικοινωνίας ή για την τιμολόγηση των παρεχομένων από τον προμηθευτή υπηρεσιών συνιστά υπέρβαση των προβλεπόμενων στα άρθρα 5 και 6 της οδηγίας 2002/58 ορίων.

126. Οι χρήστες των υπηρεσιών αυτών (στην πραγματικότητα, το σύνολο σχεδόν των πολιτών στις πιο ανεπτυγμένες κοινωνίες) έχουν, ή πρέπει να έχουν, την εύλογη προσδοκία ότι, χωρίς τη συγκατάθεσή τους, δεν θα διατηρούνται περισσότερα δεδομένα τους από εκείνα που έχουν αποθηκευτεί σύμφωνα με τα ως άνω άρθρα. Οι εξαιρέσεις του άρθρου 15, παράγραφος 1, της οδηγίας 2002/58 πρέπει να ερμηνεύονται με αφετηρία την παραδοχή αυτήν.

127. Όπως έχω ήδη εξηγήσει, το Δικαστήριο απέκλεισε, με την απόφαση Tele2 Sverige και Watson, ομοίως σε σχέση με την καταπολέμηση της τρομοκρατίας, τη δυνατότητα γενικής και χωρίς διάκριση διατήρησης των δεδομένων προσωπικού χαρακτήρα<sup>77</sup>.

<sup>74</sup> Υπόθεση C-527/15 (EU:C:2016:938, σημείο 41).

<sup>75</sup> Όπως υπενθύμισε το Δικαστήριο με τη γνωμοδότηση 1/15 (σκέψη 124), «η κοινοποίηση δεδομένων προσωπικού χαρακτήρα σε τρίτο, όπως είναι μια δημόσια αρχή, συνιστά επέμβαση στο θεμελιώδες δικαίωμα που κατοχυρώνεται με το άρθρο 7 του Χάρτη, ανεξαρτήτως της μεταγενέστερης χρήσεως των κοινοποιούμενων πληροφοριών. Το αυτό ισχύει και για τη διατήρηση δεδομένων προσωπικού χαρακτήρα, όπως και για την πρόσβαση στα δεδομένα αυτά με σκοπό τη χρήση τους από τις δημόσιες αρχές. Συναφώς, ελάχιστη σημασία έχει αν οι σχετικές με την ιδιωτική ζωή γνωστοποιούμενες πληροφορίες είναι ή όχι ευαίσθητου χαρακτήρα ή αν οι ενδιαφερόμενοι υπέστησαν ή όχι ενδεχομένως δυσμενείς συνέπειες λόγω της επεμβάσεως αυτής».

<sup>76</sup> Όπως τόνιζε ο γενικός εισαγγελέας P. Cruz Villalón με τις προτάσεις του στην υπόθεση Digital Rights (C-293/12 και C-594/12, EU:C:2013:845, σημείο 72), «η συλλογή και, κυρίως, η διατήρηση, σε γιγάντιες βάσεις δεδομένων, διαφόρων δεδομένων τα οποία παράγονται ή υποβάλλονται σε επεξεργασία στο πλαίσιο του μεγαλύτερου μέρους των συνήθων ηλεκτρονικών επικοινωνιών των πολιτών της Ένωσης συνιστά κατάφωρη επέμβαση στην ιδιωτική ζωή τους, έστω και αν απλώς δημιουργεί τις προϋποθέσεις αναδρομικού ελέγχου τόσο των προσωπικών όσο και των επαγγελματικών δραστηριοτήτων τους. Η συλλογή των δεδομένων αυτών δημιουργεί τις προϋποθέσεις επιτηρήσεως η οποία, ακόμη και αν ασκείται αναδρομικά στο πλαίσιο της αξιοποίησεως των δεδομένων αυτών, συνιστά πάντως διαρκή απειλή, καθ' όλη τη διάρκεια διατήρησεως των δεδομένων, για την άσκηση του δικαιώματος των πολιτών της Ένωσης στο απόρρητο της ιδιωτικής ζωής τους. Η γενικευμένη αίσθηση επιτηρήσεως θέτει κατά τρόπο ιδιαίτερα οξύ το ζήτημα της διάρκειας της διατήρησεως των δεδομένων».

<sup>77</sup> Απόφαση Tele2 Sverige και Watson (σκέψη 103): «δεν μπορεί [...] να προταθεί ως δικαιολογία προκειμένου εθνική ρύθμιση η οποία προβλέπει τη γενική και χωρίς διάκριση διατήρηση όλων των δεδομένων κινήσεως και των δεδομένων θέσεως να θεωρηθεί ως αναγκαία για τους σκοπούς της εν λόγω καταπολεμήσεως».

128. Όσον αφορά την κριτική που έχει ασκηθεί, φρονώ ότι η απόφαση αυτή δεν υποτιμά την τρομοκρατική απειλή ως ιδιαίτερος σοβαρό εγκληματικό είδος του οποίου εκπεφρασμένος σκοπός είναι να αμφισβητήσει την εξουσία του κράτους και να αποσταθεροποιήσει ή να διαλύσει τους θεσμούς του. Η καταπολέμηση της τρομοκρατίας είναι, κυριολεκτικώς, ζωτικής σημασίας για το κράτος και η επιτυχία της αποτελεί, για ένα κράτος δικαίου, αδιαπραγμάτευτο σκοπό γενικού συμφέροντος.

129. Όλες, κατ' ουσίαν, οι κυβερνήσεις που μετέχουν στη διαδικασία, καθώς και η Επιτροπή, επισημαίνουν ότι, πέραν των τεχνικών δυσκολιών της, μια μερική και διαφοροποιημένη διατήρηση δεδομένων προσωπικού χαρακτήρα θα στερούσε από τις εθνικές υπηρεσίες πληροφοριών τη δυνατότητα να έχουν πρόσβαση σε πληροφορίες απαραίτητες για τον εντοπισμό απειλών κατά της δημόσιας ασφάλειας και της άμυνας του κράτους, καθώς και για τη δίωξη των δραστών τρομοκρατικών επιθέσεων<sup>78</sup>.

130. Όσον αφορά την εκτίμηση αυτή, κρίνω σκόπιμο να επισημάνω ότι η καταπολέμηση της τρομοκρατίας δεν προσεγγίζεται μόνον υπό το πρίσμα της αποτελεσματικότητάς της. Εξ ου η δυσκολία της, αλλά και η σπουδαιότητά της όταν τα μέσα και οι μέθοδοί της ανταποκρίνονται στις απαιτήσεις του κράτους δικαίου, που, πάνω απ' όλα, σημαίνει υπαγωγή της εξουσίας και του καταναγκασμού στα όρια του δικαίου και, ιδίως, σε μια έννομη τάξη η οποία έχει ως λόγο και σκοπό της υπάρξεώς της την προάσπιση των θεμελιωδών δικαιωμάτων.

131. Εάν όσον αφορά την τρομοκρατία η δικαιολόγηση των μέσων της δεν ανταποκρίνεται σε κανένα άλλο κριτήριο πλην της άνευ όρων (και μέγιστης) αποτελεσματικότητας των επιθέσεων της στην καθεστηκυία τάξη, για το κράτος δικαίου η αποτελεσματικότητα μετρείται υπό όρους που δεν επιτρέπουν παρέκκλιση, για τους σκοπούς της υπερασπίσεώς του, από τις διαδικασίες και τις εγγυήσεις που το χαρακτηρίζουν ως έννομη τάξη. Εάν περιοριζόταν αποκλειστικώς και μόνο στην πρακτική αποτελεσματικότητα, το κράτος δικαίου θα έχανε την ιδιότητα που το διακρίνει και θα μπορούσε, σε εξαιρετικές περιπτώσεις, να μετατραπεί το ίδιο σε απειλή για τον πολίτη. Αν η δημόσια εξουσία είχε στη διάθεσή της εξαιρετικά μέσα για τη δίωξη του εγκλήματος, με τα οποία θα μπορούσε να αγνοήσει ή να αποδυναμώσει τα θεμελιώδη δικαιώματα, ουδόλως θα μπορούσε να διασφαλιστεί ότι η ανεξέλεγκτη και απολύτως ελεύθερη δράση της δεν θα κατέληγε τελικώς εις βάρος της ελευθερίας όλων.

132. Η αποτελεσματικότητα της δημόσιας εξουσίας, επαναλαμβάνω, συναντά έναν ανυπέρβλητο φραγμό στα θεμελιώδη δικαιώματα των πολιτών, οι περιορισμοί των οποίων, όπως ορίζει το άρθρο 52, παράγραφος 1, του Χάρτη, μπορούν να επιβάλλονται μόνο με νόμο και με σεβασμό του βασικού περιεχομένου τους «εφόσον είναι αναγκαίοι και ανταποκρίνονται πραγματικά σε στόχους γενικού ενδιαφέροντος που αναγνωρίζει η Ένωση ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων»<sup>79</sup>.

133. Όσον αφορά τους όρους υπό τους οποίους, σύμφωνα με την απόφαση *Tele2 Sverige* και *Watson*, θα μπορούσε να γίνει δεκτή η *στοχευμένη* διατήρηση δεδομένων, παραπέμπω στις προτάσεις μου στην υπόθεση *C-520/18*<sup>80</sup>.

<sup>78</sup> Την ερμηνεία αυτή δίδει, παραδείγματος χάριν, η Γαλλική Κυβέρνηση, η οποία παραθέτει συναφώς ενδεικτικά παραδείγματα σχετικά με τη χρησιμότητα της γενικής διατήρησης δεδομένων, η οποία κατέστησε δυνατή την αντίδραση του κράτους έναντι των σοβαρών τρομοκρατικών επιθέσεων που σημειώθηκαν στη χώρα της τα τελευταία έτη (σημεία 107 και 122 έως 126 των γραπτών παρατηρήσεων της Γαλλικής Κυβερνήσεως).

<sup>79</sup> Απόφαση της 15ης Φεβρουαρίου 2016, Ν. (C-601/15 PPU, EU:C:2016:84, σκέψη 50). Πρόκειται, συνεπώς, για τη δύσκολη ισορροπία μεταξύ της δημόσιας τάξεως και της ελευθερίας στην οποία έχω ήδη αναφερθεί και από την οποία διαπνέεται κατ' αρχήν όλη η νομοθεσία της Ένωσης. Παράδειγμα μπορεί να αποτελέσει η οδηγία (ΕΕ) 2017/541 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2017, για την καταπολέμηση της τρομοκρατίας και την αντικατάσταση της απόφασης-πλαίσιο 2002/475/ΔΕΥ του Συμβουλίου και για την τροποποίηση της απόφασης 2005/671/ΔΕΥ του Συμβουλίου (ΕΕ 2017, L 88, σ. 6). Ενώ στο άρθρο της 20, παράγραφος 1, ορίζει ότι τα κράτη μέλη οφείλουν να μεριμνούν ώστε οι αρμόδιοι για τη διερεύνηση ή τη δίωξη τρομοκρατικών εγκλημάτων «[να διαθέτουν] αποτελεσματικά ερευνητικά μέσα», διακρίνει στην αιτιολογική της σκέψη 21 ότι η χρήση των μέσων αυτών «θα πρέπει να επικεντρώνεται και να λαμβάνει υπόψη την αρχή της αναλογικότητας, καθώς και τη φύση και τη σοβαρότητα των υπό διερεύνηση αδικημάτων και θα πρέπει να σέβεται το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα».

<sup>80</sup> Σημεία 87 έως 95.

134. Περιστάσεις κατά τις οποίες οι πληροφορίες που έχουν στη διάθεσή τους οι υπηρεσίες ασφαλείας καθιστούν βάσιμη την υποψία ότι προετοιμάζεται τρομοκρατική επίθεση μπορούν να αποτελέσουν θεμιτή περίπτωση επιβολής υποχρεώσεων διατήρησης ορισμένων δεδομένων, πολλώ δε μάλλον όταν διαπράττεται πράγματι τέτοια επίθεση. Μολονότι, στην τελευταία περίπτωση, η διάπραξη του αδικήματος μπορεί αφεαυτής να αποτελέσει δικαιολογητικό λόγο για τη λήψη του εν λόγω μέτρου, εντούτοις η απλή υποψία ενδεχόμενης επιθέσεως θα καθιστούσε επιβεβλημένη την ύπαρξη ενός ελάχιστου βαθμού πιθανολόγησης ως προς τις περιστάσεις που τη στοιχειοθετούν, απαραίτητου για την αντικειμενική στάθμιση των ενδείξεων που ενδεχομένως τη δικαιολογούν.

135. Καίτοι δυσχερές, δεν είναι εντούτοις αδύνατο να καθοριστούν με ακρίβεια και σύμφωνα με αντικειμενικά κριτήρια τόσο οι κατηγορίες δεδομένων των οποίων η διατήρηση κρίνεται αναγκαία όσο και ο κύκλος των ενδιαφερόμενων προσώπων. Ασφαλώς, το πλέον *πρακτικό και αποτελεσματικό* θα ήταν η γενική και χωρίς διάκριση διατήρηση όσων δεδομένων μπορούν να συγκεντρώσουν οι πάροχοι των υπηρεσιών ηλεκτρονικής επικοινωνίας, όμως, όπως έχω ήδη επισημάνει, το ζήτημα δεν μπορεί να επιλυθεί υπό όρους *πρακτικής αποτελεσματικότητας*, αλλά μόνον υπό όρους *νομικής αποτελεσματικότητας*, εντός δε του πλαισίου ενός κράτους δικαίου.

136. Το έργο αυτό καθορισμού είναι αμιγώς νομοθετικό, εντός των ορίων που έχει θέσει η νομολογία του Δικαστηρίου. Παραπέμπω, εκ νέου, σε όσα εκθέτω ως προς το σημείο αυτό στις προτάσεις μου στην υπόθεση C-520/18<sup>81</sup>.

### 3) Πρόσβαση στα διατηρούμενα δεδομένα

137. Εκκινώντας από την προκειμένη ότι οι πάροχοι έχουν προβεί σε συλλογή των δεδομένων κατά τρόπο που να συνάδει προς τα άρθρα της οδηγίας 2002/58 και ότι η διατήρησή τους έχει πραγματοποιηθεί υπό τους όρους του άρθρου 15, παράγραφος 1<sup>82</sup>, η πρόσβαση των αρμοδίων αρχών στις πληροφορίες αυτές πρέπει να πραγματοποιείται σύμφωνα με τις προϋποθέσεις που έχει θέσει το Δικαστήριο και που, από πλευράς μου, αναλύω στις προτάσεις της υποθέσεως C-520/18, στις οποίες και παραπέμπω<sup>83</sup>.

138. Συνεπώς, η εθνική νομοθεσία πρέπει και εν προκειμένω να θεσπίσει τις ουσιαστικές και διαδικαστικές προϋποθέσεις που θα διέπουν την πρόσβαση των αρμοδίων αρχών στα διατηρούμενα δεδομένα<sup>84</sup>. Στο πλαίσιο των υπό κρίση αιτήσεων προδικαστικής αποφάσεως, οι προϋποθέσεις αυτές θα επέτρεπαν την πρόσβαση στα δεδομένα προσώπων για τα οποία υπάρχουν υπόνοιες ότι σχεδιάζουν, προτίθενται να διαπράξουν ή έχουν διαπράξει τρομοκρατική ενέργεια ή ακόμη ότι εμπλέκονται σε μια τέτοια ενέργεια<sup>85</sup>.

81 Σημεία 100 έως 107.

82 Υπό τον όρο ότι τηρούνται οι προϋποθέσεις που μνημονεύονται στη σκέψη 122 της αποφάσεως Tele2 Sverige και Watson: το Δικαστήριο έχει υπενθυμίσει ότι το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58 δεν επιτρέπει παρεκκλίσεις από το άρθρο 4, παράγραφοι 1 και 1α, το οποίο απαιτεί από τους παρόχους τη λήψη μέτρων προκειμένου τα διατηρούμενα δεδομένα να προστατεύονται από τους κινδύνους καταχρήσεων καθώς και από αθέμιτη πρόσβαση σε αυτά. Ως προς το ζήτημα αυτό, έκρινε ότι, «[λ]αμβανομένης υπόψη της ποσότητας των διατηρούμενων δεδομένων, του ευαίσθητου χαρακτήρα των δεδομένων αυτών, καθώς και του κινδύνου αθέμιτης προσβάσεως σε αυτά, οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλουν να εξασφαλίζουν ιδιαίτερα υψηλό επίπεδο προστασίας και ασφαλείας των εν λόγω δεδομένων, ούτως ώστε να διασφαλίζεται η απόλυτη ακεραιότητα και ο απόρρητος χαρακτήρας τους. Ειδικότερα, η εθνική ρύθμιση πρέπει να προβλέπει τη διατήρηση των δεδομένων εντός των εδαφικών ορίων της Ένωσης καθώς και την οριστική καταστροφή τους με το πέρας της διάρκειας της διατήρησώς τους».

83 Σημεία 52 έως 60.

84 Απόφαση Tele2 Sverige και Watson (σκέψη 118).

85 Όπ.π. (σκέψη 119).

139. Πάντως, αυτό που έχει σημασία, εκτός δεόντως αιτιολογημένων περιπτώσεων ανάγκης, είναι η πρόσβαση στα επίμαχα δεδομένα να υπόκειται σε προηγούμενο έλεγχο δικαστικού οργάνου ή ανεξάρτητης διοικητικής αρχής η απόφαση της οποίας απαντά σε αιτιολογημένη αίτηση των αρμοδίων αρχών<sup>86</sup>. Κατ' αυτόν τον τρόπο, εκεί όπου δεν μπορεί να είναι αποτελεσματικός ο αφηρημένος έλεγχος του νόμου, διασφαλίζεται ο συγκεκριμένος έλεγχος από την ανεξάρτητη αυτή αρχή, η οποία εγγυάται την ασφάλεια του κράτους αλλά και την προάσπιση των θεμελιωδών δικαιωμάτων των πολιτών.

*4) Υποχρέωση διατήρησης δεδομένων που επιτρέπουν την ταυτοποίηση των δημιουργών περιεχομένου, υπό το πρίσμα της οδηγίας 2000/31 (δεύτερο προδικαστικό ερώτημα στην υπόθεση C-512/18)*

140. Το αιτούν δικαστήριο αναφέρεται στην οδηγία 2000/31 ως σημείο αναφοράς προκειμένου να διαπιστωθεί εάν είναι δυνατό να επιβληθεί, σε ορισμένα πρόσωπα<sup>87</sup> και παρόχους υπηρεσιών επικοινωνίας προς το κοινό, η υποχρέωση να διατηρούν τα δεδομένα «τα οποία καθιστούν δυνατή την ταυτοποίηση κάθε προσώπου που συνέβαλε στη δημιουργία του περιεχομένου ή μέρους του περιεχομένου των παρεχόμενων από αυτά υπηρεσιών, ούτως ώστε η δικαστική αρχή να δύναται, εφόσον είναι αναγκαίο, να ζητήσει την κοινοποίησή τους με σκοπό την εφαρμογή των κανόνων περί αστικής ή ποινικής ευθύνης».

141. Συμμερίζομαι την άποψη της Επιτροπής ότι θα ήταν άτοπο να εξεταστεί η συμβατότητα της υποχρέωσης αυτής με την οδηγία 2000/31<sup>88</sup>, αφ' ης στιγμής το άρθρο 1, παράγραφος 2, στοιχείο β', της τελευταίας εξαιρεί από το πεδίο εφαρμογής της τα «θέματα σχετικά με τις υπηρεσίες της κοινωνίας της πληροφορίας που καλύπτονται ήδη από τις οδηγίες 95/46/ΕΚ και 97/66/ΕΚ», κανόνες που επί του παρόντος περιλαμβάνονται στον κανονισμό 2006/679 και την οδηγία 2002/58<sup>89</sup>, τα αντίστοιχα άρθρα των οποίων 23, παράγραφος 1, και 15, παράγραφος 1, πρέπει, κατά την κρίση μου, να ερμηνευθούν υπό τους προεκτεθέντες όρους.

**2. Ως προς την υποχρέωση συλλογής σε πραγματικό χρόνο δεδομένων κινήσεως και θέσεως (δεύτερο προδικαστικό ερώτημα της υποθέσεως C-511/18)**

142. Κατά το αιτούν δικαστήριο, το άρθρο L. 851-2 του κώδικα εσωτερικής ασφάλειας επιτρέπει, αποκλειστικά για τους σκοπούς της προλήψεως της τρομοκρατίας, τη συλλογή, σε πραγματικό χρόνο, πληροφοριών σχετικά με πρόσωπα που έχουν προηγουμένως χαρακτηριστεί ως ύποπτα για εμπλοκή σε τρομοκρατική απειλή. Κατά τον ίδιο τρόπο, το άρθρο L. 851-4, του κώδικα αυτού επιτρέπει τη διαβίβαση σε πραγματικό χρόνο, από τους παρόχους, των τεχνικών δεδομένων για τον εντοπισμό του τερματικού εξοπλισμού.

143. Κατά το αιτούν δικαστήριο, οι μέθοδοι αυτές δεν επιβάλλουν στους παρόχους πρόσθετη υποχρέωση διατήρησης πέραν αυτής που είναι αναγκαία για την τιμολόγηση και τη διάθεση των υπηρεσιών τους στην αγορά.

<sup>86</sup> Όπ.π. (σκέψη 120).

<sup>87</sup> Τα πρόσωπα τα οποία «παρέχουν [...] με σκοπό να καθίστανται προσιτά στο κοινό μέσω υπηρεσιών ηλεκτρονικής επικοινωνίας προς το κοινό, σε αποθήκευση κάθε είδους σημάτων, κειμένου, εικόνων, ήχων ή μηνυμάτων που προέρχονται από τους αποδέκτες των υπηρεσιών αυτών [...]».

<sup>88</sup> Το αιτούν δικαστήριο μνημονεύει την οδηγία αυτή, υπό γενικούς όρους και χωρίς αναφορά σε συγκεκριμένα άρθρα, στο δεύτερο ερώτημα της υποθέσεως C-512/18.

<sup>89</sup> Σημεία 112 και 113 των γραπτών παρατηρήσεων της Επιτροπής.

144. Επιπλέον, κατά το άρθρο L. 851-3 του κώδικα εσωτερικής ασφάλειας, οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών και οι τεχνικοί πάροχοι ενδέχεται να υποχρεωθούν στην «εφαρμογή αυτοματοποιημένης επεξεργασίας στα δίκτυά τους με σκοπό, ανάλογα με τις παραμέτρους που καθορίζονται στην άδεια, τον εντοπισμό συνδέσεων που δύνανται να αποκαλύψουν τρομοκρατική απειλή». Η μέθοδος αυτή δεν συνεπάγεται γενική και χωρίς διάκριση διατήρηση δεδομένων, επιδιώκει δε τη συλλογή, για περιορισμένο χρονικό διάστημα, εκείνων των δεδομένων συνδέσεως που θα μπορούσαν να έχουν σχέση με τρομοκρατικά εγκλήματα.

145. Κατά την άποψή μου, οι προϋποθέσεις που απαιτούνται για την πρόσβαση στα δεδομένα προσωπικού χαρακτήρα πρέπει να τυγχάνουν ομοίως εφαρμογής όσον αφορά την πρόσβαση σε πραγματικό χρόνο στα δεδομένα που παράγονται κατά τη διάρκεια των ηλεκτρονικών επικοινωνιών. Παραπέμπω, λοιπόν, σε όσα έχω εκθέσει επί του συγκεκριμένου αυτού σημείου. Είναι άνευ σημασίας εάν πρόκειται για δεδομένα που διατηρούνται ή για δεδομένα που λαμβάνονται τη συγκεκριμένη στιγμή, καθόσον σε αμφότερες τις περιπτώσεις γίνονται γνωστά δεδομένα προσωπικού χαρακτήρα, ανεξαρτήτως του εάν αυτά ανατρέχουν στο παρελθόν ή αφορούν το παρόν.

146. Συγκεκριμένα, εάν η πρόσβαση σε πραγματικό χρόνο είναι αποτέλεσμα συνδέσεων που έχουν εντοπιστεί μέσω αυτοματοποιημένης επεξεργασίας, όπως αυτήν που προβλέπει το άρθρο L. 851-3 του κώδικα εσωτερικής ασφάλειας, τα προκαθορισμένα για τη επεξεργασία αυτή πρότυπα και κριτήρια πρέπει να είναι συγκεκριμένα, αξιόπιστα και μην εισάγουν διακρίσεις, κατά τρόπο ώστε να διευκολύνουν την ταυτοποίηση των ατόμων που μπορεί να βαρύνονται με εύλογη υποψία συμμετοχής σε τρομοκρατικές δραστηριότητες<sup>90</sup>.

### **3. Ως προς την υποχρέωση ενημερώσεως των υποκειμένων των δεδομένων (τρίτο προδικαστικό ερώτημα της υποθέσεως C-511/18)**

147. Το Δικαστήριο έχει κρίνει ότι οι αρχές στις οποίες παρέχεται πρόσβαση στα δεδομένα οφείλουν να γνωστοποιούν το γεγονός αυτό στα υποκείμενα των δεδομένων, υπό τον όρο ότι δεν τίθενται σε κίνδυνο οι εν εξελίξει έρευνες. Ο λόγος υπάρξεως της υποχρέωσης αυτής έγκειται στο ότι οι εν λόγω πληροφορίες είναι αναγκαίες ούτως ώστε τα υποκείμενα των δεδομένων να μπορέσουν να ασκήσουν το δικαίωμα πραγματικής προσφυγής, που μνημονεύεται ρητώς στο άρθρο 15, παράγραφος 2, της οδηγίας 2002/58, σε περίπτωση προσβολής των δικαιωμάτων τους<sup>91</sup>.

148. Το Conseil d'État (Συμβούλιο της Επικρατείας) ζητεί, με το τρίτο ερώτημά του στην υπόθεση C-511/18, να μάθει εάν η απαίτηση αυτή ενημερώσεως είναι, σε κάθε περίπτωση, επιτακτικού χαρακτήρα ή εάν χωρεί παρέκκλιση από αυτήν όταν προβλέπονται άλλου είδους εγγυήσεις, όπως αυτές που περιγράφει στην απόφαση περί παραπομπής.

149. Σύμφωνα με όσα εκθέτει το αιτούν δικαστήριο<sup>92</sup>, οι μνημονευόμενες εγγυήσεις συνίστανται στη δυνατότητα όσων επιθυμούν να εξακριβώσουν εάν ορισμένη μέθοδος ενημερώσεως έχει εφαρμοστεί παρανόμως να απευθυνθούν στο ίδιο το Conseil d'État (Συμβούλιο της Επικρατείας). Το όργανο αυτό θα μπορούσε, κατά περίπτωση, να αποφασίσει την ακύρωση της εγκρίσεως του μέτρου και να διατάξει την καταστροφή των συλλεγισών πληροφοριών, στο πλαίσιο διαδικασίας στην οποία δεν ισχύει η συνήθης στις δικαστικές διαδικασίες αρχή της αντιμωλίας.

<sup>90</sup> Απόφαση Digital Rights (σκέψη 59).

<sup>91</sup> Απόφαση Tele2 Sverige και Watson (σκέψη 121).

<sup>92</sup> Σημεία 8 έως 11 της αποφάσεως περί παραπομπής.

150. Κατά το αιτούν δικαστήριο, η ρύθμιση αυτή δεν προσβάλλει το δικαίωμα αποτελεσματικής δικαστικής προστασίας. Φρονώ, ωστόσο, ότι κάτι τέτοιο θα μπορούσε, θεωρητικώς, να γίνει δεκτό σε σχέση με όσους αποφασίσουν να εξακριβώσουν εάν έχει γίνει εις βάρος τους συλλογή πληροφοριών. Αντιθέτως, το δικαίωμα δεν γίνεται σεβαστό εάν, εκείνοι, εις βάρος των οποίων έχει γίνει τέτοια ενέργεια, δεν ενημερώνονται για το γεγονός αυτό και, ως εκ τούτου, δεν μπορούν να διερωτηθούν καν εάν τα δικαιώματά τους έχουν προσβληθεί ή όχι.

151. Οι δικαστικές εγγυήσεις στις οποίες αναφέρεται το αιτούν δικαστήριο φαίνεται να συνδέονται με την πρωτοβουλία εκείνου που υποπτεύεται ότι συλλέγονται προσωπικές πληροφορίες του. Ωστόσο, η πρόσβαση στη δικαιοσύνη για την προάσπιση των δικαιωμάτων πρέπει να είναι αποτελεσματική για όλους, όπερ συνεπάγεται ότι όποιος έχει υποστεί επεξεργασία των δεδομένων του πρέπει να έχει τη δυνατότητα να αμφισβητήσει δικαστικώς τη νομιμότητα της εν λόγω επεξεργασίας και, κατά συνέπεια, πρέπει να ενημερώνεται για την ύπαρξή της.

152. Ασφαλώς, όπως προκύπτει από τις παρασχεθείσες πληροφορίες, η Δικαιοσύνη μπορεί να επιληφθεί αυτεπαγγέλτως ή κατόπιν διοικητικής καταγγελίας, πρέπει, όμως, σε κάθε περίπτωση, να δίδεται στο υποκείμενο των δεδομένων η δυνατότητα να κινήσει τη δικαστική διαδικασία, λόγος για τον οποίον είναι αναγκαίο να ενημερώνεται ότι τα δεδομένα του προσωπικού χαρακτήρα έχουν αποτελέσει αντικείμενο συγκεκριμένης επεξεργασίας. Η προάσπιση των δικαιωμάτων του δεν μπορεί να εξαρτάται από το αν αποκτά τελικώς γνώση της επεξεργασίας αυτής από τρίτους ή με ενέργειές του.

153. Επομένως, στον βαθμό που δεν τίθεται σε κίνδυνο η πορεία των ερευνών για τις οποίες έχει παρασχεθεί πρόσβαση στα διατηρούμενα δεδομένα, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται για την εν λόγω πρόσβαση.

154. Διαφορετικό ζήτημα είναι ότι, επιληφθέν το δικαστήριο με πρωτοβουλία του υποκειμένου των δεδομένων, κατόπιν ενημερώσεώς του σχετικά με την πρόσβαση στα δεδομένα του, η επακόλουθη δικαστική διαδικασία πρέπει να τηρεί τις απαιτήσεις απορρήτου και διακριτικότητας, εγγενείς στον έλεγχο της δράσεως των δημοσίων αρχών σε ευαίσθητους τομείς όπως αυτός της ασφάλειας και της άμυνας του κράτους. Το ερώτημα, ωστόσο, αυτό δεν έχει σχέση με τις υπό κρίση προδικαστικές παραπομπές, και ως εκ τούτου, δεν είναι, κατά την κρίση μου, αναγκαίο να αποφανθεί το Δικαστήριο συναφώς.

## V. Πρόταση

155. Βάσει των προεκτεθέντων, προτείνω στο Δικαστήριο να απαντήσει στο Conseil d'État (Συμβούλιο της Επικρατείας, Γαλλία) ως εξής:

«Το άρθρο 15, παράγραφος 1, της οδηγίας 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 (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες), σε συνδυασμό με τα άρθρα 7, 8, 11 και 52 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, έχει την έννοια ότι:

- 1) αντιτίθεται σε εθνική ρύθμιση η οποία, στο πλαίσιο των συνεχιζόμενων σοβαρών απειλών για την εθνική ασφάλεια, ιδίως λόγω του κινδύνου τρομοκρατίας, επιβάλλει στους διαχειριστές και παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών την υποχρέωση να διατηρούν, κατά τρόπο γενικό και χωρίς διάκριση, τα δεδομένα κινήσεως και θέσεως όλων των συνδρομητών, καθώς και τα δεδομένα που καθιστούν την ταυτοποίηση των δημιουργών του περιεχομένου που προσφέρουν οι πάροχοι των εν λόγω υπηρεσιών.

- 2) αντιτίθεται σε εθνική ρύθμιση η οποία δεν προβλέπει υποχρέωση ενημέρωσης των υποκειμένων των δεδομένων ως προς την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα από τις αρμόδιες αρχές, εκτός εάν η ενημέρωση αυτή θέτει σε κίνδυνο τη δράση των εν λόγω αρχών.
- 3) δεν αντιτίθεται σε εθνική ρύθμιση η οποία επιτρέπει τη συλλογή σε πραγματικό χρόνο των δεδομένων κινήσεως και θέσεως μεμονωμένων ατόμων, στον βαθμό κατά τον οποίον οι ενέργειες αυτές πραγματοποιούνται σύμφωνα με τις διαδικασίες που προβλέπονται για την πρόσβαση στα νομίμως διατηρούμενα δεδομένα προσωπικού χαρακτήρα καθώς και με τις ίδιες εγγυήσεις».