

Διαδίκτυο των πραγμάτων (Internet of Things-IoT): Αποικισμός της καθημερινής ζωής¹ ή νέα τεχνολογική πρόκληση;

“Το «διαδίκτυο των πραγμάτων» είναι μια μελλοντική κατάσταση, κατά την οποία καθημερινά αντικείμενα, όπως κινητά τηλέφωνα, αυτοκίνητα, οικιακές συσκευές, ρούχα, ακόμη και τρόφιμα, θα συνδέονται ασύρματα στο διαδίκτυο μέσω έξυπνων μικροκυκλωμάτων και θα μπορούν να συλλέγουν και να ανταλλάσσουν δεδομένα πάσης φύσεως, όπως θερμοκρασία τόπου και σώματος, καρδιακούς παλμούς, ταχύτητα, κατανάλωση τροφίμων ή καυσίμων κ.ο.κ. Στο πλαίσιο της παρούσης εισήγησης θα αναλυθούν οι επιπτώσεις του διαδικτύου των πραγμάτων στην προστασία της ιδιωτικότητας και θα διερευνηθεί το νομοθετικό πλαίσιο αυτού υπό το πρίσμα του Σχεδίου Κανονισμού Προστασίας Δεδομένων, ενώ παράλληλα θα προταθούν λύσεις για την ενιαία αντιμετώπιση των ζητημάτων που θα ανακύψουν από την εφαρμογή των νέων συσκευών.”

Φερενίκη Παναγοπούλου-Κουτνατζή,

Δρ. Ν. (Humboldt), Μ.Δ.Ε.
(Παν. Αθηνών), Μ.Ρ.Η. (Harvard)²

σφέροντας αυξημένη διαχείριση ποιότητας καθόλη τη διάρκεια της αλυσίδας εφοδιασμού. Επίσης, η κλοπή θα είναι πιο παρελθόν και τα δέματα δεν θα χάνονται.

4. Κομψά, μοντέρνα ρολόγια, που εκ πρώτης όψεως δεν διαφέρουν

από τα συμβατικά, καταμετρούν μέσω έξυπνων αισθητήρων πολύ χρήσιμα δεδομένα, όπως καρδιακούς παλμούς, βήματα, ανέβασμα ή κατέβασμα σκαλοπατιών, κατανάλωση θερμίδων, διάθεση, και μπορούν να φανερώσουν εάν ο χρήστης τους κοιμάται αναλύοντας παράλληλα τη συμπεριφορά του ύπνου του, τρέχει, χαζεύει, κάνει ελαφρές δουλειές ή ακόμα εάν είναι σεξουαλικά ενεργός μία συγκεκριμένη χρονική στιγμή, εξαγοντας στατιστικά μάλιστα συμπεράσματα για όλες τις σχετικές του δραστηριότητες στη διάρκεια μίας χρονικής περιόδου, ανευρέσιμα στο Διαδίκτυο μέσω μηχανών αναζήτησης⁴.

I. Εισαγωγή

Η παρούσα εισήγηση δεν αναφέρεται σε ένα σενάριο επιστημονικής φαντασίας, αλλά στην πραγματικότητα που ξεπερνά τα όρια οποιασδήποτε φαντασίας. Προς χάρην συστηματικοποίησης παρατίθενται τα ακόλουθα παραδείγματα:

1. Ένα ηλικιωμένο άτομο ξεχνάει να λάβει ένα σημαντικό χάπι. Αμέσως στέλνεται προειδοποιητικό μήνυμα σε κοινωνικό μέλος της οικογένειας ή ακόμα και σε τοπικό κέντρο έκτακτης ανάγκης, έτσι ώστε κάποιος να μπορέσει να περάσει προκειμένου να ελέγξει την κατάσταση.

2. Ένας καθηγητής πανεπιστημίου ακυρώνει μια πρωινή διάλεξη λόγω ασθένειας. Τα ξυπνητήρια των φοιτητών και οι καφετιέρες ρυθμίζονται αυτόματα, χαρίζοντάς τους μία επιπλέον ώρα ύπνου³.

3. Οτιδήποτε καταναλώνουμε ελέγχεται μέσω της χρήσεως μικροσκοπικών ετικετών. Με τον τρόπο αυτό οι παραγωγοί μπορούν να μάθουν γρήγορα τις ανάγκες των πελατών τους. Η ιστορία οποιουδήποτε προϊόντος, από την παραγωγή έως την τοποθέτησή του στο ράφι μπορεί να αποθηκευθεί, προ-

4. Βλ. Ευρωπαϊκό Γραφείο Κύπρου, Διαδίκτυο των Πραγμάτων, Διαβούλευση για έξυπνες συνδεδεμένες συσκευές, διαθέσιμη σε: <http://www.eoc.org.cy/index.php?id=3598>, τελευταίος έλεγχος: 15.5.2014. Συναφείς προς το θέμα είναι οι άδειες 1252/2013, 1316/2014, 1328/2014 που έχει χορηγήσει η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) στους δήμους Ξυλοκάστρου – Ευρωστίνης, Σκύδρας και Ζίτσας. Στις συγκεκριμένες περιπτώσεις τα δεδομένα προσωπικού χαρακτήρα τηρούνται από τον υπεύθυνο επεξεργασίας δήμο για την εκπλήρωση του σκοπού της παροχής υπηρεσιών κοινωνικής φροντίδας, πρόνοιας και ειδικότερων υπηρεσιών υγείας στους δημότες του, με προτεραιότητα τις ευπαθείς κοινωνικές ομάδες δημοτών (όπως ηλικιωμένους και άτομα με αναπηρία). Οι μετρήσεις βασικών παραμέτρων της υγείας των ωφελουμένων δημοτών πραγματοποιούνται με χρήση ειδικών, φορητών και σταθερών, ιατρικών συσκευών και μεταδίδονται στην κεντρική βάση δεδομένων του υπεύθυνου επεξεργασίας μέσω συστημάτων τηλεμετρίας και τηλεματικής. Η συμμετοχή των ωφελουμένων δημοτών στο πρόγραμμα παροχής υπηρεσιών κοινωνικής φροντίδας, πρόνοιας και ειδικότερων υπηρεσιών υγείας επιτρέπεται κατόπιν της ειδικής έγγραφης συγκαταθέσεώς τους. Στοιχεία κοινοποιούμενα στα όργανα διοίκησης του δήμου για τον σκοπό της καλύτερης οργάνωσης της κοινωνικής δράσεως δύνανται να είναι μόνο στοιχεία ανωνυμοποιημένα ή συγκεντρωτικά στατιστικά. Οι συσκευές αυτές διαθέτουν κύκλωμα κινητής τηλεφωνίας (GSM) και δέκτη συστήματος γεωγραφικού προσδιορισμού θέσεως (GPS) με δυνατότητα αποστολής των γεωγραφικών συντεταγμένων του κατόχου της συσκευής μέσω γραπτού μηνύματος SMS και GPRS καθώς και δυνατότητα προσβάσεως μέσω του διαδικτύου. Επίσης, διαθέτουν δυνατότητα ενεργοποίησης λειτουργίας συναγερμού/ειδοποίησης (alert) που περιλαμβάνει την τρέχουσα ακριβή γεωγραφική θέση του κατόχου της συσκευής ιδίως στις περιπτώσεις που α) ο κάτοχος πατήσει το κουμπί πανικού (panic button) της συσκευής β) ανιχνευθεί από τη συσκευή πτώση του κατόχου της και γ) ο κάτοχος κινηθεί εκτός των προκαθορισμένων ορίων συγκεκριμένης γεωγραφικής περιοχής ή ζώνης γεωπεριφράξεως. Επιπλέον, οι παραπάνω συσκευές διαθέτουν δυνατότητα κλήσεως για βοήθεια μέσω των προκαθορισμένων αριθμών που μπορούν να οριστούν στη συσκευή. Η δυνατότητα γεωγραφικού εντοπισμού του ωφελουμένου δημότη πρέπει να παρέχεται μόνο σε ειδικά

1. Βλ. Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing*, New Riders, Berkley 2006, σ. 33, ο οποίος χρησιμοποιεί τον όρο αποικισμός της καθημερινής ζωής (colonization of everyday life).
2. Η μελέτη αποτελεί επεξεργασμένη μορφή της εισήγησης στο 5^ο Πανελλήνιο Συνέδριο e-Θέμις με τίτλο Δίκαιο και Καινοτομία, που έλαβε χώρα στην Αράχωβα στις 7-8 Μαρτίου 2014.
3. Βλ. Digital Agenda EU, Internet of Things Europe, *Imagine Everything was linked*, διαθέσιμο σε: <http://www.youtube.com/playlist?list=PLD4B1B7AB8011CFB7>, τελευταίος έλεγχος: 15.5.2014.

5. Γυαλιά νέας τεχνολογίας, τα λεγόμενα google glasses, καταγράφουν ό,τι βλέπει αυτός που τα φοράει, πραγματοποιούν πλοήγηση στο Διαδίκτυο, τηλεφωνικές κλήσεις, έχουν δυνατότητα κεντρικής αποθηκεύσεως των δεδομένων και αυτόματης μεταφορτώσεως σε κοινωνικά δίκτυα, διαθέτουν υπηρεσίες γεωεντοπισμού, δέχονται φωνητικές εντολές κ.ο.κ.⁵

6. Αντιστοιχώς, εισερχόμενοι σε ένα σύγχρονο μουσείο⁶ βλέπουν με ειδικά γυαλιά μία εικονική ξεναγό που παρουσιάζει τα εκθέματα, ειδικά προγράμματα για παιδιά, εικονικά εκθέματα⁷ και εμπειρίες καλλιτεχνών.

7. Ευφυή δίκτυα σε οικίες ή τον εργασιακό χώρο για την καταμέτρηση και τον έλεγχο της θερμοκρασίας με βασικό σκοπό την εξοικονόμηση ενέργειας επιτρέπουν να ανιχνευθεί με τι ασχολούνται οι παρευρισκόμενοι στον οικιακό ή εργασιακό χώρο, αναλύοντας τα χαρακτηριστικά όλων με βάση τις δραστηριότητές τους.

Συνοψίζοντας τα ανωτέρω:

8. Στις μεταφορές σύντομα θα έχουμε συστήματα αυτόματης οδήγησης και οργανώσεως των μεταφορικών μέσων για περισσότερη ασφάλεια και οικονομία. Στον τομέα της υγείας προβλέπονται μία σειρά από καινοτομίες, από τη διαδραστική τηλεπαρακολούθηση των ασθενών, μέχρι την τηλεχειρουργική και τα έξυπνα φάρμακα. Οι καταναλωτές δεν θα χάνουν πια τα έξυπνα κλειδιά του σπιτιού τους, τα καθίσματα αυτοκινήτων θα αναγνωρίζουν ποιος οδηγός κάθεται σε αυτές, οι τηλεοράσεις θα ξέρουν ποιος τους παρακολουθεί και θα προβάλλουν αντίστοιχα προγράμματα, τα ρούχα θα δηλώνουν ότι πρέπει να πλυθούν και θα βοηθούν στην ανεύρεση των αξεσουάρ τους⁸. Τέλος, σημαντική είναι η αυτοματοποίηση της διαχείρισης πόρων μέσω της συνδυασμένης και αποτελεσματικής χρήσεως εναλλακτικών μορφών ενέργειας.

Πρόκειται για μία νέα τεχνολογική πρόκληση και ευλογία, την οποία δεν καλούμαστε να ανακόψουμε, αλλά να αξιολογήσουμε και να ρυθμίσουμε. Κάλιο το ρυθμίζει παρά το δαιμονίζει⁹. Διότι εάν καταλήγουμε στο να δαιμονίζουμε

κατηγορία δημοτών, όπως ηλικιωμένοι, άτομα με αναπηρία και άτομα που διαμένουν σε μειονεκτικές – απομακρυσμένες περιοχές και πάσχουν από άνοια ή κατοικούν μόνιμοι τους.

5. Πηγή: <https://www.google.com/glass/start/what-it-does/>, τελευταίος έλεγχος: 15.5.2014.
6. Βλ. *Alexandra Fidel*, Art Gets Unmarked in the Palm of Your Hand, *New York Times*, 1.12.2010, διαθέσιμο σε: <http://www.nytimes.com/2010/12/02/arts/02iht-rartsmart.html>, τελευταίος έλεγχος: 15.5.2014.
7. Πρόκειται για ένα είδος μικτής πραγματικότητας (mixed reality). Βλ. *Joshua A.T. Fairfield*, 27 *Berkeley Technology Law Journal* 2012, σ. 55 επ. (63 επ.) *Woodrow Barfield*, Commercial Speech, Intellectual Property Rights, and Advertising Using Virtual Images Inserted in TV, Film, and the Real World, 13 *UCLA Entrepreneur Law Review* 2006, σ. 153 (158-59).
8. Βλ. *Jon M. Garon*, Mortgaging the Meme: Financing and Managing Disruptive Innovation, 10 *Northwestern Journal of Technology and Intellectual Property* 2012, σ. 441 επ. (456).
9. Πρβλ. *Φερενίκη Παναγοπούλου-Κουνταζή*, Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: Σκέψεις με αφορμή την απόφαση ΔΕΕ Michael

κάθε τι το νέο και πρωτοποριακό που εισβάλλει στη ζωή μας, θα το αφήσουμε σαν άγριο αγκάθι να καταπνίγει τα πάντα και όχι σαν όμορφο τριαντάφυλλο να ομορφαίνει τη ζωή μας. Πριν όμως από οποιαδήποτε ρύθμιση απαιτείται η αξιολόγηση των επιπτώσεων αναφορικά με την ιδιωτικότητα του ατόμου. Στο πλαίσιο της παρούσης εισήγησης θα αναλυθούν οι επιπτώσεις του Διαδικτύου των Πραγμάτων (ΔιΠ) στην προστασία της ιδιωτικότητας και θα διερευνηθεί το νομοθετικό πλαίσιο αυτού υπό το πρίσμα του Σχεδίου Κανονισμού Προστασίας Δεδομένων, ενώ παράλληλα θα προταθούν λύσεις για την ενιαία αντιμετώπιση των ζητημάτων που θα ανακύψουν από την εφαρμογή των νέων συσκευών.

II. Ορισμός και στατιστικά δεδομένα

Το Διαδίκτυο των Πραγμάτων¹⁰ συνιστά μία εδώ και πολύ καιρό πολλά υποσχόμενη προέκταση του Διαδικτύου, καθώς κοινά αντικείμενα, όπως φωτιστικά, τηλεοράσεις, ζυγαριά και πολλά άλλα, διαθέτουν δυνατότητα συνδέσεως με το Διαδίκτυο¹¹. Μολονότι οι χρήστες είναι σε θέση να έχουν πρόσβαση στα δεδομένα τους στο Διαδίκτυο συνήθως αδυνατούν να εμποδίσουν τη διαβίβαση των δεδομένων τους σε τρίτους. Ήδη ο *Mark Weiser* από το 1991 έκανε λόγο για την πανταχού παρούσα υπολογιστική χρήση (ubiquitous computing), η οποία βελτιώνει τη χρήση υπολογιστή, καθιστώντας τους υπολογιστές αφενός διαθέσιμους στο φυσικό περιβάλλον και αφετέρου άορατους στο χρήστη¹². Για την αξιοποίηση των τεράστιων οικονομικών και κοινωνικών δυ-

Schwarz κατά κρατιδίου Bochum (C-291/12), ΔΙΜΕΕ 2013, σ. 482 επ. (492).

10. Άλλες τεχνικές ονομασίες του όρου είναι ubiquitous computing (πανταχού παρούσα υπολογιστική χρήση), tangible media (απτά μέσα), wearable computing (φερόμενη υπολογιστική χρήση), augmented reality (επαυξημένη πραγματικότητα), locative media (τοπικά μέσα), near-field communications (επικοινωνία κοντινού πεδίου), body-area networking (δίκτυωση με περιοχή σώματος), proactive computing (προληπτική υπολογιστική χρήση), autonomic computing (αυτόνομη υπολογιστική χρήση), embodied virtuality (ενσωματωμένη εικονικότητα). Βλ. *M. Scott Boone*, Ubiquitous Computing, Virtual Worlds, and the Displacement of Property Right, 4 *Journal of Law & Policy for the Information Society* 2008, σ. 91 επ. (101, όπ. περαιρ. παραρ.).
11. Το Διαδίκτυο των Πραγμάτων θυμίζει το Domesday Book του Γουλιέλμου του Κατακτητή (διαθέσιμο σε: <http://www.domesdaybook.co.uk/faqs.html>, τελευταίος έλεγχος: 15.5.2014), που ξεκίνησε να γράφεται το έτος 1085 με σκοπό την καταγραφή 13.418 οικισμών της Αγγλίας. Πρόκειται για μία εξαντλητική συλλογή που περιελάμβανε εκτενή αρχεία των κατοίκων γης, ενοικιαστών, φυσικών πόρων, κτιρίων, ζώων και σχεδόν όλων των ενσωμάτων αντικειμένων. Το βιβλίο έγραφε ότι δεν υπήρχε καμία απόκρυψη της γης, κανένα βόδι, αγελάδα, κοίρος που έμεινε απέξω. Μετά το θάνατό του Γουλιέλμου το 1087 το σχέδιο εγκαταλείφθηκε. Με τη σύγχρονη τεχνολογία μπορούμε όμως να πετύχουμε αυτό που παλιότερα φαινόταν ακατόρθωτο. Δεν είναι απίθανο να παρακολουθούμε τα πάντα, μολύβια, πουλόβερ, λάμπες, αυτοκίνητα συνδεδεμένα με μικροσκοπικές κεραίες. Βλ. *Katherine Albrecht*, RFID: The Domesday Scenario, in *RFID Applications, Security, and Privacy* σε: *Simson Garfinkel & Beth Rosenberg* (επιμ.), 2006, σ. 259 επ.
12. Βλ. *Mark Weiser*, The Computer for the 21st Century, *The Computer in the 21st Century*, Science America, 9/1991, σ. 78 επ., διαθέσιμο σε: <http://web.media.mit.edu/~anjchang/ti01/weiser-sciam91-ubicom.pdf>, τελευταίος έλεγχος: 15.5.2014.

νατοπών του Διαδικτύου των Πραγμάτων απαιτούνται δίκαιοι όροι ανταγωνισμού, ώστε όλοι οι συντελεστές να μπορούν να ανταγωνιστούν ισότιμα πληρώνοντας επί ίσοις όροις τις προδιαγραφές προστασίας των καταγεγραμμένων προσωπικών δεδομένων. Για την κοινωνική του αποδοχή είναι αναγκαίο να οριστεί δεοντολογικό και νομικό πλαίσιο, που θα υποστηρίζεται από την τεχνολογία και θα παρέχει στους χρήστες έλεγχο και ασφάλεια¹³.

Μία έννοια στενά συνδεδεμένη με το ΔτΠ είναι η έννοια της διάχυτης ή της πανταχού παρούσας υπολογιστικής τάσεως προς την ενσωμάτωση αισθητήρων σε αντικείμενα καθημερινής χρήσεως, ώστε να μπορούν να επεξεργαστούν και να γνωστοποιούν τα δεδομένα. Αυτό σημαίνει ότι τα αντικείμενα διαδίδονται παντού, οι συσκευές είναι συνδεδεμένες και διαρκώς διαθέσιμες στους άλλους, σύμφωνα με ένα σύνολο προκαθορισμένων κανόνων. Τα εν λόγω αντικείμενα, που ονομάζονται και έξυπνα αντικείμενα, έχουν σχεδιαστεί για να επικοινωνούν διακριτικά την παροχή δεδομένων με έναν εύκολο και αποτελεσματικό τρόπο. Η εξέλιξη του ΔτΠ περιλαμβάνει κάθε έναν από τους κύριους τομείς της σύγχρονης οικονομίας της πληροφορίας, από βιομηχανικές, μεταφορικές και λιανικές υπηρεσίες μέχρι και υπηρεσίες υγειονομικής περιθάλψεως, ασφάλειας, καταναλώσεως και οικιακές υπηρεσίες. Αυτό συνεπάγεται ένα μεγάλο αριθμό εφαρμογών σε μια σειρά από θέσεις με τη βοήθεια κάθε σχεδόν καθημερινής χρήσεως συσκευής από τα έξυπνα τηλέφωνα, τις κάμερες, ετικέτες και τα φώτα των οχημάτων, τις χειρουργικές και εμφυτευτικές συσκευές, τους συναγερμούς, τις κονσόλες παιχνιδιών και τα πλυντήρια πιάτων. Αυτό το αυξανόμενο φαινόμενο δρομολογείται από την ανάγκη μείωσης του κόστους παραγωγής και σμικρύνσεως των συσκευών, που επιτρέπουν τη σταδιακή ένταξή τους σε άλλες συσκευές, όπως τα έξυπνα τηλέφωνα.

Σήμερα, ο μέσος άνθρωπος διαθέτει τουλάχιστον δύο αντικείμενα που συνδέονται με το Διαδίκτυο· έως το 2015, ο αριθμός αυτός αναμένεται να αυξηθεί σε επτά, με είκοσι πέντε δισεκατομμύρια συσκευές συνδεδεμένες ασύρματα παγκοσμίως. Έως το 2020, ο αριθμός αυτός μπορεί να διπλασιαστεί, φτάνοντας τα πενήντα δισεκατομμύρια. Αυτό συνεπάγεται μια πιθανή μελλοντική κατάσταση, όπου θα συνδέονται πολλά καθημερινά πράγματα¹⁴.

III. Κατηγορίες συσκευών

Οι βασικές κατηγορίες των συσκευών¹⁵ είναι α) αισθητήρες αναφορικά με δεδομένα υγείας, β) συσκευές που φορά-

ει ο χρήστης (φερόμενες συσκευές) αντικαθιστώντας υπάρχοντα αντικείμενα, όπως ρολόγια και γυαλιά και γ) συσκευές οικιακού αυτοματισμού που χρησιμοποιούνται για την αυτοματοποίηση εργασιών στο σπίτι ή για τον εξ αποστάσεως έλεγχο του οικιακού περιβάλλοντος. Οι κατηγορίες αυτές δεν είναι αποκλειστικές. Χαρακτηριστικό παράδειγμα αποτελεί ένα έξυπνο ρολόι που μπορεί παράλληλα να καταγράφει και τους καρδιακούς παλμούς.

α) **Συσκευές ηλεκτρονικής υγείας** καταμετρούν δεδομένα του σώματος και είναι δημοφιλείς σε χρήστες που επιθυμούν να ελέγχουν τα δεδομένα αναφορικά με τις συνθήκες τους και τον τρόπο ζωής τους. Για τη διεξοδική ανάλυση του ύπνου, ο παρακολουθητής ύπνου (sleep tracker) πρέπει να είναι συνδεδεμένος με το άτομο κάθε βράδυ. Αντιστοίχως μετρικές βημάτων πρέπει να είναι τοποθετημένοι στο χρήστη συνεχώς, προκειμένου να υπολογίζουν επακριβώς την κατανάλωση θερμίδων. Η ενεργοποίηση αυτών των συσκευών επιφέρει πολλά πλεονεκτήματα για το χρήστη τους. Ωστόσο, δεν πρέπει να παραγνωρίζονται οι επιπτώσεις τους στην ιδιωτική ζωή του. Με την παρατήρηση τάσεων συμπεριφοράς συνάγονται πληροφορίες σχετιζόμενες με την υγεία του χρήστη. Δεν είναι λίγες οι περιπτώσεις που οι συσκευές στέλνουν ειδοποιήσεις, όταν ο χρήστης παραμελεί τη φυσική του κατάσταση αναγνωρίζοντας κάποια συμπτώματα ασθένειας. Παράλληλα, άλλες συσκευές καταμετρούν τους καρδιακούς παλμούς και τα κύματα του εγκεφάλου. Μερικές από τις συσκευές του εμπορίου παρουσιάζουν κενά ασφαλείας, επιτρέποντας σε μη εξουσιοδοτημένους την πρόσβαση σε καταγεγραμμένα δεδομένα που αναφέρονται στον υπεύθυνο επεξεργασίας. Μία από τις βασικές δυσκολίες είναι ότι οι κατασκευαστές τείνουν να ελαχιστοποιήσουν την κατανάλωση πόρων θυσιάζοντας την ασφάλεια και την προστασία της ιδιωτικής ζωής έναντι της γενικότερης βελτιώσεως των χαρακτηριστικών των συσκευών και της αυτονομίας (δηλαδή χρήση με μπαταρία). Ως εκ τούτου, η εφαρμογή κρυπτογραφικών εργαλείων που θα μειώσει σημαντικά την αυτονομία της συσκευής δεν θεωρείται ως προτεραιότητα, ιδίως στην περίπτωση ενός βηματοδότη, όπου ο χώρος της μνήμης είναι περιορισμένος.

β) **Οι συσκευές που φοράει ο χρήστης (φερόμενες συσκευές)** αναφέρονται σε μια σειρά από υπολογιστικές συσκευές που φορούνται από το χρήστη, όπως ρολόγια ή γυαλιά. Ενώ οι χρήστες των συσκευών είναι πιθανό να γνωρίζουν τις δυνατότητες άλλων ατόμων να έχουν πρόσβαση στα εν λόγω δεδομένα τους που συλλέγονται για αυτούς (π.χ. βίντεο ή μικρόφωνο) δεν είναι σε θέση να γνωρίζουν εάν οι ηλεκτρονικές αυτές συσκευές είναι ενεργοποιημένες ή όχι. Ο ιδιαίτερος κίνδυνος για την προστασία των δεδομένων έγκειται στις δυνατότητες των αισθητήρων που ενσωματώ-

13. Βλ. Ευρωπαϊκή Επιτροπή, Ψηφιακό θεματολόγιο: Η Επιτροπή ανοίγει διαβούλευση σχετικά με τις έξυπνες, συνδεδεμένες συσκευές- το «διαδίκτυο των πραγμάτων», διαθέσιμο σε: http://europa.eu/rapid/press-release_IP-12-360_el.htm, τελευταίος έλεγχος: 15.5.2014.

14. Βλ. Ευρωπαϊκό Γραφείο Κύπρου, Διαδίκτυο των Πραγμάτων, Διαβούλευση για έξυπνες συνδεδεμένες συσκευές, διαθέσιμο σε: <http://www.eoc.org.cy/index.php?id=3598>, τελευταίος έλεγχος: 15.5.2014.

15. Βλ. ανάλυση και από Γεωργία Παναγοπούλου, Διαδίκτυο των Πραγμάτων, Ζητήματα προσωπικών δεδομένων (Internet Of Things), Παρουσίαση

για την 8η Ευρωπαϊκή Ημέρα Προστασίας Προσωπικών Δεδομένων, 28.1.2014, διαθέσιμο σε: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/EUROPEAN_DP_DAY_GENERAL/2014_DP_DAY/OMILIES_2014_DP_DAY/PANAGOPOULOU_DIADIKTIO%20TON%20PRAGMATON.PDF, τελευταίος έλεγχος: 15.5.2014.

νονται στο εσωτερικό της συσκευής. Δεδομένου ότι αυτά τα αντικείμενα δεν γίνονται αντιληπτά αναφορικά με τις δυνατότητές τους, ελλοχεύει ο κίνδυνος η επεξεργασία των δεδομένων προσωπικού χαρακτήρα να λαμβάνει χώρα χωρίς έγκυρη νομική βάση, αφού το υποκείμενο των δεδομένων μπορεί να αγνοεί την ίδια τη συσκευή. Εάν τα επεξεργασμένα δεδομένα υποβληθούν σε επεξεργασία μόνον στο πλαίσιο αποκλειστικά προσωπικών ή οικιακών δραστηριοτήτων και δεν μεταβιβάζονται σε τρίτους, μπορεί να υποπέσουν στην εξαίρεση της οικιακής-προσωπικής χρήσεως¹⁶. Ωστόσο, εάν, όπως είναι συνήθως η περίπτωση, τα δεδομένα μεταφέρονται στον κατασκευαστή της συσκευής – που μπορεί να καταστεί και υπεύθυνος επεξεργασίας των δεδομένων¹⁷ – τότε η εξαίρεση της οικιακής χρήσεως παύει να υφίσταται και ο υπεύθυνος της επεξεργασίας είναι υπεύθυνος για την ενημέρωση των υποκειμένων των δεδομένων και την εξασφάλιση έγκυρης νομικής βάσεως για την επεξεργασία των δεδομένων. Επιπλέον, δεδομένου ότι οι φερόμενες συσκευές είναι πιθανό να αντικαταστήσουν τις προηγούμενες απαραιτήτως συσκευές που παρέχουν συνήθεις λειτουργίες, θα πρέπει να προσφέρουν δυνατότητα απενεργοποίησης της συλλογής και ανακλήσεως της συγκαταθέσεως για τη συλλογή στοιχείων¹⁸.

γ) Οικιακές συσκευές: Συσκευές ΔΤΠ δεν περιορίζονται στην παρακολούθηση των ατόμων, αλλά μπορούν επίσης να τοποθετηθούν σε σπίτια και γραφεία, για να παρακολουθούν τις διάφορες περιβαλλοντικές πιυχές παρέχοντας ένα μηχανισμό ελέγχου. Κατασκευαστές έχουν προτείνει συνδεδεμένα ψυγεία, πλυντήρια ρούχων, φούρνους και θερμοστάτες που μπορούν να ελεγχθούν ή να παρακολουθούνται μέσω του Διαδικτύου. Οι περισσότερες συσκευές οικιακού αυτοματισμού είναι συνεχώς συνδεδεμένες και παρέχουν τη δυνατότητα να αναφέρουν ορισμένα στοιχεία στον κατασκευαστή ή σε τρίτους. Ενώ ορισμένες από αυτές τις συσκευές δεν συλλέγουν δεδομένα που θα μπορούσαν να θεωρηθούν ευαίσθητα, όλες αυτές θα μπορούσαν να χρησιμοποιηθούν για να παρέχουν πληροφορίες για το αν ο χρήστης τους είναι στο σπίτι χρησιμοποιώντας τη συσκευή του. Συνδεδεμένες συσκευές χρησιμοποιούνται επίσης προς ανίχνευση των κινήσεων του χρήστη, όταν αυτός είναι στο σπίτι προκαλώντας κάποιες ενέργειες (π.χ. ανάβει το φως,

αλλάζει τη θερμοκρασία δωματίου κ.ο.κ.). Οι κίνδυνοι για την ιδιωτικότητα θα πρέπει να αξιολογηθούν.

IV. Οι ενδιαφερόμενοι

Για τις συσκευές του ΔΤΠ επιδεικνύουν ενδιαφέρον κατά κύριο λόγο οι κατασκευαστές συσκευών, οι οποίοι βάσει της Γνώμης 1/2010 της Ομάδας Εργασίας του άρθρου 29 θα μπορούσαν να εκληφθούν ως υπεύθυνοι επεξεργασίας¹⁹. Ενδιαφέρον έχουν επίσης οι κοινωνικές πλατφόρμες μέσω της δυνατότητας των χρηστών να μοιραστούν πληροφορίες με άλλους χρήστες, συνήθως σε όλη την πλατφόρμα κοινωνικής δικτύωσης. Η ανταλλαγή των δεδομένων των αισθητήρων με φίλους έχει ήδη προκαλέσει ζητήματα προστασίας της ιδιωτικής ζωής. Για παράδειγμα, οι χρήστες μιας προσωπικής συσκευής παρακολούθησής αποκάλυπουν ακούσιως τη σεξουαλική δραστηριότητά τους, η οποία στη συνέχεια είναι ανευρέσιμη μέσω μηχανών αναζήτησής. Ο διαμοιρασμός αυτός της πληροφορίας μπορεί να λάβει και τη μορφή αξιολογήσεως από ασφαλιστές ή εργοδότες²⁰. Κάποιος μπορεί να καταστήσει τα δεδομένα της οδηγικής συμπεριφοράς του προσβάσιμα στον ασφαλιστή του, προκειμένου να λάβει καλή αξιολόγηση και να πληρώσει χαμηλότερα ασφάλιστρα. Αυτού του είδους η διαβίβαση δεδομένων με αντάλλαγμα οικονομικό όφελος προκαλεί έντονη ανησυχία αναφορικά με την εγκυρότητα της παρεχόμενης συγκαταθέσεως του υποκειμένου των δεδομένων και πρέπει να αξιολογηθεί. Παράλληλα, ενδιαφέρον εκδηλώνουν οι προγραμματιστές εφαρμογών, οι οποίοι είναι εξουσιοδοτημένοι να έχουν πρόσβαση στα δεδομένα μέσω των εφαρμογών. Επίσης, ενδιαφέρον εκφράζουν οι διαφημιστές να παρακολουθούν και να γνωρίζουν πού βρίσκονται οι χρήστες των συσκευών, προκειμένου να τους στέλνουν στοχευμένες διαφημίσεις σχετιζόμενες με συγκεκριμένο μέρος (location-based services)²¹. Ο κίνδυνος λήψεως ανεπιθύμητης αλληλογραφίας με τον τρόπο αυτό είναι μεγάλος²². Τέλος, έντονο ενδιαφέρον έχουν οι χορηγοί των συσκευών, όπως, για παράδειγμα, οι ασφαλιστικές εταιρείες, καθώς οι συσκευές θα μπορούσαν να τους βοηθήσουν να ανιχνεύσουν, όταν ένα άτομο σταματήσει να αθλείται και δεν είναι πλέον σε πολύ καλή φυσική κατάσταση. Εάν ακόμα και μια μικρή ομάδα χρηστών συμμεριστεί την αξία των δεδομένων που παρατηρούνται από τους αισθητήρες είναι αρκετό για να επιβάλει κοινωνική πίεση έτσι ώστε να εμποδίζονται οι χρήστες να αντιγράφουν τα δε-

16. Πρβλ. Ομάδα Εργασίας του Άρθρου 29, Γνώμη 5/2009, σκ. 3.1, σχετικά με τις επιγραμμικές υπηρεσίες κοινωνικής δικτύωσης, διαθέσιμη σε: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_el.pdf, τελευταίος έλεγχος: 15.5.2014.

17. Βλ. Ομάδα Εργασίας του Άρθρου 29, Γνώμη 1/2010, σκ. III.1.a, σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία», διαθέσιμη σε: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_el.pdf#h2-5, τελευταίος έλεγχος: 15.5.2014.

18. Πρβλ. Ομάδα Εργασίας του Άρθρου 29, Γνώμη 13/2011, σκ. 5.3, σχετικά με τις υπηρεσίες εντοπισμού γεωγραφικής θέσης που παρέχονται μέσω έξυπνων κινητών συσκευών, διαθέσιμη σε: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_el.pdf, τελευταίος έλεγχος: 15.5.2014.

19. Βλ. Ομάδα Εργασίας του Άρθρου 29, Γνώμη 1/2010 αναφορικά με τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία, διαθέσιμη σε: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_el.pdf#h2-5, τελευταίος έλεγχος: 15.5.2014.

20. Βλ. *Scott R. Peppet*, *Unraveling Privacy, The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 *Nw. U. L. Rev.* (2011), σ. 1153 επ. (1156).

21. Βλ. *Nancy J. King*, *When mobile phones are RFID-equipped - Finding E.U.- U.S. solutions to protect consumer privacy and facilitate mobile commerce*, 15 *Michigan Telecommunications and Technology Law Review*, σ. 107 επ. (116 επ.).

22. Βλ. *Nancy J. King*, *οπ. ανωτ.* (υποσ. 21), σ. 141 επ.

δομένα και να τα διαμοιράζονται με ασφαλιστικές εταιρείες και εργοδότες.

V. Κίνδυνοι

Οι κίνδυνοι από την εφαρμογή των εν λόγω συσκευών δεν είναι αμελητέοι. Ο μεγαλύτερος φόβος εστιάζεται στην κατάρριψη οποιασδήποτε έννοιας ιδιωτικότητας. Το άτομο είναι υπό αέναη, μη ελεγχόμενη, αλλά και άγνωστη επιτήρηση (αδιακρίτως τόσο από ιδιώτες όσο και από το κράτος)²³, καθώς δεν υπάρχει επαρκής ενημέρωση για καταγραφή των δεδομένων στους χρήστες των συσκευών ΔΤΠ. Για παράδειγμα, ο χρήστης ενός έξυπνου ρολογιού δεν γνωρίζει ότι καθόσον γυμνάζεται, οι επιδόσεις του και η γενικότερη συμπεριφορά του αποθηκεύεται σε κεντρική βάση και τα συλλεγόμενα δεδομένα αποθηκεύονται για μακρό χρονικό διάστημα, αν όχι για πάντα, τα οποία μπορούν να οδηγήσουν σε απαγορευμένη λήψη αυτοματοποιημένων αποφάσεων. Έτσι, με βάση τη συμπεριφορά ενός ατόμου, μπορούν να ληφθούν αυτοματοποιημένες αποφάσεις, π.χ. για το αν θα πρέπει να του χορηγηθεί δάνειο από μία τράπεζα ή ασφάλιση υγείας από ασφαλιστική εταιρεία²⁴. Από ασήμαντα ή ακόμα και από ανώνυμα δεδομένα, τα οποία διασυνδέονται μπορεί να δημιουργηθεί ένα τέλειο ψυχογράφημα του υποκειμένου των δεδομένων (δημιουργία προφίλ). Επίσης, έντονος είναι ο κίνδυνος της ταξινόμησης των πολιτών σε διάφορες κατηγορίες, όπως, σε σπάταλους, επικίνδυνους, διάγοντες ανθυγιεινό τρόπο ζωής, κ.ο.κ.

Περαιτέρω, δημιουργείται και ζήτημα περιορισμού της «διανοητικής ιδιωτικότητας» (intellectual privacy)²⁵, υπό την έννοια ότι, όταν το άτομο παρακολουθείται εσαεί, εμποδίζεται στο να αναπτύξει ελεύθερα τις ιδέες και σκέψεις του. Η προστασία της «διανοητικής ιδιωτικότητας» στηρίζεται στην ιδέα ότι οι ελεύθερες και αβίαστες σκέψεις συνιστούν το θεμέλιο μίας ελεύθερης κοινωνίας και η επιτήρηση των δραστηριοτήτων, αλλά και των παραγωγικών τρόπων λήψης αποφάσεων επηρεάζει τις δραστηριότητες αυτές αρνητικά²⁶. Η πνευματική αυτή χειραγώγηση μπορεί να οδηγήσει με τη σειρά της σε επιθυμία κυριαρχίας μέσω της έμμεσης επιρροής στη λήψη αποφάσεων και της δυνατότητας να πείσει τους χρήστες σε συγκεκριμένες ενέργειες²⁷ (π.χ. αγορά

συγκεκριμένων προϊόντων, επιλογή συγκεκριμένων πολιτικών κ.ο.κ.).

Καθόσον ο χρήστης δεν είναι κατ' αρχήν σε θέση να γνωρίζει την επεξεργασία δεδομένων που διενεργείται, δεν γνωρίζει ποιοι λαμβάνουν τα δεδομένα του²⁸ και δεν μπορεί να δώσει και τη συγκατάθεσή του για την επεξεργασία των εν λόγω δεδομένων. Το ΔΤΠ εγείρει ανησυχίες σχετικά με ένα μεγάλο όγκο προσωπικών δεδομένων που συλλέγονται νόμιμα για έναν σκοπό και τυχάνουν περαιτέρω επεξεργασίας από τρίτους, προκειμένου να επαναχρησιμοποιηθούν για το δημόσιο συμφέρον ή εμπορικούς σκοπούς κατά τρόπο ασυμβίβαστο με τον αρχικό σκοπό για τον οποίο συλλέχθηκαν²⁹. Ανησυχίες προκαλούνται για τη χρήση των δεδομένων αυτών από ασφαλιστικές εταιρείες, εργοδότες, ακόμα και αστυνομικές αρχές, π.χ. για την έκδοση εντάλματος συλλήψεως. Πρόκειται για μία αέναη παρακολούθηση του χρήστη, η οποία σε διαφορετική περίπτωση επιτρέπεται μόνο υπό συγκεκριμένες προϋποθέσεις σε περιπτώσεις υπόπτων³⁰.

Περαιτέρω, δεν πρέπει να παραγνωρίζεται ο φόβος της αποκαλύψεως προτύπων συμπεριφοράς³¹ μέσω συσκευών ΔΤΠ στο βαθμό που οι αισθητήρες είναι σε θέση να επιτηρούν τους χρήστες και το περιβάλλον τους προσφέροντάς τους κάποιες υπηρεσίες και να προσαρμόζουν το περιβάλλον τους σε εντολές και σε συγκεκριμένες ανάγκες χρήστη ερμηνεύοντας το γενικότερο πλαίσιο συμπεριφοράς επί τη βάσει παλαιότερων πληροφοριών. Με τον τρόπο αυτό, εύλογα μπορεί να θεωρηθεί κανείς ότι η αέναη παρακολούθηση θα οδηγήσει σε εσωτερική πίεση αποφυγής μη συννηθισμένων συμπεριφορών προσαρμόζοντας τη ζωή τους στα αποδεκτά πρότυπα, καταπιέζοντας την ελεύθερη ανάπτυξη της προσωπικότητάς τους, όπως αυτή κατοχυρώνεται στο άρθρο 5 παρ. 1 Σ. Τέτοια παραβίαση της προσωπικότητας είναι η χρήση RFID σε μαθητικές ταυτότητες με σκοπό την παρακολούθηση των κινήσεών τους εντός του σχολείου³². Αντίστοιχο προβληματισμό προκαλεί η εγκατάσταση ανιχνευτών στις τηλεοράσεις που καταγράφουν την παρακολούθηση των χρη-

23. Βλ. *Neil M. Richards*, Symposium: Privacy and Technology: The Dangers of Surveillance, 126 *Harvard Law Review* 2013, σ. 1934 επ. (1935).

24. Σύμφωνα με το άρθρο 15 παρ. 1 της Οδηγίας 95/46/ΕΚ, τα κράτη μέλη παρέχουν σε κάθε πρόσωπο το δικαίωμα να μη συμμορφωθεί με απόφαση που παράγει νομικά αποτελέσματα έναντι αυτού ή το θίγει σημαντικά εφόσον η εν λόγω απόφαση βασίζεται αποκλειστικώς σε αυτοματοποιημένη επεξεργασία που αξιολογεί ορισμένες πιυχές της προσωπικότητάς του, όπως η απόδοσή του στην εργασία, η φερεγγυότητά, η αξιοπιστία, η διαγωγή του κ.λπ.

25. Βλ. *Neil M. Richards*, Intellectual Privacy, 87 *Texas Law Review* 2008, σ. 387 επ. (389).

26. Βλ. *Neil M. Richards*, όπ. ανωτ. (υποσ. 25), σ. 403-404.

27. Βλ. *Neil M. Richards*, όπ. ανωτ. (υποσ. 23), σ. 1955.

28. Παράδειγμα αποτελεί η περίπτωση των εταιρειών τιμολογήσεως της ασφαλίσεως των υπαλλήλων που στηρίζεται στα δεδομένα που αναγράφονται σε διάφορες συσκευές. Βλ. *With tracking devices, employers may track workers' health*, 4.1.2013, διαθέσιμο σε: <http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health>, τελευταίος έλεγχος: 15.5.2014.

29. Βλ. Ομάδα Εργασίας Άρθρου 29, Γνώμη 3/2013, αναφορικά με την αλλαγή του σκοπού επεξεργασίας, διαθέσιμο σε: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, τελευταίος έλεγχος: 15.5.2014.

30. Βλ. *Susan W. Brenner*, The Fourth Amendment in an Era of Ubiquitous Technology, 75 *Miss. Law Journal* 2005, σ. 62-63.

31. Βλ. *Lilian Mitrou*, The Impact of Communications Data Retention on Fundamental Rights and Democracy - The Case of the EU Data Retention Directive, σε: *Kevin D. Haggerty & Minas Samatas* (επιμ.), *Glasshouse Book-Routledge-Cavendish*, New York 2010, Surveillance and Democracy, σ. 127 επ. (138).

32. Αυτό συμβαίνει π.χ. σε γυμνάσιο του Τέξας. Βλ. *Jon M. Garon*, όπ. ανωτ. (υποσ. 8), σ. 456, όπ. περαιτ. παραπ.

στών τους και στέλνουν στοχευμένες διαφημίσεις διαφορετικές ανά χρήστη³³.

Οι αυξανόμενες απαιτήσεις ανταγωνισμού εύλογα μπορούν να οδηγήσουν στην υποχώρηση της ασφάλειας έναντι της αποδόσεως. Δεδομένου ότι υπάρχει ανάγκη να βελτιστοποιηθεί η χρήση των υπολογιστικών πόρων από αντικείμενα και αισθητήρες, δεν είναι σαφές με ποιο τρόπο οι εγγυήσεις για τη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας πρόκειται να εφαρμοστούν σωστά σε όλα τα επίπεδα. Κατά τον ίδιο τρόπο, η παρουσία των διαφορετικών επιπέδων επεξεργασίας δεν διασφαλίζει τον επαρκή συντονισμό μεταξύ όλων των ενδιαφερόμενων φορέων με αποτέλεσμα την παρουσία των αδύνατων σημείων που μπορούν να χρησιμοποιηθούν για την εκμετάλλευση των τρωτών σημείων. Για παράδειγμα, οι περισσότεροι από τους αισθητήρες δεν είναι σε θέση να δημιουργήσουν κρυπτογραφημένη σύνδεση, δεδομένου ότι θα οδηγήσει σε υπερβολική καταπόνηση σε λογικούς πόρους που έχουν αντίκτυπο στη φυσική αυτονομία της συσκευής.

Πέρα από τους κινδύνους στην ιδιωτική σφαίρα δεν πρέπει να παραγνωρίζονται και οι αναδυόμενοι περιορισμοί σε δικαιώματα ιδιοκτησίας. Μία μελλοντική κατάσταση θα μπορούσε π.χ. να είναι η απενεργοποίηση συσκευών, όταν δεν έχουν πληρωθεί οι απαιτούμενοι φόροι. Ένα αυτοκίνητο θα μπορούσε να αδρανοποιείται σε περίπτωση μη πληρωμής των σχετικών τελών κυκλοφορίας³⁴. Παράλληλα, δημιουργούνται πολλές επιπλοκές σε ζητήματα ευθύνης του παραγωγού για το προϊόν, αλλά και πνευματικής ιδιοκτησίας, δεδομένης της αλληλεπιδράσεως πολυάριθμων συσκευών³⁵.

Στους εν λόγω αναφερόμενους κινδύνους πρέπει να υπογραμμισθεί ο παράγοντας της απροθυμίας παραιτήσεως από τα νέα τεχνολογικά δεδομένα και υπαναχωρήσεως σε συμβατικές συσκευές. Είναι γεγονός ότι κανείς εκ των πραγμάτων δεν θα θέλει να αντικαταστήσει το ξύπινο κινητό του με μία συμβατική τηλεφωνική συσκευή.

VI. Νομοθετικό και γνωμοδοτικό πλαίσιο

α. Οδηγία 95/46/ΕΚ

Το ΔΤΠ εμπίπτει στο πεδίο εφαρμογής της Οδηγίας 95/46/ΕΚ, όταν τα δεδομένα αναφέρονται σε φυσικό πρόσωπο, καθώς θα μπορούσε να χαρακτηριστεί είτε ως επεξεργασία δεδομένων προσωπικού χαρακτήρα, κατά το άρθρο 2 στοιχ. β', είτε ως αρχείο δεδομένων προσωπικού χαρακτήρα, κατά

το άρθρο 2 στοιχ. γ. Το άρθρο 6 προβλέπει ότι τα δεδομένα που επεξεργάζονται πρέπει να είναι να είναι κατάλληλα, συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται και υφίστανται επεξεργασία. Ως εκ τούτου, μία συσκευή ΔΤΠ δεν μπορεί να συλλέγει αμέτρπητα δεδομένα δίχως λόγο. Σύμφωνα με το άρθρο 7, επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να γίνεται κατ'αρχήν μόνον εάν το πρόσωπο, στο οποίο αναφέρονται τα δεδομένα, έχει δώσει τη ρητή συγκατάθεσή του. Ιδιαίτερης βαρύτητας είναι η συλλογή ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 8 (φυλετική ή εθνική καταγωγή, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστικές οργανώσεις, υγεία και σεξουαλική ζωή). Η Οδηγία προσφέρει πλούσιο νομικό πλαίσιο για τα δικαιώματα του χρήστη, όπως π.χ. δικαίωμα ενημερώσεως (άρθρα 10, 11), προσβάσεως (άρθρο 12), αντιτάξεως (άρθρο 14). Παράλληλα, στο άρθρο 15 παρ. 1 προβλέπεται ότι τα κράτη μέλη παρέχουν σε κάθε πρόσωπο το δικαίωμα να μη συμμορφωθεί με απόφαση που παράγει νομικά αποτελέσματα έναντι αυτού ή το θίγει σημαντικά εφόσον η εν λόγω απόφαση βασίζεται αποκλειστικώς σε αυτοματοποιημένη επεξεργασία που αξιολογεί ορισμένες πτυχές της προσωπικότητάς του, όπως η απόδοσή του στην εργασία, η φερεγγυότητα, η αξιοπιστία, η διαγωγή του κ.λπ. Η διάταξη αυτή αφορά στις συσκευές ΔΤΠ, καθώς μέσω αυτών μπορούν να ληφθούν αυτοματοποιημένες αποφάσεις δυνάμει να θίξουν το άτομο (π.χ. απόρριψη ασφαλίσεώς του βάσει της εκτενούς παρακολουθήσεως της οδηγικής του συμπεριφοράς, της καταστάσεως της υγείας του, της ανεπαρκούς αθλήσεώς του κ.ο.κ.). Ιδιαίτερη βαρύτητα δίδεται στη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων εκ μέρους του υπευθύνου επεξεργασίας για την προστασία από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση, ιδίως εάν η επεξεργασία συμπεριλαμβάνει και διαβίβαση των δεδομένων μέσω δικτύου, και από κάθε άλλη μορφή αθέμιτης επεξεργασίας δεδομένων προσωπικού χαρακτήρα (άρθρο 17).

Αναφορικά με το εφαρμοστέο δίκαιο, σύμφωνα με το άρθρο 4 παρ. 1 στοιχ. α' της Οδηγίας, κάθε κράτος μέλος εφαρμόζει τις εθνικές διατάξεις που θεσπίζει δυνάμει της Οδηγίας σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον η επεξεργασία εκτελείται στο πλαίσιο των δραστηριοτήτων υπευθύνου εγκατεστημένου στο έδαφος του κράτους μέλους. Όταν ο ίδιος υπεύθυνος είναι εγκατεστημένος στο έδαφος περισσότερων του ενός κρατών μελών, πρέπει να λαμβάνει τα αναγκαία μέτρα, ώστε να εξασφαλίζεται ότι κάθε εγκατάστασή του πληροί τις απαιτήσεις που προβλέπει η εφαρμοστέα εθνική νομοθεσία. Το εθνικό δίκαιο εφαρμόζεται επίσης, σύμφωνα με το άρθρο 4 παρ. 1 στοιχ. γ', όταν ο υπεύθυνος επεξεργασίας δεν είναι εγκατεστημένος στο έδαφος της Κοινότητας και για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσφεύγει σε μέσα, αυτοματοποιημένα ή όχι, ευρισκόμενα στο έδαφος του

33. Βλ. *Chris Marlowe*, *TV Keeps an Eye on Viewers*, DIGITAL MEDIA WIRE, 22.8.2011, διαθέσιμο σε: <http://www.dmwmedia.com/news/2011/08/22/tv-keeps-an-eye-on-viewers>, τελευταίος έλεγχος: 15.5.2014.

34. Βλ. *M. Scott Boone*, όπ. ανωτ. (υποσ. 10), σ. 128.

35. Βλ. *Brian E. Cabrera*, *8 Journal of Law & Policy for the Information Society* 2012, σ. 81 επ. (86).

εν λόγω κράτους μέλους, εκτός εάν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση από το έδαφος της Ευρωπαϊκής Κοινότητας. Πολύ διαφωτιστική επί του ζητήματος είναι η απόφαση του ΔΕΕ Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos, Mario Costeja González, βάσει της οποίας εφόσον η επεξεργασία πραγματοποιείται για τις ανάγκες υπηρεσίας μηχανής αναζήτησης, την οποία εκμεταλλεύεται επιχείρηση που έχει μien έδρα σε τρίτο κράτος, αλλά διαθέτει εγκατάσταση εντός ορισμένου κράτους μέλους, εκτελείται στο πλαίσιο των δραστηριοτήτων της εν λόγω εγκαταστάσεως κατά την έννοια της Οδηγίας, εφόσον η εγκατάσταση αυτή έχει ως σκοπό την προώθηση και πώληση, εντός του κράτους μέλους, του διαφημιστικού χώρου που διατίθεται στο πλαίσιο της μηχανής αναζήτησης και που αποσκοπεί στην οικονομική εκμετάλλευση της υπηρεσίας που παρέχεται με τη μηχανή αυτή³⁶.

β. Οδηγία 2002/58/ΕΚ

Σύμφωνα με το άρθρο 5 παρ. 3 της Οδηγίας 2002/58/ΕΚ, τα κράτη μέλη μεριμνούν, ώστε η αποθήκευση πληροφοριών ή η απόκτηση προσβάσεως σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνον εάν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεσή του με βάση σαφείς και εκτενείς πληροφορίες, σύμφωνα με την Οδηγία 95/46/ΕΚ, μεταξύ άλλων για το σκοπό της επεξεργασίας. Τούτο δεν εμποδίζει οιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι απολύτως αναγκαία για να μπορεί ο πάροχος υπηρεσίας της κοινωνίας της πληροφορίας την οποία έχει ζητήσει ρητά ο συνδρομητής ή ο χρήστης να παρέχει τη συγκεκριμένη υπηρεσία. Το ζήτημα που ανακύπτει με τις συσκευές ΔιΤΠ είναι ότι ο χρήστης των συσκευών που συγκατατέθηκε στην επεξεργασία των δεδομένων του δεν είναι ο μόνος του οποίου τα δεδομένα επεξεργάζονται. Για παράδειγμα, μέσω των google glasses είναι δυνατή η βιντεοσκόπηση άλλων χρηστών χωρίς την προηγούμενη συγκατάθεσή τους. Η λήψη συγκαταθέσεως σε αυτές τις περιπτώσεις καθίσταται προβληματική.

γ. Σχέδιο Γενικού Κανονισμού Προστασίας Δεδομένων

Το Σχέδιο Κανονισμού (Γενικός Κανονισμός Προστασίας Δεδομένων)³⁷ προσφέρει πλούσια νομική βάση για ζητή-

ματα που ανακύπτουν από εφαρμογές του ΔιΤΠ. Σχετικό επί του θέματος είναι το άρθρο 7 του ΣχεδΚαν αναφορικά με τις προϋποθέσεις συγκαταθέσεως, το οποίο ορίζει, μεταξύ άλλων, στην παράγραφο 1 ότι ο υπεύθυνος επεξεργασίας φέρει το βάρος της αποδείξεως όσον αφορά την παροχή της συγκαταθέσεως του προσώπου, στο οποίο αναφέρονται τα δεδομένα στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν για συγκεκριμένους σκοπούς. Ως εκ τούτου, ο χρήστης εφαρμογών ΔιΤΠ δεν μπορεί να θεωρείται ότι συγκατατίθεται σε επεξεργασία δεδομένων του, όταν δεν είναι επαρκώς ενημερωμένος επί του θέματος. Το άρθρο 12 του ΣχεδΚαν προβλέπει διαδικασίες και μηχανισμούς για την άσκηση των δικαιωμάτων του προσώπου, στο οποίο αναφέρονται τα δεδομένα. Μεταξύ άλλων, αναφέρεται στο τελευταίο εδάφιο της παραγράφου 1 ότι εάν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία με αυτοματοποιημένα μέσα, ο υπεύθυνος επεξεργασίας προβλέπει μέσα για την υποβολή των αιτημάτων με ηλεκτρονικό τρόπο. Θεμελιώδους σημασίας είναι το δικαίωμα στη λήθη, που προβλέπεται στο άρθρο 17 του ΣχεδΚαν. Είναι γεγονός ότι η συλλογή και επεξεργασία πολυποίκιλων δεδομένων δύναται να συνθέσει ένα αριστοτεχνικό ψυχογράφημα του υποκειμένου των δεδομένων και, ως εκ τούτου, το υποκείμενο των δεδομένων δέον είναι να έχει το δικαίωμα διαγραφής των στοιχείων του, καθώς αυτά δεν θα μπορούσε να θεωρηθεί ότι συντρέχουν στη διατήρηση της ιστορικής μνήμης ή την ελευθερία της πληροφόρησης. Καθοριστική επί του θέματος είναι η απόφαση του ΔΕΕ Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos, Mario Costeja González, βάσει της οποίας ο φορέας εκμετάλλευσής μηχανής αναζήτησης στο Διαδίκτυο είναι υπεύθυνος για την εκ μέρους του επεξεργασία δεδομένων προσωπικού χαρακτήρα τα οποία περιλαμβάνονται σε ιστοσελίδες δημοσιευμένες από τρίτους³⁸.

38. Βλ. ΔΕΕ, Απόφαση Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos, Mario Costeja González, 14.5.2014 στην υπόθεση C-131/12. Σύμφωνα με την εν λόγω απόφαση, όταν, κατόπιν αναζήτησεως που έχει πραγματοποιηθεί με βάση το ονοματεπώνυμο ενός προσώπου, εμφανίζεται στον κατάλογο αποτελεσμάτων σύνδεσμος προς ιστοσελίδα που περιέχει πληροφορίες για το εν λόγω πρόσωπο, αυτό μπορεί να αποταθεί απευθείας στον φορέα εκμεταλλεύσεως της μηχανής αναζήτησεως ή, εφόσον ο τελευταίος δεν ανταποκριθεί στην αίτηση του προαναφερθέντος προσώπου, στις αρμόδιες αρχές προκειμένου να επιτύχει, υπό ορισμένες προϋποθέσεις, τη διαγραφή του επίμαχου συνδέσμου από τον κατάλογο αποτελεσμάτων. Τα πραγματικά περιστατικά της υποθέσεως έχουν ως εξής: Το 2010, ο M. Costeja González υπέβαλε στην ισπανική αρχή προστασίας δεδομένων καταγγελία κατά της La Vanguardia (εταιρία που εκδίδει καθημερινή εφημερίδα μεγάλης κυκλοφορίας στην Ισπανία) καθώς και κατά της Google Spain και της Google Inc. Ο M. Costeja González υποστήριξε ότι όταν το ονοματεπώνυμο του εισαγόταν από χρήστη του Διαδικτύου στη μηχανή αναζήτησεως της Google (Google Search), εμφανίζονταν σύνδεσμοι προς δύο σελίδες της εφημερίδας La Vanguardia δημοσιευμένες τον Ιανουάριο και τον Μάρτιο του 1998. Στις σελίδες αυτές περιλαμβάνονταν ανακοίνωση για πλειστηριασμούς ακινήτων κατόπιν κατασκέσεως που είχε επιβληθεί στον προσφεύγοντα λόγω κοινωνικοασφαλιστικών οφειλών. Με την καταγγελία αυτή, ο M. Costeja González ζήτησε, αφενός, να υποχρεωθεί η εφημερίδα να αποσύρει ή να τροποποιήσει τις επίμαχες σελίδες (ώστε να μην εμφανίζονται πλέον τα προσωπικά δεδομένα του)

Σημαντικό είναι το κατοχυρωμένο στο άρθρο 18 του ΣχεδΚαν δικαίωμα στη φορητότητα των δεδομένων. Έτσι, το πρόσωπο, στο οποίο αναφέρονται τα δεδομένα, δικαιούται, εάν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία με ηλεκτρονικά μέσα και με δομημένο και συνήθως χρησιμοποιούμενο μορφότυπο, να εξασφαλίσει από τον υπεύθυνο επεξεργασίας αντίγραφο των δεδομένων που υποβάλλονται σε επεξεργασία, σε ηλεκτρονικό και δομημένο μορφότυπο συνήθους χρήσεως, ο οποίος επιτρέπει την περαιτέρω χρήση από το πρόσωπο στο οποίο αναφέρονται τα δεδομένα. Περαιτέρω, σύμφωνα με το άρθρο 20 του ΣχεδΚαν, αναφορικά με τα μέτρα βασισμένα σε κατάρτιση προφίλ, κάθε φυσικό πρόσωπο δικαιούται να μην υπάγεται σε μέτρο, το οποίο παράγει έννομες συνέπειες για το συγκεκριμένο φυσικό πρόσωπο ή που το επηρεάζει σημαντικά, και το οποίο μέτρο βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία με σκοπό την αξιολόγη-

ή να χρησιμοποιήσει ορισμένα εργαλεία που προσφέρουν οι μηχανές αναζήτησης, προκειμένου να προστατευθούν τα δεδομένα αυτά. Αφετέρου, ο M. Costeja González ζήτησε να υποχρεωθεί η Google Spain ή η Google Inc. να διαγράψει ή να αποκρύψει τα προσωπικά δεδομένα, του ώστε να μην εμφανίζονται πλέον στα αποτελέσματα αναζήτησης και σε συνδέσμους της εφημερίδας. Στο πλαίσιο αυτό, ο M. Costeja González επισήμανε ότι η διαδικασία κατασχέσεως που είχε κινηθεί εναντίον του είχε ολοκληρωθεί και διευθετηθεί από μακρού και ότι οποιαδήποτε μεία της διαδικασίας αυτής ήταν πλέον άνευ ουσίας. Η ισπανική αρχή απέρριψε την καταγγελία κατά της εφημερίδας, εκτιμώντας ότι η δημοσίευση των επίμαχων πληροφοριών από τον εκδότη ήταν νόμιμη. Αντιθέτως, η καταγγελία έγινε δεκτή κατά το μέρος που αφορούσε την Google Spain και την Google Inc. Η ισπανική αρχή ζήτησε από τις δύο εταιρίες να λάβουν τα αναγκαία μέτρα για να διαγραφούν από το ευρετήριο τους τα επίμαχα δεδομένα και για να καταστεί ανέφικτη η μελλοντική πρόσβαση σε αυτά. Η Google Spain και η Google Inc. προσέβαλαν την απόφαση της ισπανικής αρχής ενώπιον του Audiencia Nacional (ανωτέρου ισπανικού δικαστηρίου), ζητώντας την ακύρωσή της. Στο πλαίσιο αυτό, το εν λόγω ισπανικό δικαστήριο υπέβαλε σειρά προδικαστικών ερωτημάτων στο ΔΕΕ. Σύμφωνα με το Δικαστήριο, ακόμη και η αρχικά νόμιμη επεξεργασία μη ανακρίβων δεδομένων μπορεί, με την πάροδο του χρόνου, να καταστεί αντίθετη με την οδηγία 95/46/ΕΚ, όταν, λαμβανομένου υπόψη του συνόλου των περιστάσεων που χαρακτηρίζουν τη συγκεκριμένη περίπτωση, τα δεδομένα αυτά είναι ακατάλληλα, δεν είναι ή έχουν πάψει να είναι συναφή με το οικείο ζήτημα ή είναι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους υπέστησαν επεξεργασία ή σε σχέση με τον χρόνο που έχει παρέλθει. Στο πλαίσιο της εκτιμήσεως αιτήσεως που έχει υποβάλει το υποκείμενο των δεδομένων κατά της επεξεργασίας, στην οποία έχει προβεί ο φορέας εκμεταλλεύσεως της μηχανής αναζήτησεως, πρέπει, μεταξύ άλλων, να εξετάζεται αν το υποκείμενο των δεδομένων έχει δικαίωμα να πάψει η σχετική με το πρόσωπό του πληροφορία να συνδέεται, επί του παρόντος, με το ονοματεπώνυμο του μέσω του καταλόγου αποτελεσμάτων, ο οποίος προκύπτει κατόπιν αναζήτησεως που έχει διενεργηθεί με βάση το ονοματεπώνυμο αυτό. Εφόσον συμβαίνει κάτι τέτοιο, οι σύνδεσμοι προς τις ιστοσελίδες που περιέχουν τις πληροφορίες αυτές πρέπει να απαλείφονται από τον κατάλογο αποτελεσμάτων, εκτός αν υπάρχουν ειδικοί λόγοι, όπως ο ρόλος που διαδραματίζει το υποκείμενο των δεδομένων στον δημόσιο βίο, που να δικαιολογούν υπέρτερο συμφέρον του κοινού για πρόσβαση, στο πλαίσιο αντίστοιχης αναζήτησεως στις επίμαχες πληροφορίες. Σύμφωνα με το Δικαστήριο, το υποκείμενο των δεδομένων μπορεί να απευθύνει σχετικές αιτήσεις στον φορέα εκμεταλλεύσεως της μηχανής αναζήτησεως, ο οποίος οφείλει να εξετάζει δεόντως τη βασιμότητά τους. Όταν ο υπεύθυνος της επεξεργασίας δεν ανταποκρίνεται στις αιτήσεις αυτές, το υποκείμενο των δεδομένων μπορεί να αποταθεί στην αρχή ελέγχου ή στις δικαστικές αρχές, προκειμένου αυτές να προβούν στους απαραίτητους ελέγχους και να επιβάλουν στον υπεύθυνο τη λήψη συγκεκριμένων μέτρων.

ση ορισμένων προσωπικών πτυχών που σχετίζονται με το εν λόγω φυσικό πρόσωπο ή την ανάλυση ή την πρόβλεψη ειδικότερα των επιδόσεων στην εργασία, της οικονομικής καταστάσεως, της θέσεως, της υγείας, των προσωπικών προτιμήσεων, της αξιοπιστίας ή της συμπεριφοράς του. Υψηλός είναι ο πίκυς των απαιτούμενων μέτρων ασφαλείας εκ μέρους του υπευθύνου και εκτελούντος την επεξεργασία στο άρθρο 30 ΣχεδΚαν. Συγκεκριμένα, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα, ώστε να διασφαλίσουν επίπεδο προστασίας κατάλληλο προς τους κινδύνους που αντιπροσωπεύει η επεξεργασία και η φύση των δεδομένων προσωπικού χαρακτήρα που πρέπει να προστατευθούν, λαμβάνοντας υπόψη την κατάσταση της τεχνολογίας και το κόστος της εφαρμογής τους. Καθοριστικής σημασίας είναι η ανάγκη προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, που καθιερώνεται στο άρθρο 23 του ΣχεδΚαν. Εδώ είναι και το στοιχείο του ΔΤΠ εάν θα καταφέρει να προσφέρει ανταγωνιστικές μεν, αλλά ασφαλείς για την ιδιωτικότητα συσκευές. Όχι ελάσσονος σημασίας είναι η υποχρέωση τεκμηρίωσης που καθιερώνεται στο άρθρο 28 του ΣχεδΚαν, βάσει της οποίας, κάθε υπεύθυνος επεξεργασίας και κάθε εκτελών την επεξεργασία και, εφόσον συντρέχει περίπτωση, ο εκπρόσωπος του υπευθύνου επεξεργασίας διατηρεί τεκμηρίωση όλων των πράξεων επεξεργασίας για τις οποίες είναι υπεύθυνος. Περαιτέρω, το άρθρο 31 του ΣχεδΚαν προβλέπει την κοινοποίηση παραβιάσεως δεδομένων προσωπικού χαρακτήρα στην αρχή ελέγχου. Συγκεκριμένα, σε περίπτωση παραβιάσεως δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας κοινοποιεί στην αρχή ελέγχου την παραβίαση δεδομένων προσωπικού χαρακτήρα αμελλητί και, ει δυνατόν, το αργότερο εντός 24 ωρών από τη στιγμή που την πληροφορείται. Η κοινοποίηση στην αρχή ελέγχου συνοδεύεται από αιτιολογία στις περιπτώσεις στις οποίες δεν πραγματοποιείται εντός 24 ωρών. Στην ίδια κατεύθυνση κινείται η υποχρέωση γνωστοποίησης παραβιάσεως δεδομένων προσωπικού χαρακτήρα στο πρόσωπο, στο οποίο αναφέρονται τα δεδομένα του άρθρου 32 του ΣχεδΚαν. Έτσι, όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα είναι πιθανόν να επηρεάσει δυσμενώς την προστασία των δεδομένων προσωπικού χαρακτήρα ή την ιδιωτική ζωή του προσώπου, στο οποίο αναφέρονται τα δεδομένα, ο υπεύθυνος επεξεργασίας οφείλει, μετά την κοινοποίηση που αναφέρεται στο άρθρο 31, να γνωστοποιεί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο πρόσωπο, στο οποίο αναφέρονται τα δεδομένα αμελλητί. Στην ίδια κατεύθυνση κινείται η, κατά το άρθρο 34 του ΣχεδΚαν, απαίτηση προηγούμενης εγκρίσεως και προηγούμενης διαβουλεύσεως. Συγκεκριμένα, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, ανάλογα με την περίπτωση, εξασφαλίζουν έγκριση από την αρχή ελέγχου πριν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα προκειμένου να διασφαλίζεται η συμμόρφωση της σχεδιαζόμενης επεξεργασίας προς τον παρόντα κανονισμό και,

ιδίως, να μετριάζονται οι σχετικοί κίνδυνοι για τα πρόσωπα στα οποία αναφέρονται τα δεδομένα. Σημαντική καινοτομία του ΣχεδΚαν είναι ο ορισμός του υπευθύνου προστασίας δεδομένων στα άρθρα 35, 36 και 37 αυτού. Δεδομένης της φύσεως, της εκτάσεως ή/και των σκοπών των επεξεργασιών που λαμβάνουν χώρα στο ΔτΠ, είναι γεγονός ότι απαιτείται ορισμός υπευθύνου προστασίας δεδομένων, βάσει του άρθρου 35 παρ. 1 στοιχ. γ' του ΣχεδΚαν, ο οποίος συμμετέχει δρόντως και εγκαίρως σε όλα τα ζητήματα, τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα (άρθρο 36 ΣχεδΚαν), αναλογιζομένων των προβλεπομένων στο άρθρο 37 ΣχεδΚαν³⁹ υποχρεώσεων του υπευθύνου προστασίας δεδομένων. Τέλος, από τις γενικές διατάξεις του Σχεδίου Κανονισμού ιδιαίτερης σημασίας για το ΔτΠ είναι η καινοτομία του άρθρου 3 παρ. 2, αναφορικά με το γεωγραφικό πεδίο εφαρμογής, καθώς ο Κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα προσώπων που διαμένουν στην Ένωση από υπεύθυνο επεξεργασίας μη εγκαταστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με α) την προσφορά αγαθών ή υπηρεσιών στα εν λόγω πρόσωπα στα οποία αναφέρονται τα δεδομένα στην Ένωση ή β) την παρακολούθηση της συμπεριφοράς τους.

δ) Γνωμοδοτικό πλαίσιο

Χρήσιμες για την ανάλυση του ΔτΠ είναι ποικίλες Γνώμες της Ομάδας Εργασίας του άρθρου 29. Συγκεκριμένα, πολύ χρήσιμες είναι οι εξής Γνώμες:

39. Σύμφωνα με το άρθρο 37 παρ. 1 του ΣχεδΚαν, «Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία αναθέτουν στον υπεύθυνο προστασίας δεδομένων τουλάχιστον τα ακόλουθα καθήκοντα: α) να ενημερώνει και να πληροφορεί τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία για τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό και να τεκμηριώνει την εν λόγω δραστηριότητα και τις απαντήσεις που λαμβάνει, β) να παρακολουθεί τη θέση σε ισχύ και την εφαρμογή των πολιτικών του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας και των σχετικών ελέγχων, γ) να παρακολουθεί τη θέση σε ισχύ και την εφαρμογή του παρόντος κανονισμού, ιδίως όσον αφορά τις απαιτήσεις που σχετίζονται με την προστασία των δεδομένων ήδη από τον σχεδιασμό, την προστασία των δεδομένων εξ ορισμού, την ασφάλεια των δεδομένων και την ενημέρωση των προσώπων στα οποία αναφέρονται τα δεδομένα και τα αιτήματά τους κατά την άσκηση των δικαιωμάτων τους που απορρέουν από τον παρόντα κανονισμό, δ) να διασφαλίζει ότι τηρείται η τεκμηρίωση που προβλέπεται στο άρθρο 28, ε) να παρακολουθεί την τεκμηρίωση και τις κοινοποιήσεις των παραβιάσεων των δεδομένων προσωπικού χαρακτήρα δυνάμει των άρθρων 31 και 32, στ) να παρακολουθεί τη διενέργεια της εκτίμησης επιπτώσεων σχετικά με την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και την αίτηση περί προηγούμενης έγκρισης ή προηγούμενης διαβούλευσης, εφόσον απαιτείται δυνάμει των άρθρων 33 και 34, ζ) να παρακολουθεί την απάντηση της αρχής ελέγχου σε αιτήματα και, στο πλαίσιο της αρμοδιότητας του υπευθύνου προστασίας δεδομένων, να συνεργάζεται με την αρχή ελέγχου κατόπιν αιτήματός της ή με πρωτοβουλία του υπευθύνου προστασίας δεδομένων· η) να ενεργεί ως σημείο επικοινωνίας για την αρχή ελέγχου σε ζητήματα που σχετίζονται με την επεξεργασία και να διαβουλεύεται με την αρχή ελέγχου, εφόσον απαιτείται, με δική του πρωτοβουλία.»

α) Γνώμη 5/2010 σχετικά με τις εφαρμογές RFID⁴⁰, η οποία τονίζει την ανάγκη αναδείξεως και αξιολογήσεως των κινδύνων για την ιδιωτική ζωή που συνδέονται με μία εφαρμογή RFID από τον ίδιο τον φορέα εκμεταλλεύσεως RFID.

β) Γνώμη 13/2011 σχετικά με τον γεωενοτοπισμό⁴¹, η οποία υπογραμμίζει ότι το νομικό πλαίσιο για τη χρήση δεδομένων γεωγραφικής θέσεως από έξυπνες κινητές συσκευές (τα οποία συνιστούν δεδομένα προσωπικού χαρακτήρα) ορίζεται ήδη από την Οδηγία 95/46/ΕΚ). Περαιτέρω, διακρίνει τους υπεύθυνους επεξεργασίας δεδομένων σε υπεύθυνους των υποδομών εντοπισμού γεωγραφικής θέσεως (συγκεκριμένα υπεύθυνοι της επεξεργασίας των χαρτογραφημένων σημείων πρόσβασης WiFi), σε παρόχους εφαρμογών και υπηρεσιών εντοπισμού γεωγραφικής θέσεως και σε σχεδιαστές λειτουργικών συστημάτων έξυπνων κινητών συσκευών. Η μεγάλη συνεισφορά της εν λόγω Γνώμης είναι η θέσπιση θεμιτών λόγων επεξεργασίας, βασιζομένων στην έγκυρη συγκατάθεση, η οποία δεν μπορεί να αποσιπάται βάσει γενικών όρων και προϋποθέσεων. Η συγκατάθεση πρέπει να αφορά στον εκάστοτε συγκεκριμένο σκοπό επεξεργασίας των δεδομένων από τον υπεύθυνο της επεξεργασίας, όπως για παράδειγμα την κατάρτιση προφίλ και/ή την εξειδικευμένη αντιμετώπιση με βάση τη συμπεριφορά. Σε περίπτωση που οι σκοποί της επεξεργασίας τροποποιηθούν κατά τρόπο ουσιώδη, ο υπεύθυνος της επεξεργασίας πρέπει να ζητήσει την εκ νέου συγκατάθεση. Η Γνώμη τονίζει ότι κατά την αγορά της συσκευής, οι υπηρεσίες εντοπισμού θέσεως πρέπει να είναι απενεργοποιημένες. Μηχανισμοί εξαιρέσεως δεν αποτελούν επαρκείς μηχανισμούς για τη λήψη της συγκατάθεσεως του χρήστη κατόπιν ενημερώσεως. Η Γνώμη υπογραμμίζει τη δυσκολία συγκαταθέσεως στο εργασιακό πλαίσιο και τα παιδιά⁴². Όσον αφορά τους

40. Βλ. Ομάδα Εργασίας Άρθρου 29, Γνώμη 5/2010, σχετικά με την πρόταση του κλάδου για ένα πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID, διαθέσιμη σε: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_el.pdf#h2-5, τελευταίος έλεγχος: 15.5.2014.

41. Βλ. Ομάδα Εργασίας Άρθρου 29, Γνώμη 13/2011 σχετικά με τις υπηρεσίες εντοπισμού γεωγραφικής θέσης που παρέχονται μέσω έξυπνων κινητών συσκευών, διαθέσιμη σε: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_el.pdf#h2-5, τελευταίος έλεγχος: 15.5.2014.

42. Πρβλ. ΑΠΔΠΧ, Απόφαση 112/2012, διαθέσιμη σε: www.dpa.gr, τελευταίος έλεγχος: 15.5.2014, η οποία τόνισε την ανάγκη αξιολογήσεως των κινδύνων για τα παιδιά αναφορικά με τα βραχιολάκια παρακολούθησεως της γεωγραφικής τους θέσεως και κατέληξε ότι η χρήση συστημάτων γεωενοτοπισμού σε παιδιά θα πρέπει να γίνεται κατόπιν ενημερώσεως των παιδιών, αφού συνεκτιμηθεί και η δική τους γνώμη. Άξια αναφοράς είναι η μειοψηφία της εν λόγω αποφάσεως, βάσει της οποίας η χρήση συστήματος γεωενοτοπισμού σε ανήλικο παιδί εγκυμονεί σοβαρούς και απρόβλεπτους σε μη ειδικούς κινδύνους για την ελεύθερη ανάπτυξη της προσωπικότητας των ανηλίκων και ιδίως για τη σωματική και ψυχολογική τους ανάπτυξη. Ενδεικτικά θα πρέπει να επισημανθεί ο κίνδυνος να πιστέψουν τα παιδιά ήδη από μικρή ηλικία ότι είναι φυσιολογικό - για την ασφάλειά τους - να παρακολουθούνται μέσω καμερών ή άλλων «έξυπνων» συσκευών, πεποίθηση, που αν εμπειδωθεί στην ευαίσθητη παιδική ηλικία, δύναται να διευκολύνει, μετά την ενηλικίωσή τους, την αποδοχή στενότερης παρακολούθησεως καθ' υπέρβαση των σήμερα κοινώς αποδεκτών κοινωνικών

εργαζομένους, οι εργοδότες μπορούν να χρησιμοποιούν τη συγκεκριμένη τεχνολογία μόνο εφόσον είναι αποδεδειγμένα αναγκαία για θεμιτό σκοπό και οι ίδιοι στόχοι δεν μπορούν να επιτευχθούν με λιγότερο παρεμβατικό τρόπο. Σχετικά με τα παιδιά, οι γονείς είναι αυτοί που κρίνουν αν η χρήση της εν λόγω συσκευής είναι αιτιολογημένη υπό συγκεκριμένες συνθήκες. Οφείλουν τουλάχιστον να ενημερώνουν τα παιδιά τους και να τους επιτρέπουν να συμμετέχουν στην απόφαση για τη χρήση των εν λόγω εφαρμογών το νωρίτερο δυνατό.

γ) Γνώμη 12/2011 σχετικά με τα ευφυή συστήματα μετρήσεως⁴³. Η εν λόγω Γνώμη κατέδειξε ότι τα ευφυή συστήματα μετρήσεως περικλείουν το ενδεχόμενο εφαρμογής πολυάριθμων και καινοτόμων τρόπων επεξεργασίας δεδομένων και παροχής υπηρεσιών σε καταναλωτές. Ανεξάρτητα από το είδος της επεξεργασίας, είτε είναι παρόμοια με εκείνη που εφαρμοζόταν στην προ ευφυών τεχνολογιών περίοδο ή τελείως διαφορετική, πρέπει να προσδιορίζονται με σαφήνεια οι υπεύθυνοι της επεξεργασίας δεδομένων και οι υποχρεώσεις τους που απορρέουν από τη νομοθεσία για την προστασία των δεδομένων, όπως η προσέγγιση για την «προστασία της ιδιωτικής ζωής ήδη από τον σχεδιασμό» και η προστασία της ασφάλειας και των δικαιωμάτων των υποκειμένων των δεδομένων. Τα υποκείμενα των δεδομένων πρέπει να είναι επαρκώς ενημερωμένα σχετικά με την επεξεργασία των δεδομένων τους και να έχουν επίγνωση των θεμελιωδών διαφορών στον τρόπο επεξεργασίας των δεδομένων τους, έτσι ώστε να διασφαλίζεται η εγκυρότητα της συγκατάθεσής τους.

δ) Γνώμη 2/2013 σχετικά με τις εφαρμογές των έξυπνων συσκευών⁴⁴. Σύμφωνα με την εν λόγω Γνώμη, η οποία καίρει απόλυτης εφαρμογής στην περίπτωση του ΔτΠ, ο κατακερματισμένος χαρακτήρας του οικοσυστήματος εφαρμογών, το ευρύ φάσμα δυνατοτήτων τεχνικής προσβάσεως σε δεδομένα που αποθηκεύονται σε κινητές συσκευές ή δημιουργούνται από αυτές και η έλλειψη νομικής ευαισθητοποίησης των σχεδιαστών δημιουργούν ορισμένους σοβαρούς κινδύνους όσον αφορά την προστασία των δεδομένων των χρηστών εφαρμογών. Οι κίνδυνοι αυτοί κυμαίνονται από έλλειψη διαφάνειας και έλλειψη ευαισθητο-

ποίησης των χρηστών εφαρμογών μέχρι ανεπαρκή μέτρα ασφαλείας, ανίσχυρους μηχανισμούς συγκατάθεσης, τάση μεγιστοποίησης των δεδομένων και ελαστικότητα των σκοπών επεξεργασίας των δεδομένων. Η Γνώμη θέτει πολλές υποχρεώσεις στους σχεδιαστές των εν λόγω συσκευών, οι οποίοι, μεταξύ άλλων, οφείλουν α) να γνωρίζουν και να συμμορφώνονται με τις υποχρεώσεις που υπέχουν ως υπεύθυνοι επεξεργασίας, όταν επεξεργάζονται δεδομένα που έχουν λάβει από ή που αφορούν τους τελικούς χρήστες· β) να γνωρίζουν και να συμμορφώνονται με τις υποχρεώσεις που υπέχουν ως υπεύθυνοι επεξεργασίας, όταν συνεργάζονται με εκτελούντες επεξεργασία δεδομένων, για παράδειγμα όταν αναθέτουν υπεργολαβικά τη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα σε κατασκευαστές, προγραμματιστές και, π.χ. παρόχους χώρου αποθηκεύσεως στο υπολογιστικό νέφος· γ) να ζητούν συγκατάθεση προτού η εφαρμογή αρχίσει να ανακτά ή να τοποθετεί πληροφορίες στη συσκευή, δηλαδή πριν από την εγκατάσταση της εφαρμογής· δ) να ζητούν συγκατάθεση συγκεκριμένη για κάθε κατηγορία δεδομένων, στην οποία θα αποκτήσει πρόσβαση η εφαρμογή, τουλάχιστον για τις κατηγορίες Τοποθεσία, Επαφές, Μοναδικό Αναγνωριστικό Συσκευής, Ταυτότητα του προσώπου το οποίο αφορούν τα δεδομένα, Ταυτότητα του Τηλεφώνου, Πιστωτική κάρτα και δεδομένα πληρωμών, Τηλεφωνία και Υπηρεσία Σύντομων Μηνυμάτων, Ιστορικό Περιήγησης, Ηλεκτρονικό Ταχυδρομείο, Πιστοποιήσεις κοινωνικών δικτύων και Βιομετρικά χαρακτηριστικά· ε) να έχουν επίγνωση του ότι η συγκατάθεση δεν νομιμοποιεί την υπερβολική ή δυσανάλογη επεξεργασία δεδομένων· στ) να γνωστοποιούν κατά τρόπο συγκεκριμένο και κατανοητό τους σκοπούς της επεξεργασίας δεδομένων πριν από την εγκατάσταση της εφαρμογής και να μην τροποποιούν αυτούς τους σκοπούς χωρίς ανανέωση της συγκατάθεσης· να παρέχουν πλήρη ενημέρωση αν τα δεδομένα πρόκειται να χρησιμοποιηθούν για σκοπούς τρίτων, για παράδειγμα διαφήμιση ή υπηρεσίες αναλύσεων· ζ) να επιτρέπουν στους χρήστες να ανακαλούν τη συγκατάθεσή τους και να απεγκαθιστούν την εφαρμογή και να διαγράφουν τα δεδομένα, εφόσον απαιτείται· η) να τηρούν την αρχή της ελαχιστοποίησης δεδομένων και να συλλέγουν μόνο τα δεδομένα που είναι απολύτως απαραίτητα για την εκτέλεση της επιθυμητής λειτουργικής δυνατότητας· θ) να λαμβάνουν τα αναγκαία οργανωτικά και τεχνικά μέτρα προκειμένου να εξασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα που επεξεργάζονται σε όλα τα στάδια του σχεδιασμού και της εκτέλεσης της εφαρμογής (σεβασμός της ιδιωτικής ζωής από τις προεπιλεγμένες ρυθμίσεις)· ι) να παρέχουν ένα ενιαίο σημείο επαφής για τους χρήστες της εφαρμογής· ια) να παρέχουν ευανάγνωστη, κατανοητή και ευχερώς προσπελάσιμη πολιτική προστασίας της ιδιωτικής ζωής, η οποία να ενημερώνει τους χρήστες τουλάχιστον για τα εξής:

και δικαιιοπολιτικών αρχών και αξιών. Για τους λόγους αυτούς, η χρήση του συστήματος γεωτοποιοποίησης σε ανηλίκους θα πρέπει πρώτα να αξιολογηθεί ως προς τους κινδύνους της από τους αρμόδιους φορείς της Πολιτείας (π.χ. Ινστιτούτο Υγείας του Παιδιού, Εταιρεία Προστασίας Ανηλίκων Αθηνών, Ινστιτούτο Κοινωνικής Προστασίας και Αλληλεγγύης, Συνήγορος του Παιδιού, Εθνική Επιτροπή για τα Δικαιώματα του Ανθρώπου κ.ά.) και εν συνεχεία να ληφθεί η σχετική απόφαση. Μέχρι τότε η χρήση του εν λόγω συστήματος σε ανηλίκους θα πρέπει να επιτραπεί μόνο για λόγους υγείας.

43. Βλ. Ομάδα Εργασίας Άρθρου 29, Γνώμη 12/2011 σχετικά με τα ευφυή συστήματα μέτρησης, διαθέσιμη σε: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_el.pdf#h2-5, τελευταίος έλεγχος: 15.5.2014.

44. Βλ. Ομάδα Εργασίας Άρθρου 29, Γνώμη 02/2013 για τις εφαρμογές των έξυπνων συσκευών, διαθέσιμη σε: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_el.pdf#h2-2, τελευταίος έλεγχος: 15.5.2014.

ΜΕΛΕΤΕΣ-ΓΝΩΜΟΔΟΤΗΣΕΙΣ

- ποιοι είναι (ταυτότητα και στοιχεία επικοινωνίας),
- ποιες ακριβώς κατηγορίες δεδομένων προσωπικού χαρακτήρα επιθυμεί να συλλέγει και να επεξεργάζεται η εφαρμογή,
- γιατί είναι απαραίτητη η επεξεργασία δεδομένων (για ποιους ακριβώς σκοπούς),
- αν τα δεδομένα πρόκειται να κοινοποιηθούν σε τρίτους (όχι γενική, αλλά συγκεκριμένη περιγραφή του τρίτου στον οποίο θα κοινοποιηθούν τα δεδομένα),
- ποια δικαιώματα έχουν οι χρήστες από άποψη ανάκλησης της συγκατάθεσης και διαγραφής των δεδομένων⁴⁵.

ιβ) να επιτρέπουν στους χρήστες εφαρμογών να ασκούν τα δικαιώματα προσβάσεως, διορθώσεως, διαγραφής, καθώς και το δικαίωμα ενστάσεως στην επεξεργασία των δεδομένων τους και να τους ενημερώνουν για την ύπαρξη των αντίστοιχων μηχανισμών· ιγ) να καθορίζουν εύλογη περίοδο διατηρήσεως για τα δεδομένα που συλλέγονται με την εφαρμογή και να προκαθορίζουν περίοδο αδράνειας, μετά την οποία ο λογαριασμός θεωρείται ότι έχει λήξει· ιδ) όσον αφορά τις εφαρμογές που απευθύνονται στα παιδιά: να αποδίδουν προσοχή στο όριο ηλικίας που προβλέπει η εθνική νομοθεσία για τα παιδιά ή τους ανηλίκους, να επιλέγουν την περισσότερο περιοριστική προσέγγιση όσον αφορά την επεξεργασία δεδομένων με απόλυτο σεβασμό των αρχών της ελαχιστοποίησης των δεδομένων και του περιορισμού του σκοπού, να μην επεξεργάζονται τα δεδομένα των παιδιών για σκοπούς συμπεριφορικής διαφήμισης, αμέσως ή εμμέσως, και να μην συλλέγουν μέσω των παιδιών δεδομένα σχετικά με τους συγγενείς ή/και φίλους τους.

ε) Γνώμη 3/2013 σχετικά με την αλλαγή του σκοπού επεξεργασίας⁴⁵, βάσει της οποίας δεν θα είναι θεμιτή η αλλαγή του σκοπού επεξεργασίας σε σωρεία περιπτώσεων. Σύμφωνα με την εν λόγω Γνώμη, η επεξεργασία δεδομένων για διαφορετικό σκοπό δεν σημαίνει απαραίτητα ότι είναι και αθέμιτη. Το θεμιτό της επεξεργασίας εξετάζεται κατά περίπτωση. Κρίσιμοι παράγοντες εν προκειμένω είναι: α) η σχέση ανάμεσα στους λόγους συλλογής των προσωπικών δεδομένων και τους λόγους της περαιτέρω επεξεργασίας τους, β) το πλαίσιο υπό το οποίο συλλέχθηκαν τα δεδομένα και οι λογικές προσδοκίες των υποκειμένων των δεδομένων για περαιτέρω επεξεργασία, γ) η φύση των προσωπικών δεδομένων και η επίδραση της περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων και δ) τα μέτρα ασφάλειας που έλαβε ο υπεύθυνος επεξεργασίας για να διασφαλίσει δίκαιη επεξεργασία και να αποτρέψει αδικαιολόγητη επίδραση της επεξεργασίας στα υποκείμενα των δεδομένων⁴⁶. Η Γνώμη

δεν αποφαίνεται για το εάν τα κριτήρια πρέπει να εφαρμόζονται σωρευτικά. Δεδομένου ότι κάτι τέτοιο δεν ορίζεται ρητώς, ορθότερο θα ήταν να θεωρηθεί ότι τα προτεινόμενα κριτήρια είναι καθοδηγητικά της εξετάσεως της νομιμότητας της αλλαγής του σκοπού επεξεργασίας και επιβοηθητικά της λήψης αποφάσεως και, ως εκ τούτου, δεν είναι απαραίτητο να εφαρμόζονται σωρευτικά⁴⁷. Πλούσια είναι και τα παραδείγματα που εκθέτει η Γνώμη, μεταξύ των οποίων, το αθέμιτο της χρησιμοποίησης δεδομένων από ευφυή συστήματα μέτρησης για φορολογικούς σκοπούς. Αντιθέτως, η Γνώμη θεωρεί θεμιτή τη χρησιμοποίηση των εν λόγω δεδομένων για τη μέτρηση λαθραίας χρήσεως ενέργειας.

στ) Γνώμη 4/2013 σχετικά με το υπόδειγμα για την εκτίμηση των επιπτώσεων της προστασίας δεδομένων όσον αφορά τα ευφυή δίκτυα και τα ευφυή συστήματα μέτρησης («υπόδειγμα ΕΕΠΔ»), το οποίο εκπόνησε η ομάδα εμπειρογνομιώνων 2 της ομάδας ειδικών καθηκόντων της Επιτροπής για τα ευφυή ηλεκτρικά δίκτυα⁴⁸. Η Γνώμη τονίζει την ανάγκη εκτενέστερης καθοδήγησης όσον αφορά την επιλογή νομικής βάσεως για την επεξεργασία και την επιλογή που πρέπει να διαθέτουν τα πρόσωπα, στα οποία αναφέρονται τα δεδομένα. Ειδικότερα, θα πρέπει να υπάρχει σαφής καθοδήγηση σχετικά με το τι μπορεί να γίνει χωρίς συγκατάθεση του χρήστη και το τι απαιτεί συγκατάθεση του χρήστη. Ιδιαίτερη προσοχή πρέπει να δοθεί στην εφαρμογή εξ αποστάσεως διακοπής και μεμονωμένων ενδείξεων. Εξειδικεύει ότι στις περισσότερες περιπτώσεις θα απαιτείται ελεύθερη, ειδική, εν γνώσει και ρητή συγκατάθεση για κάθε είδους επεξεργασία που βαινει πέραν της επεξεργασίας, η οποία απαιτείται για

νομίμως συλλέχθηκαν και για τον σκοπό του πειθαρχικού ελέγχου του υπαλλήλου της διενεργούσης την επεξεργασία Τράπεζας συνιστά θεμιτή μεταβολή του σκοπού της αρχικής συλλογής και επεξεργασίας των προσωπικών δεδομένων του προσφεύγοντος, με αποτέλεσμα να μην έχει λάβει χώρα παραβίαση των διατάξεων του Ν 2472/1997 και η προσφυγή πρέπει να απορριφθεί. Στην προκειμένη υπόθεση ο προσφεύγων κατήγγειλε ότι ο Επιθεωρητής Τράπεζας με την εν λόγω ιδιότητα του αναζήτησε δυσμενή για αυτόν στοιχεία στον ΤΕΙΡΕΣΙΑ. Ο Επιθεωρητής ζήτησε από τον προσφεύγοντα με επιστολή έγγραφες απόψεις του αναφορικά με αντικανονική συμμετοχή σε πιστοδότηση πελάτη, αναφέροντας μεταξύ άλλων δυσμενή στοιχεία του ΤΕΙΡΕΣΙΑ που έχουν καταχωρηθεί καταγγελίες συμβάσεων στεγαστικών δανείων και πιστωτικών καρτών στην Τράπεζα. Παράλληλα του ανακοίνωσε ότι είναι οφειλέτης σε άλλες τράπεζες σε διάφορα καταναλωτικά προϊόντα με σημαντικότερες καθυστερήσεις, γεγονός που φανερώνει αδυναμία τακτοποίησης των δόσεων. Δεδομένου ότι η συναλλακτική αυτή συμπεριφορά δεν συνάδει σε λειτουργό της Τράπεζας, σύμφωνα με τον Οργανισμό Προσωπικού, αφού τα εισοδήματά του δεν επαρκούν για την εξυπηρέτηση των μηνιαίων δόσεων τον ερώτησε πώς σκοπεύει να τακτοποιήσει –εξοφλήσει τις οφειλές.

45. Βλ. Ομάδα Εργασίας Άρθρου 29, Γνώμη 3/2013 σχετικά με τον περιορισμό του σκοπού επεξεργασίας, διαθέσιμη σε: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, τελευταίος έλεγχος: 15.5.2014.

46. Η ΑΠΔΠΧ, στην Απόφαση 66/2013, διαθέσιμη σε www.dpa.gr, τελευταίος έλεγχος: 15.5.2014, έχει κρίνει ότι η περαιτέρω επεξεργασία των δεδομένων πέραν του σκοπού για τον οποίο αρχικά

47. Βλ. Φερεινή Παναγοπούλου-Κουτνατζή, Περί της προσωπικής και οικιακής χρήσεως των προσωπικών δεδομένων, ΕφημΔΔ 2013, σ. 704 επ. (710).

48. Βλ. Ομάδα Εργασίας Άρθρου 29, Γνώμη 04/2013 σχετικά με το υπόδειγμα για την εκτίμηση των επιπτώσεων της προστασίας δεδομένων όσον αφορά τα ευφυή δίκτυα και τα ευφυή συστήματα μέτρησης («υπόδειγμα ΕΕΠΔ») το οποίο εκπόνησε η ομάδα εμπειρογνομιώνων 2 της ομάδας ειδικών καθηκόντων της Επιτροπής για τα ευφυή ηλεκτρικά δίκτυα διαθέσιμη σε: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_el.pdf#h2-5, τελευταίος έλεγχος: 15.5.2014.

(i) την παροχή ενέργειας, (ii) την τιμολόγηση της παρεχόμενης ενέργειας, (iii) την αποκάλυψη απάτης που έγκειται στη χρήση της παρεχόμενης ενέργειας χωρίς πληρωμή και (iv) την εκπόνηση συγκεντρωτικών δεδομένων απαραίτητων για την αποδοτική από άποψη ενέργειας συντήρηση του δικτύου (προβλέψεις και εκκαθάριση). Η συγκατάθεση θα απαιτείται, για παράδειγμα, μεταξύ άλλων, για λόγους εντοπισμού και αναλύσεως των χαρακτηριστικών στο πλαίσιο συμπεριφορικής διαφημίσεως. Η Γνώμη επισημαίνει ότι για να είναι έγκυρη η συγκατάθεση, οι καταναλωτές πρέπει να κατανοούν τι θα συμβεί στα δεδομένα τους. Είναι ιδιαίτερα σημαντικό, σε περίπτωση αναλύσεως των χαρακτηριστικών, να έχουν το δικαίωμα να γνωρίζουν τα ατομικά χαρακτηριστικά τους και τη λογική τυχόν αλγορίθμων που χρησιμοποιούνται για τη συγκέντρωση δεδομένων. Οι πληροφορίες για τις εξ αποστάσεως λειτουργίες διακοπής/επαναλήψεως είναι εξίσου σημαντικές: οι πελάτες πρέπει να γνωρίζουν ποια περιστατικά μπορούν να οδηγήσουν σε διακοπή.

Στη Γνώμη 07/2013 σχετικά με το υπόδειγμα για την εκτίμηση των επιπτώσεων της προστασίας δεδομένων όσον αφορά τα ευφυή δίκτυα και τα ευφυή συστήματα μέτρησης («υπόδειγμα ΕΕΠΔ»), το οποίο εκπόνησε η ομάδα εμπειρογνομόνων 2 της ομάδας ειδικών καθηκόντων της Επιτροπής για τα ευφυή ηλεκτρικά δίκτυα. Η Γνώμη αυτή τόνισε ότι πρέπει να εφαρμοστούν μηχανισμοί, ώστε να διασφαλίζεται ότι, εξ ορισμού, υποβάλλονται σε επεξεργασία μόνον εκείνα τα δεδομένα προσωπικού χαρακτήρα, τα οποία είναι αναγκαία για κάθε συγκεκριμένο σκοπό επεξεργασίας και ότι τα εν λόγω δεδομένα δεν συλλέγονται ούτε διατηρούνται πέραν του ελάχιστου απαραίτητου ορίου για τους σκοπούς αυτούς, από την άποψη τόσο της ποσότητας των δεδομένων όσο και του χρόνου της αποθηκεύσεώς τους⁴⁹.

Οι ως άνω Γνώμες φανερώνουν ότι το Διαδίκτυο των Πραγμάτων δεν είναι κάτι το εξαιρετικά νέο, το οποίο ο νομοθέτης αντιμετωπίζει με δέος. Το γνωμοδοτικό πλαίσιο είναι ήδη επαρκές. Χρήσιμη θα ήταν εξειδικευμένη Γνώμη που θα συστηματοποιούσε όλα τα ζητήματα αναφορικά με το ΔΤΠ και θα εστίαζε στην ανάγκη μη χρησιμοποίησης των εν λόγω συσκευών από ασφαλιστικές εταιρείες και εργοδότες, ακόμα και αν συναινεί ο χρήστης. Η απαγόρευση συνδιαλλαγής των δεδομένων δεν πρέπει να θεωρείται ότι συνιστά αποτέλεσμα άκρατης πατερναλιστικής αντιμετώπισης των χρηστών. Στην περίπτωση αυτή έχουμε να κάνουμε με μία επιτρεπτή ελαφρά μορφή πατερναλισμού (από την οποία πηγάζει εξάλλου και η ιδέα της προστασίας των προσωπικών δεδομένων) και όχι με την ανεπίτρεπτη σκληρή μορφή πατερναλισμού. Δικαιολογείται από το γεγονός ότι στις εν λό-

49. Βλ. Ομάδα Εργασίας Άρθρου 29, Γνώμη 07/2013 σχετικά με το υπόδειγμα για την εκτίμηση των επιπτώσεων της προστασίας δεδομένων όσον αφορά τα ευφυή δίκτυα και τα ευφυή συστήματα μέτρησης («υπόδειγμα ΕΕΠΔ») το οποίο εκπόνησε η ομάδα εμπειρογνομόνων 2 της ομάδας ειδικών καθηκόντων της Επιτροπής για τα ευφυή ηλεκτρικά δίκτυα, διαθέσιμη σε: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_el.pdf#h2-2, τελευταίος έλεγχος: 15.5.2014.

γω περιπτώσεις υπάρχει ανισότητα στη σχέση μεταξύ χρήστη και εργοδότη ή ασφαλιστή.

VII. Απαιτήσεις προστασίας δεδομένων

Με σκοπό την πρόληψη της καταχρήσεως των συλλεχθέντων δεδομένων στην περίπτωση ΔΤΠ πρέπει να ληφθούν εξ αρχής πολλά μέτρα.

Ο χρήστης οφείλει στο πλαίσιο του πληροφοριακού του αυτοκαθορισμού να γνωρίζει τα δεδομένα που συλλέγονται, τον αποδέκτη τους, τον υπεύθυνο και εκτελούντα την επεξεργασία, το σκοπό της επεξεργασίας και τις ενδεχόμενες περαιτέρω χρήσεις αυτών. Πρόσφατα πειράματα που έχουν πραγματοποιηθεί σε καταστήματα της Νέας Υόρκης και του Λονδίνου στηρίχθηκαν σε ασύρματους ικνηλάτες που μπορούν να χρησιμοποιηθούν για την καταγραφή των κινήσεων των ατόμων, προκειμένου να τους στέλνουν στοχευμένες διαφημίσεις βασισζόμενες στα ενδιαφέροντά τους, να τροποποιήσουν την οργάνωση εμπορευμάτων στα καταστήματα και τις προμήθειες⁵⁰. Αυτά τα πειράματα φανερώνουν ότι τα υποκείμενα των δεδομένων συχνά αγνοούν ότι τυγχάνουν παρακολούθησεως, δεδομένου ότι οι μηχανισμοί παρακολούθησεως έχουν σχεδιαστεί για να μένουν απαρατήρητοι. Τα υποκείμενα των δεδομένων θα πρέπει να ενημερώνονται για την παρουσία ενός τέτοιου μηχανισμού και ει δυνατόν θα πρέπει να εκπέμπεται σήμα από τη συσκευή παρακολούθησεως. Σε ορισμένες περιπτώσεις αυτό δεν είναι δυνατό, επειδή οι συσκευές λειτουργούν παθητικά με δακτυλικά αποτυπώματα.

Επόμενος σταθμός μετά τη γνώση είναι η δυνατότητα συγκαταθέσεως, δηλαδή συμφωνίας ή διαφωνίας με την εν λόγω επεξεργασία. Τα άτομα των οποίων τα δεδομένα καταγράφονται από τους αισθητήρες θα πρέπει να γνωρίζουν ότι λαμβάνει χώρα επεξεργασία των δεδομένων και θα πρέπει να είναι σε θέση να συμφωνήσουν ή να διαφωνήσουν με την εν λόγω επεξεργασία⁵¹. Προβληματισμό προκαλεί η δυσκολία συγκαταθέσεως σε πολλές περιπτώσεις, π.χ. μέσω των google glasses⁵², δεδομένου ότι αυτός που τα φοράει, ο οποίος στη συγκεκριμένη περίπτωση θα πρέπει να εκλη-

50. Βλ. *Stephanie Clifford/Quentin Hardi*, Attention, Shoppers: Store Is Tracking Your Cell, *New York Times*, 14.7.2013, διαθέσιμο σε: http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?_r=0, τελευταίος έλεγχος: 15.5.2014.

51. Βλ. Ομάδα Εργασίας Άρθρου 29, Γνώμη 15/2011 σχετικά με τον ορισμό της συγκαταθέσεως, διαθέσιμη σε: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_el.pdf#h2-4, τελευταίος έλεγχος: 15.5.2014 και Ομάδα Εργασίας Άρθρου 29, Γνώμη 4/2012 σχετικά με την απαλλαγή που ισχύει σε σχέση με τη συναίνεση για τα cookies, διαθέσιμη σε: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_el.pdf#h2-4, τελευταίος έλεγχος: 15.5.2014.

52. Σημειώνεται πάντως ότι το ζήτημα προϋπήρχε, δεδομένου ότι χρήστης πολλών συσκευών μπορεί να βιντεοσκοπήσει πολλά άτομα, χωρίς τη συγκατάθεσή τους.

φθεί ως υπεύθυνος επεξεργασίας, μπορεί να καταγράψει πολλά πρόσωπα, τα οποία δεν γνωρίζουν ότι καταγράφονται και είναι αναγνωρίσιμα μέσω ειδικής τεχνολογίας⁵³. Έτσι, ο χρήστης των γυαλιών που συγκατατέθηκε με τη συλλογή δεδομένων του κατέληξε στο να συλλέγει δεδομένα άλλων, οι οποίοι δεν συγκατατέθηκαν, ενώ έπρεπε να συγκατατεθούν. Μεγάλη έμφαση θα πρέπει συνεπώς να δοθεί στον επαναπροσδιορισμό των δεδομένων που συλλέγονται, αλλά και των υποκειμένων των δεδομένων⁵⁴. Αντίστοιχο προβληματισμό αναφορικά με τη συγκατάθεση προκαλεί η συλλογή μεγάλων δεδομένων (big data).

Συναφής με τη συγκατάθεση είναι η παροχή της δυνατότητας απενεργοποίησης επεξεργασίας των δεδομένων. Η ενεργοποίηση της επεξεργασίας των δεδομένων θα πρέπει να λαμβάνει χώρα από τον ίδιο το χρήστη, ο οποίος στη συνέχεια αν διαφωνήσει με την επεξεργασία θα πρέπει να έχει τη δυνατότητα ολικής απενεργοποίησης της επεξεργασίας. Στο σημείο αυτό εφαρμόζεται η αρχή “εν αμφιβολία υπέρ της ιδιωτικότητας”⁵⁵.

Θεμελιώδους σημασίας είναι το ζήτημα της ασφάλειας των συσκευών. Όπως αναφέρθηκε προηγουμένως, τροχοπέδη στην ασφάλεια στέκεται η ανάγκη μείωσης του κόστους και αυξήσεως της αυτονομίας της συσκευής. Για το λόγο αυτό οι

κατασκευαστές προτιμούν να επενδύουν στη βελτίωση των χαρακτηριστικών με μειωμένο κόστος και όχι στην ιδιωτικότητα, η οποία όμως θα πρέπει να συνιστά απαραίτητη προδιαγραφή της συσκευής. Χαρακτηριστικό παράδειγμα είναι ότι η εφαρμογή κρυπτογραφικών εργαλείων, που θα μειώσει σημαντικά την αυτονομία της συσκευής, αλλά θα ενισχύσει την προστασία της ιδιωτικότητας, δεν αποτελεί προτεραιότητα των κατασκευαστών. Παράλληλα, λόγω της μειωμένης ασφάλειας του ΔτΠ ασύρματες διεπαφές είναι διάτρυτες σε κακόβουλες προσβάσεις.

Άλλα προτεινόμενα μέτρα είναι η θέσπιση ορίων για τη συλλογή των δεδομένων, η αποφυγή της εξαισιμικής των δεδομένων, η δυνατότητα φορητότητας των δεδομένων μέσω της δυνατότητας στους χρήστες να επιλέξουν έναν επεξεργαστή δεδομένων που δεν είναι ο κατασκευαστής της συσκευής.

VIII. Αντί επιλόγου

Το ΔτΠ είναι μια πολλά υποσχόμενη εξέλιξη που θα μας προσφέρει αμέτρητες δυνατότητες και ευκαιρίες εργασίας. Ζητούμενο πρέπει να είναι πώς θα προστατεύσουμε τους πολίτες προτού όλες αυτές οι εφαρμογές γίνουν στο σύνολό τους πραγματικότητα. Αν θέλουμε η τεχνολογία αυτή να πετύχει πρέπει να είναι αξιόπιστη, ελεγχόμενη και να μην παραπέσει σε λάθος χέρια. Εκ των πραγμάτων η νομοθεσία έπεται δεύτερη και καταϊδρωμένη της τεχνολογίας. Είναι απαραίτητο να κάνουμε κάτι και να μην παρακολουθούμε στωικά την τεχνολογία να απομακρύνεται. Πρέπει να γνωρίζουμε πως ό,τι κάνουμε θα είναι προσωρινό, δεδομένου ότι η τεχνολογία θα μας προλάβει και πάλι και θα χρειαστεί περαιτέρω αναθεώρηση της νομοθεσίας. Για το λόγο αυτό είναι σημαντικό να ενεργήσουμε τώρα. Εάν κάνουμε κάτι πολύ αργά, θα είναι σαν να μην το έχουμε κάνει καθόλου.

* * * * *

53. Κάμερες με υψηλή ανάλυση επιτρέπουν με μια μόνο λήψη, τη βιομετρική ανάλυση του προσώπου καθενός από τους χιλιάδες θεατές που ακολουθούν μια διαδήλωση ή βρίσκονται σε ένα στάδιο, βλ. π.χ. www.gigapan.org, τελευταίος έλεγχος: 15.5.2014.

54. Βλ. Ομάδα Εργασίας Άρθρου 29, Γνώμη 3/2013 σχετικά με τον περιορισμό του σκοπού επεξεργασίας, διαθέσιμη σε: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, τελευταίος έλεγχος: 15.5.2014.

55. Για την ανάλυση της αρχής “εν αμφιβολία υπέρ της ιδιωτικότητας”, βλ. *Φερενίκη Παναγοπούλου-Κουτνατζή, Κοινωνικά Δίκτυα και Προσωπικότητα, ΔιΜΕΕ 2012, σ. 186 επ. (192).*