I

(Ψηφίσματα, συστάσεις και γνωμοδοτήσεις)

ΓΝΩΜΟΔΟΤΗΣΕΙΣ

ΕΥΡΩΠΑΙΟΣ ΕΠΟΠΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων σχετικά με τη δικτυακή ουδετερότητα, τη διαχείριση της κίνησης και την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα

(2012/C 34/01)

Ο ΕΥΡΩΠΑΙΟΣ ΕΠΟΠΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 16,

Έχοντας υπόψη τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, και ιδίως τα άρθρα 7 και 8,

Έχοντας υπόψη την οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών ([1]),

Έχοντας υπόψη τον κανονισμό (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών ([2]), και ιδίως το άρθρο 41 παράγραφος 2,

Έχοντας υπόψη την οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών ([3]),

ΕΞΕΔΩΣΕ ΤΗΝ ΑΚΟΛΟΥΘΗ ΓΝΩΜΟΔΟΤΗΣΗ:

I. **ΕΙΣΑΓΩΓΗ**

I.1. **Ιστορικό**

1. Στις 19 Απριλίου 2011, η Επιτροπή εξέδωσε ανακοίνωση για το ανοιχτό διαδίκτυο και τη δικτυακή ουδετερότητα στην Ευρώπη ([4]).

2. Η παρούσα γνωμοδότηση αποτελεί απόκριση του ΕΕΠΔ στην εν λόγω ανακοίνωση και στόχο έχει να συμβάλει στον συνεχιζόμενο διάλογο πολιτικής στην ΕΕ σχετικά με τη δικτυακή ουδετερότητα, ιδίως σε πτυχές που σχετίζονται με την προστασία των δεδομένων και την ιδιωτική ζωή.

([1]) ΕΕ L 281 της 23.11.1995, σ. 31, η «οδηγία για την προστασία των δεδομένων».
([2]) ΕΕ L 8 της 12.1.2001, σ. 1, ο «κανονισμός για την προστασία των δεδομένων».
([3]) ΕΕ L 201 της 31.7.2002, σ. 37, όπως τροποποιήθηκε από την οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009 (Βλέπε υποσημείωση 15), η «οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες».
([4]) COM(2011) 222 τελικό.

3. Η γνωμοδότηση βασίζεται στην απάντηση ([5]) του ΕΕΠΔ στη δημόσια διαβούλευση της Επιτροπής σχετικά με το ανοιχτό διαδίκτυο και τη δικτυακή ουδετερότητα στην Ευρώπη, η οποία προηγήθηκε της ανακοίνωσης της Επιτροπής. Ο ΕΕΠΔ έλαβε επίσης γνώση του πρόσφατου σχεδίου συμπερασμάτων του Συμβουλίου σχετικά με τη δικτυακή ουδετερότητα ([6]).

I.2. **Η έννοια της δικτυακής ουδετερότητας**

4. Η δικτυακή ουδετερότητα παραπέμπει στον συνεχιζόμενο διάλογο σχετικά με το κατά πόσον οι πάροχοι υπηρεσιών Διαδικτύου ([7]) πρέπει να έχουν το δικαίωμα να περιορίζουν, να φιλτράρουν ή να παρεμποδίζουν την πρόσβαση στο Διαδίκτυο ή να επηρεάζουν άλλως πως τις επιδόσεις του. Η έννοια της δικτυακής ουδετερότητας βασίζεται στην άποψη ότι οι πληροφορίες στο Διαδίκτυο πρέπει να διαβιβάζονται με αμεροληψία, ανεξαρτήτως περιεχομένου, προορισμού ή προέλευσης, καθώς και ότι οι χρήστες πρέπει να μπορούν να αποφασίζουν ποιες εφαρμογές, υπηρεσίες και υλισμικό θέλουν να χρησιμοποιούν. Αυτό σημαίνει ότι οι πάροχοι υπηρεσιών Διαδικτύου δεν μπορούν να δίνουν προτεραιότητα ή να επιβραδύνουν την πρόσβαση, κατά την κρίση τους, σε ορισμένες εφαρμογές ή υπηρεσίες όπως η διομότιμη επικοινωνία («P2P») κ.λπ. ([8]).

5. Το φιλτράρισμα, η παρεμπόδιση και ο έλεγχος της κίνησης στο δίκτυο εγείρουν σημαντικά ερωτήματα, τα οποία συχνά παραβλέπονται ή παραμερίζονται, όσον αφορά την εμπιστευτικότητα των επικοινωνιών και τον σεβασμό της ιδιωτικής ζωής των φυσικών προσώπων και των δεδομένων προσωπικού χαρακτήρα που τα αφορούν όταν χρησιμοποιούν το Διαδίκτυο. Για παράδειγμα, ορισμένες τεχνικές ελέγχου μπορεί να περιλαμβάνουν την παρακολούθηση του περιεχομένου επικοινωνιών, των δικτυακών τόπων που επισκέφθηκε ο χρήστης, των μηνυμάτων ηλεκτρονικού ταχυδρομείου που έστειλε ή έλαβε, του χρόνου κατά τον οποίο συνέβη ένα τέτοιο γεγονός, κ.λπ., επιτρέποντας το φιλτράρισμα των επικοινωνιών.

6. Ελέγχοντας τα δεδομένα των επικοινωνιών, οι πάροχοι υπηρεσιών Διαδικτύου ενδέχεται να παραβιάζουν την εμπιστευτικότητα των επικοινωνιών, η οποία αποτελεί θεμελιώδες δικαίωμα που κατοχυρώνεται στο άρθρο 8 της Ευρωπαϊκής Σύμβασης για την προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών (η «ΕΣΔΑ») και στα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ο «Χάρτης»). Η εμπιστευτικότητα προστατεύεται περαιτέρω από την παράγωγη νομοθεσία της ΕΕ, και ειδικότερα από το άρθρο 5 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

I.3. **Εστίαση και διάρθρωση της γνωμοδότησης**

7. Ο ΕΕΠΔ φρονεί ότι ένας σοβαρός διάλογος πολιτικής σχετικά με τη δικτυακή ουδετερότητα πρέπει να εξετάσει την εμπιστευτικότητα των πληροφοριών καθώς και άλλες επιπτώσεις στην ιδιωτική ζωή και στην προστασία των δεδομένων.

8. Η παρούσα γνωμοδότηση συνεισφέρει σε αυτόν τον συνεχιζόμενο διάλογο στην ΕΕ και έχει τρεις στόχους:

— Επισημαίνει τη σημασία της ιδιωτικής ζωής και της προστασίας των δεδομένων στις τρέχουσες συζητήσεις σχετικά με τη δικτυακή ουδετερότητα. Ειδικότερα, τονίζει την αναγκαιότητα σεβασμού των υφιστάμενων κανόνων για την εμπιστευτικότητα των πληροφοριών. Πρέπει να επιτρέπονται μόνον πρακτικές οι οποίες σέβονται τους κανόνες αυτούς.

— Η δικτυακή ουδετερότητα σχετίζεται με σχετικά νέες –τεχνολογικές– δυνατότητες, η δε πείρα σχετικά με τον τρόπο εφαρμογής του νομικού πλαισίου είναι ελάχιστη. Επομένως, η παρούσα γνωμοδότηση παρέχει καθοδήγηση σχετικά με τον τρόπο με τον οποίο οι πάροχοι υπηρεσιών Διαδικτύου πρέπει να εφαρμόζουν και να τηρούν το νομικό πλαίσιο για την προστασία των δεδομένων, εάν προβαίνουν σε φιλτράρισμα, παρεμπόδιση και έλεγχο της κίνησης στο δίκτυο. Η καθοδήγηση αυτή αναμένεται να αποβεί χρήσιμη για τους παρόχους υπηρεσιών Διαδικτύου καθώς και για τις αρμόδιες για την επιβολή του πλαισίου αρχές.

— Στο πλαίσιο της προστασίας των δεδομένων και της ιδιωτικής ζωής, η παρούσα γνωμοδότηση επισημαίνει τομείς οι οποίοι χρήζουν ειδικής προσοχής και ενδέχεται να απαιτήσουν τη λήψη μέτρων σε επίπεδο ΕΕ. Οι επισημάνσεις αυτές είναι ιδιαίτερα σημαντικές ενόψει του συνεχιζόμενου διαλόγου σε επίπεδο ΕΕ και των μέτρων πολιτικής τα οποία μπορεί να δρομολογήσει η Επιτροπή στο πλαίσιο αυτό.

([5]) Ο ΕΕΠΔ απάντησε τονίζοντας ότι είναι σημαντικό να ληφθούν υπόψη ζητήματα προστασίας των δεδομένων και ιδιωτικής ζωής μαζί με άλλα υφιστάμενα δικαιώματα και αξίες. Η απάντηση είναι διαθέσιμη στη διεύθυνση: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

([6]) Διαθέσιμο στη διεύθυνση http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) Περιλαμβάνει την παροχή τόσο σταθερής όσο και κινητής πρόσβασης στο Διαδίκτυο.

([8]) Παρότι η αρχή εφαρμόζεται στους παρόχους υπηρεσιών Διαδικτύου, οι οποίοι θέτουν όρια στην ταχύτητα ή στην ποσότητα των πληροφοριών που μπορεί να στείλει ή να λάβει ένας συνδρομητής μέσω συνδρομών με όρια εύρους ζώνης ή όγκου. Επομένως, βάσει της αρχής της δικτυακής ουδετερότητας, οι πάροχοι υπηρεσιών Διαδικτύου θα εξακολουθούν να μπορούν να προσφέρουν συνδρομές πρόσβασης στο Διαδίκτυο οι οποίες περιορίζουν την πρόσβαση βάσει κριτηρίων, όπως η ταχύτητα ή ο όγκος, εφόσον κάτι τέτοιο δεν συνεπάγεται διάκριση υπέρ ή κατά συγκεκριμένου περιεχομένου.

9. Ο ΕΕΠΔ γνωρίζει ότι η δικτυακή ουδετερότητα εγείρει και άλλα ζητήματα, τα οποία αναλύονται περαιτέρω στη συνέχεια, όπως εκείνα που σχετίζονται με την πρόσβαση σε πληροφορίες. Τα εν λόγω ζητήματα εξετάζονται μόνο στον βαθμό που σχετίζονται με την προστασία των δεδομένων και την ιδιωτική ζωή ή έχουν αντίκτυπο σε αυτές.

10. Η διάρθρωση της γνωμοδότησης είναι η ακόλουθη. Η ενότητα ΙΙ ξεκινά με σύντομη επισκόπηση των πρακτικών φιλτραρίσματος από τους παρόχους υπηρεσιών Διαδικτύου. Στην ενότητα ΙΙΙ περιγράφεται συνοπτικά το νομικό πλαίσιο της ΕΕ για τη δικτυακή ουδετερότητα. Η ενότητα IV περιέχει τεχνική περιγραφή, την οποία ακολουθεί αξιολόγηση των επιπτώσεων στην ιδιωτική ζωή, ανάλογα με την χρησιμοποιούμενη τεχνική. Στην ενότητα V αναλύονται οι πρακτικές λεπτομέρειες που αφορούν την εφαρμογή του ισχύοντος πλαισίου της ΕΕ για την ιδιωτική ζωή και την προστασία των δεδομένων. Βάσει της ανάλυσης αυτής, η ενότητα VI περιέχει προτάσεις για περαιτέρω εξελίξεις πολιτικής και προσδιορίζει τους τομείς οι οποίοι ενδέχεται να χρήζουν αποσαφήνισης και βελτίωσης του νομικού πλαισίου. Τα συμπεράσματα παρατίθενται στην ενότητα VII.

II. ΔΙΚΤΥΑΚΗ ΟΥΔΕΤΕΡΟΤΗΤΑ ΚΑΙ ΠΟΛΙΤΙΚΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΤΗΣ ΚΙΝΗΣΗΣ

Αυξανόμενη χρήση πολιτικών διαχείρισης της κίνησης

11. Παραδοσιακά, οι πάροχοι υπηρεσιών Διαδικτύου παρακολουθούν και επηρεάζουν την κίνηση στο δίκτυο μόνο σε συγκεκριμένες περιπτώσεις. Για παράδειγμα, οι πάροχοι υπηρεσιών Διαδικτύου εφαρμόζουν τεχνικές ελέγχου και περιορισμένη ροή πληροφοριών για να διατηρήσουν την ασφάλεια του δικτύου, π.χ. για την καταπολέμηση ιών. Επομένως, καταρχήν, το Διαδίκτυο αναπτύχθηκε διατηρώντας υψηλό βαθμό ουδετερότητας.

12. Ωστόσο, τα τελευταία χρόνια, ορισμένοι πάροχοι υπηρεσιών Διαδικτύου θέλησαν να ελέγξουν την κίνηση στο δίκτυο, προκειμένου να τη διαφοροποιήσουν και να εφαρμόσουν διαφορετικές πολιτικές σχετικά με αυτήν, για παράδειγμα, να παρεμποδίσουν συγκεκριμένες υπηρεσίες ή να παράσχουν προνομιακή πρόσβαση σε άλλες. Οι τακτικές αυτές χαρακτηρίζονται ενίοτε ως «πολιτικές διαχείρισης της κίνησης» ([9]).

13. Υπάρχουν πολλοί λόγοι για τους οποίους οι πάροχοι υπηρεσιών Διαδικτύου επιθυμούν να ελέγχουν και να διαφοροποιούν την κίνηση. Για παράδειγμα, οι πολιτικές διαχείρισης της κίνησης μπορεί να βοηθούν τους παρόχους υπηρεσιών Διαδικτύου να διαχειρίζονται την κίνηση σε περιόδους υψηλής συμφόρησης, για παράδειγμα, δίνοντας προτεραιότητα σε χρονοευαίσθητη κίνηση, όπως το βίντεο συνεχούς ροής, και υποβαθμίζοντας άλλους τύπους κίνησης που μπορεί να είναι λιγότερο χρονοευαίσθητοι, όπως η P2P ([10]). Επιπλέον, η διαχείριση της κίνησης μπορεί να είναι ένας τρόπος για να αποκτήσουν οι πάροχοι υπηρεσιών Διαδικτύου μια δυνητική ροή εσόδων, η οποία μπορεί να προέρχεται από ποικίλες πηγές. Αφενός, οι πάροχοι υπηρεσιών Διαδικτύου μπορεί να χρεώνουν τέλη σε παρόχους υπηρεσιών περιεχομένου, για παράδειγμα, σε εκείνους των οποίων οι υπηρεσίες απαιτούν τη χρήση υψηλότερου εύρους ζώνης, με αντάλλαγμα την παροχή προτεραιότητας (και, επομένως, ταχύτητας). Αυτό σημαίνει ότι η πρόσβαση σε μια ορισμένη υπηρεσία, για παράδειγμα, μια υπηρεσία βιντεοπαραγγελίας, θα είναι ταχύτερη από την πρόσβαση σε άλλη παρόμοια υπηρεσία, η οποία δεν ζήτησε υψηλή ταχύτητα μετάδοσης. Αφετέρου, έσοδα μπορούν να εξασφαλισθούν και από συνδρομητές που ενδιαφέρονται να πληρώνουν υψηλότερα (ή χαμηλότερα) τέλη για ορισμένους τύπους διαφοροποιημένων συνδρομών. Για παράδειγμα, μια συνδρομή χωρίς πρόσβαση σε P2P μπορεί να είναι φθηνότερη από μια συνδρομή η οποία παρέχει απεριόριστη πρόσβαση.

14. Εκτός από τους λόγους για τους οποίους οι ίδιοι οι πάροχοι υπηρεσιών Διαδικτύου επιθυμούν να κάνουν χρήση πολιτικών διαχείρισης της κίνησης, άλλα μέρη μπορεί επίσης να έχουν συμφέρον από τη χρήση πολιτικών διαχείρισης της κίνησης από τους παρόχους υπηρεσιών Διαδικτύου. Εάν οι πάροχοι υπηρεσιών Διαδικτύου διαχειρίζονται τα δίκτυά τους και ελέγχουν το περιεχόμενο που διέρχεται από τις εγκαταστάσεις τους, είναι πιθανό να αυξήσουν την ικανότητά τους να εντοπίζουν εικαζόμενες παράνομες χρήσεις, π.χ. κρούσματα παραβίασης δικαιωμάτων δημιουργού ή πορνογραφίας.

([9]) Βλ., για παράδειγμα, έκθεση της OFCOM με τίτλο «Site blocking to reduce online copyright infringement» (Παρεμπόδιση σε δικτυακούς τόπους για τη μείωση των επιγραμμικών παραβιάσεων δικαιωμάτων δημιουργού), η οποία εγκρίθηκε στις 27 Μαΐου 2011, διαθέσιμη στη διεύθυνση: http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: «Ορισμένοι πάροχοι υπηρεσιών Διαδικτύου εφαρμόζουν ήδη συστήματα ελέγχου πακέτων στο δίκτυό τους για τη διαχείριση της κίνησης και για άλλους σκοπούς. Επομένως, υποθέτουμε ότι η εφαρμογή τέτοιων συστημάτων είναι δυνατή, παρότι αναμένεται να επιβαρύνει υπέρμετρα από την άποψη της πολυπλοκότητας και του κόστους όσους δεν διαθέτουν ήδη τέτοιες υπηρεσίες. Λαμβανομένων υπόψη των επενδύσεων κεφαλαίου που απαιτούνται, φαίνεται ότι, βραχυπρόθεσμα έως μεσοπρόθεσμα, ο έλεγχος πακέτων εις βάθος θα είναι δυνατός μόνον από τους μεγαλύτερους παρόχους υπηρεσιών Διαδικτύου».

([10]) Η ποιότητα των εφαρμογών πραγματικού χρόνου, όπως το βίντεο συνεχούς ροής, εξαρτάται, μεταξύ άλλων, από τον χρόνο αναμονής, δηλαδή, την καθυστέρηση, για παράδειγμα, λόγω συμφόρησης στο δίκτυο.

Άλλα συμφέροντα υπό διακύβευση, περιλαμβανομένων της προστασίας των δεδομένων και της ιδιωτικής ζωής

15. Η τάση αυτή πυροδότησε τη συζήτηση σχετικά με τη νομιμότητα των συγκεκριμένων πρακτικών και, ειδικότερα, σχετικά με το κατά πόσον πρέπει να θεσπιστούν διά νόμου πρόσθετες ειδικές υποχρεώσεις δικτυακής ουδετερότητας.

16. Η αυξανόμενη χρήση πολιτικών διαχείρισης της κίνησης από τους παρόχους υπηρεσιών Διαδικτύου θα μπορούσε να περιορίσει την πρόσβαση σε πληροφορίες. Εάν η συμπεριφορά αυτή καταστεί συνήθης πρακτική και οι χρήστες δεν μπορούν (ή είναι εξαιρετικά δαπανηρό για αυτούς) να έχουν πρόσβαση στο σύνολο του Διαδικτύου όπως το γνωρίζουμε, οι σχετικοί περιορισμοί θα θέσουν σε κίνδυνο την πρόσβαση στις πληροφορίες και την ικανότητα των χρηστών να στέλνουν και να λαμβάνουν το περιεχόμενο που επιθυμούν χρησιμοποιώντας τις εφαρμογές ή τις υπηρεσίες της επιλογής τους. Το πρόβλημα αυτό μπορεί να αποφευχθεί μέσω μιας νομικά δεσμευτικής αρχής περί προστασίας της δικτυακής ουδετερότητας.

17. Για τον λόγο αυτό, ο ΕΕΠΔ εξετάζει τις επιπτώσεις της διαχείρισης της κίνησης από τους παρόχους υπηρεσιών Διαδικτύου στην προστασία των δεδομένων και στην ιδιωτική ζωή. Ειδικότερα:

— Όταν οι πάροχοι υπηρεσιών Διαδικτύου επεξεργάζονται δεδομένα κίνησης με μοναδικό σκοπό τη δρομολόγηση της ροής πληροφοριών από τον αποστολέα στον παραλήπτη, εκτελούν συνήθως περιορισμένη επεξεργασία δεδομένων προσωπικού χαρακτήρα ([11]). Όπως η ταχυδρομική υπηρεσία επεξεργάζεται τις πληροφορίες που περιέχονται στον φάκελο μιας επιστολής, ο πάροχος υπηρεσιών Διαδικτύου επεξεργάζεται τις πληροφορίες που απαιτούνται για τη δρομολόγηση της επικοινωνίας προς τον αποδέκτη. Η επεξεργασία αυτή δεν αντίκειται στις νόμιμες απαιτήσεις της προστασίας των δεδομένων, της ιδιωτικής ζωής και της εμπιστευτικότητας των επικοινωνιών.

— Ωστόσο, όταν οι πάροχοι υπηρεσιών Διαδικτύου ελέγχουν δεδομένα επικοινωνίας, προκειμένου να διαφοροποιήσουν κάθε ροή επικοινωνίας και να εφαρμόσουν συγκεκριμένες πολιτικές, οι οποίες ενδέχεται να μην είναι ευνοϊκές για φυσικά πρόσωπα, οι επιπτώσεις είναι σημαντικότερες. Ανάλογα με τις συνθήκες κάθε περίπτωσης και με τον τύπο της διενεργούμενης ανάλυσης, η επεξεργασία μπορεί να είναι εξαιρετικά παρεμβατική στην ιδιωτική ζωή και στα δεδομένα προσωπικού χαρακτήρα των φυσικών προσώπων. Αυτό καθίσταται εμφανέστερο όταν οι πολιτικές διαχείρισης αποκαλύπτουν το περιεχόμενο των επικοινωνιών φυσικών προσώπων στο Διαδίκτυο, περιλαμβανομένων των ηλεκτρονικών μηνυμάτων που έστειλαν ή έλαβαν, των δικτυακών τόπων που επισκέφθηκαν, των αρχείων που μεταφόρτωσαν κ.λπ.

III. **ΕΠΙΣΚΟΠΗΣΗ ΤΟΥ ΝΟΜΙΚΟΥ ΠΛΑΙΣΙΟΥ ΤΗΣ ΕΕ ΓΙΑ ΤΗ ΔΙΚΤΥΑΚΗ ΟΥΔΕΤΕΡΟΤΗΤΑ ΚΑΙ ΠΕΡΑΙΤΕΡΩ ΕΞΕΛΙΞΕΙΣ ΠΟΛΙΤΙΚΗΣ**

III.1. **Σύντομη παρουσίαση του νομικού πλαισίου**

18. Έως το 2009, οι νομοθετικές πράξεις της ΕΕ δεν περιείχαν διατάξεις που να απαγορεύουν ρητώς στους παρόχους υπηρεσιών Διαδικτύου το φιλτράρισμα ή την παρεμπόδιση ή τη πρόσθετη χρέωση στους συνδρομητές για την πρόσβαση σε υπηρεσίες. Ταυτόχρονα, δεν περιείχαν διατάξεις οι οποίες να αναγνωρίζουν ρητώς την πρακτική αυτή. Σε κάποιον βαθμό, η κατάσταση χαρακτηριζόταν από αβεβαιότητα.

19. Η δέσμη μέτρων για τις τηλεπικοινωνίες του 2009 άλλαξε την κατάσταση αυτή με τη θέσπιση διατάξεων που ευνοούσαν το άνοιγμα του Διαδικτύου. Για παράδειγμα, το άρθρο 8 παράγραφος 4 της οδηγίας σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (η «οδηγία-πλαίσιο») θεσπίζει υποχρέωση των κανονιστικών αρχών να προωθούν την ικανότητα των τελικών χρηστών να έχουν πρόσβαση σε περιεχόμενο, εφαρμογές ή υπηρεσίες της επιλογής τους ([12]). Η διάταξη αυτή ισχύει για το σύνολο του δικτύου και δεν αφορά επιμέρους παρόχους. Πρόσφατο σχέδιο συμπερασμάτων του Συμβουλίου τονίζει επίσης την αναγκαιότητα διατήρησης του ανοιχτού χαρακτήρα του Διαδικτύου ([13]).

([11]) Αυτό δεν περιλαμβάνει τις πράξεις που αποσκοπούν στην αύξηση της ασφάλειας του δικτύου και στον εντοπισμό επιβλαβούς κίνησης καθώς και τις πράξεις που απαιτούνται για την έκδοση λογαριασμών και τη διασύνδεση. Δεν περιλαμβάνει επίσης τις υποχρεώσεις που απορρέουν από την οδηγία για τη διατήρηση δεδομένων, δηλαδή την οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2006, για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ, (ΕΕ L 105 της 13.4.2006, σ. 54) (η «οδηγία για τη διατήρηση δεδομένων»).

([12]) Οδηγία 2002/21/ΕΚ, της 7ης Μαρτίου 2002 σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, όπως τροποποιήθηκε από την οδηγία 2009/140/ΕΚ και τον κανονισμό (ΕΚ) αριθ. 544/2009, (ΕΕ L 337 της 18.12.2009, σ. 37).

([13]) Βλ. σημείο 3 στοιχείο ε), όπου το Συμβούλιο αναγνωρίζει την αναγκαιότητα διατήρησης του ανοιχτού χαρακτήρα του Διαδικτύου, διασφαλίζοντας παράλληλα ότι μπορεί να συνεχίσει να παρέχει υπηρεσίες υψηλής ποιότητας σε ένα πλαίσιο το οποίο προάγει και σέβεται τα θεμελιώδη δικαιώματα, όπως την ελευθερία έκφρασης και την επιχειρηματική ελευθερία, καθώς και σημείο 8 στοιχείο δ), όπου το Συμβούλιο καλεί τα κράτη μέλη να προωθήσουν τον ανοικτό και ουδέτερο χαρακτήρα του Διαδικτύου ως στόχο πολιτικής.

20. Η οδηγία καθολικής υπηρεσίας ([14]) περιέχει πιο συγκεκριμένες υποχρεώσεις. Τα άρθρα 20 και 21 προβλέπουν απαιτήσεις διαφάνειας για τους περιορισμούς στην πρόσβαση ή/και στη χρήση υπηρεσιών και εφαρμογών. Η οδηγία απαιτεί επίσης ελάχιστα επίπεδα ποιότητας υπηρεσίας.

21. Για τις πρακτικές των παρόχων υπηρεσιών Διαδικτύου οι οποίες συνεπάγονται τον έλεγχο των επικοινωνιών φυσικών προσώπων, η αιτιολογική σκέψη 28 της οδηγίας για την τροποποίηση της οδηγίας για την καθολική υπηρεσία και της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ([15]) επισημαίνει ότι «ανάλογα με τη χρησιμοποιούμενη τεχνολογία και τον τύπο περιορισμού, για τέτοιους περιορισμούς απαιτείται ενδεχομένως συναίνεση του χρήστη βάσει της οδηγίας […] για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες». Στο πλαίσιο αυτό, η αιτιολογική σκέψη 28 υπενθυμίζει την αναγκαιότητα συγκατάθεσης, δυνάμει του άρθρου 5 παράγραφος 1 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, σε κάθε περιορισμό ο οποίος βασίζεται στην παρακολούθηση των επικοινωνιών. Στην ενότητα IV κατωτέρω αναλύεται περαιτέρω η εφαρμογή του άρθρου 5 παράγραφος 1 και το συνολικό νομικό πλαίσιο για την προστασία των δεδομένων και την ιδιωτική ζωή.

22. Τέλος, το άρθρο 22 παράγραφος 3 της οδηγίας για την καθολική υπηρεσία επιτρέπει πλέον στις εθνικές κανονιστικές αρχές να επιβάλλουν, εφόσον απαιτείται, ελάχιστες απαιτήσεις ποιότητας της υπηρεσίας σε παρόχους υπηρεσιών Διαδικτύου για την πρόληψη της υποβάθμισης των υπηρεσιών και της παρεμπόδισης ή της επιβράδυνσης της κίνησης σε δημόσια δίκτυα.

23. Τα ανωτέρω υποδεικνύουν ότι η ΕΕ φιλοδοξεί να υπερασπισθεί το ανοιχτό Διαδίκτυο (βλέπε άρθρο 8 παράγραφος 4 της οδηγίας-πλαισίου). Ωστόσο, αυτός ο στόχος πολιτικής, ο οποίος εφαρμόζεται στο σύνολο του δικτύου, δεν συνδέεται άμεσα με απαγορεύσεις ή υποχρεώσεις για τους επιμέρους παρόχους υπηρεσιών Διαδικτύου. Με άλλα λόγια, ένας πάροχος υπηρεσιών Διαδικτύου μπορεί να εφαρμόζει πολιτικές διαχείρισης της κίνησης οι οποίες ενδέχεται να αποκλείουν την πρόσβαση σε ορισμένες εφαρμογές, υπό τον όρο ότι οι τελικοί χρήστες είναι πλήρως ενημερωμένοι και έχουν δηλώσει τη συγκατάθεσή τους ελεύθερα, ειδικώς και ρητώς.

24. Η κατάσταση μπορεί να διαφέρει από κράτος μέλος σε κράτος μέλος. Σε ορισμένα κράτη μέλη, οι πάροχοι υπηρεσιών Διαδικτύου μπορούν, υπό συγκεκριμένες προϋποθέσεις, να εφαρμόζουν πολιτικές διαχείρισης της κίνησης, για παράδειγμα, για να παρεμποδίζουν εφαρμογές όπως φωνητικές υπηρεσίες μέσω του πρωτοκόλλου Ίντερνετ (VoIP) (στο πλαίσιο μιας φθηνότερης συνδρομής στο Διαδίκτυο), υπό τον όρο ότι τα φυσικά πρόσωπα έχουν ενημερωθεί και έχουν δώσει ελεύθερα, ειδικώς και ρητώς, τη συγκατάθεσή τους. Άλλα κράτη μέλη επέλεξαν να ενισχύσουν την αρχή της δικτυακής ουδετερότητας. Για παράδειγμα, τον Ιούλιο του 2011, η Βουλή των Κάτω Χωρών ψήφισε νόμο ο οποίος απαγορεύει γενικά στους παρόχους να παρεμποδίζουν ή να επιβραδύνουν εφαρμογές ή υπηρεσίες στο Διαδίκτυο (όπως VoIP), εκτός εάν κάτι τέτοιο είναι αναγκαίο για την ελαχιστοποίηση των συνεπειών συμφόρησης, για λόγους ακεραιότητας ή ασφάλειας, για την καταπολέμηση ανεπίκλητων ηλεκτρονικών μηνυμάτων ή βάσει δικαστικής απόφασης ([16]).

III.2. **Η ανακοίνωση για τη δικτυακή ουδετερότητα**

25. Στην ανακοίνωσή της για τη δικτυακή ουδετερότητα ([17]), η Ευρωπαϊκή Επιτροπή κατέληξε στο συμπέρασμα ότι η κατάσταση όσον αφορά τη δικτυακή ουδετερότητα απαιτεί παρακολούθηση και περαιτέρω ανάλυση. Η πολιτική της χαρακτηρίσθηκε ως «στάση αναμονής» προτού τύχουν εξέτασης πρόσθετα ρυθμιστικά μέτρα.

([14]) Οδηγία 2002/22/ΕΚ, όπως τροποποιήθηκε από την οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών, (ΕΕ L 337 της 18.12.2009, σ. 11) Σύγκρινε επίσης με το άρθρο 1 παράγραφος 3, το οποίο ορίζει ότι η οδηγία ούτε υπαγορεύει ούτε απαγορεύει την εκ μέρους των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών και υπηρεσιών για το κοινό επιβολή όρων, με τους οποίους περιορίζονται η πρόσβαση των χρηστών στις υπηρεσίες ή/και η χρήση των υπηρεσιών από αυτούς, εφόσον αυτό επιτρέπεται με βάση την εθνική νομοθεσία και είναι σύμφωνο με την κοινοτική, προβλέπει ωστόσο την υποχρέωση ενημέρωσης σχετικά με τους όρους αυτούς.

([15]) Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών.

([16]) Η πρωτότυπη ολλανδική τροπολογία είναι διαθέσιμη στη διεύθυνση: https://zoek.officielebekendmakingen.nl/kst-32549-A.html. Οι λόγοι επί των οποίων στηρίχθηκε, σύμφωνα με δημοσιεύματα του Τύπου, η συγκεκριμένη επιλογή πολιτικής δεν αφορούσαν την προστασία των δεδομένων ή της ιδιωτικής ζωής, αλλά μάλλον την πρόθεση διασφάλισής της χωρίς περιορισμούς πρόσβασης των χρηστών σε πληροφορίες. Επομένως, φαίνεται ότι ζητήματα που σχετίζονται με την πρόσβαση σε πληροφορίες αποτέλεσαν το εφαλτήριο της παρούσας τροπολογίας.

([17]) Βλέπε υποσημείωση 4.

26. Στην ανακοίνωσή της η Επιτροπή αναγνώρισε ότι κάθε μέτρο και κάθε πρόσθετη ρύθμιση θα υποβληθεί σε ενδελεχή εκτίμηση των πτυχών προστασίας των δεδομένων και ιδιωτικής ζωής. Στο σχέδιο συμπερασμάτων του Συμβουλίου σημειώνεται επίσης ότι διακυβεύονται ζητήματα προστασίας των δεδομένων και της ιδιωτικής ζωής ([18]).

27. Το ερώτημα που πρέπει να αξιολογηθεί από την άποψη της προστασίας των δεδομένων και της ιδιωτικής ζωής είναι κατά πόσον μια πολιτική «στάσης αναμονής» είναι επαρκής. Παρότι το πλαίσιο για την προστασία των δεδομένων και την ιδιωτική ζωή προβλέπει, επί του παρόντος, ορισμένες εγγυήσεις, ιδίως μέσω της αρχής της εμπιστευτικότητας των επικοινωνιών, η στενή παρακολούθηση του επιπέδου συμμόρφωσης και η έκδοση κατευθυντήριων γραμμών για πτυχές που χαρακτηρίζονται από έλλειψη σαφήνειας φαίνονται αναγκαίες. Επιπλέον, πρέπει να υποβληθούν ορισμένες προτάσεις σχετικά με την αποσαφήνιση και την περαιτέρω βελτίωση του πλαισίου, υπό το πρίσμα των τεχνολογικών εξελίξεων. Εάν η παρακολούθηση υποδείξει ότι η αγορά κινείται προς μαζικό έλεγχο των επικοινωνιών σε πραγματικό χρόνο και αναδείξει προβλήματα συμμόρφωσης προς το πλαίσιο, θα απαιτηθεί η λήψη νομοθετικών μέτρων. Συγκεκριμένες προτάσεις διατυπώνονται συναφώς στην ενότητα VI.

IV. **ΤΕΧΝΙΚΟ ΥΠΟΒΑΘΡΟ ΚΑΙ ΣΥΝΑΦΕΙΣ ΕΠΙΠΤΩΣΕΙΣ ΣΤΗΝ ΙΔΙΩΤΙΚΗ ΖΩΗ ΚΑΙ ΣΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ**

28. Προτού εξετάσουμε το θέμα εις βάθος, είναι σημαντικό να αποκτήσουμε καλύτερη εικόνα των τεχνικών ελέγχου που μπορούν να χρησιμοποιούν οι πάροχοι υπηρεσιών Διαδικτύου για τη διαχείριση της κίνησης και του τρόπου με τον οποίο τέτοιες διαδικασίες μπορούν να επηρεάσουν την αρχή της δικτυακής ουδετερότητας. Οι επιπτώσεις που συνεπάγονται οι εν λόγω τεχνικές στην ιδιωτική ζωή και στην προστασία των δεδομένων διαφέρουν σημαντικά ανάλογα με την τεχνική ή τις τεχνικές που εκάστοτε χρησιμοποιούνται. Το συγκεκριμένο τεχνικό υπόβαθρο είναι αναγκαίο για την ορθή κατανόηση και εφαρμογή του νομικού πλαισίου για την προστασία των δεδομένων, το οποίο αναλύεται στην ενότητα V. Ωστόσο, πρέπει να σημειωθεί ότι ο τομέας αυτός τελεί υπό διαρκή εξέλιξη και χαρακτηρίζεται από πολυπλοκότητα. Επομένως, η ανάλυση που ακολουθεί δεν φιλοδοξεί να εξαντλήσει το θέμα ούτε είναι πλήρως επικαιροποιημένη, αλλά παρέχει απλώς τις τεχνικές πληροφορίες που είναι απαραίτητες για την κατανόηση του νομικού συλλογισμού.

IV.1. **Διαβίβαση πληροφοριών μέσω του Διαδικτύου: βασικές αρχές**

29. Όταν ένας χρήστης διαβιβάζει μια επικοινωνία μέσω του Διαδικτύου, η πληροφορία που διαβιβάζεται υποδιαιρείται σε πακέτα. Τα πακέτα αυτά διαβιβάζονται στο Διαδίκτυο από τον αποστολέα στον αποδέκτη. Κάθε πακέτο περιλαμβάνει, μεταξύ άλλων, πληροφορίες σχετικά με την προέλευση και τον προορισμό. Επιπλέον, οι πάροχοι υπηρεσιών Διαδικτύου μπορούν να περικλείσουν τα πακέτα αυτά σε πρόσθετα επίπεδα και πρωτόκολλα ([19]), τα οποία θα χρησιμοποιηθούν για τη διαχείριση των διαφορετικών ροών κίνησης εντός του δικτύου του παρόχου υπηρεσιών Διαδικτύου.

30. Για να επανέλθουμε στην αναλογία με την ταχυδρομική επιστολή, η χρήση ενός πρωτοκόλλου διαβίβασης δικτύου ισοδυναμεί με την τοποθέτηση του περιεχομένου μιας ταχυδρομικής επιστολής σε έναν φάκελο με τη διεύθυνση προορισμού. Ακολούθως, η διεύθυνση του παραλήπτη θα διαβαστεί από την ταχυδρομική υπηρεσία, η οποία αναλαμβάνει την υποχρέωση να παραδώσει την επιστολή. Η ταχυδρομική υπηρεσία μπορεί να χρησιμοποιήσει πρόσθετα πρωτόκολλα στις εσωτερικές διαβιβάσεις της για να διαχειριστεί όλους τους φακέλους που πρέπει να διαβιβασθούν, με σκοπό κάθε φάκελος να φθάσει στον προορισμό του όπως συντάχθηκε αρχικά από τον αποστολέα. Χρησιμοποιώντας την αναλογία αυτά, κάθε πακέτο έχει δύο μέρη: πρώτον, το *ωφέλιμο φορτίο IP*, το οποίο περιέχει το περιεχόμενο της επικοινωνίας και αντιστοιχεί στην επιστολή. Περιέχει πληροφορίες οι οποίες προορίζονται μόνον για τον αποδέκτη. Δεύτερον, την *κεφαλίδα IP*, η οποία περιλαμβάνει, μεταξύ άλλων, τη διεύθυνση του αποδέκτη και του αποστολέα και αντιστοιχεί στον φάκελο. Η κεφαλίδα IP επιτρέπει στους παρόχους υπηρεσιών Διαδικτύου και άλλους διαμεσολαβητές να δρομολογήσουν το ωφέλιμο φορτίο από τη διεύθυνση προέλευσης στη διεύθυνση προορισμού.

31. Οι πάροχοι υπηρεσιών Διαδικτύου και άλλοι διαμεσολαβητές διασφαλίζουν ότι τα πακέτα IP ταξιδεύουν στο δίκτυο μέσω κόμβων, οι οποίοι διαβάζουν τις πληροφορίες της κεφαλίδας IP, τις ελέγχουν σε σχέση με πίνακες δρομολόγησης, και στη συνέχεια τις διαβιβάζουν στον επόμενο κόμβο καθ' οδόν προς τον τελικό

([18]) Βλέπε σημείο 4 στοιχείο ε), όπου το Συμβούλιο επισημαίνει σειρά ανησυχιών, προερχόμενων κυρίως από καταναλωτές και αρχές προστασίας δεδομένων, όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα.

([19]) Όπως εξηγείται περαιτέρω στην ενότητα IV.2, τα πρωτόκολλα αυτά κωδικοποιούν τις πληροφορίες που διαβιβάζονται διατερματικά με έναν συμφωνημένο τρόπο, ώστε τα μέλη που επικοινωνούν να μπορούν να κατανοούν το ένα το άλλο, όπως HTTP, FTP κ.λπ.

προορισμό. Η διαδικασία αυτή πραγματοποιείται στο δίκτυο χρησιμοποιώντας μια προσέγγιση «βέλτιστης προσπάθειας χωρίς μνήμη», καθώς όλα τα πακέτα που φθάνουν σε έναν κόμβο τυγχάνουν ουδέτερης αντιμετώπισης. Όταν διαβιβασθούν στον επόμενο κόμβο, δεν υπάρχει λόγος διατήρησης περαιτέρω πληροφοριών στον δρομολογητή ([20]).

IV.2. **Τεχνικές ελέγχου**

32. Όπως είδαμε, οι πάροχοι υπηρεσιών Διαδικτύου διαβάζουν τις κεφαλίδες IP με σκοπό τη δρομολόγησή τους προς τον προορισμό τους. Ωστόσο, όπως προαναφέρθηκε, η ανάλυση της κίνησης (η οποία περιλαμβάνει κεφαλίδες IP και ωφέλιμο φορτίο IP) μπορεί να διενεργηθεί για άλλους σκοπούς και με τη χρήση διαφορετικών τεχνολογιών. Οι νέες τάσεις μπορεί να περιλαμβάνουν, για παράδειγμα, την επιβράδυνση ορισμένων εφαρμογών που χρησιμοποιούνται από χρήστες, όπως η P2P, ή εναλλακτικά τη βελτίωση της ταχύτητας της κίνησης για ορισμένες υπηρεσίες, όπως υπηρεσίες βιντεοπαραγγελίας για προνομιακούς συνδρομητές. Παρότι όλες οι τεχνικές ελέγχου διενεργούν *από τεχνική άποψη* έλεγχο πακέτων, συνεπάγονται διαφορετικά επίπεδα παρέμβασης. Υπάρχουν δύο βασικές κατηγορίες τεχνικών ελέγχου. Η μία βασίζεται μόνον στην κεφαλίδα IP, ενώ η άλλη και στο ωφέλιμο φορτίο IP.

Βάσει των πληροφοριών της κεφαλίδας IP. Ο έλεγχος μιας κεφαλίδας πακέτου IP αποκαλύπτει ορισμένα πεδία, τα οποία ενδέχεται να επιτρέπουν στους παρόχους υπηρεσιών Διαδικτύου να εφαρμόζουν συγκεκριμένες πολιτικές για τη διαχείριση της κίνησης. Οι εν λόγω τεχνικές, οι οποίες βασίζονται μόνον στον έλεγχο των κεφαλίδων IP, επεξεργάζονται δεδομένα τα οποία, καταρχήν, προορίζονται για τη δρομολόγηση πληροφοριών για διαφορετικό σκοπό (δηλαδή διαφοροποίηση της κίνησης). Βλέποντας τη διεύθυνση IP προέλευσης, ο πάροχος υπηρεσιών Διαδικτύου μπορεί να τη συνδέσει με έναν συγκεκριμένο συνδρομητή και να εφαρμόσει προς τούτο συγκεκριμένες πολιτικές, για παράδειγμα να δρομολογήσει το πακέτο μέσω ταχύτερου ή πιο αργού συνδέσμου. Βλέποντας τη διεύθυνση IP προορισμού, ο πάροχος υπηρεσιών Διαδικτύου μπορεί επίσης να εφαρμόσει συγκεκριμένες πολιτικές, για παράδειγμα να παρεμποδίσει ή να φιλτράρει την πρόσβαση σε ορισμένους δικτυακούς τόπους.

Βάσει ελέγχου εις βάθος. Ο έλεγχος των πακέτων εις βάθος επιτρέπει στον πάροχο υπηρεσιών Διαδικτύου να αποκτήσει πρόσβαση σε πληροφορίες οι οποίες προορίζονται μόνον για τον αποδέκτη της επικοινωνίας. Για να επανέλθουμε στο παράδειγμα της ταχυδρομικής υπηρεσίας, η προσέγγιση αυτή αντιστοιχεί στο άνοιγμα του φακέλου και στην ανάγνωση της επιστολής που περιέχεται σε αυτόν για να αναλυθεί το περιεχόμενο της επικοινωνίας (το οποίο περιέχεται μέσα στα πακέτα IP), προκειμένου να εφαρμοσθεί μια συγκεκριμένη πολιτική δικτύου. Υπάρχουν διάφοροι τρόποι διενέργειας του ελέγχου, καθένας εκ των οποίων ενέχει διαφορετικές απειλές για το πρόσωπο στο οποίο αναφέρονται τα δεδομένα.

— *Έλεγχος πακέτων εις βάθος βάσει της ανάλυσης πρωτοκόλλων και στατιστικών αρχείων.* Επιπλέον του πρωτοκόλλου Ίντερνετ, σκοπός του οποίου είναι να επιτρέπει τη διαβίβαση των δεδομένων στο Διαδίκτυο, υπάρχουν πρόσθετα πρωτόκολλα, τα οποία κωδικοποιούν τις πληροφορίες που διαβιβάζονται με συμφωνημένο τρόπο (μεταφορά, σύνοδος, παρουσίαση και εφαρμογή κ.λπ.). Στόχος των εν λόγω πρωτοκόλλων είναι να διασφαλίζουν ότι τα μέρη που επικοινωνούν κατανοούν το ένα το άλλο. Για παράδειγμα, υπάρχουν ορισμένα πρωτόκολλα τα οποία συνδέονται με τη φυλλομέτρηση του Παγκόσμιου Ιστού ([21]), άλλα με τη μεταφορά αρχείων ([22]) κ.λπ. Επομένως, οι τεχνικές ελέγχου που βασίζονται στον έλεγχο πρωτοκόλλων και συνδυάζονται με στατιστική ανάλυση αποσκοπούν στην αναζήτηση συγκεκριμένων προτύπων ή αποτυπωμάτων που καθορίζουν ποια πρωτόκολλα είναι παρόντα ([23]). Οι εν λόγω τεχνικές ελέγχου επιτρέπουν στους παρόχους υπηρεσιών Διαδικτύου να κατανοούν τον τύπο επικοινωνίας (ηλεκτρονικό ταχυδρομείο, φυλλομέτρηση του Παγκόσμιου Ιστού, μεταφόρτωση αρχείων) και, ενίοτε, να προσδιορίζουν τη συγκεκριμένη υπηρεσία ή εφαρμογή που χρησιμοποιείται, όπως στην περίπτωση ορισμένων επικοινωνιών VoIP, στις οποίες τα χρησιμοποιούμενα πρωτόκολλα συνδέονται με ειδικό τρόπο με έναν συγκεκριμένο πωλητή ή πάροχο υπηρεσιών. Η γνώση του τύπου πληροφοριών μπορεί να επιτρέπει στους παρόχους υπηρεσιών Διαδικτύου να εφαρμόζουν συγκεκριμένες πολιτικές διαχείρισης της κίνησης, για παράδειγμα, για την παρεμπόδιση κίνησης στον Παγκόσμιο Ιστό. Μπορεί επίσης να αποτελεί το πρώτο βήμα που θα επιτρέψει στον πάροχο υπηρεσιών Διαδικτύου να διενεργήσει περαιτέρω αναλύσεις, οι οποίες μπορεί να απαιτούν πλήρη πρόσβαση στα μεταδεδομένα και στο περιεχόμενο της επικοινωνίας.

([20]) Παρ' όλα αυτά, ο εξοπλισμός δικτύου Διαδικτύου χρησιμοποιεί πρωτόκολλα δρομολόγησης τα οποία καταχωρίζουν δραστηριότητες, επεξεργάζονται στατιστικά στοιχεία κίνησης και ανταλλάσσουν πληροφορίες με άλλον εξοπλισμό δικτύου με σκοπό τη δρομολόγηση πακέτων IP χρησιμοποιώντας την πιο αποτελεσματική διαδρομή. Για παράδειγμα, σε περίπτωση συμφόρησης ή κατάρρευσης ενός συνδέσμου, εάν ένας δρομολογητής λάβει την πληροφορία αυτή θα επικαιροποιήσει τον πίνακα δρομολόγησης με κάποια εναλλακτική διαδρομή η οποία δεν χρησιμοποιεί τον συγκεκριμένο σύνδεσμο. Επισήμανσης χρήζει επίσης το γεγονός ότι η συλλογή και η επεξεργασία μπορούν ενίοτε να πραγματοποιούνται για σκοπούς τιμολόγησης ή ακόμη και σύμφωνα με τις απαιτήσεις της οδηγίας για τη διατήρηση δεδομένων.

([21]) HTTP — πρωτόκολλο μεταφοράς υπερκειμένου — ή HTML — γλώσσα υπερκειμενικής σήμανσης.

([22]) FTP — πρωτόκολλο μεταφοράς αρχείων.

([23]) Υπάρχουν διάφοροι τρόποι εντοπισμού των χρησιμοποιούμενων πρωτοκόλλων. Για παράδειγμα, μπορεί να γίνει αναζήτηση σε συγκεκριμένα πεδία σε εσωτερικά πρωτόκολλα, π.χ. για τον εντοπισμό θυρών που χρησιμοποιήθηκαν για την εγκαθίδρυση της επικοινωνίας. Στατιστικός χαρακτηρισμός μιας ροής επικοινωνίας μπορεί επίσης να προκύψει από την ανάλυση συγκεκριμένων πεδίων, τη συσχέτιση των πρωτοκόλλων που χρησιμοποιούνται ταυτόχρονα μεταξύ δύο διευθύνσεων IP.

— *Έλεγχος πακέτων εις βάθος βάσει της ανάλυσης του περιεχομένου της επικοινωνίας.* Τέλος, μπορούν επίσης να ελεγχθούν τα μεταδεδομένα ([24]) και το περιεχόμενο μιας επικοινωνίας. Η τεχνική αυτή συνίσταται στην παρακολούθηση όλων των πακέτων IP που αποτελούν μέρος της αρχικής ροής επικοινωνίας, ώστε να μπορεί να ανασυγκροτηθεί πλήρως και να αναλυθεί το αρχικό περιεχόμενο της επικοινωνίας. Για παράδειγμα, για τον εντοπισμό επιβλαβούς ή παράνομου περιεχομένου, όπως ιοί, παιδική πορνογραφία κ.λπ., απαιτείται ανασυγκρότηση του ίδιου του περιεχομένου ώστε να μπορεί να αναλυθεί. Πρέπει να σημειωθεί ότι ενίοτε η επικοινωνία μπορεί να κρυπτογραφηθεί ρητώς διατερματικά από τα μέρη που επικοινωνούν, η πρακτική δε αυτή θα εμποδίσει τους παρόχους υπηρεσιών Διαδικτύου να διενεργήσουν ανάλυση του περιεχομένου της επικοινωνίας.

IV.3. **Επιπτώσεις στην ιδιωτική ζωή και στην προστασία των δεδομένων**

33. Οι τεχνικές ελέγχου οι οποίες βασίζονται σε κεφαλίδες IP, και ειδικότερα εκείνες που βασίζονται σε έλεγχο πακέτων, περιλαμβάνουν την παρακολούθηση και το φιλτράρισμα των δεδομένων αυτών και έχουν σοβαρές επιπτώσεις στην ιδιωτική ζωή και στην προστασία των δεδομένων. Μπορεί επίσης να αντίκεινται στο δικαίωμα στην εμπιστευτικότητα των επικοινωνιών.

34. Η παρακολούθηση των επικοινωνιών φυσικών προσώπων έχει αφ' εαυτή σοβαρές επιπτώσεις στην ιδιωτική ζωή και στην προστασία των δεδομένων. Όμως, το πρόβλημα είναι ευρύτερο, καθώς, ανάλογα με τα αποτελέσματα που επιδιώκονται από την παρακολούθηση και την αναχαίτιση, οι επιπτώσεις στην ιδιωτική ζωή μπορεί να αυξάνονται περαιτέρω. Πράγματι, δεν είναι το ίδιο να ελέγχονται απλώς οι επικοινωνίες, για παράδειγμα, προκειμένου να διασφαλίζεται η καλή λειτουργία του συστήματος, και να ελέγχονται οι επικοινωνίες για την εφαρμογή πολιτικών οι οποίες ενδέχεται να έχουν αντίκτυπο σε φυσικά πρόσωπα. Όταν οι πολιτικές διαχείρισης της κίνησης και επιλογής επιδιώκουν μόνον την αποφυγή της συμφόρησης του δικτύου, συνήθως δεν υπάρχουν σημαντικές επιπτώσεις στην ιδιωτική ζωή των φυσικών προσώπων. Ωστόσο, οι πολιτικές διαχείρισης της κίνησης μπορεί να επιδιώκουν να παρεμποδίσουν μερικές πληροφορίες περιεχομένου ή να επηρεάσουν την επικοινωνία, για παράδειγμα, μέσω συμπεριφορικής διαφήμισης. Στις περιπτώσεις αυτές, οι συνέπειες είναι πιο παρεμβατικές. Η ανησυχία αυξάνεται, εάν αναλογιστούμε ότι ο συγκεκριμένος τύπος πληροφοριών συλλέγεται όχι για μια μικρή ομάδα φυσικών προσώπων, αλλά μάλλον σε γενικευμένη βάση, για όλους τους πελάτες παρόχων υπηρεσιών Διαδικτύου ([25]). Εάν όλοι οι πάροχοι υπηρεσιών Διαδικτύου υιοθετήσουν τεχνικές φιλτραρίσματος, αυτό μπορεί να έχει ως αποτέλεσμα γενικευμένη παρακολούθηση της χρήσης του Διαδικτύου. Επιπλέον, εάν επικεντρωθούμε στον τύπο των πληροφοριών που υποβάλλονται σε επεξεργασία, οι κίνδυνοι για την ιδιωτική ζωή είναι εμφανώς υψηλοί, καθώς μεγάλο μέρος των πληροφοριών που συλλέγονται ενδέχεται να είναι εξαιρετικά ευαίσθητες και, μετά τη συλλογή, καθίστανται διαθέσιμες σε παρόχους υπηρεσιών Διαδικτύου και σε όσους ζητούν πληροφορίες από αυτούς. Επιπλέον, οι πληροφορίες μπορεί να είναι εξαιρετικά πολύτιμες από εμπορική άποψη. Από μόνο του, το γεγονός αυτό συνιστά υψηλό κίνδυνο υφέρπουσας διεύρυνσης των αρμοδιοτήτων, όπου οι αρχικοί σκοποί μπορούν εύκολα να εξελιχθούν σε εμπορική ή άλλη εκμετάλλευση των συλλεχθεισών πληροφοριών.

35. Η ορθή εφαρμογή τεχνικών παρακολούθησης και ελέγχου και φιλτραρίσματος πρέπει να πραγματοποιείται σύμφωνα με τις ισχύουσες εγγυήσεις για την προστασία των δεδομένων και την ιδιωτική ζωή, οι οποίες θεσπίζουν όρια όσον αφορά το επιτρεπτό τέτοιων ενεργειών και τις προϋποθέσεις υπό τις οποίες αυτές είναι δυνατές. Ακολουθεί επισκόπηση των εγγυήσεων που κατοχυρώνονται στο ισχύον νομικό πλαίσιο της ΕΕ για την προστασία των δεδομένων και την ιδιωτική ζωή.

V. **ΕΦΑΡΜΟΓΗ ΤΟΥ ΝΟΜΙΚΟΥ ΠΛΑΙΣΙΟΥ ΤΗΣ ΕΕ ΓΙΑ ΤΗΝ ΙΔΙΩΤΙΚΗ ΖΩΗ ΚΑΙ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ**

36. Το πλαίσιο της ΕΕ για την προστασία των δεδομένων είναι τεχνολογικά ουδέτερο. Υπό την έννοια αυτή, δεν ρυθμίζει συγκεκριμένες τεχνικές ελέγχου όπως αυτές που περιγράφονται ανωτέρω. Η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ρυθμίζει την προστασία της ιδιωτικής ζωής στο πλαίσιο της παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα (συνήθως πρόσβαση στο

([24]) Κάθε πρωτόκολλο έχει μερικά συγκεκριμένα πεδία στην κεφαλίδα του τα οποία παρέχουν πρόσθετες άτυπες πληροφορίες για την επικοινωνία που διαβιβάζεται. Επομένως, το περιεχόμενο των εν λόγω πεδίων μπορεί να αναφέρεται ως τα μεταδεδομένα της επικοινωνίας. Παράδειγμα των πεδίων αυτών μπορεί να είναι ο αριθμός θύρας που χρησιμοποιείται, όπου, για παράδειγμα, εάν ο αριθμός είναι 80, είναι πολύ πιθανό ο τύπος επικοινωνίας να είναι φυλλομέτρηση του Παγκόσμιου Ιστού.

([25]) Βεβαίως, οι ικανότητες ιχνηλάτησης δεν είναι αποκλειστικό προνόμιο των παρόχων υπηρεσιών Διαδικτύου. Αντιθέτως, οι πάροχοι διαφημιστικών δικτύων μπορούν επίσης, μέσω της χρήσης cookies τρίτων, να εντοπίζουν χρήστες σε διάφορους δικτυακούς τόπους. Βλ., για παράδειγμα, πρόσφατο επιστημονικό άρθρο το οποίο υποστηρίζει ότι η Google είναι παρούσα σε 97 από τους 100 κορυφαίους δικτυακούς τόπους, πράγμα που σημαίνει ότι η Google μπορεί να εντοπίζει χρήστες που δεν έχουν απαλλαγεί από τα cookies τρίτων καθώς φυλλομετρούν τους δημοφιλείς αυτούς δικτυακούς τόπους. Βλ.: Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning (Flash Cookies και ιδιωτική ζωή II: τώρα με HTML5 and αναδημιουργία ETag) (29 Ιουλίου 2011). Το άρθρο είναι διαθέσιμο στη διεύθυνση του SSRN: http://ssrn.com/abstract=1898390. Ο εντοπισμός χρηστών μέσω cookies τρίτων εξετάσθηκε από την ομάδα εργασίας του άρθρου 29. Βλ. γνώμη 2/2010 σχετικά με την επιγραμμική συμπεριφορική διαφήμιση, η οποία εκδόθηκε στις 22 Ιουνίου 2010 (WP 171).

Διαδίκτυο και τηλεφωνία) ([26]), η δε οδηγία για την προστασία των δεδομένων ρυθμίζει την επεξεργασία δεδομένων γενικά. Το νομικό αυτό πλαίσιο θεσπίζει στο σύνολό του διαφορετικές υποχρεώσεις οι οποίες ισχύουν για παρόχους υπηρεσιών Διαδικτύου που επεξεργάζονται και παρακολουθούν δεδομένα κίνησης και επικοινωνιών.

V.1. **Νομικοί λόγοι για την επεξεργασία δεδομένων κίνησης και περιεχομένου**

37. Βάσει της νομοθεσίας για την προστασία των δεδομένων, η επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως είναι στην προκειμένη περίπτωση η επεξεργασία δεδομένων κίνησης και επικοινωνίας, απαιτεί επαρκή νομική βάση. Επιπλέον, της γενικής αυτής απαίτησης, ειδικές απαιτήσεις μπορεί να τυγχάνουν εφαρμογής σε συγκεκριμένες περιπτώσεις.

38. Στην προκειμένη περίπτωση, ο τύπος δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία από παρόχους υπηρεσιών Διαδικτύου αφορά τα δεδομένα κίνησης και το περιεχόμενο επικοινωνιών. Το περιεχόμενο των επικοινωνιών και τα δεδομένα κίνησης προστατεύονται αμφότερα από το δικαίωμα εμπιστευτικότητας της αλληλογραφίας, το οποίο κατοχυρώνεται στο άρθρο 8 της ΕΣΔΑ και στα άρθρα 7 και 8 του Χάρτη. Ειδικότερα, το άρθρο 5 παράγραφος 1 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, με τίτλο «Απόρρητο των επικοινωνιών», απαιτεί από τα κράτη μέλη να κατοχυρώνουν το απόρρητο των επικοινωνιών που διενεργούνται μέσω δημόσιου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών καθώς και των συναφών δεδομένων κίνησης. Ταυτόχρονα, το άρθρο 5 παράγραφος 1 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες προβλέπει ότι η επεξεργασία δεδομένων κίνησης και περιεχομένου από παρόχους υπηρεσιών Διαδικτύου μπορεί να επιτρέπεται, υπό ορισμένες προϋποθέσεις, με τη συγκατάθεση των χρηστών. Για τον σκοπό αυτό, τα κράτη μέλη 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». Το σημείο αυτό αναλύεται περαιτέρω στη συνέχεια.

39. Επιπλέον της συγκατάθεσης των ενδιαφερόμενων χρηστών, η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες προβλέπει και άλλους λόγους οι οποίοι μπορεί να νομιμοποιούν την επεξεργασία δεδομένων κίνησης και επικοινωνίας από τους παρόχους υπηρεσιών Διαδικτύου. Οι σχετικοί νομικοί λόγοι για την επεξεργασία στην προκειμένη περίπτωση είναι *i)* η παροχή της υπηρεσίας, *ii)* η προστασία της ασφάλειας της υπηρεσίας και *iii)* η ελαχιστοποίηση της συμφόρησης. Άλλοι ενδεχόμενοι λόγοι για τη νομιμοποίηση πολιτικών διαχείρισης που βασίζονται σε δεδομένα κίνησης ή επικοινωνίας εξετάζονται κατωτέρω υπό *iv)*.

i) Νομικοί λόγοι για την παροχή της υπηρεσίας

40. Όπως είδαμε στην ενότητα IV, οι πάροχοι υπηρεσιών Διαδικτύου επεξεργάζονται τις πληροφορίες σε κεφαλίδες IP με σκοπό τη δρομολόγηση κάθε πακέτου IP προς τον προορισμό του. Το άρθρο 6 παράγραφος 1 και το άρθρο 6 παράγραφος 2 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες επιτρέπουν την επεξεργασία δεδομένων κίνησης για τον σκοπό της μετάδοσης μιας επικοινωνίας. Έτσι, οι πάροχοι υπηρεσιών Διαδικτύου μπορούν να επεξεργάζονται τις πληροφορίες οι οποίες είναι αναγκαίες για την παροχή της υπηρεσίας.

ii) Νομικοί λόγοι για την προστασία της ασφάλειας της υπηρεσίας

41. Δυνάμει του άρθρου 4 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, ο πάροχος υπηρεσιών Διαδικτύου υπέχει γενική υποχρέωση να λαμβάνει ενδεδειγμένα μέτρα προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του. Η πρακτική του φιλτραρίσματος ιών μπορεί να περιλαμβάνει την επεξεργασία κεφαλίδων IP και ωφέλιμου φορτίου IP. Λαμβάνοντας υπόψη ότι το άρθρο 4 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες απαιτεί από τους παρόχους υπηρεσιών Διαδικτύου να διασφαλίζουν την ασφάλεια του δικτύου, η παρούσα διάταξη νομιμοποιεί τις τεχνικές ελέγχου που βασίζονται σε κεφαλίδες και περιεχόμενο IP οι οποίες στοχεύουν αποκλειστικά την επίτευξη του σκοπού αυτού. Στην πράξη, αυτό σημαίνει ότι, εντός των ορίων που προβλέπει η αρχή της αναλογικότητας (βλ. ενότητα V.3), οι πάροχοι υπηρεσιών Διαδικτύου μπορούν να παρακολουθούν και να φιλτράρουν δεδομένα επικοινωνίας για την καταπολέμηση ιών και γενικά για να διασφαλίζουν την ασφάλεια του δικτύου ([27]).

([26]) Η αιτιολογική σκέψη 10 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες αναφέρει τα εξής: «Στον τομέα των ηλεκτρονικών επικοινωνιών, η οδηγία 95/46/ΕΚ εφαρμόζεται ιδίως σε όλα τα ζητήματα που αφορούν την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών που δεν καλύπτονται ρητά από τις διατάξεις της παρούσας οδηγίας, συμπεριλαμβανομένων των υποχρεώσεων του υπεύθυνου επεξεργασίας και των ατομικών δικαιωμάτων». Επίσης, η αιτιολογική σκέψη 17 είναι συναφής όσον αφορά τη συγκατάθεση του προσώπου στο οποίο αναφέρονται τα δεδομένα: «Για τους σκοπούς της παρούσας οδηγίας, η συγκατάθεση του χρήστη ή του συνδρομητή, ανεξάρτητα αν αυτός είναι φυσικό ή νομικό πρόσωπο, πρέπει να έχουν την ίδια έννοια με τη συγκατάθεση του προσώπου στο οποίο αναφέρονται τα δεδομένα, όπως ορίζεται και περαιτέρω προσδιορίζεται στην οδηγία 95/46/ΕΚ».

([27]) Γνώμη 2/2006 της ομάδας εργασίας του άρθρο 29 σχετικά με το απόρρητο κατά την παροχή υπηρεσιών ελέγχου του ηλεκτρονικού ταχυδρομείου, η οποία εκδόθηκε στις 21 Φεβρουαρίου 2006 (WP 118). Στην εν λόγω γνώμη, η ομάδα εργασίας θεωρεί ότι η χρήση φίλτρων για τον σκοπό του άρθρου 4 μπορεί να είναι συμβατή με το άρθρο 5 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

iii) Νομικοί λόγοι για την ελαχιστοποίηση των συνεπειών της συμφόρησης

42. Το σκεπτικό πίσω από τον συγκεκριμένο νομικό λόγο βρίσκεται στην αιτιολογική σκέψη 22 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, η οποία εξηγεί την απαγόρευση της αποθήκευσης επικοινωνιών που προβλέπεται στο άρθρο 5 παράγραφος 1. Το εν λόγω άρθρο δεν αποκλείει την τυχόν αυτόματη, ενδιάμεση και παροδική αποθήκευση των πληροφοριών, εφόσον αυτή γίνεται με μοναδικό σκοπό την πραγματοποίηση της μετάδοσης και δεν διαρκεί περισσότερο από όσο απαιτείται για τους σκοπούς της μετάδοσης και της διαχείρισης της κυκλοφορίας και εφόσον διατηρείται η εγγύηση της εμπιστευτικότητας των επικοινωνιών.

43. Εάν υπάρχει συμφόρηση, τίθεται το ερώτημα κατά πόσον οι πάροχοι υπηρεσιών Διαδικτύου μπορούν να εξετάσουν το ενδεχόμενο να εγκαταλείψουν ή να καθυστερήσουν την κίνηση ή μάλλον να επιβραδύνουν τις μη χρονοευαίσθητες επικοινωνίες, π.χ. P2P ή κίνηση ηλεκτρονικού ταχυδρομείου, επιτρέποντας, για παράδειγμα, την κίνηση φωνής να περάσει σε αποδεκτό επίπεδο ποιότητας.

44. Λαμβάνοντας υπόψη το γενικό συμφέρον της κοινωνίας να διασφαλίσει ένα δίκτυο επικοινωνιών το οποίο μπορεί να χρησιμοποιηθεί, οι πάροχοι υπηρεσιών Διαδικτύου μπορούν να ισχυρισθούν ότι η παροχή προτεραιότητας ή ο στραγγαλισμός της κίνησης για την αντιμετώπιση της συμφόρησης είναι ένα θεμιτό και αναγκαίο μέτρο για την παροχή κατάλληλης υπηρεσίας. Αυτό σημαίνει ότι, στις συγκεκριμένες περιπτώσεις και για τον συγκεκριμένο σκοπό, θα υπάρχει ένας γενικός νομικός λόγος για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και δεν θα απαιτείται η ειδική συγκατάθεση των χρηστών.

45. Ταυτόχρονα, η ικανότητα παρέμβασης με τον τρόπο αυτό δεν είναι απεριόριστη. Εάν οι πάροχοι υπηρεσιών Διαδικτύου πρέπει να ελέγχουν τις επικοινωνίες, από την άποψη της εμπιστευτικότητας και εφαρμόζοντας αυστηρά την αρχή της αναλογικότητας, πρέπει να χρησιμοποιούν τη λιγότερο παρεμβατική διαθέσιμη μέθοδο για την επίτευξη του σκοπού αυτού (αποφεύγοντας τον έλεγχο πακέτων εις βάθος), πρέπει δε να την εφαρμόζουν μόνον για όσο διάστημα απαιτείται για να αντιμετωπισθεί η συμφόρηση.

iv) Νομικοί λόγοι για την επεξεργασία δεδομένων για άλλους σκοπούς

46. Οι πάροχοι υπηρεσιών Διαδικτύου μπορεί να θέλουν επίσης να ελέγχουν δεδομένα κίνησης και περιεχομένου για άλλους σκοπούς, για παράδειγμα, προσφέροντας ειδικού χαρακτήρα συνδρομές (π.χ. συνδρομή η οποία περιορίζει την πρόσβαση σε P2P ή συνδρομή η οποία αυξάνει την ταχύτητα για ορισμένες εφαρμογές). Ο έλεγχος και η περαιτέρω χρήση δεδομένων κίνησης και επικοινωνίας για σκοπούς διαφορετικούς από την παροχή της υπηρεσίας ή την προστασία της ασφάλειάς της και την αποσόβηση της συμφόρησης επιτρέπονται μόνον υπό αυστηρές προϋποθέσεις, σύμφωνα με το νομικό πλαίσιο.

47. Το νομικό πλαίσιο είναι κυρίως το άρθρο 5 παράγραφος 1 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, το οποίο επιβάλλει τη συγκατάθεση των ενδιαφερόμενων χρηστών για την ακρόαση, την υποκλοπή, την αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης. Στην πράξη, αυτό σημαίνει ότι η συγκατάθεση των χρηστών που συμμετέχουν σε μια επικοινωνία είναι αναγκαία για τη νομιμοποίηση της επεξεργασίας τόσο δεδομένων κίνησης όσο και δεδομένων επικοινωνίας δυνάμει του άρθρου 5 παράγραφος 1.

48. Όπως αναφέρθηκε ανωτέρω, η εφαρμογή τεχνικών ελέγχου και φιλτραρίσματος βασίζεται είτε σε κεφαλίδες IP, οι οποίες αποτελούν δεδομένα κίνησης, είτε σε έλεγχο πακέτων εις βάθος, ο οποίος περιλαμβάνει επίσης ωφέλιμο φορτίο IP και αφορά δεδομένα επικοινωνίας. Επομένως, καταρχήν, η εφαρμογή τέτοιων τεχνικών για σκοπούς διαφορετικούς από τη μετάδοση της υπηρεσίας ή την ασφάλεια απαγορεύεται, εκτός εάν ένας θεμιτός λόγος επιτρέπει την επεξεργασία, όπως η συγκατάθεση (άρθρο 5 παράγραφος 1). Ένα παράδειγμα στο οποίο εφαρμόζεται το άρθρο 5 παράγραφος 1 αφορά την περίπτωση κατά την οποία ένας πάροχος υπηρεσιών Διαδικτύου αποφασίζει να προσφέρει σε πελάτες μειωμένη τιμή για την πρόσβαση στο Διαδίκτυο με αντάλλαγμα τη λήψη συμπεριφορικής διαφήμισης από τους πελάτες, με τη χρήση ελέγχου πακέτων εις βάθος, και επομένως δεδομένων επικοινωνίας, για τον σκοπό αυτό. Κατά συνέπεια, απαιτείται πραγματική, ρητή και ενημερωμένη συγκατάθεση σύμφωνα με το άρθρο 5 παράγραφος 1.

49. Επιπλέον, το άρθρο 6 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες με τίτλο «Δεδομένα κίνησης» θεσπίζει ορισμένους κανόνες οι οποίοι εφαρμόζονται ειδικά στα δεδομένα κίνησης. Ειδικότερα, προβλέπει τη δυνατότητα των παρόχων υπηρεσιών Διαδικτύου να επεξεργάζονται δεδομένα

κίνησης βάσει της συγκατάθεσης των χρηστών να λαμβάνουν υπηρεσίες προστιθέμενης αξίας ([28]). Η εν λόγω διάταξη προσδιορίζει την απαίτηση συγκατάθεσης η οποία προβλέπεται στο άρθρο 5 παράγραφος 1 όταν διακυβεύονται δεδομένα κίνησης.

50. Στην πράξη, μπορεί να μην είναι πάντοτε εύκολο να εξακριβωθεί σε ποιες περιπτώσεις απαιτείται, για παράδειγμα, συγκατάθεση και σε ποιες περιπτώσεις η ασφάλεια του δικτύου μπορεί να νομιμοποιεί την επεξεργασία, ιδίως εάν οι σκοποί των τεχνικών ελέγχου είναι διττοί (για παράδειγμα, αποφυγή συμφόρησης και παροχή υπηρεσιών προστιθέμενης αξίας). Επισημαίνεται ότι η συγκατάθεση δεν μπορεί να γίνεται αντιληπτή ως μια εύκολη και συστημική διέξοδος για τη συμμόρφωση προς τις αρχές της προστασίας των δεδομένων.

51. Οι εμπειρίες από την εφαρμογή του πλαισίου, και ειδικότερα των διάφορων πτυχών που περιγράφονται ανωτέρω, είναι ελάχιστες. Πρόκειται για έναν τομέα στον οποίο απαιτείται περαιτέρω καθοδήγηση, όπως εξηγείται περαιτέρω στην ενότητα VI. Επιπλέον, υπάρχουν πρόσθετες, συναφείς πτυχές οι οποίες αφορούν την εξασφάλιση συγκατάθεσης και χρήζουν επίσης ειδικής εξέτασης. Οι πτυχές αυτές αναλύονται κατωτέρω.

V.2. **Ζητήματα που σχετίζονται με την παροχή ενημερωμένης συγκατάθεσης ως νομικού λόγου**

52. Η συγκατάθεση που απαιτείται βάσει των άρθρων 5 και 6 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες έχει την ίδια έννοια με τη συγκατάθεση του προσώπου στο οποίο αναφέρονται τα δεδομένα όπως ορίζεται και προσδιορίζεται περαιτέρω στην οδηγία 95/46/ΕΚ ([29]). Σύμφωνα με το άρθρο 2 στοιχείο η) της οδηγίας για την προστασία των δεδομένων, ως «συγκατάθεση του προσώπου στο οποίο αναφέρονται τα δεδομένα», νοείται «κάθε δήλωση βουλήσεως, ελευθέρας, ρητής και εν πλήρει επιγνώσει, με την οποία το πρόσωπο στο οποίο αναφέρονται τα δεδομένα δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν». Πρόσφατα, ο ρόλος και οι απαιτήσεις εγκυρότητας της συγκατάθεση εξετάσθηκαν από την ομάδα εργασίας του άρθρου 29 στη γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης ([30]).

53. Επομένως, οι πάροχοι υπηρεσιών Διαδικτύου, οι οποίοι χρειάζονται συγκατάθεση για τον έλεγχο και το φιλτράρισμα δεδομένων κίνησης και περιεχομένου, πρέπει να εξασφαλίζουν ελεύθερη, ρητή και εν πλήρει επιγνώσει δήλωση βούλησης, με την οποία το πρόσωπο στο οποίο αναφέρονται τα δεδομένα δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Αυτό επαναβεβαιώνεται στην αιτιολογική σκέψη 17 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες: «(…) Η συγκατάθεση δύναται να παρέχεται με κάθε πρόσφορο τρόπο που επιτρέπει την ελεύθερη και ενημερωμένη έκφραση των επιθυμιών του χρήστη, όπως με τη συμπλήρωση τετραγωνιδίου κατά την επίσκεψη ιστοσελίδας του Διαδικτύου». Στη συνέχεια παρατίθενται μερικά πρακτικά παραδείγματα ελεύθερης, ρητής και εν πλήρει επιγνώσει συγκατάθεσης στο παρόν πλαίσιο.

Συγκατάθεση: Ελεύθερη, ρητή και εν πλήρει επιγνώσει δήλωση βούλησης

54. *Ελεύθερη συγκατάθεση*. Οι χρήστες δεν πρέπει να υφίστανται περιορισμούς οι οποίοι συνδέουν τη συγκατάθεση με τους όρους της συνδρομής τους για πρόσβαση στο Διαδίκτυο.

55. Η συγκατάθεση των φυσικών προσώπων δεν παρέχεται ελεύθερα εάν πρέπει να συγκατατεθούν στην παρακολούθηση των δεδομένων επικοινωνίας τους προκειμένου να εξασφαλίσουν πρόσβαση σε μια υπηρεσία επικοινωνίας. Αυτό ισχύει ακόμη περισσότερο εάν *όλοι* οι πάροχοι σε μια δεδομένη αγορά προβαίνουν σε διαχείριση κίνησης για σκοπούς οι οποίοι υπερβαίνουν την ασφάλεια του δικτύου. Η μόνη επιλογή θα είναι τότε η μη απόκτηση πρόσβασης βάσει συνδρομής σε μια υπηρεσία του Διαδικτύου. Δεδομένου ότι το Διαδίκτυο έχει γίνει απαραίτητο εργαλείο για σκοπούς τόσο εργασίας όσο και ψυχαγωγίας, η άρνηση πρόσβασης βάσει συνδρομής σε μια υπηρεσία του Διαδικτύου δεν συνιστά έγκυρη εναλλακτική λύση. Το

([28]) Η αιτιολογική σκέψη 18 της οδηγίας περιέχει ενδεικτική απαρίθμηση υπηρεσιών προστιθέμενης αξίας. Δεν είναι σαφές κατά πόσον μπορεί να θεωρηθεί ότι υπηρεσίες στις οποίες εφαρμόζονται πολιτικές διαχείρισης της κίνησης περιλαμβάνονται στην απαρίθμηση. Οι πολιτικές διαχείρισης της κίνησης που στοχεύουν στην παροχή προτεραιότητας σε ορισμένους τύπους περιεχομένου μπορεί να θεωρηθούν ότι συμβάλλουν στη βελτίωση της ποιότητας της υπηρεσίας. Για παράδειγμα, η διαχείριση κίνησης η οποία συνεπάγεται απλώς την επεξεργασία κεφαλίδων IP και έχει ως στόχο να παράσχει υπηρεσίες παιγνίων υψηλής τιμής, στις οποίες η προσωπική κίνηση παιγνίου των χρηστών αποκτά προτεραιότητα μέσω του δικτύου, μπορεί να θεωρηθεί υπηρεσία προστιθέμενης αξίας. Από την άλλη πλευρά, δεν είναι καθόλου σαφές κατά πόσον η διαχείριση της κίνησης για τον στραγγαλισμό ορισμένων τύπων κίνησης, για παράδειγμα για την υποβάθμιση της κίνησης P2P, μπορεί να θεωρηθεί υπηρεσία προστιθέμενης αξίας.

([29]) Βλ. αιτιολογική σκέψη 17 και άρθρο 2 στοιχείο στ) της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

([30]) Εκδόθηκε στις 13 Ιουλίου 2011 (WP 187).

αποτέλεσμα είναι ότι τα φυσικά πρόσωπα δεν θα έχουν πραγματική ελευθερία επιλογής, δηλαδή δεν θα μπορούν να παράσχουν ελεύθερα τη συγκατάθεσή τους ([31]).

56. Ο ΕΕΠΔ φρονεί ότι υπάρχει σαφής αναγκαιότητα παρακολούθησης της αγοράς από την Επιτροπή και τις εθνικές αρχές, κυρίως για να εξακριβωθεί κατά πόσον το ενδεχόμενο αυτό –δηλαδή η ύπαρξη παρόχων που συνδέουν την παροχή υπηρεσιών τηλεπικοινωνιών με παρακολούθηση της επικοινωνίας– τείνει να καταστεί ο κανόνας. Οι πάροχοι πρέπει να προσφέρουν εναλλακτικές υπηρεσίες, περιλαμβανομένης της πρόσβασης βάσει συνδρομής στο Διαδίκτυο η οποία δεν θα υπόκειται σε διαχείριση κίνησης, χωρίς να επιβάλλουν υψηλότερο κόστος στα φυσικά πρόσωπα.

57. *Ρητή συγκατάθεση*. Η αναγκαιότητα να είναι η συγκατάθεση ρητή επιτάσσει, στην προκειμένη περίπτωση, να ζητούν οι πάροχοι υπηρεσιών Διαδικτύου συγκατάθεση για την παρακολούθηση των δεδομένων κίνησης και επικοινωνίας με σαφή και ρητό τρόπο. Σύμφωνα με την ομάδα εργασίας του άρθρου 29, «[γ]ια να είναι ρητή η συγκατάθεση πρέπει να είναι κατανοητή: θα πρέπει να αναφέρεται σαφώς και επακριβώς στο πεδίο εφαρμογής και τις συνέπειες της επεξεργασίας δεδομένων. Δεν μπορεί να ισχύει για απεριόριστο σύνολο δραστηριοτήτων επεξεργασίας». Η συγκατάθεση για τον έλεγχο δεδομένων κίνησης και επικοινωνιών δεν μπορεί, κατά πάσα πιθανότητα, να θεωρηθεί ρητή εάν «συνδέεται» με τη συγκατάθεση που αφορά τους γενικούς όρους πρόσβασης βάσει συνδρομής στην υπηρεσία. Αντιθέτως, ο ρητός χαρακτήρας απαιτεί τη χρήση στοχευμένων μέσων για την εξασφάλιση συγκατάθεσης, όπως συγκεκριμένο έντυπο συγκατάθεσης ή ένα χωριστό πλαίσιο το οποίο προορίζεται ρητώς για τον σκοπό της παρακολούθησης (αντί της πρακτικής της ενσωμάτωσης των πληροφοριών στους γενικούς όρους της σύμβασης και της αποδοχής της μέσω της υπογραφής της σύμβασης ως έχει).

58. *Συγκατάθεση εν πλήρει επιγνώσει*. Για να είναι έγκυρη η συγκατάθεση, πρέπει να παρέχεται εν πλήρει επιγνώσει. Η αναγκαιότητα παροχής πρόσφορης προηγούμενης ενημέρωσης δεν απορρέει μόνον από την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες και την οδηγία για την προστασία των δεδομένων, αλλά και από τα άρθρα 20 και 21 της οδηγίας για την καθολική υπηρεσία, όπως τροποποιήθηκε από την οδηγία 2009/136/ΕΚ ([32]). Η αναγκαιότητα ενημέρωσης και συγκατάθεσης επιβεβαιώθηκε ρητώς στην αιτιολογική σκέψη 28 της οδηγίας 2009/136/ΕΚ: «οι χρήστες θα πρέπει να είναι οπωσδήποτε πλήρως ενημερωμένοι για τυχόν περιοριστικούς όρους που επιβάλλονται στη χρήση υπηρεσιών ηλεκτρονικών επικοινωνιών από τον πάροχο υπηρεσίας ή/και δικτύου. Τα ενημερωτικά αυτά στοιχεία θα πρέπει, κατ' επιλογήν του παρόχου, να καθορίζουν σαφώς είτε τη μορφή του περιεχομένου, της εφαρμογής ή της ενεχόμενης υπηρεσίας, ή τις μεμονωμένες εφαρμογές ή υπηρεσίες, ή και τα δύο». Ακολούθως προσδιορίζεται ότι: «Ανάλογα με τη χρησιμοποιούμενη τεχνολογία και τον τύπο περιορισμού, για τέτοιους περιορισμούς απαιτείται ενδεχομένως συναίνεση του χρήστη βάσει της οδηγίας 2002/58/ΕΚ».

59. Λαμβάνοντας υπόψη την πολυπλοκότητα αυτών των τεχνικών παρακολούθησης, η παροχή ουσιαστικής προηγούμενης ενημέρωσης αποτελεί μια από τις κύριες προκλήσεις για την εξασφάλιση έγκυρης συγκατάθεσης. Οι καταναλωτές πρέπει να ενημερώνονται κατά τρόπο που να τους επιτρέπει να κατανοούν τις πληροφορίες που υποβάλλονται σε επεξεργασία, τον τρόπο χρήσης τους και τον αντίκτυπο στην εμπειρία του χρήστη, καθώς και τον βαθμό παραβίασης της ιδιωτικής ζωής που συνεπάγεται η εφαρμογή των εν λόγω τεχνικών.

60. Αυτό σημαίνει όχι μόνον ότι η ενημέρωση πρέπει να είναι σαφής και κατανοητή για τον μέσο χρήστη, αλλά και ότι οι πληροφορίες παρέχονται απευθείας στα φυσικά πρόσωπα με εμφανή τρόπο ώστε να μην μπορούν να τις παραβλέψουν.

61. *Δήλωση βούλησης*. Η συγκατάθεση βάσει του ισχύοντος νομικού πλαισίου απαιτεί επίσης θετική ενέργεια του χρήστη με την οποία δηλώνει τη συμφωνία του. Η σιωπηρή συγκατάθεση δεν πληροί τον κανόνα αυτό. Η σχετική απαίτηση επιβεβαιώνει επίσης την αναγκαιότητα χρήσης ειδικών μέσων για την εξασφάλιση συγκατάθεσης, η οποία επιτρέπει στον πάροχο υπηρεσιών Διαδικτύου να ελέγχει δεδομένα κίνησης και επικοινωνιών στο πλαίσιο της εφαρμογής πολιτικών διαχείρισης της κίνησης. Στην πρόσφατη γνώμη της σχετικά με τον ορισμό της συγκατάθεσης, η ομάδα εργασίας του άρθρου 29 τόνισε την αναγκαιότητα λεπτομερούς ανάλυσης κατά την εξασφάλιση συγκατάθεσης όσον αφορά τα διάφορα στοιχεία που απαρτίζουν την επεξεργασία δεδομένων.

([31]) Παρόμοια περίπτωση αποτελούν οι φάκελοι PNR. Αντικείμενο συζήτησης εν προκειμένω αποτέλεσε το κατά πόσον η συγκατάθεση επιβατών για τη διαβίβαση των στοιχείων κράτησης στις αρχές των ΗΠΑ ήταν έγκυρη. Η ομάδα εργασίας του άρθρου 29 θεώρησε ότι η συγκατάθεση των επιβατών δεν μπορεί να παρέχεται ελεύθερα, καθώς οι αεροπορικές εταιρείες υποχρεούνται να αποστέλλουν τα δεδομένα πριν από την αναχώρηση της πτήσης και, επομένως, οι επιβάτες δεν έχουν πραγματική επιλογή, εφόσον θέλουν να ταξιδέψουν. Γνώμη 6/2002 της ομάδας εργασίας του άρθρου 29 σχετικά με τη διαβίβαση πληροφοριών για τον κατάλογο επιβατών και άλλων δεδομένων από τις αεροπορικές εταιρείες προς τις Ηνωμένες Πολιτείες.

([32]) Οδηγία 2009/136/ΕΚ, της 25ης Νοεμβρίου 2009, για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (Βλέπε υποσημείωση 15).

62. Θα μπορούσε κανείς να ισχυριστεί ότι, εάν τα μέρη που επικοινωνούν δεν επιθυμούν τη παρακολούθηση της επικοινωνίας από παρόχους υπηρεσιών Διαδικτύου, με σκοπό την εφαρμογή πολιτικής διαχείρισης της κίνησης, μπορούν σε κάθε περίπτωση να κρυπτογραφήσουν την επικοινωνία. Η προσέγγιση αυτή μπορεί να θεωρηθεί πρακτικά χρήσιμη, ωστόσο απαιτεί κάποια προσπάθεια και τεχνικές γνώσεις και δεν μπορεί να εκληφθεί ως εξομοιούμενη με ελεύθερη, ρητή και εν πλήρει επιγνώσει συγκατάθεση. Επίσης, η χρήση τεχνικών κρυπτογράφησης δεν διατηρεί μια επικοινωνία πλήρως εμπιστευτική, καθώς τουλάχιστον ο πάροχος υπηρεσιών Διαδικτύου μπορεί να έχει πρόσβαση στις πληροφορίες της κεφαλίδας IP για τη δρομολόγηση της επικοινωνίας και θα είναι επίσης σε θέση να εφαρμόσει στατιστική ανάλυση.

63. Σύμφωνα με το άρθρο 5 παράγραφος 1 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, πρέπει να εξασφαλισθεί συγκατάθεση από τους ενδιαφερόμενους χρήστες. Σε πολλές περιπτώσεις, ο χρήστης θα είναι το ίδιο πρόσωπο με τον συνδρομητή, πράγμα που επιτρέπει την παροχή της συγκατάθεσης κατά τη συνδρομή στην υπηρεσία τηλεπικοινωνιών. Σε άλλες περιπτώσεις, όπως όταν εμπλέκονται περισσότερα πρόσωπα, η συγκατάθεση των ενδιαφερόμενων χρηστών πρέπει να εξασφαλισθεί χωριστά. Το γεγονός αυτό μπορεί να εγείρει πρακτικά ζητήματα, τα οποία εξετάζονται κατωτέρω.

Συγκατάθεση όλων των ενδιαφερόμενων χρηστών

64. Το άρθρο 5 παράγραφος 1 προβλέπει τη συγκατάθεση των χρηστών για τη νομιμοποίηση της επεξεργασίας. Η συγκατάθεση πρέπει να εξασφαλισθεί από *όλους τους χρήστες* που εμπλέκονται σε μια επικοινωνία. Η απαίτηση αυτή βασίζεται στο σκεπτικό ότι μια επικοινωνία αφορά συνήθως τουλάχιστον δύο φυσικά πρόσωπα (τον αποστολέα και τον αποδέκτη). Για παράδειγμα, εάν ένας πάροχος υπηρεσιών Διαδικτύου σαρώνει ωφέλιμο φορτίο IP το οποίο αφορά ένα μήνυμα ηλεκτρονικού ταχυδρομείου, ελέγχει πληροφορίες οι οποίες σχετίζονται τόσο με τον αποστολέα όσο και με τον αποδέκτη του μηνύματος.

65. Κατά την επιτήρηση και την παρακολούθηση κίνησης και επικοινωνιών (για παράδειγμα, ορισμένης κίνησης στον Παγκόσμιο Ιστό), μπορεί να αρκεί για τους παρόχους υπηρεσιών Διαδικτύου η εξασφάλιση της συγκατάθεσης του χρήστη, δηλαδή του συνδρομητή. Αυτό συμβαίνει επειδή το άλλο μέρος της επικοινωνίας, στην προκειμένη περίπτωση, ένας δικτυακός τόπος, δεν μπορεί να θεωρηθεί «ενδιαφερόμενος χρήστης» ([33]). Ωστόσο, η κατάσταση μπορεί να είναι πιο πολύπλοκη όταν μια τέτοια παρακολούθηση περιλαμβάνει τον έλεγχο του περιεχομένου μηνυμάτων ηλεκτρονικού ταχυδρομείου και, επομένως, προσωπικές πληροφορίες του αποστολέα και του αποδέκτη του μηνύματος, οι οποίοι ενδέχεται να μην έχουν αμφότεροι συμβατική σχέση με τον ίδιο πάροχο υπηρεσιών Διαδικτύου. Πράγματι, στις περιπτώσεις αυτές, ο πάροχος υπηρεσιών Διαδικτύου επεξεργάζεται δεδομένα προσωπικού χαρακτήρα (όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου και δυνητικά ευαίσθητα δεδομένα περιεχομένου) μη πελατών. Από πρακτική άποψη, η εξασφάλιση συγκατάθεσης από τα συγκεκριμένα φυσικά πρόσωπα μπορεί να είναι πιο δύσκολη, καθώς πρέπει να γίνει κατά περίπτωση και όχι επ' ευκαιρία της σύναψης συμφωνίας για την παροχή της υπηρεσίας τηλεπικοινωνιών. Δεν είναι επίσης ρεαλιστικό να υποτεθεί ότι η συγκατάθεση του συνδρομητή παρέχεται επίσης για λογαριασμό άλλων χρηστών, όπως μπορεί να συμβαίνει συχνά σε ιδιωτικά νοικοκυριά.

66. Στο πλαίσιο αυτό, ο ΕΕΠΔ φρονεί ότι οι πάροχοι υπηρεσιών Διαδικτύου πρέπει να δεσμεύονται από τις ισχύουσες νομικές απαιτήσεις και να εφαρμόζουν πολιτικές οι οποίες δεν περιλαμβάνουν την παρακολούθηση και τον έλεγχο πληροφοριών. Η δέσμευση αυτή έχει ακόμη μεγαλύτερη σημασία όσον αφορά υπηρεσίες επικοινωνιών οι οποίες εμπλέκουν τρίτους που δεν μπορούν να συγκατατεθούν στην παρακολούθηση, ιδίως σε σχέση με μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται ή λαμβάνονται (αυτό δεν ισχύει όταν ο σκοπός βασίζεται σε λόγους ασφάλειας).

67. Ταυτόχρονα, επισημαίνεται ότι το εθνικό δίκαιο εφαρμογής του άρθρου 5 παράγραφος 1 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ενδέχεται να μην εισάγει πάντοτε ικανοποιητική ρύθμιση ως προς το σημείο αυτό. Εξάλλου, φαίνεται ότι απαιτείται γενικότερα καλύτερη καθοδήγηση όσον αφορά τις απαιτήσεις της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες στο πλαίσιο αυτό. Επομένως, ο ΕΕΠΔ καλεί την Επιτροπή να δραστηριοποιηθεί συναφώς και να αναλάβει σχετική πρωτοβουλία η οποία θα μπορεί να επωφεληθεί από τις πληροφορίες από τις αρχές ελέγχου που συμμετέχουν στην ομάδα εργασίας του άρθρου 29 και από άλλους ενδιαφερομένους. Εφόσον κριθεί αναγκαίο, σχετική υπόθεση θα πρέπει να αχθεί ενώπιον του Δικαστηρίου προκειμένου να αποσαφηνισθούν πλήρως η έννοια και οι συνέπειες του άρθρου 5 παράγραφος 1.

([33]) Ανεξάρτητα από τις περιπτώσεις στις οποίες η κίνηση στον Παγκόσμιο Ιστό περιλαμβάνει τη διαβίβαση προσωπικών πληροφοριών, όπως είναι, για παράδειγμα, φωτογραφίες φυσικών προσώπων που μπορούν να αναγνωρισθούν οι οποίες δημοσιεύονται σε έναν δικτυακό τόπο. Η επεξεργασία τέτοιων πληροφοριών απαιτεί ορισμένη νομική βάση, όμως δεν καλύπτεται από το άρθρο 5 παράγραφος 1, καθώς τα εν λόγω πρόσωπα δεν είναι «ενδιαφερόμενοι χρήστες».

V.3. **Αναλογικότητα — αρχή της ελαχιστοποίησης των δεδομένων**

68. Το άρθρο 6 στοιχείο γ) της οδηγίας για την προστασία των δεδομένων θεσπίζει την αρχή της αναλογικότητας ([34]), η οποία εφαρμόζεται στους παρόχους υπηρεσιών Διαδικτύου, καθώς είναι υπεύθυνοι της επεξεργασίας των δεδομένων κατά την έννοια της οδηγίας, όταν προβαίνουν σε παρακολούθηση και φιλτράρισμα.

69. Δυνάμει της εν λόγω αρχής, τα δεδομένα προσωπικού χαρακτήρα μπορούν να υποβάλλονται σε επεξεργασία μόνον εφόσον «είναι κατάλληλα, συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται και υφίστανται επεξεργασία». Η εφαρμογή της αρχής συνεπάγεται την ανάγκη αξιολόγησης του κατά πόσον τα μέσα επεξεργασίας των δεδομένων και οι τύποι των δεδομένων προσωπικού χαρακτήρα που χρησιμοποιούνται κατά την επεξεργασία ανταποκρίνονται στο κριτήριο της προσφορότητας και πιθανολογείται ευλόγως ότι μπορούν να επιτύχουν τους στόχους τους. Εάν το συμπέρασμα είναι ότι συλλέγονται περισσότερα δεδομένα από όσα απαιτούνται, η αρχή δεν πληρούται.

70. Η συμμόρφωση ορισμένων τύπων τεχνικών ελέγχου προς την αρχή της αναλογικότητας πρέπει να αξιολογείται κατά περίπτωση. Δεν είναι εφικτό να εξαχθούν συμπεράσματα *in abstracto*. Ωστόσο, μπορούμε να επισημάνουμε διάφορες επιμέρους πτυχές οι οποίες χρήζουν εξέτασης κατά την αξιολόγηση της συμμόρφωσης προς την αρχή της αναλογικότητας.

71. *Η ποσότητα των πληροφοριών που υποβάλλονται σε επεξεργασία*. Η εξονυχιστική επιτήρηση των επικοινωνιών πελατών παρόχων υπηρεσιών Διαδικτύου είναι στις περισσότερες περιπτώσεις υπερβολική και παράνομη. Το γεγονός ότι η επιτήρηση αυτή μπορεί να γίνεται με μη προφανή και δύσκολα αντιληπτά από τα ενδιαφερόμενα πρόσωπα μέσα αυξάνει τον αντίκτυπο στην ιδιωτική ζωή. Οι πάροχοι υπηρεσιών Διαδικτύου πρέπει να αξιολογούν ποια μέσα από αυτά που βρίσκονται στη διάθεσή τους είναι τα λιγότερο παρεμβατικά για την επίτευξη του ζητούμενου αποτελέσματος. Για παράδειγμα, μπορεί η παρακολούθηση κεφαλίδων IP να επιτύχει το ζητούμενο αποτέλεσμα αντί του ελέγχου πακέτων εις βάθος; Ακόμη και κατά τον έλεγχο πακέτων εις βάθος, η αναγνώριση ορισμένων μόνον πρωτοκόλλων μπορεί να παράσχει τις αναγκαίες πληροφορίες. Η εφαρμογή εγγυήσεων προστασίας των δεδομένων, περιλαμβανομένης της οιονεί ανωνυμοποίησης, μπορεί επίσης να είναι συναφής. Το αποτέλεσμα της αξιολόγησης πρέπει να επιβεβαιώνει ότι η επεξεργασία των δεδομένων είναι αναλογική.

72. *Τα αποτελέσματα της επεξεργασίας (άμεσα συνδεδεμένα με τους σκοπούς)*. Ενδέχεται να μην τηρείται η αρχή της αναλογικότητας σε περιπτώσεις στις οποίες οι πάροχοι υπηρεσιών Διαδικτύου χρησιμοποιούν πολιτικές διαχείρισης της κίνησης οι οποίες αποκλείουν την πρόσβαση σε ορισμένες υπηρεσίες χωρίς να παρέχουν, ως αντάλλαγμα, εύλογο μερίδιο του προκύπτοντος οφέλους στους χρήστες.

73. Υπενθυμίζεται ότι η αρχή της αναλογικότητας εξακολουθεί να εφαρμόζεται ακόμη και αν πληρούνται άλλες υποχρεωτικές νομικές απαιτήσεις, ακόμη και εάν ο πάροχος υπηρεσιών Διαδικτύου εξασφάλισε, για παράδειγμα, τη συγκατάθεση φυσικών προσώπων για την παρακολούθηση περιεχομένου. Αυτό σημαίνει ότι η επεξεργασία δεδομένων η οποία διενεργείται μέσω παρακολούθησης περιεχομένου μπορεί να εξακολουθεί να είναι παράνομη, εάν παραβιάζει την υποκείμενη θεμελιώδη αρχή της αναλογικότητας.

V.4. **Ασφάλεια και οργανωτικά μέτρα**

74. Το άρθρο 4 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες απαιτεί ρητώς από τους παρόχους υπηρεσιών Διαδικτύου να λαμβάνουν τεχνικά και οργανωτικά μέτρα ώστε να διασφαλίζεται i) ότι μόνον εξουσιοδοτημένοι υπάλληλοι έχουν πρόσβαση σε δεδομένα προσωπικού χαρακτήρα για νόμιμους σκοπούς, ii) η προστασία των δεδομένων προσωπικού χαρακτήρα από τυχαία ή παράνομη επεξεργασία και iii) η εφαρμογή μιας πολιτικής ασφάλειας όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Επιτρέπει επίσης στις αρμόδιες εθνικές αρχές να διενεργούν ελέγχους των ως άνω μέτρων.

75. Επιπλέον, δυνάμει του άρθρου 4 παράγραφοι 3 και 2 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, οι πάροχοι υπηρεσιών Διαδικτύου υποχρεούνται επίσης να κοινοποιούν αντίστοιχα την παραβίαση δεδομένων στην αρμόδια εθνική αρχή, καθώς και στα επηρεαζόμενα φυσικά πρόσωπα στην περίπτωση που η κοινοποίηση μπορεί να έχει αρνητικές συνέπειες για αυτά.

76. Η επεξεργασία προσωπικών πληροφοριών οι οποίες περιέχονται στις επικοινωνίες, με στόχο την εφαρμογή πολιτικών διαχείρισης της κίνησης, μπορεί να παράσχει στους παρόχους υπηρεσιών Διαδικτύου πρόσβαση σε δεδομένα τα οποία είναι ακόμη πιο ευαίσθητα από τα δεδομένα κίνησης.

([34]) Όπως αναφέρθηκε ανωτέρω, η οδηγία για την προστασία των δεδομένων εφαρμόζεται σε όλα τα θέματα που αφορούν την προστασία θεμελιωδών δικαιωμάτων και ελευθεριών τα οποία δεν καλύπτονται ρητώς από την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

77. Επομένως, οι πολιτικές ασφάλειας που αναπτύσσουν οι πάροχοι υπηρεσιών Διαδικτύου πρέπει να ενσωματώνουν συγκεκριμένες εγγυήσεις, προκειμένου να διασφαλίζεται ότι τα μέτρα που λαμβάνονται είναι πρόσφορα για την αποτροπή των εν λόγω κινδύνων. Ταυτόχρονα, οι αρμόδιες για τον έλεγχο των μέτρων αυτών εθνικές αρχές πρέπει να είναι ιδιαίτερα αυστηρές. Τέλος, πρέπει να διασφαλίζεται η ύπαρξη αποτελεσματικών διαδικασιών κοινοποίησης για την ενημέρωση των προσώπων στα οποία αναφέρονται τα δεδομένα των οποίων οι πληροφορίες παραβιάστηκαν και ενδέχεται, επομένως, να επηρεασθούν αρνητικά.

VI. ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΗ ΛΗΨΗ ΜΕΤΡΩΝ ΠΟΛΙΤΙΚΗΣ ΚΑΙ ΝΟΜΟΘΕΤΙΚΩΝ ΜΕΤΡΩΝ

78. Οι τεχνικές ελέγχου οι οποίες βασίζονται σε δεδομένα κίνησης και σε έλεγχο ωφέλιμων φορτίων IP, δηλαδή στο περιεχόμενο των επικοινωνιών, ενδέχεται να αποκαλύψουν τη δραστηριότητα των χρηστών στο Διαδίκτυο: τους δικτυακούς τόπους που επισκέπτονται και τις δραστηριότητες των τόπων αυτών, τη χρήση εφαρμογών P2P, τη μεταφόρτωση αρχείων, τα μηνύματα ηλεκτρονικού ταχυδρομείου που απέστειλαν και έλαβαν, τους αποστολείς των μηνυμάτων, το θέμα των μηνυμάτων, τους όρους αποστολής κ.λπ. Οι πάροχοι υπηρεσιών Διαδικτύου ενδέχεται να θέλουν να χρησιμοποιήσουν τις πληροφορίες αυτές για να δώσουν προτεραιότητα σε συγκεκριμένες μορφές επικοινωνίας, όπως τη βιντεοπαραγγελία, σε σχέση με άλλες. Ενδέχεται, επίσης, να θέλουν να τις χρησιμοποιήσουν για να εντοπίσουν ιούς ή για να καταρτίσουν προφίλ τα οποία προορίζουν προς χρήση για συμπεριφορική διαφήμιση. Οι ενέργειες αυτές παρεμβαίνουν στο δικαίωμα της εμπιστευτικότητας των επικοινωνιών.

79. Ανάλογα με τις τεχνικές που χρησιμοποιούνται και με τα συγκεκριμένα χαρακτηριστικά κάθε περίπτωσης, οι επιπτώσεις στην ιδιωτική ζωή αυξάνονται. Όσο πιο εξονυχιστική είναι η παρακολούθηση και η ανάλυση των πληροφοριών που συλλέγονται τόσο μεγαλύτερη είναι η σύγκρουση με την αρχή της εμπιστευτικότητας των επικοινωνιών. Οι σκοποί για τους οποίους πραγματοποιείται η παρακολούθηση και οι προβλεπόμενες εγγυήσεις για την προστασία των δεδομένων αποτελούν επίσης κρίσιμα στοιχεία για τον καθορισμό του βαθμού παρέμβασης στην ιδιωτική ζωή και στα δεδομένα προσωπικού χαρακτήρα των φυσικών προσώπων. Η παρεμπόδιση και η παρακολούθηση για σκοπούς καταπολέμησης κακόβουλου λογισμικού, με την εφαρμογή αυστηρών περιορισμών όσον αφορά τη διατήρηση και τη χρήση των ελεγχόμενων δεδομένων, δεν μπορούν να συγκριθούν με καταστάσεις στις οποίες οι πληροφορίες καταχωρίζονται για την κατάρτιση προφίλ προς χρήση για συμπεριφορική διαφήμιση.

80. Καταρχήν, ο ΕΕΠΔ φρονεί ότι το ισχύον πλαίσιο της ΕΕ για την ιδιωτική ζωή και την προστασία των δεδομένων, εφόσον ερμηνευθεί, εφαρμοσθεί και επιβληθεί ορθά, είναι κατάλληλο ώστε να διασφαλίζεται ο σεβασμός του δικαιώματος στην εμπιστευτικότητα των επικοινωνιών και, γενικότερα, η μη διακύβευση της προστασίας της ιδιωτικής ζωής και της προστασίας των δεδομένων των φυσικών προσώπων ([35]). Οι πάροχοι υπηρεσιών Διαδικτύου δεν πρέπει να χρησιμοποιούν τέτοιους μηχανισμούς, εάν δεν έχουν εφαρμόσει ορθά το νομικό πλαίσιο. Ειδικότερα, τα συναφή στοιχεία του πλαισίου τα οποία πρέπει να λαμβάνουν υπόψη και να σέβονται οι πάροχοι υπηρεσιών Διαδικτύου περιλαμβάνουν τα ακόλουθα:

— Οι πάροχοι υπηρεσιών Διαδικτύου μπορούν να εφαρμόζουν πολιτικές διαχείρισης της κίνησης, με σκοπό την ασφαλή παροχή της υπηρεσίας, περιλαμβανομένου του περιορισμού της συμφόρησης, δυνάμει των άρθρων 4 και 6 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

— Οι πάροχοι υπηρεσιών Διαδικτύου χρειάζονται έναν ειδικό νομικό λόγο, ενδεχομένως τη συγκατάθεση των χρηστών, για να εφαρμόσουν πολιτικές διαχείρισης της κίνησης οι οποίες συνεπάγονται την επεξεργασία δεδομένων κίνησης ή/και επικοινωνίας για σκοπούς διαφορετικούς από τους προαναφερθέντες. Για παράδειγμα, η κατόπιν ενημέρωσής τους συγκατάθεση των χρηστών είναι απαραίτητη για την παρακολούθηση και το φιλτράρισμα των επικοινωνιών φυσικών προσώπων προκειμένου να περιορισθεί (ή να επιτραπεί) η πρόσβαση σε ορισμένες εφαρμογές και υπηρεσίες, όπως P2P ή VoIP.

— Η συγκατάθεση πρέπει να είναι ελεύθερη, ρητή και εν πλήρει επιγνώσει. Πρέπει να δηλώνεται μέσω θετικής ενέργειας. Οι απαιτήσεις αυτές δίνουν μεγάλη έμφαση στην αναγκαιότητα να ενταθούν οι προσπάθειες ώστε να διασφαλίζεται ότι τα φυσικά πρόσωπα ενημερώνονται κατάλληλα, με τρόπο άμεσο, κατανοητό και συγκεκριμένο, ώστε να μπορούν να αξιολογούν τις συνέπειες των πρακτικών και να λαμβάνουν τελικά μια ενημερωμένη απόφαση. Λαμβάνοντας υπόψη την πολυπλοκότητα των τεχνικών αυτών, η παροχή ουσιαστικής προηγούμενης ενημέρωσης στους χρήστες αποτελεί μια από τις κύριες προκλήσεις προκειμένου η συναίνεση που θα εξασφαλισθεί να είναι έγκυρη. Επίσης, δεν πρέπει να επιβάλλονται τιμωρητικού χαρακτήρα συνέπειες (περιλαμβανομένου του πρόσθετου οικονομικού κόστους) για τους χρήστες που δεν συγκατατίθενται σε οποιαδήποτε παρακολούθηση.

([35]) Η πεποίθηση αυτή δεν θίγει την αναγκαιότητα αλλαγών στη νομοθεσία βάσει άλλων παραγόντων, ιδίως στο πλαίσιο της γενικής αναθεώρησης του νομικού πλαισίου της ΕΕ για την προστασία των δεδομένων, με σκοπό να καταστεί πιο αποτελεσματικό εν όψει των νέων τεχνολογιών και της παγκοσμιοποίησης.

— Η αρχή της αναλογικότητας διαδραματίζει κρίσιμο ρόλο όταν οι πάροχοι υπηρεσιών Διαδικτύου εφαρμόζουν πολιτικές διαχείρισης της κίνησης, όποιος και αν είναι ο νομικός λόγος για την επεξεργασία και ο σκοπός: παροχή της υπηρεσίας, αποφυγή της συμφόρησης ή παροχή ειδικού χαρακτήρα συνδρομητικών υπηρεσιών με ή χωρίς πρόσβαση σε ορισμένες υπηρεσίες και εφαρμογές. Η εν λόγω αρχή περιορίζει την ικανότητα των παρόχων υπηρεσιών Διαδικτύου να παρακολουθούν το περιεχόμενο των επικοινωνιών των φυσικών προσώπων όταν αυτό συνεπάγεται την επεξεργασία υπερβολικών πληροφοριών ή δημιουργεί οφέλη μόνον για τους παρόχους υπηρεσιών Διαδικτύου. Το επιτρεπτό των διαδικασιών που εφαρμόζουν, από τεχνική άποψη, οι πάροχοι υπηρεσιών Διαδικτύου εξαρτάται από το επίπεδο παρέμβασης των τεχνικών, τα ζητούμενα αποτελέσματα (από τα οποία ενδέχεται να αντλούν οφέλη) και τις συγκεκριμένες εγγυήσεις που εφαρμόζονται για την προστασία της ιδιωτικής ζωής και των δεδομένων. Πριν από την εφαρμογή τεχνικών ελέγχου, οι πάροχοι υπηρεσιών Διαδικτύου πρέπει να αξιολογούν κατά πόσον αυτές είναι σύμφωνες προς την αρχή της αναλογικότητας.

81. Παρότι το νομικό πλαίσιο περιλαμβάνει επί του παρόντος σχετικές προϋποθέσεις και εγγυήσεις, πρέπει να δοθεί ιδιαίτερη προσοχή στο κατά πόσον οι πάροχοι υπηρεσιών Διαδικτύου πληρούν πραγματικά τις νομικές απαιτήσεις, κατά πόσον παρέχουν την αναγκαία ενημέρωση στους καταναλωτές ώστε αυτοί να κάνουν ουσιαστικές επιλογές, και κατά πόσον τηρούν την αρχή της αναλογικότητας. Σε εθνικό επίπεδο, μεταξύ των αρμοδίων για τα ως άνω ζητήματα αρχών περιλαμβάνονται οι εθνικές αρχές τηλεπικοινωνιών, αφενός, και οι εθνικές αρχές προστασίας των δεδομένων, αφετέρου. Σε επίπεδο ΕΕ, στους συναφείς φορείς περιλαμβάνεται ο Φορέας Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC). Ο ΕΕΠΔ μπορεί επίσης να διαδραματίσει κάποιον ρόλο στο πλαίσιο αυτό.

82. Εκτός από την παρακολούθηση του υφιστάμενου επιπέδου συμμόρφωσης, και δεδομένης της σχετικά καινοτόμου δυνατότητας των μαζικών ελέγχων των επικοινωνιών σε πραγματικό χρόνο, ορισμένες συναφείς με την εφαρμογή του πλαισίου πτυχές που αποτέλεσαν αντικείμενο εξέτασης της παρούσας γνωμοδότητης χρήζουν εμβριθέστερης ανάλυσης και αποσαφήνισης. Καθοδήγηση χρήσιμη σε περισσότερους τομείς μπορεί να παρασχεθεί ως προς τα ακόλουθα θέματα:

— Καθορισμός των θεμιτών πρακτικών ελέγχου για τη διασφάλιση της ομαλής ροής της κίνησης, οι οποίες ενδέχεται να μην απαιτούν τη συγκατάθεση των χρηστών, όπως, για παράδειγμα, η καταπολέμηση των ανεπίκλητων μηνυμάτων. Επιπλέον της παρεμβατικότητας της εφαρμοζόμενης παρακολούθησης, έχουν σημασία πτυχές όπως, για παράδειγμα, το επίπεδο διαταραχής της ομαλής ροής της κίνησης σε αντίθετη περίπτωση.

— Καθορισμός των τεχνικών ελέγχου που μπορούν να εφαρμοσθούν για σκοπούς ασφάλειας, οι οποίες ενδέχεται να μην απαιτούν τη συγκατάθεση των χρηστών.

— Καθορισμός των περιπτώσεων στις οποίες η παρακολούθηση απαιτεί τη συγκατάθεση των φυσικών προσώπων, και ιδίως τη συγκατάθεση όλων των ενδιαφερόμενων χρηστών, καθώς και των επιτρεπόμενων τεχνικών παραμέτρων που η τήρησή τους θα διασφαλίζει ότι η τεχνική ελέγχου δεν συνεπάγεται επεξεργασία δεδομένων δυσανάλογη σε σχέση με τους επιδιωκόμενους σκοπούς.

— Επιπλέον, στις τρεις προαναφερθείσες περιπτώσεις, ενδέχεται να απαιτείται καθοδήγηση σχετικά με την εφαρμογή των αναγκαίων εγγυήσεων προστασίας των δεδομένων (περιορισμός του σκοπού, ασφάλεια κ.λπ.).

83. Δεδομένου ότι στον συγκεκριμένο τομέα συντρέχουν σωρευτικώς τόσο εθνικές όσο και ενωσιακές αρμοδιότητες, ο ΕΕΠΔ φρονεί ότι είναι απαραίτητη η ανταλλαγή απόψεων και εμπειριών για την αναζήτηση εναρμονισμένων προσεγγίσεων στα προαναφερθέντα ζητήματα. Για τον σκοπό αυτό, ο ΕΕΠΔ εισηγείται τη δημιουργία μιας πλατφόρμας ή μιας ομάδας εμπειρογνωμόνων, η οποία πρέπει να περιλαμβάνει εκπροσώπους των εθνικών ρυθμιστικών αρχών, την ομάδα εργασίας του άρθρου 29, τον ΕΕΠΔ και τον BEREC. Πρώτος στόχος της εν λόγω πλατφόρμας πρέπει να είναι η παροχή καθοδήγησης, τουλάχιστον στα θέματα που προσδιορίσθηκαν ανωτέρω, προκειμένου να διασφαλίζονται αξιόπιστες και εναρμονισμένες προσεγγίσεις και ίσοι όροι ανταγωνισμού. Ο ΕΕΠΔ απευθύνει έκκληση στην Επιτροπή να οργανώσει τη συγκεκριμένη πρωτοβουλία.

84. Τέλος, τόσο οι εθνικές αρχές όσο και οι συναφείς προς αυτές αρχές στην ΕΕ, περιλαμβανομένων του BEREC και της Επιτροπής, πρέπει να στρέψουν ιδιαιτέρως την προσοχή τους στις εξελίξεις της αγοράς στον συγκεκριμένο τομέα. Από την άποψη της προστασίας των δεδομένων και της ιδιωτικής ζωής, είναι ιδιαίτερα προβληματικό το σενάριο βάσει του οποίου οι πάροχοι υπηρεσιών Διαδικτύου εφαρμόζουν σε τακτική βάση πολιτικές διαχείρισης της κίνησης προσφέροντας συνδρομές οι οποίες βασίζονται στο φιλτράρισμα της πρόσβασης σε περιεχόμενο και εφαρμογές. Εάν μια τέτοια εξέλιξη τείνει να επιβληθεί, θα πρέπει να θεσπισθεί νομοθεσία για την αντιμετώπιση της κατάστασης.

VII. **ΣΥΜΠΕΡΑΣΜΑΤΑ**

85. Η αυξανόμενη εξάρτηση των παρόχων υπηρεσιών Διαδικτύου από τεχνικές παρακολούθησης και ελέγχου παραβιάζει την ουδετερότητα του Διαδικτύου και την εμπιστευτικότητα των επικοινωνιών. Η εξέλιξη αυτή εγείρει σοβαρά προβλήματα όσον αφορά την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα των χρηστών.

86. Καθώς η ανακοίνωση της Επιτροπής για το ανοιχτό διαδίκτυο και τη δικτυακή ουδετερότητα στην Ευρώπη άπτεται μόνον ακροθιγώς των συγκεκριμένων ζητημάτων, ο ΕΕΠΔ φρονεί ότι πρέπει να γίνουν περισσότερα προκειμένου να διαμορφωθεί μια ικανοποιητική πολιτική για το μέλλον. Επομένως, με την παρούσα γνωμοδότηση συνεισφέρει στον συνεχιζόμενο διάλογο πολιτικής για τη δικτυακή ουδετερότητα, ιδίως όσον αφορά πτυχές που σχετίζονται με την προστασία των δεδομένων και την ιδιωτική ζωή.

87. Ο ΕΕΠΔ εκτιμά ότι οι εθνικές αρχές και ο BEREC πρέπει να παρακολουθούν την κατάσταση στην αγορά. Η παρακολούθηση αυτή πρέπει να έχει ως αποτέλεσμα τη διαμόρφωση σαφούς εικόνας η οποία θα περιγράφει κατά πόσον η αγορά κινείται προς μαζικό έλεγχο των επικοινωνιών σε πραγματικό χρόνο και ζητήματα τα οποία σχετίζονται με τη συμμόρφωση προς το νομικό πλαίσιο.

88. Η παρακολούθηση της αγοράς πρέπει να συνοδεύεται από περαιτέρω ανάλυση των συνεπειών των νέων πρακτικών σε σχέση με την προστασία των δεδομένων και την ιδιωτική ζωή στο Διαδίκτυο. Στην παρούσα γνωμοδότηση παρουσιάζονται ορισμένοι τομείς οι οποίοι θα μπορούσαν να αντλήσουν οφέλη από την τυχόν αποσαφήνισή τους. Παρότι οργανισμοί και φορείς της ΕΕ, όπως ο BEREC, η ομάδα εργασίας του άρθρου 29 και ο ΕΕΠΔ έχουν ενδεχομένως τη δυνατότητα να αποσαφηνίσουν τις συνθήκες εφαρμογής του πλαισίου, ο ΕΕΠΔ φρονεί ότι η Επιτροπή έχει καθήκον να συντονίσει και να κατευθύνει τον διάλογο. Επομένως, καλεί την Επιτροπή να αναλάβει μια πρωτοβουλία με τη συμμετοχή όλων των ενδιαφερομένων σε μια πλατφόρμα ή ομάδα εργασίας, με τον στόχο αυτό. Μεταξύ των ζητημάτων που απαιτούν περαιτέρω ανάλυση, πρέπει να εξετασθούν τα ακόλουθα σημεία:

— καθορισμός των θεμιτών πρακτικών ελέγχου προκειμένου να διασφαλίζεται η ομαλή ροή της κίνησης, οι οποίες μπορούν να εφαρμόζονται για σκοπούς ασφάλειας

— καθορισμός των περιπτώσεων στις οποίες η παρακολούθηση απαιτεί τη συγκατάθεση των φυσικών προσώπων, και ιδίως τη συγκατάθεση όλων των ενδιαφερόμενων χρηστών, και των επιτρεπόμενων τεχνικών παραμέτρων ώστε να διασφαλίζεται ότι η τεχνική ελέγχου δεν συνεπάγεται επεξεργασία δεδομένων δυσανάλογη σε σχέση με τους επιδιωκόμενους σκοπούς

— στις προαναφερθείσες περιπτώσεις, ενδέχεται να απαιτείται καθοδήγηση σχετικά με την εφαρμογή των αναγκαίων εγγυήσεων για την προστασία των δεδομένων (περιορισμός του σκοπού, ασφάλεια κ.λπ.).

89. Ανάλογα με τα πορίσματα, ενδέχεται να απαιτηθεί η λήψη πρόσθετων νομοθετικών μέτρων. Σε μια τέτοια περίπτωση, η Επιτροπή πρέπει να προτείνει μέτρα πολιτικής με στόχο την ενίσχυση του νομικού πλαισίου και την εμπέδωση της ασφάλειας δικαίου. Τα νέα μέτρα πρέπει να αποσαφηνίζουν τις πρακτικές συνέπειες της αρχής της δικτυακής ουδετερότητας, κάτι που έχει ήδη γίνει σε ορισμένα κράτη μέλη, και να διασφαλίζουν τη δυνατότητα της πραγματικής επιλογής των χρηστών, ιδίως μέσω της υποχρέωσης των παρόχων υπηρεσιών Διαδικτύου να προσφέρουν συνδέσεις χωρίς παρακολούθηση.

Βρυξέλλες, 7 Οκτωβρίου 2011.

Peter HUSTINX

Ευρωπαίος Επόπτης Προστασίας Δεδομένων