



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
**Εθνικόν και Καποδιστριακόν
Πανεπιστήμιον Αθηνών**
— ΙΔΡΥΘΕΝ ΤΟ 1837 —

ΝΟΜΙΚΗ ΣΧΟΛΗ

ΕΝΙΑΙΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΚΑΤΕΥΘΥΝΣΗ: ΑΣΤΙΚΟ ΔΙΚΑΙΟ
ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΕΤΟΣ: 2011-2012

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της Σοφίας Ιωάννου Τζαβέλλα
A.M.: 1134

**Η υποχρέωση – καθήκον επιμέλειας του παρόχου στα
ηλεκτρονικά δίκτυα**

Επιβλέποντες:

Κωνσταντίνος Χριστοδούλου

Καλλιόπη Χριστακάκου

Ελισσάβετ Πούλου

Αθήνα, Νοέμβριος 2017

Copyright © [*Ονοματεπώνυμο, χρονολογία δημοσίευσης*]

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα.

Οι απόψεις και θέσεις που περιέχονται σε αυτήν την εργασία εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Η υποχρέωση – καθήκον επιμέλειας του παρόχου στα ηλεκτρονικά δίκτυα

Σοφία Ι. Τζαβέλλα

Α.Μ.: 1134

ΕΠΙΒΛΕΠΩΝ: ΚΩΝΣΤΑΝΤΙΝΟΣ ΧΡΙΣΤΟΔΟΥΛΟΥ, Καθηγητής

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ:

ΚΑΛΛΙΟΠΗ ΧΡΙΣΤΑΚΑΚΟΥ, Καθηγήτρια

ΕΛΙΣΣΑΒΕΤ ΠΟΥΛΟΥ, Λέκτορας

ΝΟΕΜΒΡΙΟΣ 2017

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία αφορά στην έρευνα της έκτασης της ευθύνης που έχει ο πάροχος ηλεκτρονικού δικτύου σχετικά με τη λήψη μέτρων ασφαλείας που προστατεύουν την ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα των πληροφοριών που διακινούνται μέσω αυτού από κακόβουλες ενέργειες τρίτων, ιδίως ενόψει της ρύθμισης του άρθρου 37 του ν. 4070/2012.

Η ανωτέρω έρευνα αφορά την ενδοσυμβατική ευθύνη του παρόχου ηλεκτρονικού δικτύου και δεν επεκτείνεται σε θέματα προσβολής πνευματικής ιδιοκτησίας, απορρήτου των επικοινωνιών, προσβολής προσωπικότητας. Ομοίως, η παρούσα εργασία δεν ασχολείται με τυχόν ποινικές εκφάνσεις της ευθύνης του παρόχου ηλεκτρονικού δικτύου.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ηλεκτρονικό Αστικό Δίκαιο

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Ηλεκτρονικό Αστικό Δίκαιο, ευθύνη παρόχου, νόμος 4070/2012

ABSTRACT

The present essay is about investigating the extent of the liability of the electronic network provider regarding taking of security measures in order to protect the integrity, availability and confidentiality of information that is being transferred via it, by malicious third party actions, in particular with a view to regulating Article 37 of the 4070/2012.

The above research concerns the intra-contractual liability of the electronic network provider and does not extend to issues of intellectual property, privacy of communications, personality insult. Similarly, this paper does not deal with any criminal aspects of the responsibility of the electronic network provider.

SUBJECT AREA: Electronic Civil Law

KEY WORDS: Electronic Civil Law, provider liability, law 4070/2012

Στο σύζυγό μου

ΠΕΡΙΕΧΟΜΕΝΑ

I. ΕΙΣΑΓΩΓΗ	9
1. Στόχοι - Οριοθέτηση του θέματος	9
2. Ορισμός της έννοιας της ασφάλειας των δικτύων ηλεκτρονικών υπολογιστών.	13
II. Η ΕΥΘΥΝΗ ΤΟΥ ΠΑΡΟΧΟΥ ΔΙΚΤΥΟΥ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ ΣΥΜΦΩΝΑ ΜΕ ΤΙΣ ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ (ΑΚ, ν. 2251/1994)... ..	15
1. Ενδοσυμβατική ευθύνη.	15
2. Λοιπές νομικές βάσεις θεμελίωσης της ευθύνης του παρόχου.....	19
III. Η ΕΥΘΥΝΗ ΤΟΥ ΜΕΣΑΖΟΝΤΟΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΚτΠ ΣΥΜΦΩΝΑ ΜΕ ΤΟ Π.Δ. 131/2003.....	21
1. Η έννοια και ο ρόλος του παρόχου υπηρεσιών διαδικτύου. Οι διακρίσεις των παρόχων υπηρεσιών διαδικτύου.	22
2. Η ευθύνη του μεσάζοντος παροχής υπηρεσιών της ΚτΠ σύμφωνα με την Οδηγία 2000/31/ΕΚ, όπως ενσωματώθηκε στο εθνικό δίκαιο με το π.δ. 131/2003.	25
3. Η προβληματική της ρυθμίσεως της απαλλαγής του μεσάζοντος παροχής υπηρεσιών της ΚτΠ από την ευθύνη του. Η έκταση της απαλλαγής.....	29
IV. Η ΕΥΘΥΝΗ ΤΟΥ ΠΑΡΟΧΟΥ ΔΗΜΟΣΙΟΥ ΔΙΚΤΥΟΥ ΣΥΜΦΩΝΑ ΜΕ ΤΟ Ν. 4070/2012.....	35
1. Η ρύθμιση της Οδηγίας 2009/140/ΕΚ.....	35
2. Η μεταφορά της Οδηγίας 2009/140/ΕΚ στο ελληνικό δίκαιο με το ν. 4070/2012.	41
3. Τα προβλήματα από τη μεταφορά της Οδηγίας 2009/140/ΕΚ. Η εφαρμογή της ρύθμισης του ν. 4070/2012.....	45
4. Ο Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών.....	50
5. Σύγκριση των υποχρεώσεων των παρόχων κατ' άρθρο 37 ν. 4070/2012 με συναφείς ρυθμίσεις του ελληνικού δικαίου.	65

V. Η ΑΣΦΑΛΕΙΑ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ.	69
1. Η οδηγία 2002/58/ΕΚ και ο ν. 3471/2006.....	69
2. Οι νέες ρυθμίσεις της οδηγίας 2009/136/ΕΚ και του ν. 4070/2012.	75
3. Σύγκριση των ρυθμίσεων της οδηγίας 2002/58/ΕΚ και του ν. 3471/2006 με τις τροποποιήσεις της οδηγίας 2009/136/ΕΚ και του ν. 4070/2012	85
VI. ΣΥΜΠΕΡΑΣΜΑΤΑ.....	88
VII. ΕΠΙΛΟΓΟΣ	94
VII. ΒΙΒΛΙΟΓΡΑΦΙΑ - ΑΡΘΟΓΡΑΦΙΑ.....	88

I. ΕΙΣΑΓΩΓΗ

1. ΣΤΟΧΟΙ - ΟΡΙΟΘΕΤΗΣΗ ΤΟΥ ΘΕΜΑΤΟΣ

Τις τελευταίες δεκαετίες, ο σύγχρονος άνθρωπος καλείται να ανταπεξέλθει με ετοιμότητα και με αποτελεσματικότητα στις προκλήσεις ενός νέου ψηφιακού κόσμου, ο οποίος, με το πρόσχημα των πολυεπίπεδων διευκολύνσεων που προσφέρει, εισβάλλει κυριαρχικά σε όλο και περισσότερους τομείς της καθημερινότητας. Όμως, από την «ηλεκτρονική» ζωή δεν απουσιάζει το στοιχείο του κινδύνου, το οποίο λαμβάνει διάφορες μορφές και εξελίσσεται παράλληλα με τις νέες τεχνολογίες. Μάλιστα, οι αυξανόμενες παραβιάσεις ασφάλειας επιφέρουν σημαντική οικονομική ζημία, βλάπτουν την ανάπτυξη του ηλεκτρονικού εμπορίου και κυρίως υπονομεύουν την εμπιστοσύνη των χρηστών¹. Όπως, δε, έχει ειπωθεί χαρακτηριστικά² «η ηλεκτρονική γειτνίαση μπορεί να μας εκθέσει σε κλοπές, κατασκοπείες, παραποιήσεις προσωπικοτήτων, αποπλανήσεις ανηλίκων και απειλές... Μια αλλαγή θα είναι απαραίτητη: αυξημένος συντονισμός των νόμων μεταξύ των κρατών και διαφόρων εθνών, για το απλό λόγο ότι η Πληροφοριακή Αγορά δεν αναγνωρίζει εθνικά σύνορα...».

Στην κατεύθυνση αυτή, φαίνεται να κινείται, κατά το χρονικό διάστημα των τελευταίων ετών, η νομοπαραγωγική μηχανή της Ευρωπαϊκής Ένωσης. Ειδικότερα, ο Ευρωπαίος νομοθέτης για πρώτη φορά έκανε λόγο για την ανάγκη λήψης μέτρων προς το σκοπό της επίτευξης της ασφάλειας των δικτύων και των πληροφοριών με τον κανονισμό 460/2004ΕΚ³. Στις αιτιολογικές σκέψεις του εν λόγω κανονισμού, διατυπώνεται η παραδοχή ότι «οι ηλεκτρονικοί υπολογιστές και η δικτύωση έχουν τώρα γίνει πανταχού

¹ Βλ. *Κωνσταντίνο Π. Θεοδωρίδη*, European Network and Information Security Agency, Η εξασφάλιση της ΕΕ ξεκινά από το Ηράκλειο, ΔΙΜΕΕ 2005, σελ. 394.

² Μιχάλης Δερτούζος, διευθυντής του Εργαστηρίου Επιστήμης των Υπολογιστών στο Ινστιτούτο Τεχνολογίας της Μασαχουσέτης των ΗΠΑ (MIT), βλ. ειδικότερα *Κωνσταντίνο Π. Θεοδωρίδη*, ό.π., όπου και περαιτέρω παραπομπές.

³ Κανονισμός 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 10^{ης} Μαρτίου 2004, *Για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών*.

παρούσες υποδομές, ακριβώς όπως συνέβη με την ηλεκτροδότηση και την ύδρευση»⁴. Ως εκ τούτου, η ασφάλεια των δικτύων επικοινωνιών και των συστημάτων πληροφοριών, ιδίως η διαθεσιμότητά τους, αποτελεί για την κοινωνία αιτία ολοένα και μεγαλύτερης ανησυχίας, λόγω κυρίως της πιθανότητας να ανακύψουν προβλήματα σε βασικά συστήματα πληροφοριών, που να οφείλονται στην πολυπλοκότητα των συστημάτων, σε ατυχήματα, σφάλματα και επιθέσεις, και τα οποία μπορούν να έχουν συνέπειες για την υλική υποδομή παροχής υπηρεσιών ζωτικής σημασίας για την ευημερία των πολιτών της Ευρωπαϊκής Ένωσης. Στο πλαίσιο αυτό ιδρύθηκε ο Ευρωπαϊκός Οργανισμός για την ασφάλεια δικτύων και πληροφοριών⁵, με σκοπό να λειτουργεί ως σημείο αναφοράς και να εμπνέει εμπιστοσύνη χάρη στην ανεξαρτησία του, την ποιότητα των συμβουλών που θα παρέχει και των πληροφοριών που θα διαδίδει, τη διαφάνεια των διαδικασιών και του τρόπου λειτουργίας του, καθώς επίσης και την ταχύτητά του κατά την εκτέλεση των καθηκόντων που του έχουν ανατεθεί⁶.

Αρκετά χρόνια αργότερα, και έχοντας μεσολαβήσει σημαντικές τεχνολογικές εξελίξεις, ο Ενωσιακός νομοθέτης επανήλθε στο θέμα της ασφάλειας των ηλεκτρονικών δικτύων με τις οδηγίες 2009/140/EK και 2009/136/EK, με τις οποίες καθιερώθηκε η ρητή υποχρέωση των κρατών μελών να μεριμνούν, ώστε οι πάροχοι δημοσίων δικτύων ηλεκτρονικών επικοινωνιών να λαμβάνουν τα απαιτούμενα μέτρα για την ασφάλεια και την ακεραιότητα των δικτύων τους. Ειδικότερα, με την οδηγία 2009/140/EK προβλέπεται η υποχρέωση των κρατών μελών να μεριμνούν ώστε οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό να λαμβάνουν πρόσφορα τεχνικά και

⁴ Βλ. αιτιολογική σκέψη υπ' αρ. 1 του Κανονισμού 460/2004.

⁵ Ο νέος αυτός οργανισμός που ονομάστηκε ENISA (European Network and Information Security Agency), ιδρύθηκε στις 14.03.2004, με προσωρινή έδρα στις Βρυξέλλες. Το Δεκέμβριο του 2004, ορίστηκε με απόφαση της συνόδου του Ευρωπαϊκού Συμβουλίου, η οριστική έδρα του στις Βούτες Ηρακλείου, όπου και μεταφέρθηκε και λειτουργεί έκτοτε από το Σεπτέμβριο του 2005. Έτσι, ο ENISA έγινε ο δεύτερος οργανισμός της Ευρωπαϊκής Ένωσης, μετά το CEDEFOP στη Θεσσαλονίκη, που φιλοξενείται στην ελληνική επικράτεια, βλ. ειδικότερα *Κωνσταντίνο Π. Θεοδωρίδη*, ό.π. Ακολουθώντας, με τον Κανονισμό 1007/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24^{ης} Σεπτεμβρίου 2008 και με τον Κανονισμό 580/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8^{ης} Ιουνίου 2011, παρατάθηκε η διάρκεια του ENISA.

⁶ Βλ. αιτιολογική σκέψη υπ' αρ. 11 του Κανονισμού 460/2004.

οργανωτικά μέτρα για την κατάλληλη διαχείριση του κινδύνου σχετικά με την ασφάλεια των δικτύων και υπηρεσιών αυτών. Επίσης, με την οδηγία 2009/136/EK, διευρύνθηκε η υποχρέωση των παρόχων διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα επικοινωνιών να λαμβάνουν μέτρα για την ασφάλεια των προσωπικών δεδομένων σε σχέση με τις υπηρεσίες που παρέχουν.

Σε εθνικό επίπεδο, ο Έλληνας νομοθέτης, μετά την πολυετή σιωπή του μετά το π.δ. 131/2003, το οποίο αποτελεί ενσωμάτωση ευρωπαϊκής νομοθεσίας⁷, επανήλθε με τον «πολυνόμο» 4070/2012, με τον οποίο μεταξύ πλήθους άλλων ρυθμίσεων, ενσωμάτωσε και τις ανωτέρω οδηγίες 2009/140/EK και 2009/136/EK. Ενόψει, δε, αυτών των νομοθετικών αλλαγών, εκδόθηκαν νέες κανονιστικές πράξεις από τις αρμόδιες ανεξάρτητες αρχές, οι οποίες προβλέπουν τα ειδικά μέτρα που θα πρέπει να λαμβάνουν οι πάροχοι ηλεκτρονικών δικτύων προς εκπλήρωση της υποχρέωσής τους να μεριμνούν για την ασφάλεια των δικτύων τους⁸.

Μάλιστα, υπό το πρίσμα των ανωτέρω νομοθετικών ρυθμίσεων, υποστηρίζεται ότι, πλέον η ασφάλεια των ηλεκτρονικών δικτύων δεν αποτελεί απλώς παρεπόμενη υποχρέωση των παρόχων, που εξαντλείται στην υποχρέωση ενημέρωσης του εκάστοτε χρήστη⁹ για την ανασφάλεια του δικτύου τους. Αντιθέτως, οι πάροχοι που δραστηριοποιούνται στα ηλεκτρονικά δίκτυα διαφαίνεται ότι φέρουν ένα είδος οιονεί αντικειμενικής ευθύνης να τηρούν τις διατάξεις του νόμου, ώστε να διασφαλίζεται για τους χρήστες των δικτύων τους ένα ικανοποιητικό επίπεδο ασφάλειας. Η εν λόγω υποχρέωση αφορά: α) τη διάσταση των ηλεκτρονικών επικοινωνιών, δηλαδή την εξασφάλιση ικανοποιητικού επιπέδου ως προς την τεχνική υποδομή του δικτύου, β) τη διάσταση της προστασίας των προσωπικών δεδομένων, δηλαδή να μην προκαλείται ανασφάλεια ή να μη θίγεται η ακεραιότητα των

⁷ Συγκεκριμένα αποτελεί ενσωμάτωση της οδηγίας 2000/31/EK.

⁸ Βλ. ΑΔΑΕ απόφαση υπ' αρ. 205/2013 (ΦΕΚ Β' 1742/15-7-2013) και απόφαση υπ' αρ. 675/2013 (ΦΕΚ Β' 107/24-1-2013).

⁹ Βλ. Γιώργο Ν. Γιαννόπουλο, Η ευθύνη των παρόχων υπηρεσιών στο Internet, Η ανατροπή της ασυλίας τους από τη νομοθεσία για: ηλεκτρονικές επικοινωνίες (μετά το ν. 4070/2012), προστασία προσωπικών δεδομένων, απόρρητο επικοινωνιών, πνευματική ιδιοκτησία, εκδ. Νομική Βιβλιοθήκη, Αθήνα 2013, σελ. 60.

δικτύων λόγω παράνομης ή αθέμιτης επεξεργασίας προσωπικών δεδομένων και γ) τη διάσταση της προστασίας του απορρήτου¹⁰. Σύμφωνα με την περιγραφή αυτή, σημαντικός αριθμός παράνομων ενεργειών θα μπορούσε να υποστηριχθεί ότι εμπίπτει στην έννοια της «ασφάλειας και ακεραιότητας των δικτύων».

Σκοπός της παρούσας εργασίας είναι ο προσδιορισμός της έκτασης καθήκοντος – επιμέλειας του παρόχου ηλεκτρονικού δικτύου σχετικά με τη λήψη μέτρων ασφαλείας που προστατεύουν την ακεραιότητα των δικτύων από κακόβουλες ενέργειες τρίτων και η ευθύνη του από την ύπαρξη σχετικών ελλείψεων ασφαλείας του δικτύου. Ιδίως θα ασχοληθούμε με τη ρύθμιση του άρθρου 37 του ν. 4070/2012, η οποία υποστηρίζεται ότι «αντικειμενικοποιεί», κατά κάποιον τρόπο, την ευθύνη των παρόχων για ασφαλή ηλεκτρονικά δίκτυα, καθώς την ανάγει σε κύρια συμβατική τους υποχρέωση. Παράλληλα, θα μας απασχολήσει η διαφορετική μεταχείριση των παρόχων αναφορικά με την προστασία των προσωπικών δεδομένων στα δίκτυα ηλεκτρονικών επικοινωνιών και υπηρεσιών, όπως αυτή αποτυπώνεται στο άρθρο 12 του ν. 3471/2006, η οποία επίσης, κατά παράδοξο τρόπο, εισήχθη με τον ίδιο ν. 4070/2012. Στο πλαίσιο αυτό, θα επιχειρηθεί μία σύγκριση των ανωτέρω διατάξεων προκειμένου να καταλήξουμε στον προσδιορισμό της ευθύνης των παρόχων ηλεκτρονικών δικτύων σύμφωνα τα σημερινά δεδομένα.

Αντιθέτως, η έρευνά μας δε θα επεκταθεί στο χώρο της ποινικής ευθύνης των παρόχων των ηλεκτρονικών δικτύων, ούτε στην αναζήτηση της ευθύνης των τρίτων που προβαίνουν σε παραβίαση της ασφάλειας και επηρεάζουν την ακεραιότητα των δικτύων. Περαιτέρω, αντικείμενο της παρούσας εργασίας δεν είναι η διάσταση της προστασίας του απορρήτου, ούτε η εξασφάλιση της αποτελεσματικής προστασίας της πνευματικής ιδιοκτησίας στα ηλεκτρονικά δίκτυα. Επίσης, δε θα ασχοληθούμε με τις προσβολές της προσωπικότητας, οι οποίες πραγματοποιούνται μέσω των ηλεκτρονικών δικτύων.

¹⁰ Βλ. Γιώργο Ν. Γιαννόπουλο, ό.π.

2. ΟΡΙΣΜΟΣ ΤΗΣ ΕΝΝΟΙΑΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΔΙΚΤΥΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ.

Πριν προχωρήσουμε στην ανάλυση της σχετικής νομοθεσίας, που αναφέρεται στην έκταση της ευθύνης των παρόχων ηλεκτρονικών δικτύων, είναι σκόπιμο να ασχοληθούμε με τον προσδιορισμό της έννοιας της ασφάλειας δικτύων ηλεκτρονικών υπολογιστών και πληροφοριών.

Σύμφωνα με τον διεθνώς αποδεκτό ορολογικό προσδιορισμό της¹¹ και όπως ρητά προβλέπεται στον κανονισμό 460/2004ΕΚ¹² ασφάλεια δικτύων και πληροφοριών είναι η δυνατότητα ενός δικτύου ή ενός συστήματος πληροφοριών να ανθίσταται, σε συγκεκριμένο επίπεδο εμπιστοσύνης, σε ατυχήματα ή σε παράνομες ή κακόβουλες δράσεις, οι οποίες θέτουν σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα και την εμπιστευτικότητα, όσον αφορά τα δεδομένα που έχουν αποθηκευτεί ή μεταδίδονται, καθώς και τις σχετικές υπηρεσίες που προσφέρονται από τα εν λόγω δίκτυα ή συστήματα ή είναι προσβάσιμες μέσω αυτών.

Ο ανωτέρω ορισμός ακολουθεί το τρίπτυχο της CIA (Confidentiality, Integrity, Availability)¹³. Ειδικότερα, η έννοια της ασφάλειας απαρτίζεται από τρεις υποκείμενες έννοιες και δη:

Α) Από την έννοια της **Εμπιστευτικότητας** (confidentiality)¹⁴, η οποία συνίσταται στην προστασία των επικοινωνιών ή των αποθηκευμένων δεδομένων από την υποκλοπή και την ανάγνωση από μη εξουσιοδοτημένα πρόσωπα.

¹¹ Βλ. *Σωκράτη Κάτσικα*, Ασφάλεια Υπολογιστών, Τόμος α', σελ. 49-50, Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα 2001.

¹² Βλ. Κανονισμό 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 10^{ης} Μαρτίου 2004, *Για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών*, άρθρο 4, περίπτωση (γ).

¹³ Βλ. *Ανάργυρο Χρυσάνθου*, Κεφάλαιο 19^ο- Ζητήματα Ασφαλείας Δεδομένων, σε Λεωνίδας Γ. Κοτσαλής, *Προσωπικά Δεδομένα*, σελ. 383-384, Νομική Βιβλιοθήκη, έκδ. 2016.

¹⁴ Βλ. *Gary Stoneburner*, NIST, SP 800-33:Computer Security, NIST, December 2001, σελ. 2 – 5, Κανονισμός 460/2004, άρθρο 4, περίπτωση (ζ).

Β) Από την έννοια της **Ακεραιότητας** (integrity)¹⁵, η οποία αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και στην αποτροπή της πρόσβασης ή/και χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια.

Γ) Από την έννοια της **Διαθεσιμότητας** (availability)¹⁶, η οποία έγκειται στην εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών, όποτε αυτό απαιτείται ή όποτε οι τελευταίοι το απαιτούν¹⁷.

Άμεσο συμπλήρωμα του ανωτέρω ορισμού της ασφάλειας αποτελεί η αρχή της «μη αποκήρυξης» (non-repudiation). Αναλυτικότερα, πρόκειται για μία αρχή με βάση την οποία ένα άτομο ή μία οντότητα δεν μπορεί να αρνηθεί ότι προέβη σε μία ενέργεια. Για παράδειγμα, ο παραλήπτης ενός μηνύματος δεν μπορεί να αρνηθεί ότι παρέλαβε το μήνυμα¹⁸.

Οι προαναφερόμενες αρχές αποτελούν τις συνιστώσες, που συνθέτουν την έννοια της ασφάλειας και οι οποίες, καταρχήν, έχουν την ίδια βαρύτητα. Όμως, είναι δυνατόν, ανάλογα με τη συγκεκριμένη περίπτωση, να δίνεται μεγαλύτερη έμφαση σε μία από αυτές. Έτσι, σε διαφορετικά συστήματα, που εξυπηρετούν διαφορετικούς σκοπούς, προσδίδεται μεγαλύτερη σημασία σε μία ή περισσότερες από τις ανωτέρω τρεις αρχές. Για παράδειγμα, στην περίπτωση του παρόχου υπηρεσιών internet (ISP), δίνεται μεγαλύτερη

¹⁵Βλ. Dieter Gollman, Computer Security, Wiley, 1999, σελ. 5-9, Ronald L. Krutz, Russell Dean Vines, The CISSP Pre Guide: Mastering the Ten Domains of Computer Security, Wiley, 2001, σελ. 1-3.

¹⁶ Βλ. Dieter Gollman, ό.π., Ronald L. Krutz, ό.π, Κανονισμός 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 10^{ης} Μαρτίου 2004, Για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών, άρθρο 4, περίπτωση (δ).

¹⁷ Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι, είτε προσωρινά, είτε μόνιμα. Η άρνηση υπηρεσιών δεν προκαλείται αναγκαία από εχθρική επίθεση. Για παράδειγμα, το ίδιο αποτέλεσμα προκαλείται από το φαινόμενο Slashdot, κατά το οποίο ένας σύνδεσμος προς μια ιστοσελίδα φιλοξενούμενη σε διακομιστή με σύνδεση χαμηλής χωρητικότητας δημοσιεύεται σε δημοφιλή ιστότοπο, με συνέπεια εκατοντάδες χιλιάδες αναγνώστες να υπερφορτώσουν τη σύνδεση της αναφερομένης ιστοσελίδας.

¹⁸ Βλ. Ανάργυρο Χρυσάνθου, ό.π., σελ. 384.

βαρύτητα στην εξασφάλιση της Διαθεσιμότητας του δικτύου. Αντιθέτως, στην περίπτωση του στρατού, δίνεται έμφαση στην Εμπιστευτικότητα του δικτύου του, καθώς μόνο εξουσιοδοτημένοι χρήστες θα πρέπει να έχουν πρόσβαση στις πληροφορίες που διακινούνται σε αυτό. Εδώ, μάλιστα, υπάρχει και κατηγοριοποίηση πρόσβασης, καθώς διαφορετικά άτομα έχουν και διαφορετικού επιπέδου πρόσβαση στην διακινούμενη πληροφορία. Αντιθέτως, οι περισσότερες επιχειρήσεις θα πρέπει να δίνουν έμφαση και στις τρεις αυτές αρχές, με ίσως λίγο μεγαλύτερη στην Ακεραιότητα των δεδομένων τους.

II. Η ΕΥΘΥΝΗ ΤΟΥ ΠΑΡΟΧΟΥ ΔΙΚΤΥΟΥ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ ΣΥΜΦΩΝΑ ΜΕ ΤΙΣ ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ (ΑΚ, Ν. 2251/1994).

1. ΕΝΔΟΣΥΜΒΑΤΙΚΗ ΕΥΘΥΝΗ.

Ο πάροχος συνδέεται με τον χρήστη-πελάτη του με ορισμένη συμβατική σχέση, από την οποία απορρέουν ορισμένα δικαιώματα και υποχρεώσεις και συγκεκριμένα, οι υποχρεώσεις του παρόχου σχετικά με την ποιότητα και τις ιδιότητες των παρεχόμενων υπηρεσιών. Ως εκ τούτου, η ευθύνη του παρόχου λόγω προβλημάτων που σχετίζονται με την έλλειψη ασφάλειας στο ηλεκτρονικό δίκτυο, καθώς επίσης και η υποχρέωσή του να προβαίνει στην λήψη των αναγκαίων προληπτικών μέτρων για τη θωράκιση του δικτύου, βρίσκεται σε άμεση συνάρτηση με το είδος και το περιεχόμενο της καταρτισθείσας συμβάσεως.

Η νομική φύση της σύμβασης παροχής δικτύου εξαρτάται προεχόντως από την εκάστοτε βούληση των μερών. Επιπροσθέτως, καθοριστική για τον προσδιορισμό της νομικής φύσης της σύμβασης είναι και η αντικειμενική σημασία¹⁹ τυχόν προβλεπόμενων περισσότερων παροχών²⁰. Λαμβάνοντας, λοιπόν, υπόψη τα ανωτέρω κριτήρια και τις συγκεκριμένες συνθήκες της κάθε

¹⁹ Βλ. *Κωνσταντίνο Χριστοδούλου*, Αστική Ευθύνη του παρόχου δικτύου ως μεσάζοντος στην παροχή υπηρεσιών της κοινωνίας της πληροφορίας, ΔΙΜΕΕ 2004, σελ. 351.

²⁰ Π.χ. επιπρόσθετων παροχών λογισμικού, υπηρεσιών ηλεκτρονικού ταχυδρομείου, εξοπλισμού (hardware) κλπ.

περίπτωσης θα πρέπει να γίνεται η υπαγωγή σε ορισμένο από τους γνωστούς συμβατικούς τύπους ή σε περισσότερους, εάν πρόκειται για μικτή σύμβαση. Επίσης, ανάλογα με το είδος του προβλήματος που θα προκαλείται από τις ενέργειες τρίτων, εξαιτίας των ελλείψεων ασφάλειας του δικτύου, θα πρέπει να κρίνεται αν πρόκειται για αδυναμία εκπλήρωσης, υπερημερία ή πλημμελή εκπλήρωση, προκειμένου να γίνεται υπαγωγή στις οικείες διατάξεις.

Ειδικότερα, έχει υποστηριχθεί²¹ ότι η σύμβαση παροχής υπηρεσιών δικτύου ενέχει το στοιχείο της διαμεσολάβησης και ως εκ τούτου, συνιστά –με την κοινοτική έννοια του όρου²²- σύμβαση παροχής υπηρεσιών. Περαιτέρω, διατυπώθηκε η άποψη²³ ότι η εν λόγω σύμβαση αποτελεί *suì generis* σύμβαση, η οποία ρυθμίζεται καθοριστικά από την τηλεπικοινωνιακή νομοθεσία και θεωρείται υπό τους όρους του ΑΚ ως μικτή, αμφοτεροβαρής, διαρκής σύμβαση, που περιέχει στοιχεία εντολής, μίσθωσης πράγματος, μίσθωσης έργου και ανεξάρτητων υπηρεσιών.

Επίσης, γίνεται δεκτό²⁴ ότι η σύμβαση παροχής υπηρεσιών δικτύου παρουσιάζει προεχόντως τα χαρακτηριστικά της σύμβασης μίσθωσης πράγματος. Ειδικότερα, σημειώνεται ότι το δίκτυο, ως πράγμα ή προσοδοφόρο έννομο αγαθό είναι δυνατόν να αποτελέσει αντικείμενο σύμβασης μίσθωσης. Πολλώ δε μάλλον, καθόσον σε κάθε περίπτωση σύμβασης παροχής δικτύου, κοινό χαρακτηριστικό της παροχής του μεσάζοντος-παρόχου είναι η χορήγηση στον πελάτη-χρήστη ενός κωδικού (password) για την πρόσβαση στο δίκτυο. Με την έννοια αυτή, η σύμβαση παροχής δικτύου θα διέπεται καταρχήν από τις διατάξεις του ΑΚ 574 επ., η δε σχετική ευθύνη του παρόχου δεν υπόκειται σε οιαδήποτε βραχεία

²¹ Βλ. Γιώργο Ν. Γιαννόπουλο, ό.π., σελ. 44, Κωνσταντίνο Χριστοδούλου, ό.π.

²² Ως υπηρεσία ορίζεται σύμφωνα με το άρθρο 57 ΣΛΕΕ (πρώην 50 της ΣυνθΕΚ) «...κάθε μη μισθωτή οικονομική δραστηριότητα, που παρέχεται κατά κανόνα έναντι αμοιβής», βλ. Γιώργο Ν. Γιαννόπουλο, ό.π., υποσ. 187.

²³ Βλ. Ιωάννη Καρακώστα, Δίκαιο και Internet, Νομικά ζητήματα του διαδικτύου, εκδ. Δίκαιο & Οικονομία. Π. Ν. Σάκκουλας, Αθήνα 2003, σελ. 25 επ., του ιδίου, Το δίκαιο του internet, ΝοΒ 1998, σελ. 1174 επ.

²⁴ Βλ. Κωνσταντίνο Χριστοδούλου, Επιτομή Ηλεκτρονικού Αστικού Δικαίου, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή 2013, σελ. 76-77, ιδίου, Αστική Ευθύνη του παρόχου δικτύου ως μεσάζοντος στην παροχή υπηρεσιών της κοινωνίας της πληροφορίας, ό.π., σελ. 351 επ.

παραγραφή²⁵. Σύμφωνα με την ως άνω άποψη²⁶, ο πάροχος του δικτύου θα ευθύνεται σε αποζημίωση καταρχήν για κάθε υπαίτια εκ μέρους του ανασφάλεια του δικτύου σύμφωνα με το άρθρο 577 εδάφιο β' ΑΚ. Βέβαια, δεν θα ευθύνεται, αν - χωρίς υπαιτιότητά του - τρίτος απέκτησε τον κωδικό πρόσβασης (password) και έτσι έχει ακώλυτη πρόσβαση στο δίκτυο, όπως συνάγεται από το άρθρο 596 εδάφιο α' ΑΚ. Επίσης, ο πελάτης - χρήστης δικαιούται, σύμφωνα με τα προβλεπόμενα στο άρθρο 576 εδάφιο α' ΑΚ, να αποδεσμευθεί μερικά ή ολικά και ειδικότερα, να καταγγείλει, να μην καταβάλει ή να μειώσει τα τέλη πρόσβασης-μίσθωμα, αν το μίσθιο δεν είναι κατάλληλο για τη συμφωνημένη χρήση, δηλαδή αν δεν είναι ασφαλές. Αντιθέτως, ο χρήστης δεν απαλλάσσεται των τελών πρόσβασης, αν η πρόσβασή του στο δίκτυο κωλύεται από λόγους που αφορούν τον ίδιο κατά το άρθρο 596 εδάφιο α' ΑΚ. Σχετικά με την εφαρμογή της εν λόγω διάταξης, σημειώνουμε ότι αφορά μόνον στην καταβολή του μισθώματος, δηλαδή του ανταλλάγματος για την πρόσβαση στο δίκτυο και δη για όσο χρόνο διαρκεί το «κώλυμα» στην πρόσβαση. Δεν καλύπτει άλλες «περαιτέρω» ζημίες του χρήστη εξαιτίας του κωλύματος αυτού, οι οποίες αναφέρονται, όχι στην αξία της πρόσβασης καθ' αυτής, αλλά σε άλλα αγαθά του χρήστη, προσωπικά ή περιουσιακά (π.χ. φήμη, λογισμικό, προσωπικά δεδομένα κ.ά.), που διακυβεύθηκαν ή προσβλήθηκαν από το συγκεκριμένο «κώλυμα» στην πρόσβαση.

Υπό την έννοια του ανωτέρω άρθρου, ως «κώλυμα» της πρόσβασης στο δίκτυο, ήτοι της χρήσης του μισθίου, θα πρέπει να νοηθεί οποιαδήποτε πλημμέλεια ή ανασφάλεια του δικτύου, στο μέτρο που αυτή εμποδίζει την «κατάλληλη», δηλαδή, την ασφαλή για το μισθωτή - χρήστη χρήση του. Περαιτέρω, στο πλαίσιο αυτό, ως λόγος αφορών στο πρόσωπο του μισθωτή-χρήστη θα πρέπει να νοηθεί κάθε γεγονός που δεν οφείλεται ούτε σε

²⁵ Βλ. *Κωνσταντίνο Χριστοδούλου*, ό.π., υποσ. 24, ο οποίος επικαλείται από τη νομολογία την υπ' αρ. 664/2004 απόφαση του ΜΠΑ (αδμ.), κατά την οποία η εκδίκαση των σχετικών διαφορών υπάγεται στη διαδικασία των άρθρων 647 ΚΠολΔ επ.. Ωστόσο, βλ. *Γιώργο Ν. Γιαννόπουλο*, ό.π., υποσ. 189, ο οποίος θεωρεί ότι δεν μπορεί να γίνει επίκληση της ανωτέρω αποφάσεως για την υπαγωγή της συμβάσεως παροχής δικτύου στη σύμβαση της μίσθωσης, καθόσον δεν αφορά σε κλασική σύμβαση πρόσβασης, αλλά ειδικώς σε μίσθωση συγκεκριμένου τηλεπικοινωνιακού κυκλώματος (leased line) και επομένως δεν υπάρχει αντιστοιχία.

²⁶ Βλ. *Κωνσταντίνο Χριστοδούλου*, ό.π., *Επιτομή Ηλεκτρονικού Αστικού Δικαίου*, εκδ. Αντ. Ν. Σάκουλα, Αθήνα-Κομοτηνή 2013, σελ. 352.

υπαιτιότητα του παρόχου ή παράβαση των υποχρεώσεών του, ούτε σε γενικούς λόγους αναφερόμενους στο όλο δίκτυο. Υπαιτιότητα του χρήστη δεν είναι αναγκαία. Αρκεί το κώλυμα να ανέκυψε ως εκ της χρήσεως του δικτύου εκ μέρους του πελάτη κι όχι από εγγενή ελαττώματα του συστήματος πρόσβασης. Το ίδιο θα πρέπει να γίνει δεκτό και στην περίπτωση που το κώλυμα ή η ανασφάλεια του δικτύου ανέκυψε μεν από λόγους ανεξάρτητους από τον πελάτη, αλλά ο τελευταίος παρέλειψε να ειδοποιήσει σχετικώς τον πάροχο όπως όφειλε (ΑΚ 589, 336β), με αποτέλεσμα να εξακολουθεί η πλημμέλεια, η οποία σε διαφορετική περίπτωση θα αντιμετωπιζόταν²⁷. Συνεπώς, με βάση τα παραπάνω δεδομένα, θα μπορούσε κανείς να καταλήξει²⁸ στο συμπέρασμα ότι σε κάθε περίπτωση ανασφαλούς πρόσβασης στο δίκτυο και ανεξάρτητα από το στοιχείο της υπαιτιότητας, ο πελάτης-χρήστης θα δικαιούται είτε να επικαλεστεί τη διάταξη 576 εδάφιο α' ΑΚ αιτούμενος τη μείωση του τιμήματος, είτε να καταγγείλει τη σύμβαση κατ' άρθρο 585 ΑΚ.

Επιπροσθέτως, έχει διατυπωθεί η άποψη²⁹ ότι η δογματική υπαγωγή της σύμβασης πρόσβασης δικτύου σε μία και μόνο συγκεκριμένη επώνυμη σύμβαση του ΑΚ, και μάλιστα στη σύμβαση μίσθωσης, δε φαίνεται να δίνει ικανοποιητική λύση στο πρόβλημα. Πρώτον, διότι οι περισσότερες περιπτώσεις προβλημάτων ασφάλειας ή ακεραιότητας του δικτύου, που καθιστούν τελικώς πλημμελή ή μη προσήκουσα την πρόσβαση, οφείλονται σε δραστηριότητα τρίτων, οπότε δεν είναι δυνατόν να προσδιοριστεί ποιος (ο ενδιάμεσος-εκμισθωτής ή ο χρήστης-μισθωτής) είχε καθήκον να λάβει μέτρα προστασίας, ώστε να υπάρξει ανάλογη εφαρμογή της διάταξης 596 εδάφιο α'. Δεύτερον, διότι στη βασική σχέση μεταξύ χρήστη και παρόχου που επιτρέπει την πρόσβαση ως εμπορική δραστηριότητα, οι υποχρεώσεις των μερών αποτυπώνονται συνήθως συμβατικώς. Όμως, αυτό δεν είναι απαραίτητο κατά την πρόσβαση σε ενδιάμεσους παρόχους που απλώς προσφέρουν

²⁷ Βλ. Κωνσταντίνο Χριστοδούλου, ό.π., σελ. 353.

²⁸ Βλ. Κωνσταντίνο Χριστοδούλου, ό.π.

²⁹ Βλ. Γιώργο Ν. Γιαννόπουλο, ό.π., σελ. 45.

περιεχόμενο³⁰. Το ίδιο ισχύει και για τους παρόχους που επιτρέπουν την πρόσβαση στο διαδίκτυο (π.χ. πανεπιστήμια, οργανισμοί), με τους οποίους οι χρήστες δεν έχουν συνάψει τυπική σύμβαση, ειδικώς για τους κανόνες πρόσβασης. Ακόμα δυσκολότερη είναι η περιστασιακή πρόσβαση σε ανοικτά δίκτυα (wi-fi). Σε όλες αυτές τις περιπτώσεις, δεν υπάρχει συνήθως τυπική συμβατική καταγραφή των υποχρεώσεων των μερών, ενώ τις περισσότερες φορές, οι πάροχοι φροντίζουν να περιορίζουν την ευθύνη τους με μονομερείς ρήτρες, ενταγμένες σε ΓΟΣ, που αναρτούν κάθε φορά στην οικεία ιστοσελίδα.

Συνεπώς, ενόψει των ανωτέρω, και υπό τις επιφυλάξεις του ιδιωτικού διεθνούς δικαίου σχετικά με το ισχύον κάθε φορά δίκαιο, η περαιτέρω έρευνα της νομικής φύσης της σύμβασης παροχής υπηρεσιών δικτύου δεν επιλύει το πρόβλημα της ευθύνης του παρόχου για ελλείψεις στην ασφάλεια του δικτύου. Έτσι, για μεν την περίπτωση της παροχής υπηρεσιών φιλοξενίας³¹, δηλαδή της παραχώρησης χώρου που συνίσταται σε μνήμη και ισχύ του επεξεργαστή του υπολογιστή, η υπαγωγή στην έννοια της μίσθωσης πράγματος αποτελεί ικανοποιητική λύση. Όμως, για τις υπόλοιπες περιπτώσεις παροχής υπηρεσιών ηλεκτρονικού δικτύου, παρίσταται³² ως μάλλον καταλληλότερη επιλογή, η ad hoc αναζήτηση της εκάστοτε βούλησης των μερών και η αντικειμενική σημασία των τυχόν προβλεπόμενων παροχών-υπηρεσιών, πέραν των βασικών. Υπό το πρίσμα αυτό, θα πρέπει να κριθεί τόσο η έκταση της υποχρέωσης του παρόχου για την ασφάλεια του δικτύου, όσο οι τυχόν οφειλόμενες υπηρεσίες προστασίας ή ασφάλειας, οι οποίες έχουν συμφωνηθεί στο πλαίσιο της σύμβασης.

2. ΛΟΙΠΕΣ ΝΟΜΙΚΕΣ ΒΑΣΕΙΣ ΘΕΜΕΛΙΩΣΗΣ ΤΗΣ ΕΥΘΥΝΗΣ ΤΟΥ ΠΑΡΟΧΟΥ.

Εκτός από τη νομική βάση της ενδοσυμβατικής ευθύνης, η ευθύνη του παρόχου ηλεκτρονικού δικτύου λόγω ελλείψεων στην ασφάλεια, θα μπορούσε

³⁰ Όπως για παράδειγμα μηχανισμοί έρευνας, εγκυκλοπαίδειες, ιστολόγια, ιστοσελίδες κοινωνικής δικτύωσης, ιστοσελίδες δημοπρασιών.

³¹ Βλ. ειδικότερα Κεφάλαιο ΙΙΙ της παρούσας, Ενότητες 1 και 2.

³² Βλ. Γιώργο Ν. Γιαννόπουλο, ό.π., σελ. 46.

να θεμελιωθεί και στις διατάξεις για την αδικοπραξία, αλλά και στις ευρύτερης προστασίας διατάξεις για τον καταναλωτή και τα προσωπικά δεδομένα. Επισημαίνεται, δε, ότι ανάλογα με το είδος και το αποτέλεσμα της έλλειψης στην ασφάλεια του ηλεκτρονικού δικτύου, η ευθύνη του παρόχου δύναται να θεμελιώνεται και σε ειδικότερες διατάξεις, όπως σε αυτές για την προστασία της πνευματικής ιδιοκτησίας, για την προστασία των σημάτων, καθώς και στις διατάξεις για την προσβολή της προσωπικότητας³³.

Ειδικότερα, η θεμελίωση της ευθύνης του παρόχου στη νομική βάση της αδικοπραξίας παρουσιάζει δυσκολία, η οποία έγκειται κυρίως στην απόδειξη της ζημίας του χρήστη. Περαιτέρω, εξίσου δυσχερής είναι και η απόδειξη του αιτιώδους συνδέσμου μεταξύ της παράνομης συμπεριφοράς του παρόχου, η οποία εντοπίζεται στην παράλειψή του να λάβει τα απαιτούμενα μέτρα προκειμένου να καταστεί το δίκτυο ασφαλές απέναντι στις κακόβουλες ενέργειες τρίτων. Με δεδομένο, μάλιστα, το γεγονός ότι οι ζημίες του χρήστη εξαιτίας ελλείψεως ασφαλείας στο δίκτυο θα προκαλούνται, συνήθως, από τη δράση τρίτων προσώπων, ο πάροχος του δικτύου δεν θα ευθύνεται σχετικώς, παρά μόνον λόγω της παράλειψής του να προστατεύσει αποτελεσματικά τον πελάτη του, η οποία προσδιορίζεται από την έκταση του αντιστοίχου, παραπάνω εκτεθέντος συμβατικού «καθήκοντος προστασίας» του δικτύου³⁴. Το ζήτημα αποκτά και τεχνική διάσταση, αφού με την πληθώρα ενδιάμεσων και δωσιδικιών, που μεσολαβούν για την μετάδοση των πληροφοριών στο διαδίκτυο, είναι πολύ δύσκολο να αποδειχθεί ποιος είναι από όλους που ευθύνεται για την έλλειψη στην ασφάλεια³⁵.

Αντιθέτως, ευρύτερη νομική προστασία για τον χρήστη-πελάτη, θα μπορούσε να επιτευχθεί μέσω της θεμελίωσης της ευθύνης του παρόχου είτε στις διατάξεις του άρθρου 8 του ν. 2251/1994 για τη νόθο αντικειμενική ευθύνη του παρέχοντος υπηρεσίες, είτε στη νομοθεσία για τα προσωπικά δεδομένα³⁶.

³³ Όπως ήδη αναφέρθηκε ανωτέρω (Κεφάλαιο I, Ενότητα 1), στο πλαίσιο της παρούσας εργασίας δεν θα εξετασθούν τα ζητήματα προσβολής πνευματικής ιδιοκτησίας, σημάτων και προσωπικότητας.

³⁴ Βλ. *Κωνσταντίνο Χριστοδούλου*, ό.π. σελ. 354.

³⁵ Βλ. *Γιώργο Ν. Γιαννόπουλο*, ό.π., σελ. 47.

³⁶ Βλ. κατωτέρω, κεφάλαιο VI της παρούσας.

Αναλυτικότερα, στο πλαίσιο των σχέσεων των ηλεκτρονικώς επικοινωνούντων μερών μεταξύ τους, ο πάροχος δικτύου ενεργεί ως άγγελος, καταρχήν μεν ενεργητικός (του αποστολέα), άλλοτε δε (και) παθητικός (του αποδέκτη του μηνύματος), σε περίπτωση που έχει συμφωνηθεί διαφορετικά μεταξύ τους, ενώ στην κλιμακωτή προμήθεια δικτύου ενεργεί ως υποάγγελος³⁷. Συνεπώς, ο πάροχος προσφέρει, εν τοις πράγμασι, τις υπηρεσίες και προς τα δύο επικοινωνούντα μέρη, αποστολέα και αποδέκτη, ευθυνόμενος ως εκ τούτου απέναντι και στους δύο, ακόμη και αν δεν τον συνδέει με το καθένα συμβατική σχέση σύμφωνα με το άρθρο 8 ν. 2251/1994.

Έτσι, άσχετα με το αν προϋπόθεση για τη γένεση μιας τέτοιας ευθύνης αποτελεί η παρανομία ή όχι, βέβαιο είναι ότι απαιτείται η παρασχεθείσα υπηρεσία να κριθεί ως αντικειμενικώς πλημμελής, ήτοι, στην προκείμενη περίπτωση, να γίνει δεκτό ότι η παράλειψη του παρόχου να προστατεύσει την ασφάλεια της επικοινωνίας του πελάτη του αντιβαίνει σε αντίστοιχο καθήκον του παρόχου προς προστασία της ασφαλείας της πρόσβασης στο δίκτυο³⁸. Περαιτέρω, προκειμένου να μπορεί να γίνει επίκληση της ως άνω ρυθμίσεως, είναι αναγκαίο να συντρέχουν και οι λοιπές προϋποθέσεις που προβλέπει το πραγματικό της και δη ο χρήστης-πελάτης να είναι καταναλωτής, δηλαδή τελικός αποδέκτης της παρεχόμενης υπηρεσίας. Στο σημείο αυτό, θα πρέπει να σημειώσουμε ότι αν ο πάροχος είναι εγκατεστημένος στην Ελλάδα, για τη σύναψη της σύμβασης θα πρέπει να τηρηθούν ως ελάχιστο περιεχόμενο, τα προβλεπόμενα στον Κώδικα Δεοντολογίας της ΕΕΤΤ για την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών στους καταναλωτές³⁹.

III. Η ΕΥΘΥΝΗ ΤΟΥ ΜΕΣΑΖΟΝΤΟΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΚΤΠ ΣΥΜΦΩΝΑ ΜΕ ΤΟ Π.Δ. 131/2003.

³⁷ Βλ. *Κωνσταντίνο Χριστοδούλου*, ό.π., σελ. 354-355.

³⁸ Βλ. *Κωνσταντίνο Χριστοδούλου*, Ευθύνη του παρόχου δικτύου για προσβολές της ιδιωτικής σφαίρας, ΔΙΜΕΕ 2010, σελ. 329., ιδίου *Επιτομή Ηλεκτρονικού Αστικού Δικαίου*, ό.π., σελ. 78.

³⁹ Βλ. *Γιώργο Ν. Γιαννόπουλο*, ό.π., υποσ. 202.

1. Η ΕΝΝΟΙΑ ΚΑΙ Ο ΡΟΛΟΣ ΤΟΥ ΠΑΡΟΧΟΥ ΥΠΗΡΕΣΙΩΝ ΔΙΑΔΙΚΤΥΟΥ. ΟΙ ΔΙΑΚΡΙΣΕΙΣ ΤΩΝ ΠΑΡΟΧΩΝ ΥΠΗΡΕΣΙΩΝ ΔΙΑΔΙΚΤΥΟΥ.

Ειδική είναι η περίπτωση της ευθύνης του παρόχου υπηρεσιών διαδικτύου (ISP) εξαιτίας ελλείψεως ασφάλειας στο δίκτυό του απέναντι στη δράση τρίτων προσώπων κατά τα ανωτέρω. Συγκεκριμένα, με τον όρο πάροχος υπηρεσιών διαδικτύου νοείται η επιχείρηση η οποία παρέχει στους απλούς χρήστες πρόσβαση σε διάφορες υπηρεσίες διαδικτύου έναντι συνδρομής. Πέραν, δε, της πρόσβασης στο διαδίκτυο, οι επιχειρήσεις αυτές παρέχουν επίσης και πρόσθετες υπηρεσίες, όπως για παράδειγμα διατήρηση ηλεκτρονικού ταχυδρομείου και φιλοξενία ιστοσελίδων⁴⁰.

Σε ευρωπαϊκό επίπεδο, ο νομοθετικός προσδιορισμός του φορέα παροχής υπηρεσιών διαδικτύου αποτυπώθηκε στην οδηγία 2000/31/EK για το ηλεκτρονικό εμπόριο⁴¹ ως κάθε φυσικό ή νομικό πρόσωπο που παρέχει μία υπηρεσία της Κοινωνίας της Πληροφορίας και ενσωματώθηκε αυτούσια στο εθνικό δίκαιο με το π.δ. 131/2003⁴². Περαιτέρω, ως υπηρεσίες της Κοινωνίας της Πληροφορίας ορίζονται οι υπηρεσίες που παρέχονται συνήθως έναντι αμοιβής με ηλεκτρονικά μέσα εξ αποστάσεως και κατόπιν προσωπικής επιλογής ενός αποδέκτη των υπηρεσιών⁴³.

Η διαμεσολάβηση των παρόχων υπηρεσιών διαδικτύου καθίσταται απαραίτητη για τη διενέργεια των οποιωνδήποτε διαδικτυακών συναλλαγών ενόψει του τρόπου λειτουργίας και της τεχνολογίας του διαδικτύου. Αυτό προκύπτει από μία συνοπτική ανάλυση του τρόπου λειτουργίας του διαδικτύου, που δεν είναι τίποτα άλλο από ένα παγκόσμιο δίκτυο διασυνδεδεμένων υπολογιστών, στο οποίο οι ψηφιακές πληροφορίες μεταφέρονται από τον έναν υπολογιστή στον άλλο, μέχρι να φτάσουν στον τελικό τους αποδέκτη. Η μεταφορά αυτή διενεργείται μέσω της αντιγραφής

⁴⁰ Για την έννοια του παρόχου υπηρεσιών διαδικτύου βλ. *Chris Reed*, *Internet Law: Text and Materials*, second edition, Cambridge University Press 2004, σελ. 27 επ., *Φαίνη Κατσανάκη*, Ευθύνη παρόχων υπηρεσιών Internet κατά τη διαμεσολάβηση στη διακίνηση παράνομου υλικού, ΧρΙΔ 2008, σελ. 272.

⁴¹ Βλ. Άρθρο 2 περίπτωση β' της οδηγίας 2000/31/EK για το ηλεκτρονικό εμπόριο.

⁴² Βλ. Άρθρο 1 παράγραφος 1 του π.δ. 131/2003.

⁴³ Βλ. Άρθρο 1 παράγραφος 2 της οδηγίας 1998/34/EK, όπως τροποποιήθηκε από την οδηγία 1998/48/EK και ενσωματώθηκε στο εθνικό δίκαιο με το π.δ. 39/2001, άρθρο 2, παράγραφος 2.

των ψηφιακών πληροφοριών, που στέλνονται σε πακέτα από υπολογιστή σε υπολογιστή, μέσω της χρήσης ενός συνόλου πρωτοκόλλων επικοινωνίας γνωστό ως “TCP/IP”. Το TCP (Transfer Control Protocol) ελέγχει την ανταλλαγή πακέτων των πληροφοριών μεταξύ υπολογιστών, ενώ το IP (Internet Protocol) καθορίζει την κατεύθυνση κάθε πακέτου μέσω ενός συστήματος διευθύνσεων και περιέχει τους κανόνες για την αρίθμηση των πακέτων των δεδομένων, ώστε να διασφαλίζεται ότι ο τελικός αποδέκτης θα τα τοποθετήσει με τη σωστή σειρά⁴⁴.

Ενόψει της ανάλυσης αυτής, γεννάται το ερώτημα ποια θα πρέπει να είναι η ευθύνη των παρόχων υπηρεσιών διαδικτύου, όταν ο ρόλος τους ουσιαστικά περιορίζεται στην αντιγραφή και μετάδοση των πακέτων σύμφωνα με το πρωτόκολλο TCP/IP. Έτσι, έχει υποστηριχθεί η άποψη ότι ο πάροχος υπηρεσιών διαδικτύου δε μεταφέρει δικές του ιδέες, ούτε έχει τη συντακτική ευθύνη των μεταδιδόμενων πληροφοριών, αλλά απλώς διευκολύνει την επικοινωνία, όπως ακριβώς τα κυκλώματα του ΟΤΕ⁴⁵. Η άποψη αυτή επικράτησε, επηρεάζοντας τη διαμόρφωση της ευρωπαϊκής νομοθεσίας και συγκεκριμένα την οδηγία 2000/31/EK για το ηλεκτρονικό εμπόριο, όπως θα δούμε στη συνέχεια, η οποία ακολουθώντας ενσωματώθηκε στα εθνικά δίκαια, καθιερώνοντας τον κανόνα του ανεύθυνου του παρόχου υπηρεσιών διαδικτύου, υπό ορισμένες, βέβαια, προϋποθέσεις. Όμως, προτού αναφερθούμε στη σχετική ευρωπαϊκή και εθνική νομοθεσία και στη δυνάμει αυτών οριοθέτηση της ευθύνης του παρόχου υπηρεσιών διαδικτύου, παρίσταται χρήσιμη η κατηγοριοποίησή τους ανάλογα με το είδος της δραστηριότητάς τους και ακολούθως η συσχέτιση της ανωτέρω κατηγοριοποίησης με την έκταση της προβλεπόμενης ευθύνης τους για την κάθε περίπτωση.

Ειδικότερα, η επιχειρούμενη κατηγοριοποίηση ερείδεται στην τριχοτόμηση της ευθύνης των παρόχων υπηρεσιών διαδικτύου σύμφωνα με το γερμανικό νόμο *Teledienstegesetz* του 1997 για τη χρήση των ηλεκτρονικών πληροφοριακών και επικοινωνιακών υπηρεσιών, όπως αυτός τροποποιήθηκε από την

⁴⁴ Βλ. *Chris Reed*, ό.π., σελ. 8 επ., *Φαίνη Κατσανάκη*, ό.π., σελ. 272.

⁴⁵ Βλ. *Κωνσταντίνο Χριστοδούλου*, Προστασία της προσωπικότητας και της συμβατικής ελευθερίας στα κοινωφελή δίκτυα, εκδόσεις Αντ. Ν. Σάκουλα, Αθήνα – Κομοτηνή 2007, σελ. 46 επ.

ενσωμάτωση της οδηγίας 2000/31/EK. Η κατηγοριοποίηση αυτή βασίζεται στο κριτήριο εάν το διαβιβαζόμενο στο διαδίκτυο περιεχόμενο προέρχεται από τον πάροχο ή αν αυτό είναι ξένο ως προς τον τελευταίο⁴⁶. Έτσι, διακρίνουμε στην πρώτη κατηγορία τους παρόχους πληροφοριών ή περιεχομένου (Content Providers), οι οποίοι είναι πρόσωπα που διοχετεύουν στο διαδίκτυο ίδιες πληροφορίες, είτε με τη μορφή ιστοσελίδας, είτε μέσω ηλεκτρονικών επιστολών (e-mails), είτε κατά τη συμμετοχή σε ομάδες συζητήσεων (newsgroups), οπότε και υπέχουν την ευθύνη για το περιεχόμενο των διοχετευόμενων πληροφοριών κατά τις κείμενες διατάξεις, χωρίς να απαιτείται ειδική διάταξη νόμου που να αφορά στην ευθύνη τους ή να παραπέμπει στις κείμενες διατάξεις. Βέβαια, θα πρέπει να σημειώσουμε ότι κατά την κρατούσα και ορθή άποψη, οι ξένες πληροφορίες καθίστανται ίδιες, όταν επιλέγονται και παρέχονται μετά γνώσεως του περιεχομένου τους⁴⁷. Οι πάροχοι πληροφοριών ή περιεχομένου (Content Providers) διαφοροποιούνται από τους φορείς υπηρεσιών διαδικτύου (Internet Services Providers), με κριτήριο την παροχή στο διαδίκτυο ιδίων ή μη πληροφοριών.

Στην ευρύτερη κατηγορία των φορέων παροχής υπηρεσιών υπάγονται οι πάροχοι υπηρεσιών αποθήκευσης πληροφοριών (Host Service Providers), η δραστηριότητα των οποίων έγκειται στην αποθήκευση των πληροφοριών και οι πάροχοι υπηρεσιών πρόσβασης (Access Providers), η υπηρεσία των οποίων συνίσταται στην απλή μετάδοση των ξένων πληροφοριών ή στην παροχή πρόσβασης στο διαδίκτυο. Η διάκριση μεταξύ των δύο τελευταίων κατηγοριών συνίσταται στον έλεγχο των πληροφοριών, με την έννοια της τεχνικής δυνατότητας ταχείας απόσυρσης των πληροφοριών ή διακοπής πρόσβασης σε αυτές, η οποία δυνατότητα, όπως θα δούμε, τέθηκε ως προϋπόθεση από το νομοθέτη για τον αποκλεισμό της ευθύνης του παρόχου υπηρεσιών αποθήκευσης.

⁴⁶ Βλ. Στέργιο Σπυρόπουλο, Η διάκριση των παρόχων υπηρεσιών στο διαδίκτυο και η οριοθέτηση της ευθύνης τους με βάση την κοινοτική Οδηγία 2000/31/EK σχετικά με το ηλεκτρονικό εμπόριο, ΔΙΜΕΕ 2005, σελ. 372 επ.

⁴⁷ Βλ. Στέργιο Σπυρόπουλο, ό.π., σελ. 374.

2. Η ΕΥΘΥΝΗ ΤΟΥ ΜΕΣΑΖΟΝΤΟΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΚΤΠ ΣΥΜΦΩΝΑ ΜΕ ΤΗΝ ΟΔΗΓΙΑ 2000/31/ΕΚ, ΟΠΩΣ ΕΝΣΩΜΑΤΩΘΗΚΕ ΣΤΟ ΕΘΝΙΚΟ ΔΙΚΑΙΟ ΜΕ ΤΟ Π.Δ. 131/2003.

Ο κοινοτικός νομοθέτης με την οδηγία 2000/31/ΕΚ για το ηλεκτρονικό εμπόριο, έθεσε ως στόχο του την εξάλειψη των νομικών εμποδίων που παρακωλύουν την καλή λειτουργία της εσωτερικής αγοράς και καθιστούν λιγότερο ελκυστική την άσκηση της ελευθερίας εγκατάστασης και της ελευθερίας παροχής υπηρεσιών⁴⁸ στο χώρο του διαδικτύου. Τα εμπόδια αυτά απορρέουν από τις αποκλίσεις των νομοθεσιών, καθώς και από την έλλειψη ασφάλειας δικαίου. Ενόψει των ανωτέρω, η οδηγία 2000/31/ΕΚ πραγματεύεται κυρίως τα ζητήματα εκείνα, τα οποία, κατά την κρίση του νομοθέτη, δημιουργούν προβλήματα στην εσωτερική ευρωπαϊκή αγορά, αποσκοπώντας, σε τελική ανάλυση, στη δημιουργία ενός νομικού πλαισίου για την εξασφάλιση της ελεύθερης κυκλοφορίας των υπηρεσιών της Κοινωνίας της Πληροφορίας⁴⁹.

Στο πλαίσιο αυτό, ρυθμίστηκε και το θέμα της ευθύνης των μεσαζόντων παροχής υπηρεσιών της ΚτΠ με τις διατάξεις των άρθρων 12 έως 15 της οδηγίας 2000/31/ΕΚ. Σε επίπεδο εθνικού δικαίου, οι εν λόγω ρυθμίσεις ενσωματώθηκαν με το π.δ. 131/2003 και δη με τα άρθρα 11 έως 14 αυτού. Μάλιστα, στη ρύθμιση της ευθύνης του παρόχου υπηρεσιών της ΚτΠ, ακολουθείται οριζόντια προσέγγιση του θέματος, δηλαδή ανεξάρτητα από τον κλάδο δικαίου στον οποίο στηρίζεται η ευθύνη του. Επιπροσθέτως, η διαμόρφωση της ευθύνης των παρόχων υπηρεσιών της ΚτΠ βρίσκεται σε συνάρτηση με το είδος των παρεχόμενων υπηρεσιών σύμφωνα με την κατηγοριοποίηση των παρόχων υπηρεσιών διαδικτύου που επιχειρήθηκε στο αμέσως προηγούμενο κεφάλαιο⁵⁰.

Ειδικότερα, η ευθύνη των παρόχων υπηρεσιών αποθήκευσης πληροφοριών (Host Service Providers) ρυθμίζεται από το άρθρο 14 της Οδηγίας 2000/31/ΕΚ, όπως ενσωματώθηκε στο εθνικό δίκαιο με το άρθρο 13 του π.δ.

⁴⁸ Βλ. *Φαίνη Κατσανάκη*, ό.π., σελ. 274.

⁴⁹ Βλ. αιτιολογικές σκέψεις υπ' αριθμόν 5 και 6 του Προοιμίου της οδηγίας 2000/31/ΕΚ.

⁵⁰ Βλ. ενότητα υπό 1 του παρόντος κεφαλαίου.

131/2003, στο οποίο προβλέπεται ως προϋπόθεση για τον αποκλεισμό της ευθύνης ότι ο πάροχος της υπηρεσίας αποθήκευσης δε γνωρίζει πραγματικά⁵¹ ότι πρόκειται για παράνομη δραστηριότητα ή πληροφορία και σε ό,τι αφορά σε αξιώσεις αποζημιώσεως, δε γνωρίζει τα γεγονότα ή τις περιστάσεις από τις οποίες προκύπτει η παράνομη δραστηριότητα ή πληροφορία. Επίσης, ο πάροχος υπηρεσιών αποθήκευσης δεν ευθύνεται εάν, μόλις αντιληφθεί ότι συμβαίνει κάτι από τα προαναφερθέντα περιστατικά, αποσύρει ταχέως τις πληροφορίες ή καθιστά την πρόσβαση σε αυτές αδύνατη. Όμως, τα ανωτέρω δεν εφαρμόζονται, όταν ο αποδέκτης της υπηρεσίας ενεργεί υπό την εξουσία ή τον έλεγχο του παρόχου των υπηρεσιών αποθήκευσης. Προκύπτει, λοιπόν, ότι προκειμένου να πληρούται η πρώτη προϋπόθεση απαλλαγής από την αστική ευθύνη του παρόχου, αρκεί η ευθύνη του να στηρίζεται σε δόλο και όχι σε βαρεία αμέλεια, καθόσον η έλλειψη της γνώσης αναφέρεται στα γεγονότα ή στις περιστάσεις από τις οποίες προέρχεται η παράνομη δραστηριότητα ή πληροφορία και επομένως το κατά πόσο προκύπτει η παράνομη δραστηριότητα ή πληροφορία, θα εξαρτηθεί από τη γνώση των περιστάσεων που τη συναπαρτίζουν⁵².

Περαιτέρω, όσον αφορά στη δεύτερη προϋπόθεση απαλλαγής του παρόχου υπηρεσιών αποθήκευσης, προβλέπεται ότι σε περίπτωση που ο πάροχος αντιληφθεί το παράνομο, οφείλει χωρίς υπαίτια καθυστέρηση να αποσύρει τις πληροφορίες ή να καθιστά αδύνατη την πρόσβαση σε αυτές. Είναι εύλογο, ότι οι παράνομες πληροφορίες θα πρέπει να αποθηκεύονται στο διακομιστή του ιδίου του παρόχου. Η ρύθμιση αυτή έχει υποστεί μεγάλη κριτική, καθώς δε διευκρινίζεται πότε μπορεί να θεωρηθεί ότι ο πάροχος έχει αντιληφθεί το παράνομο υπό την έννοια της διατάξεως, εάν για παράδειγμα αρκεί και απλή ειδοποίηση⁵³, χωρίς να ενδιαφέρει η βασιμότητα αυτής. Στην πράξη, δε, παρατηρείται ότι οι πάροχοι προκειμένου να μπορούν να επικαλεστούν την απαλλαγή της ευθύνης τους, προβαίνουν σε άμεση απόσυρση των

⁵¹ Η έλλειψη παραγματικής γνώσης κατά το γράμμα του νόμου, που ισοδυναμεί με την ύπαρξη άμεσου δόλου τουλάχιστον β' βαθμού, αφορά στη στοιχειοθέτηση της ποινικής ευθύνης του παρόχου υπηρεσιών αποθήκευσης.

⁵² Βλ. Στέργιο Σπυρόπουλο, ό.π., σελ. 376.

⁵³ Βλ. Στέργιο Σπυρόπουλο, ό.π., κατά τον οποίο αρκεί και απλή ειδοποίηση του παρόχου.

πληροφοριών κατόπιν παραλαβής οιασδήποτε ειδοποίησης, έστω και αβάσιμης, με αποτέλεσμα να θίγονται τα δικαιώματα του παρόχου των πληροφοριών⁵⁴. Μπορεί, μάλιστα, η ίδια η οδηγία να προβλέπει ρητά⁵⁵ ότι η απόσυρση των πληροφοριών και η απενεργοποίηση της πρόσβασης σε αυτές οφείλει να επιχειρείται τηρουμένης της αρχής της ελευθερίας της έκφρασης και των οικείων εθνικών διαδικασιών, όμως, στο βαθμό τέτοιου είδους διαδικασίες δεν έχουν θεσπιστεί από τις εθνικές νομοθεσίες, ο προσανατολισμός αυτός του κοινοτικού νομοθέτη καταλήγει να είναι μάλλον «ευχολόγιο».

Ακολούθως, σχετικά με τους παρόχους υπηρεσιών πρόσβασης (Access Providers) προβλέπεται στο άρθρο 12 της Οδηγίας 2000/31/EK, όπως ενσωματώθηκε στο εθνικό δίκαιο με το άρθρο 11 του π.δ. 131/2003, ότι δεν υπέχουν καμία ευθύνη εφόσον δεν αποτελούν την αφετηρία της μετάδοσης των πληροφοριών, δεν επιλέγουν τον αποδέκτη των μεταδιδόμενων πληροφοριών και δεν επιλέγουν ούτε τροποποιούν τις μεταδιδόμενες πληροφορίες. Η ρύθμιση αυτή αφορά στην απαλλαγή του παρόχου για υπηρεσίες που περιορίζονται στην τεχνική διαδικασία χειρισμού και παροχής πρόσβασης στο διαδίκτυο και ως εκ τούτου, έχουν εντελώς παθητικό και τεχνικό χαρακτήρα, αφού ο πάροχος ούτε γνωρίζει, ούτε ελέγχει καθ' οιονδήποτε τρόπο τις μεταδιδόμενες πληροφορίες. Στο πεδίο της διάταξης αυτής, εμπίπτει προεχόντως η μεταφορά δεδομένων μέσω διαδικτύου (Network Providing), η οποία συνήθως περιλαμβάνει την υπηρεσία δρομολόγησης (routing), την αποστολή ηλεκτρονικής αλληλογραφίας και την υπηρεσίας διανομής ηλεκτρονικής αλληλογραφίας (mailing lists)⁵⁶.

Στο σημείο αυτό, θα πρέπει να σημειώσουμε ότι από το γράμμα της διατάξεως συνάγεται ότι, πληρουμένων των προϋποθέσεων που ορίζονται σε αυτήν, ο πάροχος απαλλάσσεται σε κάθε περίπτωση, ανεξάρτητα από τη γνώση του ή μη, σχετικά με το παράνομο των μεταδιδόμενων πληροφοριών. Ωστόσο, μία τέτοια ερμηνεία θα προσέκρουε στο σκοπό της οδηγίας 2000/31/EK, καθώς οι εξαιρέσεις από την ευθύνη που προβλέπονται από την

⁵⁴ Βλ. *Φαίνη Κατσανάκη*, ό.π., σελ. 277, όπου περαιτέρω παραπομπές.

⁵⁵ Βλ. υπ' αριθμόν 46 αιτιολογική σκέψη στο προοίμιο της οδηγίας 2000/31/EK.

⁵⁶ Βλ. *Ιωάννη Ιγγλεζάκη*, *Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου*, εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη 2003, σελ. 171-172.

οδηγία αυτή, καλύπτουν μόνο τις περιπτώσεις στις οποίες οι δραστηριότητες του φορέα παροχής υπηρεσιών της ΚτΠ περιορίζονται στην τεχνική διαδικασία χειρισμού και παροχής πρόσβασης σε δίκτυο επικοινωνίας διά του οποίου μεταδίδονται. Οι δραστηριότητες αυτές έχουν εντελώς τεχνικό, αυτόματο και παθητικό χαρακτήρα, πράγμα που συνεπάγεται ότι ο φορέας παροχής υπηρεσιών της ΚτΠ, ούτε γνωρίζει, ούτε ελέγχει τις πληροφορίες που μεταδίδει ή αποθηκεύει⁵⁷.

Ειδική περίπτωση αποτελεί η αυτόματη, ενδιάμεση και προσωρινή αποθήκευση σε κρυφή μνήμη (Caching) ξένων πληροφοριών, με σκοπό τη μεταγενέστερη μετάδοσή τους μετά από αίτημα ορισμένου χρήστη, η οποία υπάγεται στο πεδίο δραστηριοτήτων των παρόχων υπηρεσιών πρόσβασης και ρυθμίζεται από το άρθρο 13 της οδηγίας 2000/31/EK, όπως ενσωματώθηκε στο εθνικό δίκαιο με το άρθρο 12 του π.δ. 131/2003. Σύμφωνα με τις διατάξεις αυτές, ο πάροχος της προαναφερόμενης υπηρεσίας δεν ευθύνεται εάν δεν τροποποιεί τις πληροφορίες, τηρεί τους όρους πρόσβασης και τους κανόνες που αφορούν την ενημέρωση των πληροφοριών, οι οποίοι καθορίζονται κατά ευρέως αναγνωρισμένο τρόπο και χρησιμοποιούνται από τον κλάδο. Επίσης, θα πρέπει ο πάροχος της υπηρεσίας προκειμένου να μην υπέχει ευθύνη, να μην παρεμποδίζει τη νόμιμη χρήση της τεχνολογίας, η οποία αναγνωρίζεται και χρησιμοποιείται ευρέως από τον κλάδο, προκειμένου να αποκτήσει δεδομένα σχετικά με τη χρησιμοποίηση των πληροφοριών και να ενεργεί άμεσα προκειμένου να αποσύρει τις πληροφορίες που αποθήκευσε ή να καταστήσει την πρόσβαση σε αυτές αδύνατη, μόλις αντιληφθεί ότι οι πληροφορίες έχουν αποσυρθεί από το σημείο του δικτύου στο οποίο βρίσκονταν αρχικά ή η πρόσβαση στις πληροφορίες κατέστη αδύνατη ή μια δικαστική ή διοικητική αρχή διέταξε την απόσυρση των πληροφοριών ή απαγόρευσε την πρόσβαση σε αυτές.

Πέραν, δε, της ρύθμισης της ευθύνης των παρόχων υπηρεσιών της ΚτΠ ανά κατηγορία και ανάλογα με το είδος των παρεχόμενων υπηρεσιών, το άρθρο 15 της Οδηγίας 2000/31/EK, όπως ενσωματώθηκε στο εθνικό δίκαιο με το

⁵⁷ Βλ. υπ' αρ. 42 αιτιολογική σκέψη του προοιμίου της οδηγίας 2000/31/EK.

άρθρο 14 του π.δ. 131/2003 καθιερώνει την απουσία γενικής υποχρέωση ελέγχου των παρόχων. Ειδικότερα, σύμφωνα με αυτήν, οι φορείς παροχής υπηρεσιών δεν έχουν, για την παροχή υπηρεσιών που αναφέρονται στα άρθρα 11, 12, 13, γενική υποχρέωση ελέγχου των αποθηκευμένων ή μεταδιδόμενων από αυτούς πληροφοριών, ούτε υποχρέωση δραστήριας αναζήτησης γεγονότων ή περιστάσεων που δείχνουν ότι πρόκειται για παράνομες δραστηριότητες. Εντούτοις, στην παράγραφο 2 του ιδίου άρθρου, θεμελιώνεται υποχρέωση των παρόχων να ενημερώνουν πάραυτα τις αρμόδιες αρχές για τυχόν υπόνοιες περί χορηγούμενων παράνομων πληροφοριών ή δραστηριοτήτων που επιχειρούν αποδέκτες των υπηρεσιών τους, καθώς και να ανακοινώνουν στις αρμόδιες αρχές, κατ' αίτησή τους, πληροφορίες οι οποίες διευκολύνουν τον εντοπισμό των αποδεκτών της υπηρεσίας τους, με τους οποίους έχουν συμφωνίες υπηρεσιών αποθήκευσης.

Η ratio legis της ανωτέρω ρυθμίσεως είναι προφανής και συνίσταται στην προστασία των παρόχων υπηρεσιών διαδικτύου από την υποχρέωση διαρκούς ελέγχου και επαγρύπνησης, προκειμένου να μπορούν να επικαλούνται την απαλλαγή της ευθύνης τους, η οποία προβλέπεται στα αμέσως προηγούμενα άρθρα 11, 12, 13 του π.δ. 131/2003. Μάλιστα, εκ πρώτης όψεως, σύμφωνα με τη γραμματική ερμηνεία της διατάξεως, η ευθύνη του παρόχου υπηρεσιών της ΚτΠ περιορίζεται μόνο στις περιπτώσεις δόλου, αποκλειομένων αυτών της αμέλειας, είτε βαρείας, είτε ελαφράς. Ωστόσο, η άποψη αυτή, δύσκολα συμβιβάζεται με τη δεύτερη παράγραφο του άρθρου 14 του π.δ. 131/2003, κατά την οποία καθιερώνεται υποχρέωση ενημέρωσης των αρμόδιων αρχών για παράνομες πληροφορίες ή δραστηριότητες, που υποπίπτουν στην αντίληψη του παρόχου. Η προβληματική αυτή θα εξεταστεί στην αμέσως επόμενη ενότητα.

3. Η ΠΡΟΒΛΗΜΑΤΙΚΗ ΤΗΣ ΡΥΘΜΙΣΕΩΣ ΤΗΣ ΑΠΑΛΛΑΓΗΣ ΤΟΥ ΜΕΣΑΖΟΝΤΟΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΚΤΠ ΑΠΟ ΤΗΝ ΕΥΘΥΝΗ ΤΟΥ. Η ΕΚΤΑΣΗ ΤΗΣ ΑΠΑΛΛΑΓΗΣ.

Με τη διάταξη του άρθρου 14 του π.δ. 131/2003, ο νομοθέτης φαίνεται *prima facie*, ότι επεδίωξε να περιορίσει την εξ αμελείας ευθύνη του μεσάζοντος στην

ΚΤΠ, σχετικά με το περιχόμενο των αποθηκευμένων ή μεταδιδόμενων από αυτούς πληροφοριών. Μάλιστα, τόσο η ανωτέρω γενική ρύθμιση, όσο και οι περιπτωσιολογικότερες διατάξεις των άρθρων 11, 12, 13 του π.δ. 131/2003, έχουν αποκλειστικώς αρνητικό χαρακτήρα, καθόσον θεμελιώνουν νόμιμο λόγο απαλλαγής από την ευθύνη και όχι νόμιμο λόγο ευθύνης, η πρόβλεψη του οποίου εναπόκειται ειδικότερα στους εθνικούς νομοθέτες. Περαιτέρω, ο ως άνω λόγος απαλλαγής από την ευθύνη αναφέρεται αδιακρίτως σε κάθε είδος ευθύνης προς αποζημίωση, ανεξάρτητα εάν πρόκειται για ευθύνη από σύμβαση, αδικοπρακτική, ακόμα και για ευθύνη του παρέχοντος υπηρεσίες σύμφωνα με το άρθρο 8 του ν. 2251/1994⁵⁸ και επίσης, σε κάθε είδος ευθύνης ανεξάρτητα από το εάν θεμελιώνεται στις διατάξεις του αστικού ή του ποινικού δικαίου.

Η ratio της ανωτέρω ρυθμίσεως έχει δύο πτυχές, η μία εκ των οποίων αναφέρεται στη φύση των παρεχόμενων υπηρεσιών, ενώ η δεύτερη έχει οικονομική διάσταση. Ειδικότερα, όσον αφορά στην πρώτη, η απαλλαγή της ευθύνης του παρόχου εδράζεται στο ότι αυτός δεν είναι παρά μόνο ο αγγελιοφόρος, άλλως ο διακομιστής, ο οποίος δεν νομιμοποιείται να ελέγχει τις μεταφερόμενες ή τις αποθηκευόμενες πληροφορίες και ως εκ τούτου δεν είναι δυνατόν να ευθύνεται για το περιεχόμενό τους⁵⁹. Εντούτοις, υποστηρίζεται και η άποψη ότι στην ψηφιακή πραγματικότητα, το ζήτημα είναι πολύπλοκο, αφού μόνο ο πάροχος είναι αυτός που μπορεί εν τοις πράγμασι και έχει την τεχνική δυνατότητα να εγγυηθεί για την ασφάλεια των μεταδιδόμενων ή αποθηκευόμενων πληροφοριών⁶⁰, καθόσον μόνο αυτός γνωρίζει τη διάρθρωση και τις διασυνδέσεις του δικτύου, τη διαδρομή που ακολουθούν τα πακέτα των πληροφοριών και γενικά τη φυσική και λογική δομή του δικτύου.

Όσον αφορά στη δεύτερη πτυχή της αιτιολογικής βάσης της ρυθμίσεως, η οποία έχει οικονομικό χαρακτήρα, προβάλλεται το επιχείρημα ότι η καθιέρωση

⁵⁸ Βλ. *Κωνσταντίνο Χριστοδούλου*, Αστική Ευθύνη του παρόχου δικτύου ως μεσάζοντος στην παροχή υπηρεσιών της κοινωνίας της πληροφορίας, ό.π., σελ. 354.

⁵⁹ Η προϋπόθεση αυτή προβλέπεται ρητά στην υπ' αριθμόν 42 αιτιολογική σκέψη του προοιμίου της οδηγίας 2000/31/EK.

⁶⁰ Βλ. *Κωνσταντίνο Χριστοδούλου*, ό.π.

ευθύνης του παρόχου για αμέλεια θα καθιστούσε αναγκαίο το νομοθετικό προσδιορισμό του μέτρου της απαιτούμενης επιμέλειας, γεγονός που θα επηρέαζε αναπόδραστα την αγορά των προτύπων ασφαλείας δικτύων. Πέραν δε αυτού, διατυπώθηκε η άποψη ότι σε μία τέτοια περίπτωση, η καθιέρωση της ευθύνης εξ αμελείας θα μπορούσε να θεωρηθεί ως παρέμβαση του νομοθέτη υπέρ ορισμένων παρόχων δικτύων σε βάρος άλλων, με μικρότερη οικονομική επιφάνεια και συνεπώς και με λιγότερες δυνατότητες λήψεως των απαιτούμενων μέτρων, η οποία τελικά θα είχε ως αποτέλεσμα τη διασάλευση της κατοχυρωμένης ελευθερίας του ανταγωνισμού κατά παράβαση της σχετικής ευρωπαϊκής νομοθεσίας.

Περαιτέρω, εξετάζοντας το ζήτημα από τη σκοπιά της ιστορίας δικαίου, θα μπορούσε κανείς να παρατηρήσει ότι αν η καθιέρωση της ευθύνης από αμέλεια κατέστη επιτακτική εξαιτίας της ανθρώπινης προόδου, καθόσον η υπεύθυνη συμμετοχή σε μία εξελιγμένη κοινωνία απαιτεί πλέον εγρήγορση και επιμέλεια και δεν αρκείται απλώς στην έλλειψη δόλου, πρόκειται πάλι για την ίδια πρόοδο, στην ανεξέλεγκτη, αυτή τη φορά, έξαρσή της, η οποία καθιστά προβληματική την ευθύνη από αμέλεια. Πολλώ δε μάλλον, καθόσον η καθιέρωση ενός κοινώς αποδεκτού και σταθερού μέτρου επιμέλειας σε έναν εκρηκτικά προοδεύοντα και μεταβαλλόμενο κόσμο παρίσταται, αν όχι σχεδόν αδύνατη, πάντως εξαιρετικά δυσχερής⁶¹.

Στο πλαίσιο αυτό, και παρά τη συνηγορία του γραμματικού επιχειρήματος υπέρ του περιορισμού της ευθύνης μόνο σε περιπτώσεις δόλου, μέσα από την τελολογική προσέγγιση της ρυθμίσεως, καταλήγουμε ότι η εξ αμελείας ευθύνη θα πρέπει να αποκλείεται, όταν έχει ως επακόλουθο τη χειραγώγηση της αγοράς μέσω της επιβολής μίας συγκεκριμένης τεχνολογίας. Αν, όμως, πρόκειται για μία τόσο εξώφθαλμη παράλειψη λήψης μέτρων ασφαλείας, ώστε η κατάγνωση εξ αμελείας ευθύνης δε θα απέκλειε κανένα σύγχρονο τεχνολογικό προϊόν, τότε θα ήταν ανακόλουθο με τις γενικές αρχές, που διέπουν την αστική ευθύνη, και δη με τις επιταγές των διατάξεων των άρθρων

⁶¹ Βλ. *Κωνσταντίνο Χριστοδούλου*, ό.π. υποσημείωση 13.

330 και 332 του ΑΚ, να απαιτείται δόλος⁶². Προχωρώντας ακόμα ένα βήμα, και χρησιμοποιώντας τη γραμματική ερμηνεία, διαπιστώνουμε ότι ο νομοθέτης κάνει λόγο για απουσία γενικής υποχρέωσης ελέγχου και όχι για απουσία οποιασδήποτε υποχρέωσης ελέγχου, οπότε, καθίσταται σαφές, ότι μία σχεδόν γενική απαλλαγή από την ευθύνη, ακόμα και για βαρεία αμέλεια θα συνεπαγόταν την οποιοσθώρηση του νομικού πολιτισμού σε πρωιμότερα στάδια⁶³. Η ερμηνεία αυτή συμφωνεί και με τη βούληση του ιστορικού νομοθέτη, ο οποίος ρητά δεν απέκλεισε a priori οποιουδήποτε είδους έλεγχο από την πλευρά του παρόχου. Μάλιστα, όπως ρητά αναφέρεται στην οδηγία 2000/31/ΕΚ, τα κράτη μέλη δεν μπορούν να επιβάλλουν γενική υποχρέωση ελέγχου στους φορείς παροχής υπηρεσιών, όμως αυτό δεν αφορά τις υποχρεώσεις ελέγχου σε ορισμένες περιπτώσεις και ειδικότερα δε θίγει τις εντολές των εθνικών αρχών σύμφωνα με την εθνική νομοθεσία⁶⁴.

Σήμερα δε, δεκαεπτά χρόνια μετά την υιοθέτηση της οδηγίας 2000/31/ΕΚ, η αγορά των προϊόντων ασφάλειας έχει εξελιχθεί σε τέτοιο βαθμό και έχουν αναδειχθεί πολλές τεχνολογίες οι οποίες ανταποκρίνονται στις εξειδικευμένες ανάγκες των διαφόρων μεσαζόντων υπηρεσιών της ΚτΠ, ώστε μάλλον δύσκολα μπορεί να γίνει λόγος για νόθευση της αγοράς υπό τις παρούσες συνθήκες⁶⁵. Στην υιοθέτηση αυτής της ερμηνείας συνηγορεί και η συχνή πλέον επιβολή υποχρέωσης ελέγχου στους μεσάζοντες σε ειδικές περιπτώσεις, οι οποίες προβλέπονται από την εθνική νομοθεσία και, όπως προαναφέρθηκε, δεν αποκλείονται από την οδηγία 2000/31/ΕΚ δημιουργώντας, έτσι, ένα σχήμα σχεδόν οξύμωρο, καθόσον στη μία περίπτωση θα θεμελιώνεται ευθύνη του μεσάζοντος μόνο για δόλο, ενώ στην

⁶² Τη συσταλτική ερμηνεία του όρου απουσία γενικής υποχρέωσης ελέγχου φαίνεται να επιλέγει και η γερμανική νομολογία, με την ευκαιρία ελέγχου της νομιμότητας των καταχωριζόμενων domain names, βλ. *Κωνσταντίνο Χριστοδούλου*, ό.π. όπου και περαιτέρω παραπομπές.

⁶³ Βλ. *Κωνσταντίνο Χριστοδούλου*, Ευθύνη του παρόχου δικτύου για προσβολές της ιδιωτικής σφαίρας, ό.π., σελ. 328 επ.

⁶⁴ Βλ. υπ' αρ. 47 αιτιολογική σκέψη του προοιμίου της οδηγίας 2000/31/ΕΚ.

⁶⁵ Στο πλαίσιο αυτό κινείται η νεότερη νομοθεσία. Έτσι στην οδηγία 2009/140/ΕΚ, ο Ευρωπαίος νομοθέτης αυξάνει τον πήχυ της επιμέλειας του παρόχου, χωρίς να λαμβάνει υπόψιν του ότι κατ' αυτόν τον τρόπο μπορεί να επηρεάσει τον ανταγωνισμό, αλλά αντίθετα θέτει ως κύριο στόχο των νέων ρυθμίσεων που εισάγει την ανάπτυξη του ανταγωνισμού στις ηλεκτρονικές επικοινωνίες, βλ. υπ' αρ. 5 αιτιολογική σκέψη του προοιμίου της οδηγίας 2009/140/ΕΚ.

άλλη περίπτωση για κάθε αμέλεια, χωρίς, ωστόσο, να υφίσταται κάποιος ιδιαίτερος λόγος που να δικαιολογεί μία τόσο διαφοροποιημένη αντιμετώπιση, αλλά αντίθετα θα πρόκειται για, κατά βάσιν, όμοιες περιπτώσεις.

Προς την κατεύθυνση αυτή κινείται και η πρόσφατη νομολογία των ελληνικών δικαστηρίων⁶⁶, με την ευκαιρία της εξέτασης του ζητήματος της παράνομης διακίνησης έργων πνευματικής ιδιοκτησίας στο διαδίκτυο και την εξ αυτής ευθύνη των φορέων παροχής πρόσβασης στο διαδίκτυο. Ειδικότερα, σύμφωνα με αυτήν, «ο νόμιμος λόγος απαλλαγής από την ευθύνη αφορά κάθε ευθύνη για συμπεριφορά που υπάγεται σε οποιαδήποτε απαγορευτική διάταξη νόμου, ανεξαρτήτως αν υπάγεται στο ποινικό ή στο αστικό, στο δίκαιο ανταγωνισμού ή πνευματικής ιδιοκτησίας. Η ιδιότυπη, όμως, αυτή ασυλία των φορέων παροχής πρόσβασης στο διαδίκτυο, δεν είναι απόλυτη, καθώς ρητά προβλέπεται ότι είναι δυνατή σε αυτούς η επιβολή με δικαστική απόφαση ή διοικητική πράξη μέτρων για την παύση ή την πρόληψη τυχόν παραβάσεων σε σχέση με τη διαδικτυακά διακινούμενη πληροφορία». Ομοίως, προβάλλεται ότι, «... η ρύθμιση του άρθρου 14 ΠΔ 131/2003 αποκλείει την, είτε με εθνικό νόμο είτε με δικαστική απόφαση ή διοικητική πράξη, επιβολή υποχρέωσης προς τους παρόχους πρόσβασης για την γενικευμένη εφαρμογή τέτοιων τεχνολογιών «φιλτραρίσματος». Μία τέτοια, άλλωστε, υποχρέωση θα ήταν ασύμβατη με βασικά ανθρώπινα δικαιώματα, όπως η ελευθερία έκφρασης αλλά και το δικαίωμα πρόσβασης στην κοινωνία της πληροφορίας, που θεμελιώνονται στην Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου και αναγνωρίζονται ως αναπόσπαστο κομμάτι του Ευρωπαϊκού Κοινοτικού Δικαίου. Για τη διασάφηση του ζητήματος κρίνεται εύλογη η καταφυγή στις σκέψεις της αντίστοιχης οδηγίας. Ειδικότερα, κατά τη σκέψη 47 αυτής, υποχρεώσεις - προληπτικού μεταξύ άλλων -ελέγχου για τους παρόχους πρόσβασης είναι δυνατές, μόνο αν αυτές αφορούν σε συγκεκριμένες περιπτώσεις και όχι αν εισάγουν γενικευμένο «φιλτράρισμα» πληροφοριών»⁶⁷.

⁶⁶ Βλ. την πρόσφατη υπ' αρ. 4658/2012 ΜΠΑ, Τράπεζα Νομικών Πληροφοριών ΝΟΜΟΣ, Διονυσία Καλλινίκου, ΧρΙΔ 2012, σελ. 373 επ., *Μιχαήλ Μαργαρίτης* ΝοΒ 2012, σελ. 1206 επ.

⁶⁷ Βλ. σχετική απόφαση Δ.Ε.Κ. της 12ης Ιουλίου 2011 C-324/09, L' Oreal κατά eBay, ειδικά σκέψεις 126-143, Τράπεζα Νομικών Πληροφοριών Eur-Lex.

Ενόψει των ανωτέρω απόψεων, αναφορικά με την ευθύνη του παρόχου υπηρεσιών διαδικτύου σχετικά με το περιεχόμενο των πληροφοριών που μεταφέρονται ή αποθηκεύονται, όπως προκύπτει από την αδιάσπικτη διατύπωση των άρθρων 14 σε συνδυασμό με τα άρθρα 11, 12, 13 του π.δ. 131/2003 προκύπτει ότι ο πάροχος δε θα πρέπει να ευθύνεται παρά μόνο σε περίπτωση δόλου, καθόσον δεν υπέχει καμία γενική υποχρέωση ελέγχου ή δραστήριας αναζήτησης του παρανόμου των πληροφοριών. Ωστόσο, σύμφωνα με την μάλλον κρατούσα άποψη, η οποία ερμηνεύει τη ρύθμιση προσεγγίζοντάς την από γραμματική, ιστορική και τελεολογική σκοπιά υποστηρίζεται ότι ο πάροχος θα πρέπει να ευθύνεται τουλάχιστον και για τις περιπτώσεις βαρείας αμέλειάς του. Περαιτέρω, έχει διατυπωθεί η γνώμη ότι δικαιολογημένη, από την πλευρά του ευρωπαϊκού δικαίου, παρίσταται η αυστηρότερη ρύθμιση της ευθύνης του παρόχου, όταν αυτός είναι και φορέας Καθολικής Υπηρεσίας, οπότε και η απαλλαγή του προβλέπεται μόνο όταν συντρέχουν περιστατικά που ανάγονται σε ανωτέρα βία⁶⁸, ακριβώς λόγω της σε ευρωπαϊκό επίπεδο καθιερωμένης ιδιαιτερότητας του θεσμού αυτού, ως παροχικού των αναφαίρετων κοινωνικών αγαθών⁶⁹. Ωστόσο, θα πρέπει να αναφέρουμε ότι η επίκληση των ανωτέρω διατάξεων για την Καθολική Υπηρεσία μόνο ενδεικτικό χαρακτήρα μπορεί να έχει, καθόσον έχουν πλέον καταργηθεί⁷⁰.

Μολαταύτα, η ανωτέρω απαλλαγή του παρόχου συναρτάται μόνο με την ευθύνη του για το παράνομο περιεχόμενο των πληροφοριών που μετακινούνται ή αποθηκεύονται. Αυτό, συνάγεται ευθέως από το γράμμα του άρθρου 14 του π.δ. 131/2003, που κάνει λόγο ότι οι φορείς παροχής

⁶⁸ Βλ. άρθρο 9, της υπ' αρ. 44035/1626/1-8-2007 (ΦΕΚ Β'1481/2007) απόφασης του Υπουργού Μεταφορών και Επικοινωνιών κατά το οποίο «Χωρίς περιορισμό των διατάξεων της παρούσας, ο πάροχος Καθολικής Υπηρεσίας δεν θεωρείται ότι έχει παραβιάσει διάταξη της παρούσας απόφασης, λόγω μη τήρησης ή πλημμελούς ή εκπρόθεσμης τήρησης των όρων της παρούσας, όταν αυτό οφείλεται σε ανωτέρα βία, η οποία έχει αιτιώδη συνάφεια με τη μη τήρηση των όρων της παρούσας απόφασης. Ενδεικτικά συνιστούν ανωτέρα βία τα ακόλουθα γεγονότα: ο πόλεμος, οι πράξεις δολιοφθοράς, οι τρομοκρατικές πράξεις, οι θεομηνίες, οι εκρήξεις και οι πυρκαγιές, οι μη οφειλόμενες ενέργειες σε βαρεία αμέλεια του παρόχου Καθολικής Υπηρεσίας και οι εμπορικοί αποκλεισμοί».

⁶⁹ Βλ. *Κωνσταντίνος Χριστοδούλου*, ό.π., υποσημ. 34.

⁷⁰ Με το άρθρο 80, παράγραφος 2α του ν. 4070/2012 (ΦΕΚ Α' 82/2012) καταργήθηκε ο ν. 3431/2006 και ως εκ τούτου και η εξουσιοδοτική του διάταξη 46 δυνάμει της οποίας εκδόθηκε η υπ' αρ. 44035/1626/1-8-2007 υπουργική απόφαση για το περιεχόμενο της Καθολικής Υπηρεσίας.

υπηρεσιών δεν έχουν, για την παροχή υπηρεσιών που αναφέρονται στα άρθρα 10, 11 και 12 του ως άνω π.δ., γενική υποχρέωση ελέγχου των πληροφοριών που μεταδίδουν ή αποθηκεύουν, ούτε γενική υποχρέωση δραστήριας αναζήτησης γεγονότων ή περιστάσεων που δείχνουν ότι πρόκειται για παράνομες δραστηριότητες. Επομένως, οι φορείς παροχής υπηρεσιών δεν απαλλάσσονται από την ευθύνη τους για πράξεις ή παραλείψεις, οι οποίες δεν έχουν σχέση με την παροχή υπηρεσιών που αναφέρονται στα άρθρα 10, 11 και 12 του π.δ. 131/2003 και δη με τις μεταφερόμενες ή αποθηκευόμενες πληροφορίες καθαυτές.

Έτσι, σε κάθε άλλη περίπτωση προβλημάτων ασφάλειας του δικτύου, που δεν εξασφαλίζεται η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα των διακινούμενων πληροφοριών, στο βαθμό που θα ανέμενε ο μέσος συνετός χρήστης του δικτύου, ο πάροχος του δικτύου δεν απαλλάσσεται από την ευθύνη του σύμφωνα με το άρθρο 14 του π.δ. 131/2003. Συνεπώς, αναφορικά με την πρόκληση ζημίας στον χρήστη, η οποία θα συνδεόταν αιτιωδώς με τα ανωτέρω προβλήματα ασφαλείας του δικτύου, το μέτρο της εξ αυτής ευθύνης του παρόχου θα προσδιοριζόταν καταρχήν σύμφωνα με την τυχόν ειδική νομοθεσία⁷¹ και σε κάθε περίπτωση σύμφωνα με την διάταξη του άρθρου 330 του ΑΚ, δηλαδή για δόλο και αμέλεια, εκτός εάν είχε συμφωνηθεί κάποιος περιορισμός της ευθύνης μεταξύ χρήστη και παρόχου, οπότε το κύρος της συμφωνίας αυτής θα κρινόταν από τη διάταξη του άρθρου 332 του ΑΚ⁷².

IV. Η ΕΥΘΥΝΗ ΤΟΥ ΠΑΡΟΧΟΥ ΔΗΜΟΣΙΟΥ ΔΙΚΤΥΟΥ ΣΥΜΦΩΝΑ ΜΕ ΤΟ Ν. 4070/2012.

1. Η ΡΥΘΜΙΣΗ ΤΗΣ ΟΔΗΓΙΑΣ 2009/140/ΕΚ.

Ο Ευρωπαϊός νομοθέτης κατά τρόπο σχεδόν πανηγυρικό, αναφέρει στο προοίμιο της οδηγίας 2009/140/ΕΚ, ότι η λειτουργία των πέντε οδηγιών που

⁷¹ Βλ. αμέσως επόμενο κεφάλαιο της παρούσας.

⁷² Μία τέτοιου είδους συμφωνία, εφόσον περιλαμβάνονταν σε προδιατυπωμένους όρους, θα κρινόταν και σύμφωνα με το άρθρο 2 του ν. 2251/1994 για τον τυχόν καταχρηστικό χαρακτήρα της.

συνιστούν το υφιστάμενο κανονιστικό πλαίσιο της Ευρωπαϊκής Ένωσης για τα δίκτυα και τις υπηρεσίες ηλεκτρονικών επικοινωνιών⁷³ υπάγεται σε περιοδική ανασκόπηση, ιδίως ώστε να διαπιστωθεί κατά πόσον επιβάλλεται η τροποποίηση των εν λόγω πράξεων υπό το φως των εξελίξεων στην τεχνολογία και στην αγορά⁷⁴. Κατόπιν, δε, της δημόσιας διαβούλευσης που προηγήθηκε, διαπιστώθηκε ότι ο κατακερματισμός της κανονιστικής ρύθμισης και οι ασυνέπειες στις δραστηριότητες των εθνικών κανονιστικών αρχών, απειλούν όχι μόνο την ανταγωνιστικότητα του τομέα, αλλά και τα σημαντικά ωφέλη για τους καταναλωτές από το διασυνοριακό ανταγωνισμό. Στην κατεύθυνση αυτή, με την οδηγία 2009/140/EK επιχειρείται η μεταρρύθμιση του κανονιστικού πλαισίου της Ευρωπαϊκής Ένωσης με στόχο την ολοκλήρωση της εσωτερικής αγοράς ηλεκτρονικών επικοινωνιών μέσω της ενισχύσεως του κοινοτικού μηχανισμού κανονιστικής ρύθμισης των φορέων εκμετάλλευσης που διαθέτουν σημαντική ισχύ στις βασικές αγορές⁷⁵.

Ειδικότερα, αναφορικά με το ζήτημα της ασφάλειας των ηλεκτρονικών δικτύων, ο Ευρωπαίος νομοθέτης θέτει την εξασφάλιση της αξιοπιστίας και ασφαλούς επικοινωνίας πληροφοριών μέσω των δικτύων ηλεκτρονικών επικοινωνιών ως έναν από τους βασικούς άξονες της μεταρρύθμισης που επιχειρείται με την οδηγία 2009/140/EK. Μάλιστα, όπως αναφέρεται στο προοίμιο της ως άνω οδηγίας⁷⁶, ο σύνθετος χαρακτήρας των συστημάτων, τεχνικές αστοχίες ή ανθρώπινα λάθη, ατυχήματα ή προσβολές ενδέχεται να έχουν συνέπειες για τη λειτουργία και τη διάθεση των υλικών υποδομών που παρέχουν υπηρεσίες καθοριστικής σημασίας για την ευημερία των πολιτών της Ευρωπαϊκής Ένωσης, περιλαμβανομένων των υπηρεσιών ηλεκτρονικής

⁷³ Ειδικότερα πρόκειται για την οδηγία 2002/21/EK (καλούμενη και ως «οδηγία – πλαίσιο»), την οδηγία 2002/19/EK (οδηγία για την πρόσβαση), την οδηγία 2002/20/EK (οδηγία για την αδειοδότηση), την οδηγία 2002/22/EK (οδηγία για την καθολική υπηρεσία) και την οδηγία 2002/58/EK (οδηγία για την προστασία της ιδιωτικής ζωής στο τομέα των ηλεκτρονικών επικοινωνιών), καλούμενες από κοινού «η οδηγία – πλαίσιο και οι ειδικές οδηγίες».

⁷⁴ Βλ. υπ' αρ. 1 αιτιολογική σκέψη του προοιμίου της οδηγίας 2009/140/EK.

⁷⁵ Σύμφωνα με την αιτιολογική σκέψη υπ' αρ. 2 του προοιμίου της οδηγίας 2009/140/EK, η ρύθμιση αυτή συμπληρώνεται από τον κανονισμό (ΕΚ) αρ. 1211/2009 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2009, για την ίδρυση του φορέα Εθνικών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC) και της Υπηρεσίας.

⁷⁶ Βλ. υπ' αριθμόν 44 αιτιολογική σκέψη του προοιμίου της οδηγίας 2009/140/EK.

διακυβέρνησης. Τόσο Ευρωπαϊκός Οργανισμός για την Ασφάλεια δικτύων και Πληροφοριών (ENISA), όσο και οι εθνικές ρυθμιστικές αρχές θα πρέπει να διαθέτουν τα απαραίτητα μέσα για την εκτέλεση των καθηκόντων τους περιλαμβανομένης της δυνατότητας να αποκτήσουν επαρκείς πληροφορίες, ώστε να είναι σε θέση να εκτιμήσουν το επίπεδο ασφάλειας δικτύων ή υπηρεσιών, καθώς και περιεκτικά και αξιόπιστα δεδομένα σχετικά με τρέχοντα συμβάντα ασφάλειας που είχαν σημαντικό αντίκτυπο στη λειτουργία δικτύων ή υπηρεσιών.

Ενόψει των ανωτέρω ζητημάτων που τίθενται, τα οποία όπως προαναφέρθηκε αποτυπώνονται στις ως άνω αιτιολογικές σκέψεις της οδηγίας, προβλέπονται με τις ρυθμίσεις των άρθρων 13α και 13β, αφενός οι υποχρεώσεις των παρόχων δημοσίων δικτύων επικοινωνιών ή υπηρεσιών ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό, για την τήρηση των οποίων μεριμνούν τα κράτη μέλη, αφετέρου οι τρόποι για την εφαρμογή και επιβολή των υποχρεώσεων αυτών από τα κράτη μέλη.. Ειδικότερα, σύμφωνα με τις υποχρεώσεις που προβλέπονται στο άρθρο 13α, τα κράτη μέλη μεριμνούν ώστε οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό να λαμβάνουν πρόσφορα τεχνικά και οργανωτικά μέτρα για την κατάλληλη διαχείριση του κινδύνου όσον αφορά την ασφάλεια των δικτύων και υπηρεσιών. Λαμβανομένων υπόψη των πλέον πρόσφατων τεχνικών δυνατοτήτων, τα μέτρα αυτά πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τον υπάρχοντα κίνδυνο. Λαμβάνονται ιδίως μέτρα για την αποτροπή και ελαχιστοποίηση του αντικτύπου συμβάντων που θέτουν σε κίνδυνο την ασφάλεια χρηστών και διασυνδεδεμένων δικτύων. Επιπλέον, τα κράτη μέλη πρέπει να μεριμνούν ώστε οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών να λαμβάνουν όλα τα κατάλληλα μέτρα για την εξασφάλιση της ακεραιότητας των δικτύων τους, εξασφαλίζοντας τη συνέχεια της παροχής των υπηρεσιών που διανέμονται μέσω των αυτών.

Επίσης, προβλέπεται ότι τα κράτη μέλη θα πρέπει να μεριμνούν ώστε οι επιχειρήσεις που παρέχουν πρόσβαση σε δημόσια δίκτυα επικοινωνιών ή σε υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό να κοινοποιούν στην αρμόδια εθνική ρυθμιστική αρχή κάθε παραβίαση της

ασφάλειας ή απώλεια της ακεραιότητας που είχε σημαντικό αντίκτυπο στη λειτουργία δικτύων ή υπηρεσιών. Περαιτέρω, επιδιώκοντας την αντιμετώπιση του προβλήματος σε κοινή βάση από όλα τα κράτη μέλη, ορίζεται ότι η αρμόδια εθνική αρχή κατά περίπτωση ενημερώνει σχετικά για τις ανωτέρω παραβάσεις τις αρμόδιες εθνικές αρχές στα άλλα κράτη μέλη, καθώς και τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια δικτύων και Πληροφοριών (ENISA). Ακόμα, η οικεία εθνική ρυθμιστική αρχή μπορεί να ενημερώσει το κοινό ή να απαιτήσει την ενημέρωση αυτή από τις επιχειρήσεις, εφόσον κρίνει ότι η αποκάλυψη της παραβίασης είναι προς το δημόσιο συμφέρον. Επιπροσθέτως, η οικεία εθνική ρυθμιστική αρχή υποβάλλει κατ' έτος στην Επιτροπή και στον ENISA συνοπτική έκθεση σχετικά με τις κοινοποιήσεις που έχει παραλάβει και τη δράση της σχετικά με αυτές. Η Επιτροπή, λαμβάνοντας ιδιαίτερως υπόψη της τη γνώμη του ENISA, μπορεί να εγκρίνει κατάλληλα τεχνικά εκτελεστικά μέτρα με στόχο την εναρμόνιση των μέτρων που αναφέρονται στις παραγράφους 1, 2 και 3 του άρθρου 13α, περιλαμβανομένων μέτρων που ορίζουν τις περιστάσεις, τη μορφή και τις διαδικασίες που ισχύουν για τις απαιτήσεις κοινοποίησης. Αυτά τα τεχνικά εκτελεστικά μέτρα⁷⁷ θα βασίζονται στο μεγαλύτερο δυνατό βαθμό στα ευρωπαϊκά και διεθνή πρότυπα και δεν εμποδίζουν τα κράτη μέλη να επιβάλουν συμπληρωματικές απαιτήσεις προς επίτευξη των στόχων της κατάλληλης διαχείρισης του κινδύνου και της εξασφάλισης της ακεραιότητας των δικτύων σύμφωνα με τα προαναφερόμενα.

Σχετικά με την επιβολή των μέτρων του άρθρου 13α, προβλέπεται στο άρθρο 13β ότι τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες εθνικές ρυθμιστικές αρχές διαθέτουν την εξουσία έκδοσης δεσμευτικών οδηγιών, συμπεριλαμβανομένων εκείνων που αφορούν τις προθεσμίες εφαρμογής, προς τις επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών διαθέσιμες στο κοινό. Ακόμα, τα κράτη μέλη μεριμνούν ώστε οι αρμόδιες εθνικές ρυθμιστικές αρχές να διαθέτουν την εξουσία να απαιτούν από τις επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες

⁷⁷ Βλ. άρθρο 13^α, παρ. 4 της οδηγίας 2009/140/EK, κατά το οποίο τα εν λόγω εκτελεστικά μέτρα, αποσκοπούν σε τροποποίηση μη ουσιωδών στοιχείων της οδηγίας 2009/140/EK με συμπλήρωσή της με νέα μη ουσιώδη στοιχεία, θεσπίζονται σύμφωνα με την κανονιστική διαδικασία με έλεγχο στην οποία παραπέμπει το άρθρο 22 παράγραφος 3 της οδηγίας αυτής.

ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό: α) να παρέχουν πληροφορίες απαραίτητες για την εκτίμηση της ασφάλειας και της ακεραιότητας των υπηρεσιών και δικτύων τους, περιλαμβανομένων τεκμηριωμένων πολιτικών ασφάλειας, και β) να υποβάλλονται σε έλεγχο ασφάλειας που διενεργείται από ειδικευμένο ανεξάρτητο φορέα ή αρμόδια εθνική αρχή και να θέτουν τα σχετικά πορίσματα στη διάθεση της εθνικής ρυθμιστικής αρχής. Επιπροσθέτως, τα κράτη μέλη μεριμνούν ώστε οι αρμόδιες εθνικές αρχές να διαθέτουν όλες τις απαραίτητες εξουσίες για τη διερεύνηση περιπτώσεων μη συμμόρφωσης, και των επιπτώσεών τους στην ασφάλεια και ακεραιότητα των δικτύων.

Μάλιστα, ορίζεται ρητά, ότι οι εν λόγω διατάξεις σχετικά με τις κατά τα ανωτέρω απονεμόμενες εξουσίες ελέγχου των παρόχων, στις αρμόδιες εθνικές ρυθμιστικές αρχές, θεσπίζονται με την επιφύλαξη του άρθρου 3 της ίδιας οδηγίας⁷⁸, που προβλέπει τη λήψη μέτρων σχετικά με την εξασφάλιση

⁷⁸ Συγκεκριμένα, σύμφωνα με το άρθρο 3: τα κράτη μέλη μεριμνούν για την αμεροληψία, τη διαφάνεια και την έγκαιρη δράση των εθνικών κανονιστικών αρχών κατά την άσκηση των εξουσιών τους. Τα κράτη μέλη μεριμνούν ώστε οι εθνικές ρυθμιστικές αρχές να διαθέτουν επαρκείς χρηματοδοτικούς και ανθρώπινους πόρους για την εκτέλεση των καθηκόντων που τους έχουν ανατεθεί. 3α. Υπό την επιφύλαξη των διατάξεων των παραγράφων 4 και 5, οι εθνικές ρυθμιστικές αρχές που είναι υπεύθυνες για την εκ των προτέρων κανονιστική ρύθμιση των αγορών ή για την επίλυση των διαφορών μεταξύ επιχειρήσεων σύμφωνα με το άρθρο 20 ή 21 της παρούσας οδηγίας ενεργούν ανεξάρτητα και δεν ζητούν ούτε λαμβάνουν οδηγίες από κανέναν άλλον φορέα σε σχέση με την εκτέλεση των καθηκόντων αυτών που τους έχουν ανατεθεί βάσει εθνικών νομοθετικών ρυθμίσεων που υλοποιούν την κοινοτική νομοθεσία. Αυτό δεν εμποδίζει την επιτήρηση σύμφωνα με το εθνικό συνταγματικό δίκαιο. Εξουσία αναστολής ή ακύρωσης αποφάσεων των εθνικών κανονιστικών αρχών διαθέτουν αποκλειστικά τα όργανα προσφυγής που έχουν συγκροτηθεί σύμφωνα με το άρθρο 4. Τα κράτη μέλη εξασφαλίζουν ότι ο επικεφαλής εθνικής ρυθμιστικής αρχής στην οποία αναφέρεται το πρώτο εδάφιο ή ενδεχομένως τα μέλη του συλλογικού οργάνου που ασκούν το καθήκον αυτό ή ο αντικαταστάτης του μπορούν να απολυθούν μόνον εφόσον δεν καλύπτουν πλέον τους απαιτούμενους όρους για την εκτέλεση των καθηκόντων τους, όπως αυτά καθορίζονται εκ των προτέρων στην εθνική νομοθεσία. Η απόφαση απόλυσης του επικεφαλής της εν λόγω εθνικής ρυθμιστικής αρχής ή ενδεχομένως των μελών του συλλογικού οργάνου που ασκούν τη λειτουργία αυτή, λαμβάνει δημοσιότητα κατά τη χρονική στιγμή της απόλυσης. Ο απολυθείς επικεφαλής της εθνικής ρυθμιστικής αρχής ή ενδεχομένως τα μέλη του συλλογικού οργάνου που ασκούν τη λειτουργία αυτή λαμβάνουν δήλωση των λόγων απόλυσής τους και δικαιούνται να ζητήσουν και να επιτύχουν τη δημοσίευσή της, σε περίπτωση που αυτό δεν θα συνέβαινε διαφορετικά. Τα κράτη μέλη εξασφαλίζουν ότι οι εθνικές ρυθμιστικές αρχές που αναφέρονται στην πρώτη υποπαράγραφο διαθέτουν χωριστούς ετήσιους προϋπολογισμούς. Οι προϋπολογισμοί δημοσιοποιούνται. Τα κράτη μέλη μεριμνούν επίσης ώστε να διαθέτουν οι εθνικές ρυθμιστικές αρχές επαρκείς οικονομικούς και ανθρώπινους πόρους που θα τους επιτρέπουν να συμμετέχουν ενεργά και να συνεισφέρουν στον Φορέα Ευρωπαϊκών Ρυθμιστικών Αρχών στις Ηλεκτρονικές Επικοινωνίες (BEREC). 3β. Τα κράτη μέλη εξασφαλίζουν ότι οι αρμόδιες εθνικές ρυθμιστικές αρχές υποστηρίζουν ενεργά τους στόχους του BEREC όσον αφορά την προώθηση μεγαλύτερου ρυθμιστικού συντονισμού και συνέπειας. 3γ. Τα κράτη μέλη εξασφαλίζουν ότι οι εθνικές

της αμεροληψίας και της διαφάνειας των αρχών. Ομοίως, η προϋπόθεση της αμεροληψίας των εθνικών ρυθμιστικών αρχών και η σημασία της για όλες τις ρυθμίσεις που εισάγονται με την οδηγία 2009/140/EK, τονίζεται και στο προοίμιό της⁷⁹, όπου αναφέρεται ότι θα πρέπει να ενισχυθεί η ανεξαρτησία τους, ώστε να εξασφαλισθεί αποτελεσματικότερη εφαρμογή του κανονιστικού και να αυξηθεί το κύρος τους και η προβλεψιμότητα των αποφάσεων τους. Για τον σκοπό αυτό, θα πρέπει να υπάρξει ρητή πρόβλεψη στην εθνική νομοθεσία που θα εξασφαλίσει ότι, κατά την άσκηση των καθηκόντων της, μια εθνική ρυθμιστική αρχή υπεύθυνη για την εκ των προτέρων κανονιστική ρύθμιση των αγορών ή για την επίλυση των διαφορών μεταξύ επιχειρήσεων προστατεύεται έναντι εξωτερικών παρεμβάσεων ή πολιτικών πιέσεων που ενδέχεται να θέσουν σε κίνδυνο την ανεξάρτητη αξιολόγησή της στα θέματα των οποίων επιλαμβάνεται. Τέλος, τέθηκε προθεσμία για τη μεταφορά των ρυθμίσεων της οδηγίας αυτής στο εθνικό δίκαιο, έως την 25^η Μαΐου 2011.

Ενόψει των ανωτέρω, παρατηρούμε ότι οι διατάξεις αυτές αυξάνουν κατά πολύ τον πήχη των υποχρεώσεων επιμέλειας των παρόχων δημοσίων δικτύων επικοινωνιών ή υπηρεσιών ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό, υποχρεώνοντάς τους στη λήψη μέτρων ανάλογα αφενός με τον υπάρχοντα κίνδυνο, αφετέρου με τις πλέον πρόσφατες τεχνολογικές εξελίξεις. Περαιτέρω, τα μέτρα αυτά, οργανωτικά και τεχνικά, θα πρέπει να είναι πρόσφορα ώστε να επιτυγχάνεται τόσο η αποτροπή και ελαχιστοποίηση του αντικτύπου των συμβάντων που θέτουν σε κίνδυνο την ασφάλεια, όσο και η ακεραιότητα των δικτύων υπό την έννοια της συνέχειας παροχής των υπηρεσιών που διανέμονται μέσω αυτών. Η βούληση αυτή του ευρωπαϊκού νομοθέτη είναι σαφής, όπως προκύπτει και από το προοίμιο της οδηγίας 2009/140/EK⁸⁰, όπου αναφέρεται ότι, δεδομένου ότι η επιτυχής εφαρμογή επαρκούς βαθμού ασφάλειας δεν αποτελεί ενέργεια που πραγματοποιείται άπαξ, αλλά συνεχή διαδικασία εφαρμογής, ανασκόπησης

ρυθμιστικές αρχές λαμβάνουν ιδιαιτέρως υπόψη τις γνώμες και τις κοινές θέσεις που εκδίδει ο BEREC κατά τη λήψη των αποφάσεών τους για τις εθνικές τους αγορές.

⁷⁹ Βλ. υπ' αρ. 13 αιτιολογική σκέψη του προοιμίου της οδηγίας 2009/140/EK.

⁸⁰ Βλ. υπ' αριθμόν 44 αιτιολογική σκέψη του προοιμίου της οδηγίας 2009/140/EK.

και ενημέρωσης, θα πρέπει να απαιτείται από τους παρόχους δικτύου και υπηρεσιών ηλεκτρονικών επικοινωνιών να λαμβάνουν μέτρα για τη διασφάλιση της ακεραιότητας και της ασφαλείας τους, σύμφωνα με τους κινδύνους που έχουν εκτιμηθεί και επί τη βάση των πρόσφατων εξελίξεων της σχετικής τεχνολογίας.

2. Η ΜΕΤΑΦΟΡΑ ΤΗΣ ΟΔΗΓΙΑΣ 2009/140/ΕΚ ΣΤΟ ΕΛΛΗΝΙΚΟ ΔΙΚΑΙΟ ΜΕ ΤΟ Ν. 4070/2012.

Μετά την παρέλευση της ανωτέρω προθεσμίας ενσωμάτωσης στο εθνικό δίκαιο, ο Έλληνας νομοθέτης, με το ν. 4070/2012 «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις» (ΦΕΚ Α' 82/10-4-2012) εισήγαγε στο ελληνικό δίκαιο τις οδηγίες 2009/136/ΕΚ και 2009/140/ΕΚ. Μάλιστα, όπως αναφέρεται στην αιτιολογική έκθεση⁸¹ του νόμου αυτού, ο στόχος για το νέο νόμο είναι να αποτελέσει ένα σαφές θεσμικό πλαίσιο για τη λειτουργία της αγοράς ηλεκτρονικών επικοινωνιών στην Ελλάδα, το οποίο θα συμβάλει στην ελεύθερη παροχή δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, στην εξασφάλιση σε κάθε επιχείρηση του δικαιώματος παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών, εγκατάστασης, επέκτασης, λειτουργίας, ελέγχου και διάθεσης δικτύων ηλεκτρονικών επικοινωνιών, στην προστασία του ανταγωνισμού και την αποφυγή στρέβλωσης της αγοράς, μεριμνώντας για την κατά το μέτρο του δυνατού τεχνολογική ουδετερότητα των κανονιστικών ρυθμίσεων που επιβάλλονται, ιδίως εκείνων που στοχεύουν στη διασφάλιση αποτελεσματικού ανταγωνισμού, στην προαγωγή του ανταγωνισμού στην παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών και συναφών ευκολιών και υπηρεσιών, καθώς και στις πολιτικές διασφάλισης του δημοσίου συμφέροντος, στη συμβολή στην ανάπτυξη της ενιαίας ευρωπαϊκής αγοράς και στην προαγωγή των συμφερόντων των χρηστών. Συνακολούθως, με το νέο αυτό νόμο καταργείται το υφιστάμενο μέχρι τότε νομικό πλαίσιο

⁸¹ Βλ. Αιτιολογική έκθεση ν. 4070/2012, Μέρος Α', Κεφάλαιο Ι, σελ. 1,

λειτουργίας του ν. 3431/2006⁸², ο οποίος είχε ενσωματώσει το σχετικό ευρωπαϊκό ρυθμιστικό πλαίσιο για τις ηλεκτρονικές επικοινωνίες⁸³.

Ειδικότερα, σχετικά με την υποχρέωση λήψης μέτρων ασφαλείας από τον πάροχο δημόσιου δικτύου επικοινωνιών ή υπηρεσιών ηλεκτρονικών επικοινωνιών, προβλέπεται στο άρθρο 37 του ν. 4070/2012 ότι οι επιχειρήσεις που δραστηριοποιούνται στον τομέα αυτό πρέπει να λαμβάνουν πρόσφορα τεχνικά και οργανωτικά μέτρα για την κατάλληλη διαχείριση του κινδύνου όσον αφορά στην ασφάλεια των δικτύων και υπηρεσιών. Τα μέτρα αυτά, λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες, πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τον υφιστάμενο κίνδυνο. Αναλυτικότερα, οι επιχειρήσεις αυτές λαμβάνουν ιδίως μέτρα για την αποτροπή και ελαχιστοποίηση των επιπτώσεων από περιστατικά ασφαλείας που επηρεάζουν τους χρήστες και τα διασυνδεδεμένα δίκτυα. Επίσης, στην επόμενη παράγραφο του παραπάνω άρθρου ορίζεται ότι οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών λαμβάνουν όλα τα κατάλληλα μέτρα για την εξασφάλιση της ακεραιότητας των δικτύων τους, έτσι ώστε να διασφαλίζεται η συνέχεια της παροχής των υπηρεσιών που διανέμονται μέσω των δικτύων αυτών. Τα μέτρα που αναφέρονται στις ανωτέρω παραγράφους καθορίζονται από την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) με κανονιστικές πράξεις⁸⁴.

Η εποπτεία της εφαρμογής των επιβαλλόμενων μέτρων ασφαλείας ανατίθεται στην Α.Δ.Α.Ε⁸⁵ και στην Ε.Ε.Τ.Τ. Έτσι, ακολουθώντας τις επιταγές της ευρωπαϊκής νομοθεσίας, ο Έλληνας νομοθέτης ορίζει ότι οι επιχειρήσεις που

⁸² Ν. 3431/2006 «Περί Ηλεκτρονικών Επικοινωνιών και άλλες διατάξεις» (ΦΕΚ Α' 13/3-2-2006).

⁸³ Με το ν. 3431/2006 ενσωματώθηκε στο ελληνικό δίκαιο το ευρωπαϊκό ρυθμιστικό πλαίσιο για τις ηλεκτρονικές επικοινωνίες, το οποίο συνίσταται από τις οδηγίες 2002/19/EK, 2002/20/EK, 2002/21/EK, 2002/22/EK και 2002/77/EK.

⁸⁴ Βλ. την υπ' αρ. 205/2013 απόφαση της Α.Δ.Α.Ε. «Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών» (ΦΕΚ Β' 1742/15-5-2013), σύμφωνα με το άρθρο 37 παράγραφοι 1 και 2 του ν. 4070/2012, η οποία αναλύεται στην ενότητα 4 του παρόντος κεφαλαίου.

⁸⁵ Ειδικά για την Α.Δ.Α.Ε., ορίζεται ότι κατά την άσκηση του ελέγχου της, έχει την εξουσία και τις αρμοδιότητες που προβλέπονται από το ν. 3115/2003 (Α'47), το ν. 703/1977 (Α'278) και το ν. 3674/2008 (Α'136), όπως ισχύουν.

παρέχουν πρόσβαση σε δημόσια δίκτυα επικοινωνιών ή σε υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό, κοινοποιούν στην Ε.Ε.Τ.Τ. κάθε παραβίαση της ασφάλειας ή απώλεια της ακεραιότητας που είχε σημαντικό αντίκτυπο στη λειτουργία δικτύων ή υπηρεσιών, η οποία με τη σειρά της κοινοποιεί κάθε παραβίαση της ασφάλειας ή απώλεια της ακεραιότητας στην Α.Δ.Α.Ε. Κατά περίπτωση, η Α.Δ.Α.Ε. ενημερώνει τις αρμόδιες εθνικές αρχές στα άλλα κράτη - μέλη, καθώς και τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA). Η Ε.Ε.Τ.Τ. μπορεί να ενημερώσει το κοινό ή να απαιτήσει την ενημέρωση αυτή από τις επιχειρήσεις, εφόσον κρίνει ότι η αποκάλυψη της παραβίασης είναι προς το δημόσιο συμφέρον. Η Ε.Ε.Τ.Τ. υποβάλλει κατ' έτος στην Ευρωπαϊκή Επιτροπή και στον ENISA συνοπτική έκθεση σχετικά με τις κοινοποιήσεις που έχει παραλάβει και τη δράση που έχει αναλάβει σύμφωνα με την παρούσα παράγραφο.

Επιπλέον, η Ε.Ε.Τ.Τ. μπορεί να εκδίδει δεσμευτικές υποδείξεις, στο πλαίσιο εφαρμογής των κανονιστικών πράξεων, όσον αφορά στην ασφάλεια των δικτύων και υπηρεσιών και στην εξασφάλιση της ακεραιότητας των δικτύων τους, συμπεριλαμβανομένων εκείνων που αφορούν τις προθεσμίες εφαρμογής, προς τις επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών διαθέσιμες στο κοινό. Ακόμα, η Ε.Ε.Τ.Τ. μπορεί να απαιτεί από τις επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό, να παρέχουν σε αυτήν πληροφορίες απαραίτητες για την εκτίμηση της ασφάλειας και της ακεραιότητας των υπηρεσιών και δικτύων τους, περιλαμβανομένων τεκμηριωμένων πολιτικών ασφαλείας. Τέλος, ο έλεγχος ασφάλειας διενεργείται από την Α.Δ.Α.Ε., η οποία θέτει τα σχετικά πορίσματά της στη διάθεση της Ε.Ε.Τ.Τ.. Το κόστος του ελέγχου επιβαρύνει την ελεγχόμενη επιχείρηση.

Στο σημείο αυτό, δεν μπορούμε παρά να μην παρατηρήσουμε ότι ο καθορισμός των αρμοδίων αρχών σύμφωνα με τις επιλογές του Έλληνα νομοθέτη, όπως αναλυτικά εκτίθενται ανωτέρω, αποκτά σχεδόν «αινιγματικές

διαστάσεις»⁸⁶. Ειδικότερα, σύμφωνα με την παράγραφο υπ' αρ. 3 του άρθρου 37 του ν. 4070/2012, τα μέτρα των παραγράφων 1 και 2 του ως άνω άρθρου καθορίζονται με κανονιστική πράξη της Α.Δ.Α.Ε., η οποία ως εκ τούτου καθορίζεται ως η αρμόδια εθνική ρυθμιστική αρχή. Αντίθετα, σύμφωνα με την παράγραφο υπ' αρ. 4 του αυτού άρθρου, οι παραβιάσεις ασφάλειας και η απώλεια ακεραιότητας του δικτύου γνωστοποιούνται στην Ε.Ε.Τ.Τ., η οποία συνακολούθως ορίζεται ως αρμόδια εθνική αρχή κοινοποιήσεων του νέου άρθρου 13^α, παράγραφος 3, εδ. α' της οδηγίας 2002/21/ΕΚ. Η Ε.Ε.Τ.Τ. με τη σειρά της υποχρεούται να ενημερώσει την Α.Δ.Α.Ε., η οποία είναι αρμόδια να ενημερώσει τις αρμόδιες εθνικές αρχές στα κράτη μέλη και τον ENISA.

Επίσης, η Ε.Ε.Τ.Τ. είναι αρμόδια να ενημερώνει το κοινό και να υποβάλει σχετική ετήσια έκθεση στην Ευρωπαϊκή Επιτροπή και τον ENISA. Επιπροσθέτως, η Ε.Ε.Τ.Τ. μπορεί σύμφωνα με την παράγραφο υπ' αρ. 6 του ως άνω άρθρου του ν. 4070/2012 να εκδίδει δεσμευτικές υποδείξεις στο πλαίσιο εφαρμογής των κανονιστικών πράξεων της Α.Δ.Α.Ε. και να απαιτεί από τους παρόχους σύμφωνα με την παράγραφο υπ' αρ. 7 του ιδίου άρθρου να της παρέχουν πληροφορίες σχετικά με την εκτίμηση της ασφάλειας και ακεραιότητας των δικτύων τους και επίσης σχετικά με την πολιτική ασφάλειας που ακολουθούν. Αντιθέτως, ο έλεγχος ασφάλειας, σύμφωνα με την παράγραφο υπ' αρ. 8 του ιδίου άρθρου έχει ανατεθεί στην Α.Δ.Α.Ε., η οποία κοινοποιεί τα πορίσματά της στην Ε.Ε.Τ.Τ.

Ενόψει του προπεριγραφόμενου σχήματος διάρθρωσης των αρμοδιοτήτων των εθνικών αρχών, ο Έλληνας νομοθέτης φαίνεται να επιλέγει το ακόλουθο, μάλλον «πρωτοποριακό»⁸⁷ σύστημα: α. η Α.Δ.Α.Ε. νομοθετεί, καθόσον ορίζει με κανονιστική πράξη της τα μέτρα των παραγράφων υπ' αρ. 1 και 2 του άρθρου 37 του ν. 4070/2012, β. η Ε.Ε.Τ.Τ. εφαρμόζει, καθώς ορίζεται ως η αρμόδια αρχή προς την οποία γίνονται οι κοινοποιήσεις των περιστατικών παραβίασης ασφάλειας και που η ίδια σε δεύτερο στάδιο τα κοινοποιεί σε Α.Δ.Α.Ε., Ευρωπαϊκή Επιτροπή και ENISA και η οποία τέλος είναι αυτή που μπορεί να απαιτεί από τους παρόχους πληροφόρηση σχετικά με την εκτίμηση

⁸⁶ Βλ. Γιώργο Ν. Γιαννόπουλο, ό.π., σελ. 197.

⁸⁷ Βλ. Γιώργο Ν. Γιαννόπουλο, ό.π.

της ασφάλειας και ακεραιότητας των δικτύων τους και με την πολιτική ασφάλειας τους και γ. η Α.Δ.Α.Ε. ελέγχει την εφαρμογή των ανωτέρω , κοινοποιώντας τα πορίσματά της στην Ε.Ε.Τ.Τ. Η μέχρι σήμερα εφαρμογή της κείμενης νομοθεσίας έχει καταδείξει πολυάριθμα προβλήματα στην κατανομή των ρόλων μεταξύ των εν λόγω αρχών. Ενόψει αυτών, η εκτεθείσα πολύπλοκη δομή μάλλον θα ενισχύσει τις υπάρχουσες γραφειοκρατικές αγκυλώσεις παρά θα επιλύσει τα προβλήματα, πολύ περισσότερο σε έναν τομέα που λόγω των ιδιαίτερων συνθηκών του, απαιτούνται αστραπιαίες αντιδράσεις⁸⁸.

3. ΤΑ ΠΡΟΒΛΗΜΑΤΑ ΑΠΟ ΤΗ ΜΕΤΑΦΟΡΑ ΤΗΣ ΟΔΗΓΙΑΣ 2009/140/ΕΚ. Η ΕΦΑΡΜΟΓΗ ΤΗΣ ΡΥΘΜΙΣΗΣ ΤΟΥ Ν. 4070/2012.

Από την παραπάνω επισκόπηση της ρύθμισης των διατάξεων του άρθρου 37 του ν. 4070/2012 προκύπτει ότι ο Έλληνας νομοθέτης, έστω και καθυστερημένα, καθόσον η ενσωμάτωση στο ελληνικό δίκαιο πραγματοποιήθηκε πολύ μετά την παρέλευση της ταχθείσας προθεσμίας μεταφοράς, υιοθέτησε «σχεδόν αυτούσιες» τις σχετικές διατάξεις της οδηγίας 2009/140/ΕΚ, η οποία εξάλλου είναι οδηγία πλήρους εναρμόνισης. Ωστόσο, *prima facie*, η ελληνική ρύθμιση φαίνεται να περιορίζει την ισχύ των επιταγών του ευρωπαϊκού δικαίου, αφού σύμφωνα με την παράγραφο 3 του άρθρου 37, τα μέτρα ασφάλειας που θα πρέπει να λάβουν οι πάροχοι καθορίζονται από την Α.Δ.Α.Ε, η οποία, μάλιστα, εξέδωσε προς τούτο κανονιστικές πράξεις⁸⁹. Επισημαίνεται, δε, ότι σύμφωνα με το άρθρο 13β, παράγραφος 1 και σύμφωνα με το προοίμιο⁹⁰ της ανωτέρω οδηγίας, προβλέπεται ότι για την εφαρμογή των επιβαλλόμενων μέτρων ασφαλείας στους παρόχους, οι εθνικές ρυθμιστικές αρχές θα πρέπει να είναι εξοπλισμένες με την εξουσία να εκδίδουν δεσμευτικές οδηγίες προς αυτούς.

⁸⁸ Βλ. Γιώργο Ν. Γιαννόπουλο, ό.π.

⁸⁹ Βλ. ανωτέρω παραπομπή υπ' αρ. 85.

⁹⁰ Βλ. υπ' αρ. 46 αιτιολογική σκέψη του προοιμίου της οδηγίας 2009/140/ΕΚ, κατά την οποία «...Οι εθνικές ρυθμιστικές αρχές θα πρέπει να διαθέτουν την εξουσία να εκδίδουν δεσμευτικές οδηγίες όσον αφορά τεχνικά μέτρα εφαρμογής που θεσπίζονται σύμφωνα με την οδηγία 2002/21/ΕΚ..... ».

Όμως, σε κανένα σημείο της εν λόγω οδηγίας, δεν αναφέρεται ότι τα επιβαλλόμενα μέτρα ασφαλείας, εξειδικεύονται και προσδιορίζονται από τις οικείες αρμόδιες εθνικές αρχές. Πολλώ, δε, μάλλον, αφού ένας τέτοιου είδους προσδιορισμός των επιβαλλόμενων μέτρων ασφάλειας, θα μπορούσε ενδεχομένως να επιφέρει τη διασάλευση της υγιούς λειτουργίας του ανταγωνισμού, εάν προωθούσε τη χρήση ορισμένων τεχνολογιών αντί άλλων⁹¹. Αντιθέτως, όπως προκύπτει τόσο από το προοίμιο της ως άνω οδηγίας⁹², όσο και από την αιτιολογική έκθεση του ελληνικού νόμου⁹³, ο πρωταρχικός στόχος των νέων ρυθμίσεων είναι η υγιής ανάπτυξη του ανταγωνισμού. Στο πνεύμα αυτό, ο Ευρωπαίος νομοθέτης αρκείται στην επιβολή υποχρεώσεων στους παρόχους των δημοσίων δικτύων για τη λήψη μέτρων ασφάλειας, αφήνοντας στους ίδιους τους παρόχους να επιλέξουν ποια θα είναι αυτά τα μέτρα, ανάλογα με τις ανάγκες του δικτύου τους και της επιχείρησής τους. Θέτει, όμως, τον πήχυ των μέτρων αυτών, τα οποία θα πρέπει «λαμβάνομένων υπόψη των πλέον πρόσφατων τεχνικών δυνατοτήτων, να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τον υπάρχοντα κίνδυνο⁹⁴».

Όπως, μάλιστα, έχει διατυπωθεί⁹⁵, πρόκειται για αμφίβολη εξουσιοδότηση προς την Α.Δ.Α.Ε. να εξειδικεύσει και να ερμηνεύσει αυθεντικώς, συστήλλοντας ή επεκτείνοντας, τα παραγγέλματα του ενωσιακού δικαίου. Λαμβανομένου, δε, υπόψη ότι η προθεσμία για συμμόρφωση στην οδηγία 2009/140/ΕΚ είχε προ πολλού παρέλθει, πριν από την έκδοση της ούτως ή άλλως προβληματικής απόφασης της Α.Δ.Α.Ε., είχε υποστηριχθεί η άποψη ότι το δημιουργούμενο κενό θα έπρεπε να πληρωθεί σύμφωνα με το ενωσιακό δίκαιο, ήτοι ότι η διάταξη του άρθρου 37 παράγραφοι 1, 2 του ν. 4070/2012 παράγει ήδη αμέσως τα έννομα αποτελέσματά της και ως εκ τούτου, οι πάροχοι των δημοσίων δικτύων θα υποχρεούνταν ήδη από την

⁹¹ Για παράδειγμα, προτείνοντας ως μέτρο ασφάλειας την τοποθέτηση της τεχνολογίας Firewall, αντί αυτής του Data Leakage.

⁹² Βλ. υπ' αρ. 5 αιτιολογική σκέψη του προοιμίου της οδηγίας 2009/140/ΕΚ.

⁹³ Βλ. ανωτέρω Κεφάλαιο V, ενότητα 2.

⁹⁴ Βλ. άρθρο 13^α, παράγραφος 1 οδηγίας 2009/140/ΕΚ.

⁹⁵ Βλ. Κωνσταντίνος Χριστοδούλου, *Επιτομή Ηλεκτρονικού Αστικού Δικαίου*, ό.π., σελ.80-81.

έκδοση της οδηγίας στη λήψη όλων των κατάλληλων μέτρων για την ασφάλεια και την ακεραιότητα των δικτύων αυτών. Σημειωτέον, ότι μετά την έστω καθυστερημένη έκδοση της απόφασης της Α.Δ.Α.Ε.⁹⁶, η ως άνω άποψη στερείται πρακτικής σημασίας, αφού οι πάροχοι δημόσιων δικτύων επικοινωνιών ή υπηρεσιών ηλεκτρονικών επικοινωνιών, υπέχουν την υποχρέωση λήψης όλων των μέτρων ασφάλειας, όπως πλέον αυτά εξειδικεύονται στη σχετική απόφαση.

Επιπροσθέτως, θα πρέπει στο σημείο αυτό να διευκρινιστεί ότι από την ως άνω αναφερόμενη υποχρέωση λήψης μέτρων ασφάλειας, εξαιρούνται ρητά⁹⁷ τα κρατικά ηλεκτρονικά δίκτυα, ακόμα και εάν αυτά είναι δημόσια. Ως δημόσιο δίκτυο, σύμφωνα με το νομοθετικό ορισμό του εν λόγω νόμου⁹⁸ νοείται το δίκτυο ηλεκτρονικών επικοινωνιών, το οποίο χρησιμοποιείται, εν όλω ή κυρίως, για την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών που υποστηρίζουν τη μεταφορά πληροφοριών μεταξύ σημείων τερματισμού δικτύου. Προκειμένου, δε να αποφευχθούν στρεβλώσεις στη σχετική αγορά, θα πρέπει ο όρος κρατικά δίκτυα να εκληφθεί με τη λειτουργική σημασία του, ήτοι με αναφορά στην κυριαρχική διοίκηση. Συνεπώς, απόκειται στο κράτος η ρύθμιση της ασφάλειας των αστυνομικών ή στρατιωτικών ηλεκτρονικών επικοινωνιών του, ενώ αντιθέτως, τα δίκτυα που ενέχουν κοινωφελείς κρατικές δραστηριότητες, μεταξύ των οποίων και η λεγόμενη «παροχική διοίκηση», ως υπηρεσία γενικού οικονομικού συμφέροντος⁹⁹, υπόκειται στο αυξημένο καθήκον ασφάλειας που απορρέει από την οδηγία 2009/140/EK και το ν. 4070/12¹⁰⁰.

Σχετικά, δε, με τις αρμοδιότητες που απονέμονται στην Α.Δ.Α.Ε., προβληματική εμφανίζεται και η διάταξη της παραγράφου υπ' αρ. 9 του άρθρου 37 του ν. 4070/2012 κατά την οποία ορίζεται ότι η τελευταία κατά την άσκηση του ελέγχου της, έχει την εξουσία και τις αρμοδιότητες που

⁹⁶ Βλ. ανωτέρω παραπομπή υπ' αρ. 85,

⁹⁷ Βλ. άρθρο 1, παράγραφος 2 ν. 4070/2012.

⁹⁸ Βλ. άρθρο 2, περίπτωση στ ν. 4070/2012.

⁹⁹ Υπό την έννοια του άρθρου 106, παράγραφος 2 ΣΑΕΕ.

¹⁰⁰ Βλ. *Κωνσταντίνο Χριστοδούλου*, ό.π.

προβλέπονται από το ν. 3115/2003¹⁰¹, το ν. 703/1977¹⁰² και το ν. 3673/2008¹⁰³, όπως ισχύουν. Αφενός ο ν. 703/1977 είχε ήδη καταργηθεί ρητώς από το ν. 3959/2011¹⁰⁴ ένα έτος νωρίτερα από την εισαγωγή του νόμου 4070/2012 και συνεπώς, η φράση «όπως ισχύει» δεν παραπέμπει στο νέο νόμο περί ελεύθερου ανταγωνισμού. Αφετέρου, και αν ακόμα η λανθασμένη παραπομπή διορθωθεί στο σωστό, θα πρέπει να διευκρινιστεί ρητώς ότι η βούληση του Έλληνα νομοθέτη ήταν να εφοδιαστεί η Α.Δ.Α.Ε. στο πλαίσιο του συνταγματικώς προσδιορισμένου σκοπού της μόνο με ανακριτικές και ελεγκτικές αρμοδιότητες της Επιτροπής Ανταγωνισμού και όχι να υπεισέλθει στον έλεγχο των θεμάτων ανταγωνισμού¹⁰⁵.

Στο ίδιο συμπέρασμα οδηγεί και η διάταξη της παραγράφου υπ' αρ. 2 του άρθρου 6 του ν. 3115/2003, η οποία ορίζει τις αρμοδιότητες της Α.Δ.Α.Ε. και η οποία, ομοίως, παραπέμπει στον καταργηθέντα ν. 703/1977 διευκρινίζοντας ότι «... τα μέλη και το προσωπικό της Α.Δ.Α.Ε., ... έχουν προς διαπίστωση των παραβάσεων της νομοθεσίας περί προστασίας του απορρήτου, τις εξουσίες και τα δικαιώματα που προβλέπονται στο ν. 703/1977, όπως ισχύει...». Ωστόσο, όπως ήδη ειπώθηκε ανωτέρω, ο ν. 703/1977 καταργήθηκε με το ν. 3959/2011 και ως εκ τούτου θα πρέπει να διορθωθεί η λανθασμένη παραπομπή σε αυτόν κατά το άρθρο 37, παράγραφος 9 του ν. 4070/2012. Διαφορετικά, η ανωτέρω λανθασμένη διατύπωση θα μπορούσε πιθανόν να παρερμηνευθεί ως δήθεν βούληση του νομοθέτη να απονείμει επιπροσθέτως στην Α.Δ.Α.Ε. και την επίβλεψη του ανταγωνισμού στα θέματα ασφάλειας ηλεκτρονικών επικοινωνιών¹⁰⁶, γεγονός που βέβαια δεν προκύπτει από το πνεύμα του ν. 4070/2012.

¹⁰¹ Ν. 3115/2003, «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών», ΦΕΚ Α' 47/2003.

¹⁰² Ν. 703/1977, «Έλεγχος Μονοπωλίων-Ολιγοπωλίων-Ελεύθερος Ανταγωνισμός», ΦΕΚ Α' 278/1977.

¹⁰³ Ν. 3674/2008, «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις», ΦΕΚ Α' 136/2008.

¹⁰⁴ Β. άρθρο 51 ν. 3959/2011 «Προστασία του ελεύθερου ανταγωνισμού», ΦΕΚ Α' 93/2011.

¹⁰⁵ Βλ. Γιώργο Ν. Γιαννόπουλο, ό.π., σελ. 198.

¹⁰⁶ Βλ. Γιώργο Ν. Γιαννόπουλο, ό.π.

Περαιτέρω, με εξουσιοδοτική βάση την παράγραφο 4 του άρθρου 37 του ως άνω νόμου, εκδόθηκε η υπ' αρ. 675/7/2013 απόφαση της Ε.Ε.Τ.Τ.¹⁰⁷ σχετικά με υποχρέωση των επιχειρήσεων που παρέχουν πρόσβαση σε δημόσια δίκτυα επικοινωνιών ή σε υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό, να κοινοποιούν στην Ε.Ε.Τ.Τ. κάθε παραβίαση της ασφάλειας ή απώλεια της ακεραιότητας, που είχε σημαντικό αντίκτυπο στη λειτουργία δικτύων ή υπηρεσιών τους. Ειδικότερα, στην εν λόγω απόφαση της Ε.Ε.Τ.Τ., προσδιορίζεται η έννοια του περιστατικού ασφάλειας¹⁰⁸, το οποίο ορίζεται ως ένα γεγονός το οποίο επηρεάζει την ακεραιότητα δικτύου ηλεκτρονικών επικοινωνιών ή τη συνέχεια παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών. Ρητά τονίζεται ότι στην έννοια αυτή δεν εμπίπτουν γεγονότα που επηρεάζουν το απόρρητο των επικοινωνιών¹⁰⁹, καθώς και προγραμματισμένες εργασίες συντήρησης ή αναβάθμισης συστημάτων οι οποίες επηρεάζουν τη συνέχεια παροχής υπηρεσιών στο βαθμό που αυτές υλοποιούνται σύμφωνα με τον προγραμματισμένο από τον πάροχο χρονοδιάγραμμα.

Επίσης, ορίζεται¹¹⁰ με βάση ορισμένη ποσοτική κλίμακα που υιοθετείται για τη μέτρηση του μεγέθους των περιστατικών ασφάλειας, το πότε ένα τέτοιο περιστατικό έχει «σημαντικό αντίκτυπο» κατά το νόμο, ώστε να υφίσταται υποχρέωση γνωστοποίησής του στην Ε.Ε.Τ.Τ. Τέλος, τίθεται η προθεσμία για τη δήλωση στην Ε.Ε.Τ.Τ του περιστατικού ασφάλειας από τον πάροχο σε δεκαπέντε εργάσιμες ημέρες¹¹¹ και επίσης αναφέρεται ότι οι πάροχοι οφείλουν να υποβάλουν εντός είκοσι εργασίμων ημερών από τη δημοσίευση της απόφασης, τις αναφορές ασφάλειας για όσα περιστατικά ασφάλειας έχουν λάβει χώρα από την 1/1/2012 μέχρι τη θέση της σε ισχύ.

¹⁰⁷ Βλ. υπ' αρ. 675/7/2013 απόφαση της Ε.Ε.Τ.Τ (ΦΕΚ Β' 107/24-1-20013).

¹⁰⁸ Βλ. άρθρο 2 της υπ' αρ. 675/7/2013 απόφασης της Ε.Ε.Τ.Τ (ΦΕΚ Β' 107/24-1-20013).

¹⁰⁹ Τα γεγονότα αυτά εμπίπτουν στο πεδίο εφαρμογής της υπ' αρ. 165/2011 απόφασης της Α.Δ.Α.Ε «Κανονισμός για τη διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών » (ΦΕΚ Β' 2715/17-11-2011).

¹¹⁰ Βλ. άρθρο 4 της υπ' αρ. 675/7/2013 απόφασης της Ε.Ε.Τ.Τ (ΦΕΚ Β' 107/24-1-20013).

¹¹¹ Βλ. άρθρο 6 της υπ' αρ. 675/7/2013 απόφασης της Ε.Ε.Τ.Τ (ΦΕΚ Β' 107/24-1-2013).

4. Ο ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΚΑΙ ΤΗΝ ΑΚΕΡΑΙΟΤΗΤΑ ΔΙΚΤΥΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ.

Σύμφωνα με τα προβλεπόμενα στο άρθρο 37 του ν. 4070/2012, η Α.Δ.Α.Ε. επεξεργάστηκε και έθεσε σε δημόσια διαβούλευση το σχέδιο «Κανονισμού για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών». Κατόπιν, εκδόθηκε η υπ' αρ. 205/2013 απόφαση της Α.Δ.Α.Ε. «Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών»¹¹²¹¹³ (εφεξής ο «Κανονισμός»). Ο Κανονισμός περιλαμβάνει συνολικά 21 άρθρα, με τα πρώτα δύο να αφορούν σε γενικές ρυθμίσεις σχετικά με το σκοπό-πεδίο εφαρμογής αυτού και στους ορισμούς των εννοιών του αντίστοιχα. Ακολούθως, στο άρθρο 3 ορίζονται οι γενικές υποχρεώσεις των παρόχων, ενώ στα άρθρα 5 έως 18 προσδιορίζονται οι ειδικές υποχρεώσεις που υπέχουν οι πάροχοι για την εκπλήρωση του ίδιου σκοπού (π.χ. υποχρέωση αποτίμησης κινδύνου, υποχρέωση εξασφάλισης επιχειρησιακής συνέχειας, υποχρέωση εξασφάλισης φυσικής ασφάλειας κλπ.).

Κατά την κατ' ιδίαν εξέταση των άρθρων του Κανονισμού και δη σύμφωνα με το άρθρο 1, ο σκοπός που τίθεται εν προκειμένω είναι ο καθορισμός των τεχνικών και οργανωτικών μέτρων που πρέπει να λαμβάνουν οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό για : α) την κατάλληλη διαχείριση του κινδύνου όσον αφορά στην ασφάλεια των δικτύων και υπηρεσιών, ώστε να εξασφαλίζεται επίπεδο ασφάλειας ανάλογο προς τον υφιστάμενο κίνδυνο, β) την αποτροπή και ελαχιστοποίηση των επιπτώσεων από περιστατικά ασφαλείας που επηρεάζουν τους χρήστες και τα διασυνδεδεμένα δίκτυα, γ) την ακεραιότητα των δικτύων τους, ώστε να διασφαλίζεται η συνέχεια της παροχής των υπηρεσιών που διανέμονται μέσω των δικτύων αυτών.

¹¹² ΦΕΚ Β' 1742/15-5-2013.

¹¹³ Ήδη μετά τη συμπλήρωση τριών ετών από την έκδοσή του Κανονισμού, ξεκίνησαν οι διαδικασίες για την τροποποίησή του, με τη δημόσια διαβούλευση να έχει ολοκληρωθεί στις 5 Οκτωβρίου 2016.

Στο άρθρο 2 του Κανονισμού επιχειρείται ο προσδιορισμός των βασικών του εννοιών. Ειδικότερα, ως ακεραιότητα ορίζεται η κατάσταση κατά την οποία το δίκτυο διατηρεί τη λειτουργικότητα για τη οποία έχει σχεδιαστεί. Περαιτέρω, ως περιστατικό ασφάλειας ορίζεται το γεγονός το οποίο επηρεάζει την ακεραιότητα δικτύου ηλεκτρονικών επικοινωνιών ή τη συνέχεια παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών. Διευκρινίζεται ότι δεν εμπίπτουν στην εν λόγω έννοια γεγονότα που επηρεάζουν το απόρρητο των επικοινωνιών καθώς και προγραμματισμένες εργασίες συντήρησης ή αναβάθμισης συστημάτων, οι οποίες επηρεάζουν τη συνέχεια παροχής υπηρεσιών, στο βαθμό που αυτές υλοποιούνται σύμφωνα με το προγραμματισμένο για τον πάροχο χρονοδιάγραμμα.. Τέλος, ορίζονται ως Συστήματα Δικτύου και Υπηρεσιών (εφεξής «ΣΔΥ») το υλικό και λογισμικό του παρόχου που είναι απαραίτητο για τη λειτουργία του δικτύου και των υπηρεσιών ηλεκτρονικών επικοινωνιών¹¹⁴. Για τους υπόλοιπους όρους που χρησιμοποιούνται στον Κανονισμό υπάρχει ρητή παραπομπή στους ορισμούς που περιλαμβάνονται στο ν. 4070/2012.

Στο άρθρο 3 του Κανονισμού προβλέπονται οι γενικές υποχρεώσεις του παρόχου για την πραγμάτωση των σκοπών που τίθενται κατά το άρθρο 1. Αναλυτικότερα, ορίζεται ότι ο πάροχος οφείλει να λαμβάνει όλα τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ικανοποίηση του σκοπού του Άρθρου 1. Επίσης, προβλέπεται η υποχρέωση του παρόχου για την τήρηση αρχείου σχετικά με την αναλυτική αντιστοίχιση της πολιτικής ασφάλειας με τις απαιτήσεις του κανονισμού, κατά την περίπτωση που αποφασιστεί από την Ε.Ε.Τ.Τ. η υποβολή τεκμηριωμένης πολιτικής ασφάλειας¹¹⁵, καθώς επίσης και η υποχρέωση καταγραφής και επαρκούς τεκμηρίωσης κάθε αδυναμίας συμμόρφωσης με αυτόν. Ακόμα, αναφέρεται ότι για την υλοποίηση των μέτρων και των απαιτήσεων του κανονισμού, ορίζονται, τεκμηριώνονται, εφαρμόζονται και αναθεωρούνται συγκεκριμένες διαδικασίες και οργανωτικές δομές. Προς το σκοπό αυτό, ορίζονται, περαιτέρω, συγκεκριμένες διοικητικές

¹¹⁴ Στον Κανονισμό αναφέρονται ενδεικτικά ως ΣΔΥ τα μέσα μετάδοσης και διασύνδεσης, οι μεταγωγείς (switches), οι δρομολογητές (router), τα συστήματα για την πρόσβαση στο διαδίκτυο, τα συστήματα διαχείρισης και εποπτείας αυτών και οι εξυπηρετητές ηλεκτρονικού ταχυδρομείου (e-mail servers).

¹¹⁵ Σύμφωνα με το άρθρο 37 παράγραφος 7 του ν. 4070/2012.

οντότητες ή φυσικά πρόσωπα και επιφορτίζονται με συγκεκριμένες αρμοδιότητες σχετικά με την εφαρμογή των μέτρων.

Επιπροσθέτως, στο πλαίσιο των γενικών του υποχρεώσεων, ο πάροχος οφείλει να ορίσει συγκεκριμένο εργαζόμενο του ως υπεύθυνο για την ασφάλεια και την ακεραιότητα των δικτύων και υπηρεσιών του, ο οποίος θα είναι επιφορτισμένος με την ευθύνη ελέγχου της υλοποίησης των μέτρων και των απαιτήσεων του κανονισμού και του οποίου τα στοιχεία επικοινωνίας θα κοινοποιούνται στην Α.Δ.Α.Ε. Επιπλέον, ο πάροχος υποχρεούται να διατηρεί τα στοιχεία για τα οποία προβλέπεται η υποχρέωση τήρησης στα άρθρα 4 έως 19 του παρόντος Κανονισμού, για χρονικό διάστημα δύο (2) ετών από την καταγραφή ή δημιουργία του αντίστοιχου τηρούμενου στοιχείου¹¹⁶. Επίσης, ο πάροχος ευθύνεται για το σύνολο των πράξεων οποιουδήποτε συνεργάτη, φυσικού ή νομικού προσώπου, χρησιμοποιεί για την κατασκευή, εγκατάσταση, συντήρηση ή λειτουργία του δικτύου του και για την παροχή των υπηρεσιών ηλεκτρονικών επικοινωνιών, τον οποίο οφείλει να ενημερώνει προσηκόντως σχετικά με τα τηρούμενα μέτρα για την ασφάλεια και την ακεραιότητα των δικτύων και υπηρεσιών του, λαμβάνοντας υπόψη τη φύση της παρεχόμενης εργασίας, και να απαιτεί την αποδοχή, εκ μέρους τους, της υποχρέωσης τήρησης εκείνων των μέτρων ασφάλειας που έχουν εφαρμογή σύμφωνα με την εργασία που προσφέρει ο καθένας από αυτούς. Περαιτέρω, σε περιπτώσεις εκτάκτων αναγκών ο πάροχος οφείλει να συνεργάζεται με τις αρμόδιες αρχές, και να εφαρμόζει όποτε αυτό είναι αναγκαίο σχέδιο εκτάκτων αναγκών, με το οποίο θα προσδιορίζεται η διαδικασία με την οποία θα παρέχει υπηρεσίες σε περιοχές που έχουν κηρυχτεί σε έκτακτη ανάγκη και για όσο διάστημα αυτή υφίσταται σύμφωνα με την κείμενη νομοθεσία. Τέλος, ο πάροχος πρέπει να συμμορφώνεται με πρότυπα ή προδιαγραφές που θεσπίζονται σε κοινοτικό επίπεδο, χαρακτηρίζονται ως υποχρεωτικές και έχουν δημοσιευθεί σε κατάλογο προτύπων ή και προδιαγραφών στην Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων για την παροχή υπηρεσιών, τεχνικών διεπαφών ή και λειτουργιών δικτύων, ενώ σε

¹¹⁶ Υπό την επιφύλαξη, βέβαια, των διατάξεων των ν.3471/2006, ν.3783/2009 και ν.3917/2011, όπως ισχύουν, καθώς και του άρθρου 5 παράγραφος 9 εδ. β' της υπ' αριθμ.675/7 Απόφασης της ΕΕΤΤ «Υποβολή Αναφορών Παρόχων σχετικά με την Αδιάλειπτη Λειτουργία Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών».

περίπτωση που δεν έχουν δημοσιευθεί τέτοια πρότυπα με άλλα αναγνωρισμένα διεθνή πρότυπα¹¹⁷. Ο πάροχος εφαρμόζει πάντοτε την τελευταία έκδοση των προτύπων αυτών.

Εν συνεχεία, ορίζονται οι ειδικές υποχρεώσεις του παρόχου αναφορικά με την εκπλήρωση των στόχων που έχουν τεθεί στο άρθρο 1. Ειδικότερα, στο άρθρο 4 του Κανονισμού, προβλέπονται τα επιχειρησιακά μέτρα που οφείλει να λάβει ο πάροχος. Συγκεκριμένα, ο πάροχος εντοπίζει τις επιχειρησιακές λειτουργίες και τους πόρους που υποστηρίζουν τις λειτουργίες αυτές και σχετίζονται ή μπορεί να επηρεάσουν την ακεραιότητα του δικτύου και τη διαθεσιμότητα των υπηρεσιών και προσδιορίζει τις επιπτώσεις που δύνανται να επέλθουν από διαταραχές που μπορεί να επηρεάσουν τις εν λόγω επιχειρησιακές λειτουργίες. Επίσης, ο πάροχος ορίζει το αποδεκτό χρονικό διάστημα αποκατάστασης των επιχειρησιακών λειτουργιών από τις πιθανές διαταραχές, έτσι ώστε να επηρεαστεί κατ' ελάχιστον η λειτουργία του δικτύου και η διαθεσιμότητα των υπηρεσιών και κατηγοριοποιεί τις επιχειρησιακές λειτουργίες του σε σχέση με τις προτεραιότητες για αποκατάσταση και προσδιορίζει τις κρίσιμες επιχειρησιακές λειτουργίες. Περαιτέρω, καθορίζει τους πόρους (ΣΔΥ, εγκαταστάσεις, προσωπικό) που απαιτούνται για τη συνέχιση κάθε κρίσιμης επιχειρησιακής λειτουργίας, καθώς και τυχόν εξαρτήσεις αυτών. Επιπροσθέτως, αναθεωρεί περιοδικά, και κατ' ελάχιστον ανά δύο (2) έτη, την Ανάλυση Επιχειρησιακών Επιπτώσεων λαμβάνοντας υπόψη: α) επιχειρησιακές, οργανωτικές, ή τεχνολογικές αλλαγές, β) αλλαγές στο νομοθετικό πλαίσιο, σε εθνικό ή κοινοτικό επίπεδο και γ) τα αποτελέσματα των διενεργούμενων ελέγχων και δ) άλλα δεδομένα τα οποία οφείλει να λάβει υπόψη του. Ο πάροχος τηρεί καταγεγραμμένα τα ακόλουθα: α) περιγραφή της εφαρμοσθείσας μεθοδολογίας ανάλυσης επιχειρησιακών επιπτώσεων, β) τα αποτελέσματα της ανάλυσης επιχειρησιακών επιπτώσεων, γ) τα ενδιάμεσα αποτελέσματα μεταξύ όλων των σταδίων προκειμένου όλη η διαδικασία να είναι τεκμηριωμένη και πλήρης.

¹¹⁷ Ειδικότερα, σε περίπτωση που δεν έχουν δημοσιευθεί κοινοτικά πρότυπα και προδιαγραφές, εφαρμόζονται πρότυπα ή και προδιαγραφές που θεσπίζονται από τους Ευρωπαϊκούς Οργανισμούς Τυποποίησης και έχουν υιοθετηθεί με αποφάσεις του Υπουργού Ανάπτυξης, Ανταγωνιστικότητας, Υποδομών, Μεταφορών και Δικτύων. Ελλείψει τέτοιων προτύπων ή και προδιαγραφών, εφαρμόζονται διεθνή πρότυπα ή συστάσεις που εγκρίνονται από τη Διεθνή Ένωση Τηλεπικοινωνιών (ITU), τον Διεθνή Οργανισμό Τυποποίησης (ISO) ή τη Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC).

Επίσης, σύμφωνα με το άρθρο 5 του Κανονισμού, ο πάροχος υποχρεούται να υλοποιεί αποτίμηση κινδύνου. Έτσι, αναγνωρίζει και εξετάζει τόσο ενδογενείς απειλές, οι οποίες εξαρτώνται από το επίπεδο της εσωτερικής αξιοπιστίας, ασφάλειας και ανθεκτικότητας του δικτύου, όσο και εξωγενείς απειλές, όπως καιρικές συνθήκες, φυσικές καταστροφές, ατυχήματα και πράξεις δολιοφθοράς, οι οποίες μπορούν να προκαλέσουν προσωρινή ή παρατεταμένη διακοπή των κρίσιμων επιχειρησιακών λειτουργιών. Επίσης, εξετάζει απειλές, οι οποίες ενδεχομένως προέρχονται από άλλα διασυνδεδεμένα δίκτυα, καταρτίζει κατάλογο με διαφορετικές εκτιμώμενες βλάβες που μπορούν να συμβούν σε πόρους του λόγω της εκδήλωσης των απειλών και αναγνωρίζει τα ευάλωτα σημεία και τις αδυναμίες των πόρων, (ΣΔΥ, εγκαταστάσεις, προσωπικό), που απαιτούνται για τη συνέχιση κάθε κρίσιμης επιχειρησιακής λειτουργίας.

Σε συνάρτηση με τα ανωτέρω, ο πάροχος, στο πλαίσιο της αποτίμησης του κινδύνου που υλοποιεί, αξιολογεί την πιθανότητα πραγματοποίησης των απειλών που έχει αναγνωρίσει, εκτιμά την επίδρασή τους στη λειτουργία του δικτύου και των παρεχόμενων υπηρεσιών, λαμβάνοντας υπόψη τα ευάλωτα σημεία και τις αδυναμίες του δικτύου του. Ακόμα, λαμβάνοντας υπόψη τα αποτελέσματα της αποτίμησης κινδύνου, προσδιορίζει τον τρόπο με τον οποίο θα αντιμετωπίσει τους κινδύνους που σχετίζονται με τις κρίσιμες επιχειρησιακές λειτουργίες, εφαρμόζει τα κατάλληλα μέτρα για την αντιμετώπισή τους και προσδιορίζει και εφαρμόζει διαδικασίες αξιολόγησης της αποτελεσματικότητας των μέτρων που εφαρμόζει. Επιπροσθέτως, ο πάροχος αναθεωρεί την αποτίμηση κινδύνου περιοδικά, και κατ' ελάχιστον ανά δύο (2) έτη, λαμβάνοντας υπόψη: α) την αποτελεσματικότητα των εφαρμοζόμενων μέτρων, β) την αναγνώριση νέων απειλών, γ) οργανωτικές ή τεχνολογικές αλλαγές, δ) αλλαγές στο νομοθετικό πλαίσιο, σε εθνικό ή κοινοτικό επίπεδο, ε) τα αποτελέσματα των ελέγχων που πραγματοποιούνται από τις Ελεγκτικές Αρχές και τις σχετικές υποδείξεις τους και στ) άλλα γεγονότα που θα έθεταν νέα δεδομένα τα οποία οφείλει να λάβει υπόψη. Ο πάροχος, επίσης, οφείλει να τηρεί καταγεγραμμένα: α) την περιγραφή της εφαρμοσθείσας μεθοδολογίας αξιολόγησης επικινδυνότητας, β) τα αποτελέσματα της αξιολόγησης επικινδυνότητας, γ) τα προτεινόμενα μέτρα

και δ) τα ενδιάμεσα αποτελέσματα μεταξύ όλων των σταδίων, προκειμένου όλη η διαδικασία να είναι τεκμηριωμένη και πλήρης.

Σύμφωνα με το άρθρο 6 του Κανονισμού, ο πάροχος υποχρεούται να εξασφαλίσει την επιχειρησιακή συνέχεια, τηρώντας τις ακόλουθες απαιτήσεις και δη: α) να ορίζει το προσωπικό που εμπλέκεται στην περίπτωση που απειλείται η επιχειρησιακή συνέχεια του παρόχου, καθώς και του ρόλου και των αρμοδιοτήτων του προσωπικού αυτού, β) να ορίζει τις συνθήκες κατά τις οποίες ενεργοποιείται το σχέδιο επιχειρησιακής συνέχειας και το εξουσιοδοτημένο για την ενεργοποίησή του προσωπικό, γ) να ορίζει τις διαδικασίες διάχυσης πληροφορίας στο αρμόδιο προσωπικό σχετικά με το εκάστοτε πρόβλημα, δ) να ορίζει τις λειτουργικές διαδικασίες για την ανάλυση και εκτίμηση του προβλήματος, ε) να ορίζει τις ενέργειες κατά προτεραιότητα, τις διαδικασίες και τους πόρους που απαιτούνται για την αποκατάσταση του δικτύου και των υπηρεσιών και το χρονοδιάγραμμα υλοποίησης, στ) να ορίζει τους εκτιμώμενους χρόνους αποκατάστασης σε διαφορετικές συνθήκες βλάβης, ζ) να ορίζει τους τρόπους και στοιχεία επικοινωνίας του προσωπικού του παρόχου με τεχνικούς, προμηθευτές, εργολάβους του παρόχου, με παρόχους άλλων δικτύων καθώς και διαδικασίες συνεργασίας μεταξύ τους, που αφορούν στην υλοποίηση του σχεδίου επιχειρησιακής συνέχειας, η) ορίζει τις πληροφορίες σχετικά με τη διαθεσιμότητα εξοπλισμού αντικατάστασης και θ) να ορίζει την αξιολόγηση των μέτρων που ελήφθησαν για την επίλυση συγκεκριμένου προβλήματος και διαδικασίες αναθεώρησης του σχεδίου επιχειρησιακής συνέχειας. Στο πλαίσιο αυτό, επίσης, ο πάροχος προσδιορίζει τα απαιτούμενα μέτρα, με στόχο τη διατήρηση της διαθεσιμότητας του δικτύου και των υπηρεσιών που παρέχονται στο κοινό και τη διατήρηση του υψηλότερου δυνατού επιπέδου υπηρεσιών, για την ανταπόκριση στις απαιτήσεις των δημοσίων αρχών σε περίπτωση καταστροφικής βλάβης ή ανωτέρας βίας και ορίζει προσωπικό, το οποίο θα είναι υπεύθυνο για την εκπόνηση και την αναθεώρηση του σχεδίου ανάκαμψης από καταστροφή. Τα μέτρα για την τήρηση των ανωτέρω απαιτήσεων, θα αναθεωρούνται και θα αναπροσαρμόζονται από τον πάροχο σε τακτά χρονικά διαστήματα, λαμβάνοντας υπόψη περιστατικά ασφάλειας που ενδεχομένως έλαβαν χώρα κατά το παρελθόν και τα αποτελέσματα που

προκύπτουν από δοκιμές και ασκήσεις. Επιπλέον, τα μέτρα αυτά θα τηρούνται καταγεγραμμένα, καθώς και τα ενδιάμεσα αποτελέσματα, μεταξύ όλων των σταδίων εκπόνησής τους, προκειμένου όλη η διαδικασία να είναι τεκμηριωμένη και πλήρης.

Επίσης, όπως ορίζεται στο άρθρο 7 του Κανονισμού, ο πάροχος οφείλει να ελέγχει το δίκτυό του και να προβαίνει σε προγραμματισμένες ασκήσεις (δοκιμές), τεχνικούς ελέγχους διείσδυσης (penetrations tests) και αξιολόγηση αδυναμιών ασφάλειας (vulnerability assessment). Ως εκ τούτου, οφείλει να διαθέτει καταγεγραμμένες διαδικασίες βάσει των οποίων πραγματοποιούνται οι συγκεκριμένοι έλεγχοι. Η συχνότητα και το εύρος των ελέγχων καθορίζεται από τους κινδύνους που έχουν αναγνωριστεί και από τα εφαρμοζόμενα μέτρα ασφάλειας. Επίσης, ο πάροχος, λαμβάνοντας υπόψη του τα αποτελέσματα των ανωτέρω ελέγχων, προσδιορίζει τις διορθωτικές ενέργειες και τροποποιεί και ενημερώνει τα σχέδιά του σύμφωνα με αυτές. Επιπροσθέτως, σε σχέση με τη διενέργεια των ως άνω ελέγχων, τηρεί καταγεγραμμένα τα ακόλουθα: α) περιγραφή της εφαρμοσθείσας μεθοδολογίας τους, β) τα αποτελέσματα των εν λόγω ελέγχων αποτελεσματικότητας, γ) τα ενδιάμεσα αποτελέσματα μεταξύ όλων των σταδίων εκπόνησης των ανωτέρω ελέγχων αποτελεσματικότητας, ώστε η όλη διαδικασία να είναι τεκμηριωμένη και πλήρης.

Ακολούθως, στο άρθρο 8, καθορίζεται η υποχρέωση αποδεκτής χρήσης του δικτύου από όλους τους προστηθέντες του παρόχου. Αναλυτικότερα, οι εργαζόμενοι και συνεργάτες του παρόχου οφείλουν να συμμορφώνονται προς τα μέτρα που προβλέπονται στον Κανονισμό. Για το σκοπό αυτό, ο πάροχος οφείλει να καταγράφει τον τρόπο με τον οποίο εξασφαλίζει ότι οι εργαζόμενοι και οι συνεργάτες του λαμβάνουν γνώση και έχουν αποδεχτεί τα μέτρα για την ασφάλεια και την ακεραιότητα των δικτύων και υπηρεσιών. Επιπλέον, ο πάροχος οφείλει να ενημερώνει με πρόσφορα μέσα και να εκπαιδεύει τους εργαζόμενους και συνεργάτες του σχετικά με τα ανωτέρω μέτρα. Οι εργαζόμενοι και συνεργάτες του παρόχου, οι οποίοι αποκτούν πρόσβαση στα ΣΔΥ και τα δεδομένα αυτών, δεν επιτρέπεται να αποκαλύπτουν οποιαδήποτε πληροφορία ή στοιχείο υποπίπτει στην αντίληψή τους ή την κατοχή τους, ως αποτέλεσμα της φύσης της εργασίας τους. Περαιτέρω, οι εργαζόμενοι και

συνεργάτες του παρόχου υποχρεούνται να ενημερώνουν άμεσα το αρμόδιο προσωπικό του σε περίπτωση που υποπέσει στην αντίληψή τους ένα κενό ασφάλειας ή σχετικό περιστατικό που θέτει σε κίνδυνο την ακεραιότητα των παρεχόμενων δικτύων και υπηρεσιών.

Το άρθρο 9 αναφέρεται στην υποχρέωση του παρόχου να μεριμνά για τη φυσική ασφάλεια των εγκαταστάσεων στις οποίες είναι εγκατεστημένα ΣΔΥ. Τα μέτρα που λαμβάνονται για τη φυσική ασφάλεια περιλαμβάνουν την αποτροπή μη εξουσιοδοτημένης πρόσβασης και την προστασία από φυσικές καταστροφές, που προκαλούνται από φαινόμενα όπως ο σεισμός, η υγρασία, οι πλημμύρες, η υπερθέρμανση, η φωτιά, ο κεραυνός. Στο πλαίσιο αυτό, ο πάροχος οφείλει να διαθέτει και να εφαρμόζει διαδικασία φυσικής πρόσβασης, στην οποία περιγράφονται αναλυτικά όλες οι ενέργειες που απαιτούνται για την φυσική πρόσβαση των εργαζομένων, συνεργατών και επισκεπτών στις εγκαταστάσεις του. Επίσης, οφείλει να ορίσει ασφαλείς χώρους εντός των εγκαταστάσεών του, στους οποίους εγκαθίστανται τα ΣΔΥ. Οι χώροι αυτοί, πρέπει να προστατεύονται με επιπρόσθετους ισχυρούς μηχανισμούς ασφάλειας και ελεγχόμενης πρόσβασης, τηρουμένης της κείμενης νομοθεσίας, οι οποίοι επιτρέπουν τον έλεγχο της πρόσβασης και την ταυτοποίηση των ατόμων που εισέρχονται σε αυτούς¹¹⁸.

Περαιτέρω, ο πάροχος οφείλει να λαμβάνει υπόψη του, κατά την επιλογή ή κατασκευή των εγκαταστάσεων, στις οποίες εγκαθιστά ΣΔΥ, καθώς και κατά την τοποθέτηση εξοπλισμού και υλοποίηση μέτρων φυσικής προστασίας, τις ιδιαίτερες φυσικές και άλλες συνθήκες οι οποίες επικρατούν στην περιοχή¹¹⁹. Ακόμα, ο πάροχος μεριμνά ώστε τα κρίσιμα στοιχεία του δικτύου να είναι εγκατεστημένα σε διαφορετικές εγκαταστάσεις ή σε χώρους φυσικά ανεξάρτητους. Όπου αυτό δεν είναι δυνατόν, αυτά θα πρέπει να προστατεύονται από ανεξάρτητα μέσα φυσικής προστασίας. Τέλος, επιλέγει, όπου είναι τεχνικά εφικτό, την υπόγεια εγκατάσταση καλωδίων από την

¹¹⁸ Ενδεικτικά αναφέρονται τα ακόλουθα μέτρα: κλειστό κύκλωμα τηλεόρασης, αυτόματο σύστημα συναγερμού που αναφέρει κάθε εξωτερική παραβίαση εντός των χώρων, ειδικές κάρτες αναγνώρισης για τους εργαζόμενους και τους συνεργάτες του παρόχου.

¹¹⁹ Ενδεικτικά αναφέρονται τα ακόλουθα μέτρα: ανιχνευτής φωτιάς, θερμοκρασίας και υγρασίας.

εναέρια εγκατάσταση, συνεργάζεται με τις υπηρεσίες, οι οποίες ενδεχομένως εκτελούν εργασίες δημόσιου ενδιαφέροντος, όπως ενδεικτικά έργα οδοποιίας ή αποχέτευσης, με στόχο την ελαχιστοποίηση της πιθανότητας ζημίας στα ΣΔΥ και μεριμνά για την τακτική συντήρηση των εγκαταστάσεων, στις οποίες είναι εγκατεστημένα ΣΔΥ.

Με το άρθρο 10 του Κανονισμού ιδρύεται η υποχρέωση του παρόχου να εξασφαλίζει ότι υπάρχει στο δίκτυό του η κατάλληλη εφεδρεία, έτσι ώστε πιθανή βλάβη σε κάποιο ΣΔΥ να μην επηρεάσει καθοριστικά τη λειτουργία του δικτύου ή τις παρεχόμενες υπηρεσίες. Έτσι, οφείλει να υλοποιεί λύσεις εφεδρείας, οι οποίες είναι ανάλογες της κρισιμότητας των ΣΔΥ, όπως αυτή έχει προκύψει από την Αξιολόγηση Επικινδυνότητας. Για τα κρίσιμα ΣΔΥ, ο πάροχος υλοποιεί λύσεις αυτόματης εφεδρείας, οι οποίες επιτρέπουν την αδιάλειπτη λειτουργία του δικτύου. Σε περιπτώσεις που για κρίσιμα ΣΔΥ δεν είναι δυνατή η ύπαρξη μηχανισμού αυτόματης εφεδρείας, ο πάροχος οφείλει να λάβει όλα τα απαραίτητα μέτρα και να προβεί στις απαραίτητες ενέργειες για την ταχεία αποκατάσταση των λειτουργιών τους και την ελαχιστοποίηση των επιπτώσεων ενδεχόμενης βλάβης αυτών. Όπου υπάρχει η δυνατότητα, ο πάροχος υλοποιεί την εφεδρεία με τέτοιο τρόπο, ώστε τα ΣΔΥ, τα οποία παρέχουν εφεδρεία μεταξύ τους, να είναι τοποθετημένα σε διαφορετικές εγκαταστάσεις. Εάν τα ΣΔΥ αυτά δεν είναι τεχνικά εφικτό να τοποθετηθούν σε διαφορετικές εγκαταστάσεις, θα πρέπει, όπου αυτό είναι δυνατόν, να είναι τοποθετημένα σε χώρους με ανεξάρτητα μέσα φυσικής προστασίας. Περαιτέρω, ο πάροχος διασφαλίζει ότι υπάρχουν λειτουργικά διαθέσιμοι εφεδρικοί μηχανισμοί εναλλάξιμης και φυσικά ανεξάρτητης όδευσης, ιδίως για βαθμίδες του δικτύου υψηλότερης ιεραρχικά τάξης του δικτύου πρόσβασης.

Επιπλέον, σύμφωνα με το άρθρο 11, ο πάροχος οφείλει να μεριμνά για την προστασία των ΣΔΥ από διακοπές ή διαταραχές του δημοσίου δικτύου τροφοδοσίας ισχύος, ώστε να εξασφαλίζεται η αδιάλειπτη λειτουργία των στοιχείων αυτών. Ειδικότερα, ο πάροχος οφείλει να μεριμνά ώστε η παροχή του δημοσίου δικτύου τροφοδοσίας ισχύος προς τα ΣΔΥ να γίνεται βάσει των ενδεδειγμένων προδιαγραφών. Στην περίπτωση διακοπής του δημοσίου δικτύου τροφοδοσίας ισχύος, ο πάροχος οφείλει να εφαρμόζει τρόπους/μέσα εφεδρικής τροφοδοσίας. Για τον καθορισμό του χρόνου για τον οποίο

εξασφαλίζεται η συνέχεια λειτουργίας των ΣΔΥ μέσω εφεδρικής τροφοδοσίας, λαμβάνονται υπόψη τα αποτελέσματα της Αξιολόγησης Επικινδυνότητας. Όπου αυτό είναι δυνατόν, τα ΣΔΥ δεν εξυπηρετούνται από την ίδια πηγή τροφοδοσίας. Τα εφαρμοζόμενα μέσα συντηρούνται σύμφωνα με τις προδιαγραφές του κατασκευαστή και λαμβάνονται όλα τα μέτρα για την εξασφάλιση της εύρυθμης λειτουργίας τους. Σε περίπτωση που για τη λειτουργία των μέσων εφεδρικής τροφοδοσίας απαιτούνται πρώτες ύλες ή άλλα υλικά, ο πάροχος οφείλει να διαθέτει και να εφαρμόζει διαδικασίες για την εξασφάλιση της επαρκούς διαθεσιμότητάς τους.

Εν συνεχεία, κατά τα προβλεπόμενα στο άρθρο 12, ο πάροχος οφείλει να διαθέτει μηχανισμούς ελέγχου λογικής πρόσβασης για την απόκτηση πρόσβασης των εργαζομένων και συνεργατών του στα ΣΔΥ. Συγκεκριμένα, ο ελάχιστος έλεγχος πρόσβασης επιτυγχάνεται με τη χρήση ενός λογαριασμού πρόσβασης, που αποτελείται από ένα ζεύγος ονόματος χρήστη και κωδικού πρόσβασης. Κατά τη λογική πρόσβαση των εργαζομένων και συνεργατών του παρόχου στα ΣΔΥ θα πρέπει να εξασφαλίζεται η αντιστοίχιση του συγκεκριμένου προσώπου, η οποία μάλιστα θα καταγράφεται σε ειδικό αρχείο, με την πρόσβαση και τις ενέργειες που τελούνται σε κάθε ΣΔΥ, είτε αυτή πραγματοποιείται από προσωπικό λογαριασμό πρόσβασης είτε από κοινό ή προκαθορισμένο λογαριασμό. Πέραν αυτού, ο πάροχος οφείλει να καταγράφει τις διαφορετικές κατηγορίες χρηστών και τα δικαιώματα πρόσβασης που αποδίδονται σε αυτές για κάθε ΣΔΥ. Στην κατεύθυνση αυτή, ο πάροχος οφείλει να διαθέτει διαδικασία διαχείρισης χρηστών, στην οποία περιγράφεται κάθε περίπτωση προσθήκης ή διαγραφής χρηστών και η απονομή και η μεταβολή των δικαιωμάτων ή επιπέδων πρόσβασης και να διαθέτει κανόνες, οι οποίοι τηρούνται σε σχετικό αρχείο, αναφορικά με τη δημιουργία και διαχείριση των λογαριασμών πρόσβασης.

Η λογική πρόσβαση εργαζομένων και συνεργατών στα ΣΔΥ θα πρέπει να περιορίζεται στις περιπτώσεις που αυτό είναι απαραίτητο για τις επιχειρησιακές ανάγκες του παρόχου. Επίσης, ο πάροχος οφείλει να έχει καταγεγραμμένα τα ΣΔΥ, στα οποία επιτρέπεται η λογική πρόσβαση, καθώς και τους τρόπους με τους οποίους πραγματοποιείται αυτή από τους εργαζόμενους και τους συνεργάτες και να διατηρεί αρχείο με τους

εργαζόμενους και συνεργάτες, οι οποίοι έχουν εξουσιοδοτηθεί για χρήση της λογικής πρόσβασης. Η λογική πρόσβαση των εργαζομένων και συνεργατών πραγματοποιείται με χρήση μηχανισμών ασφαλούς αυθεντικοποίησης και κρυπτογράφησης. Επιπροσθέτως, η λογική πρόσβαση των συνεργατών του παρόχου θα πρέπει να επιτρέπεται μόνο για συγκεκριμένο χρονικό διάστημα, λαμβανομένου υπόψη του απαιτούμενου χρόνου διεκπεραίωσης της αντίστοιχης εργασίας. Αυτό είναι δυνατόν είτε με τη χρήση προσωρινών κωδικών, οι οποίοι θα μεταβάλλονται μετά το πέρας του προκαθορισμένου χρονικού διαστήματος, είτε με την απενεργοποίηση των λογαριασμών μετά το πέρας του διαστήματος αυτού. Τέλος, ο πάροχος οφείλει να επιτρέπει τη λογική πρόσβαση των συνεργατών του μόνο κατόπιν έγκρισης των σχετικών αιτημάτων, στα οποία αναγράφονται όλες οι

σχετικές πληροφορίες (λόγος της πρόσβασης, σύστημα, χρονικό διάστημα).

Το άρθρο 13 καθιερώνει την υποχρέωση του παρόχου να μεριμνά για την ασφάλεια του περιμέτρου δικτύου. Ο πάροχος, δηλαδή, οφείλει να πραγματοποιεί λογικό διαχωρισμό του δικτύου του από εξωτερικά δίκτυα και κατάτμηση αυτού σε ζώνες ασφάλειας ή υποδίκτυα με στόχο την απομόνωση των ΣΔΥ σε ζώνες ασφάλειας, τον έλεγχο ροής δεδομένων μεταξύ τους και την προστασία από κακόβουλες ενέργειες. Προς το σκοπό αυτό, οφείλει να διαθέτει μηχανισμούς και συστήματα¹²⁰ των οποίων η λειτουργία και η τεχνική διαμόρφωση λαμβάνει υπόψη τις διεθνείς, ευρέως αποδεκτές πρακτικές και πρότυπα και την αποτίμηση κινδύνου, όπως περιγράφεται στο άρθρο 5 του Κανονισμού, καθώς επίσης και να διατηρεί τη διαμόρφωση των προαναφερομένων μηχανισμών και συστημάτων πλήρως επικαιροποιημένη. Η λειτουργία των ανωτέρω μηχανισμών και συστημάτων πρέπει να είναι απρόσκοπτη και συνεχής, με την εξαίρεση των περιπτώσεων προγραμματισμένης συντήρησης ή αναβάθμισης. Ο πάροχος οφείλει να παραμετροποιεί και να διαμορφώνει τους ως άνω μηχανισμούς και συστήματα, κατά τέτοιο τρόπο, ώστε να επιτυγχάνεται ο περιορισμός της εξάπλωσης και των επιπτώσεων του κακόβουλου λογισμικού και επίσης οφείλει να καταγράφει την αρχιτεκτονική που έχει υλοποιηθεί, τις ζώνες

¹²⁰ Ενδεικτικά αναφέρονται: αναχώματα ασφάλειας, συστήματα ανίχνευσης και αποτροπής εισβολών, λίστες ελέγχου πρόσβασης, ιδεατά ιδιωτικά δίκτυα κλπ.

ασφάλειας και τα ΣΔΥ που έχουν τοποθετηθεί σε κάθε ζώνη, λαμβάνοντας υπόψη τους μηχανισμούς και τα συστήματα, που χρησιμοποιεί. Στην περίπτωση που διατίθενται στο κοινό υπηρεσίες που απαιτούν πρόσβαση σε εξυπηρετητές από εξωτερικά δίκτυα¹²¹, τα ΣΔΥ που προσφέρουν αυτές τις υπηρεσίες πρέπει να τοποθετούνται σε μία ή περισσότερες αποστρατικοποιημένες ζώνες.

Κατά το άρθρο 14, ο πάροχος οφείλει να παρακολουθεί την υφιστάμενη κίνηση του δικτύου και τη διαθεσιμότητα των προσφερόμενων υπηρεσιών, να πραγματοποιεί συνεχείς μετρήσεις κίνησης και φόρτου του δικτύου να αναλύει τα προβλήματα και να προβλέπει τις μελλοντικές του ανάγκες, ώστε να προβαίνει έγκαιρα στις απαραίτητες ενέργειες για τη διασφάλιση της διαθεσιμότητας¹²². Ειδικότερα, ο πάροχος οφείλει να προστατεύει το δίκτυό του από συνθήκες αυξημένης κίνησης και να χρησιμοποιεί τεχνικές διαχείρισης κίνησης για να παρακολουθεί και να ελέγχει την κίνηση στο δίκτυό του και να εντοπίζει έγκαιρα την αύξηση κίνησης, προβαίνοντας στις κατάλληλες ενέργειες, ώστε να προστατεύει το δίκτυό του από ενδεχόμενη συμφόρηση λόγω αυξημένης κίνησης, εξασφαλίζοντας παράλληλα τη βελτιστοποίηση της απόδοσης του δικτύου. Περαιτέρω, ο πάροχος οφείλει να προβαίνει σε προβλέψεις αναφορικά με περιοδικά ή μη γεγονότα, τα οποία ενδέχεται να προκαλέσουν σημαντική αύξηση της κίνησης στο δίκτυό του, όπως είναι για παράδειγμα οι εθνικές ή θρησκευτικές εορτές και οι διαγωνισμοί εθνικής εμβέλειας σε ιδιαίτερα περιορισμένο χρονικό διάστημα. Επίσης, οφείλει να παρακολουθεί την επικαιρότητα, στο βαθμό που αυτή ενδέχεται να επηρεάσει την κίνηση στο δίκτυό του, όπως, ενδεικτικά, σε περίπτωση καταστροφών ή φυσικών φαινομένων, εθνικής ή τοπικής εμβέλειας. Ακόμα, υποχρεούται να καταγράφει τις τεχνικές διαχείρισης κίνησης και τις συνθήκες υπό τις οποίες τις εφαρμόζει.

Στο πλαίσιο αυτό, ο πάροχος καταγράφει τα μέτρα τα οποία χρησιμοποιεί, προκειμένου να εξασφαλίσει την προτεραιότητα της κίνησης προς τις υπηρεσίες έκτακτης ανάγκης, ιδιαίτερα σε καταστάσεις εκτάκτων συνθηκών.

¹²¹ Π.χ. υπηρεσίες ηλεκτρονικού ταχυδρομείου.

¹²² Όπως για παράδειγμα η εισαγωγή νέων ΣΔΥ, η επέκταση ή αναβάθμιση υφιστάμενων ΣΔΥ και η αλλαγή στη διαμόρφωση των ΣΔΥ.

Επίσης, εξασφαλίζει τους απαραίτητους μηχανισμούς, ώστε πιθανή βλάβη σε κάποιο ΣΔΥ να μην επηρεάσει καθοριστικά τη λειτουργία του δικτύου ή τις παρεχόμενες υπηρεσίες. Ως εκ τούτου, οφείλει να διαθέτει κατάλληλους μηχανισμούς για τη διαχείριση του δικτύου του, ώστε να προλαβαίνει τυχόν βλάβες ή να τις αποκαθιστά άμεσα σε περίπτωση εμφάνισής τους¹²³. Ο πάροχος αξιολογεί και αξιοποιεί πιθανές πληροφορίες που προκύπτουν από χρήστες του δικτύου σχετικά με προβλήματα που παρουσιάζονται αναφορικά με τη διαθεσιμότητα. Επιπλέον, ενημερώνεται συνεχώς, μέσω συστημάτων παρακολούθησης και ενημέρωσης, για ενέργειες ή αλλαγές που γίνονται στα ΣΔΥ, οι οποίες είναι πιθανόν να οδηγήσουν στην εκδήλωση περιστατικού ασφάλειας¹²⁴.

Σύμφωνα με το άρθρο 15 καθιερώνεται η διπλή υποχρέωση του παρόχου αφενός για συντήρηση του εξοπλισμού του, αφετέρου για διαχείριση των αλλαγών των ΣΔΥ. Αναλυτικότερα, ο πάροχος οφείλει να εκτελεί προληπτική συντήρηση του εξοπλισμού του, καθώς και των κτηρίων στα οποία αυτός στεγάζεται, βάσει προδιαγεγραμμένου χρονοδιαγράμματος, προκειμένου να ελαχιστοποιηθεί η πιθανότητα δυσλειτουργίας του δικτύου και των παρεχόμενων υπηρεσιών. Επίσης, υποχρεούται να πραγματοποιεί τις εργασίες συντήρησης, αναβάθμισης ή άλλες τεχνικές επεμβάσεις στο δίκτυο και τις παρεχόμενες υπηρεσίες, χωρίς να διακόπτεται η λειτουργία τους. Όπου αυτό δεν είναι τεχνικά εφικτό, ο πάροχος επιλέγει οι εργασίες αυτές να πραγματοποιούνται σε ώρες χαμηλής κίνησης. Παράλληλα, ο πάροχος οφείλει να διαθέτει διαδικασία διαχείρισης αλλαγών, στην οποία περιγράφονται όλες οι ενέργειες που απαιτούνται για κάθε αλλαγή στο υλικό ή λογισμικό των ΣΔΥ, καθώς επίσης και να εξασφαλίζει ότι υπάρχουν ανά πάσα στιγμή διαθέσιμα αντίγραφα ασφαλείας της πλέον πρόσφατης διαμόρφωσης του εξοπλισμού του, τα οποία είναι απαραίτητα για την αποκατάσταση του

¹²³ Ως τέτοιου είδους μηχανισμοί αναφέρονται ενδεικτικά η βλαβοληψία, η προληπτική συντήρηση, η διαχείριση ανταλλακτικών, η διαδικασία εσωτερικής κλιμάκωσης αναφοράς προβλημάτων, οι δείκτες αποκατάστασης βλαβών με τους προμηθευτές.

¹²⁴ Ενδεικτικά αναφέρονται οι επανειλημμένες ανεπιτυχείς προσπάθειες πρόσβασης, οι αλλαγές στη διαμόρφωση του ΣΔΥ, οι αλλαγές στην κατάσταση και τη λειτουργία του ΣΔΥ, όπως η επανεκκίνηση ή η βίαιη διακοπή λειτουργίας του ΣΔΥ.

δικτύου του και των παρεχόμενων υπηρεσιών. Τα αντίγραφα ασφαλείας φυλάσσονται σε προστατευμένο χώρο.

Όπως προβλέπεται στο άρθρο 16, ο πάροχος υποχρεούται να καταγράφει ειδικώς τα συμβάντα ασφαλείας στο δίκτυό του. Η εν λόγω καταγραφή περιλαμβάνει: α) την αρχιτεκτονική και τις επιμέρους μεθόδους δημιουργίας, συλλογής, αποθήκευσης και διαχείρισης των αρχείων καταγραφής, β) πλήρη περιγραφή του περιεχομένου αυτών και γ) τα μέτρα για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητάς αυτών. Ο πάροχος εξασφαλίζει ότι, κατ' ελάχιστο, καταγράφονται τα ακόλουθα: α) οι προσβάσεις (επιτυχών και ανεπιτυχών προσπαθειών) σε χώρους, εγκαταστάσεις και ΣΔΥ, β) οι ενέργειες των χειριστών και διαχειριστών κατά την πρόσβασή τους στα ΣΔΥ, γ) οι μεταβολές στην διαμόρφωση των ΣΔΥ και δ) τα συμβάντα που αφορούν στην ασφάλεια, και ιδίως όταν σχετίζονται με αλλαγές στην κατάσταση και στην λειτουργία των ΣΔΥ. Επιπροσθέτως, ο πάροχος εξασφαλίζει ότι οι απαιτούμενες καταγραφές είναι πλήρεις και συνεχείς και ότι οι καταγεγραμμένες πληροφορίες προστατεύονται από οποιαδήποτε αλλοίωση και μη εξουσιοδοτημένη πρόσβαση.

Το άρθρο 17 αναφέρεται στη διαχείριση των περιστατικών ασφαλείας. Συγκεκριμένα, ο πάροχος οφείλει να εφαρμόζει διαδικασία διαχείρισης περιστατικών ασφαλείας, η οποία θα ενεργοποιείται αμελλητί σε κάθε περίπτωση περιστατικού ασφαλείας. Η διαδικασία διαχείρισης περιστατικών ασφαλείας προβλέπει τις ακόλουθες ενέργειες: α) την καταγραφή στοιχείων για κάθε περιστατικό ασφαλείας, β) τη διερεύνηση των αιτιών και τον προσδιορισμό των τεχνικών ή/και οργανωτικών αδυναμιών στις οποίες ενδεχομένως οφείλεται το περιστατικό ασφαλείας, γ) την υλοποίηση των ενεργειών αποκατάστασης με συγκεκριμένο χρονοδιάγραμμα και δ) την ενημέρωση του υπεύθυνου ασφαλείας και ακεραιότητας δικτύου και υπηρεσιών, των αρμοδίων στελεχών του παρόχου και των αρμοδίων Αρχών. Ο πάροχος οφείλει να διατηρεί όλα τα έγγραφα που σχετίζονται με τα περιστατικά ασφαλείας, από τα οποία θα τεκμηριώνεται η εκτέλεση των αντίστοιχων προβλεπόμενων ενεργειών.

Κατά το άρθρο 18, που αφορά στην υποχρέωση του παρόχου εσωτερικού ελέγχου για την ασφάλεια και την ακεραιότητα των δικτύων και υπηρεσιών, ο τελευταίος οφείλει να διαθέτει και να εφαρμόζει διαδικασία εσωτερικού ελέγχου εφαρμογής των μέτρων για την ασφάλεια και την ακεραιότητα των δικτύων και υπηρεσιών, στην οποία περιγράφονται τα ακόλουθα στάδια: α) προετοιμασία του ελέγχου (καθορισμός ΣΔΥ / εγκαταστάσεων / επιμέρους πολιτικών που θα ελεγχθούν, χρονοδιάγραμμα, κ.λπ.), β) διεξαγωγή του ελέγχου και γ) αποτελέσματα του ελέγχου (τυχόν ευρήματα, επιγενόμενες ενέργειες κλπ.). Για κάθε εσωτερικό έλεγχο, ο πάροχος οφείλει να διατηρεί σε αρχείο την τεκμηρίωση κάθε σταδίου του ελέγχου. Ο εσωτερικός έλεγχος είναι δυνατόν να πραγματοποιείται από εξωτερικό φορέα ή από εξουσιοδοτημένους προς τούτο εργαζόμενους του παρόχου.

Σε συνάρτηση με το άρθρο 37 παράγραφος 9 του ν. 4070/2012 και την προβλεπόμενη σε αυτό αρμοδιότητα της Α.Δ.Α.Ε. να διενεργεί σχετικούς ελέγχους, το άρθρο 19 του Σχεδίου Κανονισμού ορίζει ότι οι πάροχοι υποβάλλονται σε έλεγχο ασφάλειας, αυτεπαγγέλτως ή κατόπιν καταγγελίας, που διενεργείται από την Α.Δ.Α.Ε., σύμφωνα με τα προβλεπόμενα στο άρθρο 37 του ν.4070/2012. Σύμφωνα με το άρθρο αυτό, κατά τη διενέργεια του ελέγχου της, η Α.Δ.Α.Ε. έχει την εξουσία και τις αρμοδιότητες που προβλέπονται από το ν.3115/2003, το ν.703/1977 και το ν.3674/2008, όπως ισχύουν. Στο σημείο αυτό, θα πρέπει να τονίσουμε ότι πιθανόν από παραδρομή δεν αναφέρεται ότι ο ν. 703/1977 αντικαταστάθηκε από το ν. 3959/2011, γεγονός που ήδη σχολιάστηκε ανωτέρω¹²⁵. Αντιθέτως, στο προοίμιο του Σχεδίου Κανονισμού, ήδη διευκρινίζεται ότι ο ν. 703/1977 αντικαταστάθηκε από το ν. 3959/2011, όπως ισχύει.

Στις τελικές διατάξεις, σύμφωνα με το άρθρο 20 προβλέπεται ότι οι όροι του Κανονισμού είναι υποχρεωτικοί για τον πάροχο και, σε περίπτωση που απαιτηθεί η κατάρτιση εκ μέρους του παρόχου πολιτικής ασφαλείας, περιλαμβάνονται στους όρους αυτής. Επίσης, διευκρινίζεται ότι οι διατάξεις του κανονισμού δεν αφορούν την κατ' άρθρο 67 παρ.3 του ν.4070/2012 εξασφάλιση διαθεσιμότητας κατά την παροχή διαθέσιμων στο κοινό

¹²⁵ Βλ. παραπομπή υπ' αρ. 72 της παρούσας εργασίας.

τηλεφωνικών υπηρεσιών μέσω δημόσιων δικτύων επικοινωνιών σε περιπτώσεις καταστροφικής βλάβης δικτύου ή σε περίπτωση ανωτέρας βίας¹²⁶.

5. ΣΥΓΚΡΙΣΗ ΤΩΝ ΥΠΟΧΡΕΩΣΕΩΝ ΤΩΝ ΠΑΡΟΧΩΝ ΚΑΤ' ΑΡΘΡΟ 37 Ν. 4070/2012 ΜΕ ΣΥΝΑΦΕΙΣ ΡΥΘΜΙΣΕΙΣ ΤΟΥ ΕΛΛΗΝΙΚΟΥ ΔΙΚΑΙΟΥ.

Στο δίκαιό μας, εκτός από την υποχρέωση λήψης μέτρων ασφάλειας που απευθύνεται στους παρόχους δημοσίων δικτύων ή υπηρεσιών ηλεκτρονικών επικοινωνιών, που προβλέπεται στο άρθρο 37 του ν. 4070/2012, απαντώνται και άλλες παρεμφερείς ρυθμίσεις, τόσο στον ίδιο ως άνω νόμο, όσο και σε άλλα νομοθετήματα. Για το λόγο αυτό, παρίσταται αναγκαία η σύγκριση των εν λόγω ρυθμίσεων και η οριοθέτηση του πεδίου εφαρμογής τους σε σχέση με αυτό του άρθρου 37 του ν. 4070/2012.

Ειδικότερα, στο άρθρο 67, παράγραφος 3 του ν. 4070/2012, προβλέπεται ότι, προκειμένου οι επιχειρήσεις που παρέχουν διαθέσιμες στο κοινό τηλεφωνικές υπηρεσίες μέσω δημόσιων δικτύων επικοινωνιών να εξασφαλίζουν τη μέγιστη δυνατή διαθεσιμότητα αυτών σε περιπτώσεις καταστροφικής βλάβης δικτύου ή σε περίπτωση ανωτέρας βίας, υποχρεούνται να λαμβάνουν όλα τα απαιτούμενα μέτρα. Οι ανωτέρω επιχειρήσεις υποχρεούνται να λαμβάνουν όλα τα απαραίτητα μέτρα για να διασφαλίζουν αδιάλειπτη πρόσβαση σε υπηρεσίες έκτακτης ανάγκης. Προς το σκοπό αυτό, με κοινή απόφαση¹²⁷ των Υπουργών Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων, κατόπιν εισήγησης της Ε.Ε.Τ.Τ., καθορίζονται οι ελάχιστες υποχρεώσεις, προς τις οποίες οφείλουν να συμμορφώνονται οι επιχειρήσεις.

Συγκρίνοντας την ως άνω διάταξη με αυτή του άρθρου 37, διαπιστώνουμε ότι πρόκειται, για μία σαφώς πιο περιορισμένης εμβέλειας ρύθμιση, καθόσον αφενός εδώ υπόχρεοι για τη λήψη μέτρων είναι μόνο οι πάροχοι τηλεφωνικών υπηρεσιών μέσω δημόσιων δικτύων επικοινωνιών, αφετέρου η λήψη των

¹²⁶ Για το άρθρο 67 παράγραφος 3 του ν. 4070/2012, βλ. επόμενο κεφάλαιο της παρούσας.

¹²⁷ Η απόφαση αυτή δεν έχει εκδοθεί μέχρι σήμερα.

μέτρων έχει ως στόχο την εξασφάλιση της διαθεσιμότητας των δικτύων τους σε περιπτώσεις ανωτέρας βίας και τη διασφάλιση της πρόσβασης σε υπηρεσίες έκτακτης ανάγκης. Αντιθέτως, η υποχρέωση του άρθρου 37 είναι ευρύτερη, αφού απευθύνεται στους παρόχους δημοσίου δικτύου ή υπηρεσιών ηλεκτρονικών επικοινωνιών. Περαιτέρω, έχει χαρακτήρα προεχόντως προληπτικό, αφού θέτει ως σκοπό τη θωράκιση των δικτύων, την ανθεκτικότητά τους απέναντι στον υπάρχοντα κίνδυνο μέσω της υιοθέτησης των πλέον πρόσφατων τεχνολογικών δυνατοτήτων.

Ωστόσο, μέσα από μία προσεκτικότερη προσέγγιση των διατάξεων, διαπιστώνουμε ότι ελοχεύει πράγματι κίνδυνος σύγχυσης, στο βαθμό που το πεδίο εφαρμογής τους αλληλοκαλύπτεται. Συγκεκριμένα, όπως προκύπτει από την παράγραφο 2 του άρθρου 37, οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών υποχρεούνται στη λήψη των κατάλληλων μέτρων με σκοπό την εξασφάλιση της ακεραιότητας των δικτύων τους. Όμως, στις εν λόγω επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών συγκαταλέγονται και εκείνες που παρέχουν διαθέσιμες στο κοινό τηλεφωνικές υπηρεσίες μέσω δημόσιων δικτύων επικοινωνιών στις οποίες απευθύνεται η επιταγή του άρθρου 67 παράγραφος 3. Έτσι, οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών, στις οποίες εμπίπτουν και εκείνες που παρέχουν διαθέσιμες στο κοινό τηλεφωνικές υπηρεσίες μέσω δημόσιων δικτύων επικοινωνιών, θα πρέπει να λαμβάνουν τα κατάλληλα μέτρα για την εξασφάλιση της ακεραιότητας των δικτύων τους σύμφωνα με το άρθρο 37 παράγραφος 2. Στα μέτρα αυτά βέβαια, περιλαμβάνονται αυτά που επιτάσσει το άρθρο 67 και τα οποία αποσκοπούν στην εξασφάλιση της μέγιστης δυνατής διαθεσιμότητάς τους σε περιπτώσεις καταστροφικής βλάβης ή ανωτέρας βίας, καθώς επίσης και στη διασφάλιση αδιάλειπτης πρόσβασης σε υπηρεσίες έκτακτης ανάγκης. Επομένως, καθίσταται σαφές ότι διατάξεις αυτές αλληλοκαλύπτονται κατά ένα μέρος και ότι το πρόβλημα αυτό θα πρέπει να λυθεί από τον ίδιο το νομοθέτη, ο οποίος θα πρέπει να ερμηνεύσει αυθεντικά τις ανωτέρω ρυθμίσεις, οριοθετώντας τις.

Πέραν δε των ανωτέρω, η ρύθμιση του άρθρου 37, θα μπορούσε να συγκριθεί με τη συναφή, προγενέστερη διάταξη του άρθρου 57 παράγραφος

4 του ν. 3431/2006¹²⁸. Σύμφωνα με αυτήν, οι επιχειρήσεις που λειτουργούν δημόσια τηλεφωνικά δίκτυα σε σταθερές θέσεις¹²⁹ οφείλουν να εξασφαλίζουν την ακεραιότητα του δικτύου και σε περίπτωση καταστροφικής βλάβης του δικτύου ή σε περίπτωση ανωτέρας βίας, τη διαθεσιμότητα του δημόσιου τηλεφωνικού δικτύου και των δημόσιων τηλεφωνικών υπηρεσιών σε σταθερές θέσεις, υποχρεούνται να λαμβάνουν όλα τα απαιτούμενα μέτρα. Ομοίως υποχρεούνται να λαμβάνουν όλα τα απαραίτητα μέτρα για να διασφαλίζουν αδιάκοπη πρόσβαση σε υπηρεσίες έκτακτης ανάγκης. Με κοινή απόφαση των Υπουργών Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης και Μεταφορών και Επικοινωνιών, κατόπιν εισήγησης της Ε.Ε.Τ.Τ., καθορίζονται οι ελάχιστες υποχρεώσεις τους προς την κατεύθυνση αυτή.

Εκ πρώτης όψεως, η ρύθμιση αυτή έχει στενότερο πεδίο εφαρμογής σε σχέση με το άρθρο 37 του ν. 4070/2012, καθόσον απευθύνεται μόνο στις επιχειρήσεις που λειτουργούν δημόσια τηλεφωνικά δίκτυα σε σταθερές θέσεις. Η υποχρέωση των επιχειρήσεων αυτών καλύπτει τη λήψη μέτρων με σκοπό την εξασφάλιση της ακεραιότητας των δικτύων τους, με έμφαση στις περιπτώσεις καταστροφικής βλάβης του δικτύου ή σε περίπτωση ανωτέρας βίας, καθώς επίσης και την διασφάλιση της αδιάκοπης πρόσβασης σε υπηρεσίες έκτακτης ανάγκης. Οι υποχρεώσεις αυτές εξειδικεύονται στην υπ' αρ. 7560/153/2012 Κ.Υ.Α.¹³⁰, που εκδόθηκε κατ' εξουσιοδότηση του άρθρου 57 παράγραφος 4 του ν. 3431/2006.

Στο πλαίσιο αυτό, οι εν λόγω επιχειρήσεις οφείλουν να συμμορφώνονται κατ' ελάχιστο με τις ακόλουθες υποχρεώσεις¹³¹: α) Να υλοποιούν Ανάλυση Επιχειρησιακών Επιπτώσεων (Business Impact Analysis) και Αξιολόγηση

¹²⁸ Καταργήθηκε με το άρθρο 80 παράγραφος 2α του ν. 4070/2012.

¹²⁹ Η διατύπωση αυτή δεν είναι ακριβής. Προφανώς, ο νομοθέτης εννοεί εδώ τις επιχειρήσεις που παρέχουν υπηρεσίες σταθερής τηλεφωνίας.

¹³⁰ Πρόκειται για την υπ' αρ. 7560/153/2012 Κ.Υ.Α. «Ελάχιστες υποχρεώσεις για τη διασφάλιση της ακεραιότητας των δημόσιων τηλεφωνικών δικτύων και δημόσιων τηλεφωνικών υπηρεσιών σε σταθερές θέσεις» (ΦΕΚ Β' 305/14-2-2012).

¹³¹ Βλ. άρθρο 3 παράγραφος 1 της υπ' αρ. 7560/153/2012 ΚΥΑ.

Επικινδυνότητας (Risk Assessment)¹³² βασιζόμενη σε πρότυπη αναγνωρισμένη μέθοδο, προκειμένου να εντοπίσουν σημαντικές αδυναμίες και ευάλωτα σημεία στις δικτυακές τους υποδομές. β) Να διαθέτουν καταγεγραμμένα Σχέδια Επιχειρησιακής Συνέχειας (Business Continuity Plans) βασισμένα στην Αξιολόγηση Επικινδυνότητας την οποία έχουν πραγματοποιήσει για το δίκτυο και τις υπηρεσίες τους¹³³. γ) Ειδικότερα για τις καταστάσεις εκτάκτων συνθηκών, καταστροφικής βλάβης και ανωτέρας βίας, να καταρτίζουν Σχέδιο Ανάκαμψης από Καταστροφή (Disaster Recovery Plan). δ) Να είναι συνεχώς ενημερωμένοι για την κατάσταση του δικτύου τους και άλλου εξοπλισμού ή εγκαταστάσεων από τα οποία εξαρτάται η λειτουργία του δικτύου, μέσω διαδικασιών και συστημάτων παρακολούθησης¹³⁴. Προς τούτο, ο κάθε πάροχος αξιολογεί και αξιοποιεί και πιθανές πληροφορίες/καταγγελίες που προκύπτουν από χρήστες του δικτύου σχετικά με προβλήματα που παρουσιάζονται προκειμένου να εντοπίσει βλάβες του δικτύου. ε) Να διασφαλίζουν την ανθεκτικότητα του δικτύου τους. Μεριμνούν ότι ο χρησιμοποιούμενος εξοπλισμός είναι από τη φύση του αξιόπιστος (reliable), ασφαλής έναντι εξωτερικών απειλών και ικανός να λειτουργήσει ακόμα και με κάποιο βαθμό βλάβης (fault tolerant). Λαμβάνουν υπόψη τους θέματα εφεδρείας¹³⁵ και φυσικής ασφάλειας¹³⁶, κατά το σχεδιασμό και την επιλογή της αρχιτεκτονικής του δικτύου. Επιδιώκουν την αποφυγή μοναδικών σημείων αποτυχίας (Single Point of Failure) στο δίκτυό τους, σημεία δηλαδή τα οποία αν παρουσιάσουν βλάβη, οδηγούν σε διακοπή της λειτουργίας του δικτύου. στ) Διαθέτουν επαρκές και καταρτισμένο προσωπικό και κατάλληλο εξοπλισμό για την αποκατάσταση της λειτουργίας του δικτύου και των παρεχόμενων υπηρεσιών καθ' όλη τη διάρκεια του εικοσιτετράωρου.

Συνοψίζοντας, καταλήγουμε ότι οι διατάξεις του άρθρου 37 του ν. 4070/2012 σε σχέση με τις λοιπές ανωτέρω ρυθμίσεις διαφέρουν κατά το ότι αφενός απευθύνονται σε άλλες κατηγορίες παρόχων δημοσίων δικτύων, αφετέρου

¹³² Πρβλ. άρθρο 5 Κανονισμού.

¹³³ Πρβλ. άρθρο 6 Κανονισμού.

¹³⁴ Πρβλ. άρθρο 14 του Κανονισμού.

¹³⁵ Πρβλ. άρθρο 10 του Κανονισμού.

¹³⁶ Πρβλ. άρθρο 9 του Κανονισμού.

διότι έχουν πολύ μεγαλύτερο πεδίο εφαρμογής. Αναλυτικότερα, με τις εν λόγω διατάξεις οι απορρέουσες υποχρεώσεις από το άρθρο αυτό, κατατείνουν όχι μόνο στην εξασφάλιση της διαθεσιμότητας των δικτύων σε περίπτωση ανωτέρας βίας, αλλά στη διασφάλιση της ακεραιότητας και της ασφάλειας τους σε κάθε περίπτωση. Επίσης, η έκταση της ευθύνης των παρόχων επιτείνεται, με μέτρο σύγκρισης τις τελευταίες τεχνολογικές εξελίξεις. Για το λόγο αυτό κρίνεται αναγκαία η οριοθέτηση από το νομοθέτη της έκτασης του πεδίου εφαρμογής των διατάξεων 37 και 67 του ν. 4070/2012. Τέλος, από την επισκόπηση των ανωτέρω προγενέστερων παρεμφερών ρυθμίσεων, διαπιστώνουμε την ύπαρξη πολλών κοινών σημείων μεταξύ της υπ' αρ. 7560/153/2012 Κ.Υ.Α. και του Κανονισμού, γεγονός που μας οδηγεί στο συμπέρασμα ότι η εν λόγω Κ.Υ.Α. αποτέλεσε πιθανόν ένα «πρότυπο» σχετικά με τις ελάχιστες υποχρεώσεις διαθεσιμότητας που βαρύνουν τους παρόχους δημοσίων δικτύων επικοινωνιών, οι οποίες, βέβαια, εμπλουτίστηκαν και με τις λοιπές υποχρεώσεις ασφάλειας που προβλέπει ο Κανονισμός.

V. Η ΑΣΦΑΛΕΙΑ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ.

1. Η ΟΔΗΓΙΑ 2002/58/ΕΚ ΚΑΙ Ο Ν. 3471/2006.

Όπως είναι φυσικό, οι αυξημένες -χάρη στην τεχνολογία- δυνατότητες συλλογής, επεξεργασίας και ποικίλης χρήσης πληροφοριών που αφορούν το άτομο, συνεπάγονται κινδύνους για επεμβάσεις στην ιδιωτική ζωή του. Αυτή ακριβώς, η ανησυχία από τους κινδύνους που διατρέχει η ιδιωτική ζωή του σύγχρονου ανθρώπου, ενόψει των αυξημένων δυνατοτήτων της τεχνολογίας της πληροφορικής, γέννησε και την προβληματική για την προστασία των δεδομένων προσωπικού χαρακτήρα¹³⁷. Περαιτέρω, η επεξεργασία των προσωπικών δεδομένων στο χώρο των ηλεκτρονικών δικτύων παρουσιάζει σημαντικές ιδιαιτερότητες σε σχέση με τις λοιπές μορφές επεξεργασίας,

¹³⁷ Βλ. *Ιωάννη Ιγγλεζάκη*, Δίκαιο της Πληροφορικής, εκδ. Σάκουλα Αθήνα –Θεσσαλονίκη, 2008, σελ. 221.

γεγονός που ανέδειξε και την αναγκαιότητα θέσπισης ειδικής ρύθμισης. Αναλυτικότερα, η βασικότερη ειδοποιός διαφορά των περιστάσεων επεξεργασίας των προσωπικών δεδομένων στα ηλεκτρονικά δίκτυα, είναι ότι για να δραστηριοποιηθεί το υποκείμενο στο δίκτυο, θα πρέπει -εκ των πραγμάτων- να παράσχει στον πάροχο του δικτύου, ή ακόμα και να «συνδημιουργήσει» μαζί του, μία σειρά από προσωπικά δεδομένα, τα λεγόμενα «εξωτερικά» και επομένως το υποκείμενο «αυτοεκτίθεται» κατά κάποιον τρόπο¹³⁸, και μάλιστα τις περισσότερες φορές με δική του πρωτοβουλία.

Οι ιδιαιτερότητες αυτές, κατέδειξαν την ανεπάρκεια αντιμετώπισης της προστασίας δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες στο πλαίσιο των γενικών κανόνων για την προστασία των δεδομένων προσωπικού χαρακτήρα και ανάγκη θέσπισης ειδικών διατάξεων. Η προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες έχει δύο πλευρές, καθώς η σχετική ρύθμιση θα έπρεπε, αφενός να κατατείνει στην προστασία των εξωτερικών δεδομένων του εκάστοτε συνδεόμενου προς το δίκτυο χρήστη (π.χ. ηλεκτρονική διεύθυνση, αριθμός κλήσης του χρήστη και του συνομιλητή, συχνότητα επικοινωνίας και εν γένει πρόσβασης στο δίκτυο κ.λπ.), αφετέρου να άπτεται της διαφύλαξης των εσωτερικών δεδομένων, δηλαδή αυτών που αφορούν στο περιεχόμενο της επικοινωνίας του και γενικά των συναλλαγών του μέσω του Διαδικτύου (π.χ. για τις γνωριμίες του, τις ανάγκες του, τις συνήθειές του, το ημερήσιο πρόγραμμα δραστηριοτήτων του)¹³⁹. Έτσι, τόσο ο κοινοτικός όσο και ο εσωτερικός νομοθέτης λαμβάνοντας υπόψη τα πιο πάνω δεδομένα προέβησαν σε θέσπιση ειδικών ρυθμίσεων: ο μεν πρώτος με την οδηγία 2002/58/ΕΚ¹⁴⁰, ο δε δεύτερος με την αντίστοιχη πράξη προσαρμογής, το Ν. 3471/2006¹⁴¹.

¹³⁸ Βλ. *Κωνσταντίνο Χριστοδούλου*, ό.π.

¹³⁹ Βλ. *Ιωάννη Πιτσιρίκο*, Δεδομένα προσωπικού χαρακτήρα στο Διαδίκτυο υπό το πρίσμα του ν. 3471/2006 (όπως τροποποιήθηκε από τους ν. 3917/2001, 4070/2012), Πειραϊκή Νομολογία 2012, σελ. 216.

¹⁴⁰ 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

Ειδικότερα, σε ευρωπαϊκό επίπεδο, εκδόθηκε η οδηγία 2002/58/EK σε αντικατάσταση της οδηγίας 1997/66/EK¹⁴², καθόσον θεωρήθηκε αναγκαίο από τον κοινοτικό νομοθέτη να προσαρμοστεί το νομοθετικό πλαίσιο στις εξελίξεις των αγορών και των τεχνολογιών των ηλεκτρονικών επικοινωνιών, προκειμένου να παρέχει το ίδιο επίπεδο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής σε όλους τους χρήστες υπηρεσιών επικοινωνιών διαθέσιμων στο κοινό¹⁴³. Αναλυτικότερα, με τις εισαγόμενες ρυθμίσεις τέθηκε ως στόχος η εναρμόνιση της σχετικής νομοθεσίας των κρατών μελών ώστε να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και να διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Κοινότητα. Επιπλέον, εξειδικεύουν και συμπληρώνουν την οδηγία 95/46/EK που αφορά στην εν γένει προστασία των προσωπικών δεδομένων¹⁴⁴, όμως εισάγουν και σημαντικές διαφοροποιήσεις από αυτήν, καθώς παρέχουν προστασία των εννόμων συμφερόντων υποκειμένων που είναι νομικά πρόσωπα.

Συγκεκριμένα, αναφορικά με το θέμα της ασφάλειας των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες προβλέπεται¹⁴⁵ ότι ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να λαμβάνει - εν ανάγκη από κοινού με τον φορέα παροχής του δημοσίου δικτύου επικοινωνιών - τα ενδεδειγμένα τεχνικά και οργανωτικά

ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).

¹⁴¹ Ν. 3471/2006 «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997» (ΦΕΚ Α' 133/28-6-2006).

¹⁴² Οδηγία 1997/66/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15^{ης} Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και της προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα.

¹⁴³ Βλ. υπ' αρ. 4 αιτιολογική σκέψη του προοιμίου της οδηγίας 2002/58/EK.

¹⁴⁴ Οδηγία 1995/46/EK 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.

¹⁴⁵ Βλ. άρθρο 4 της οδηγίας 2002/58/EK.

μέτρα, προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του. Λαμβανομένων υπόψη των πλέον πρόσφατων τεχνικών δυνατοτήτων και του κόστους εφαρμογής τους, τα μέτρα αυτά πρέπει να κατοχυρώνουν επίπεδο ασφαλείας ανάλογο προς τον υπάρχοντα κίνδυνο. Σε περίπτωση, δε, που υπάρχει ιδιαίτερος κίνδυνος παραβίασης της ασφαλείας του δικτύου, ο φορέας που παρέχει διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών οφείλει να ενημερώνει τους συνδρομητές για τον κίνδυνο αυτό και, εφόσον ο κίνδυνος κείται εκτός του πεδίου των μέτρων που οφείλει να λαμβάνει ο πάροχος της υπηρεσίας, για όλες τις τυχόν δυνατότητες αποτροπής του, καθώς και για το αναμενόμενο κόστος τους.

Ως τέτοιοι, ιδιαίτεροι κίνδυνοι θεωρούνται σύμφωνα με το νομοθέτη¹⁴⁶ αυτοί που ενδέχεται να προκύψουν κυρίως για τις υπηρεσίες ηλεκτρονικών επικοινωνιών σε ένα ανοικτό δίκτυο, όπως το Διαδίκτυο ή η αναλογική κινητή τηλεφωνία. Επίσης, είναι πολύ σημαντική η πλήρης ενημέρωση των χρηστών των υπηρεσιών να είναι σχετικά με τους υφιστάμενους κινδύνους ασφαλείας που δεν αντιμετωπίζονται με μέτρα που δύναται να λάβει ο πάροχος των υπηρεσιών. Περαιτέρω, οι πάροχοι υπηρεσιών που προσφέρουν διαθέσιμες στο κοινό υπηρεσίες επικοινωνιών μέσω του Διαδικτύου, θα πρέπει να ενημερώνουν τους χρήστες και τους συνδρομητές σχετικά με τα μέτρα προστασίας που μπορούν να λαμβάνουν για την ασφάλεια των επικοινωνιών τους, για παράδειγμα χρησιμοποιώντας συγκεκριμένους τύπους λογισμικού ή τεχνολογίες κρυπτογράφησης.

Ωστόσο, η απαίτηση να ενημερώνονται οι συνδρομητές για ιδιαίτερους κινδύνους ασφαλείας, δεν απαλλάσσει τους παρόχους των υπηρεσιών από την υποχρέωση να λαμβάνουν, με ίδιες δαπάνες, κατάλληλα και άμεσα μέτρα για να αποτρέπονται τυχόν νέοι, απρόβλεπτοι κίνδυνοι ασφαλείας και να αποκαθίσταται το κανονικό επίπεδο ασφαλείας της υπηρεσίας¹⁴⁷. Η παροχή πληροφοριών για τους κινδύνους ασφαλείας στον συνδρομητή θα πρέπει να είναι δωρεάν, εκτός από τυχόν συμβολικό τίμημα το οποίο μπορεί να οφείλει ο συνδρομητής όταν δέχεται ή συλλέγει τις πληροφορίες, παραδείγματος χάριν,

¹⁴⁶ Βλ. υπ' αρ. 20 αιτιολογική σκέψη του προοιμίου της οδηγίας 2002/58/EK.

¹⁴⁷ Ομοίως, βλ. προηγούμενη υποσημείωση.

όταν φορτώνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου. Η έννοια της ασφάλειας, εν προκειμένω, εκτιμάται σύμφωνα με το άρθρο 17 της οδηγίας 95/46/ΕΚ¹⁴⁸.

Όπως συμβαίνει συνήθως, πολύ μετά την παρέλευση της σχετικής προθεσμίας¹⁴⁹, ο Έλληνας νομοθέτης, ενσωμάτωσε την ανωτέρω οδηγία στο εθνικό δίκαιο με το ν. 3471/2006. Ο νόμος αυτός δεν παρουσιάζει αυτοτέλεια¹⁵⁰, αλλά συμπληρώνει και εξειδικεύει το γενικό πλαίσιο για την προστασία των προσωπικών δεδομένων. Ως εκ τούτου¹⁵¹ για κάθε ζήτημα σχετικό με την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών, που δεν ρυθμίζεται ειδικότερα με το ν. 3471/2006 εφαρμόζεται ο ν. 2472/1997¹⁵², ο οποίος, επίσης εφαρμόζεται και για κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται στο πλαίσιο μη διαθέσιμων στο κοινό δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών¹⁵³. Η ratio του ν. 3471/2006 είναι η προστασία θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών¹⁵⁴. Επιπλέον, όσον αφορά στις προβλέψεις του νόμου για τις απαιτήσεις ασφάλειας των προσωπικών δεδομένων, ο Έλληνας νομοθέτης, ενσωμάτωσε

¹⁴⁸ Σύμφωνα με την παράγραφο υπ' αρ. 1 του οποίου: «Τα κράτη μέλη προβλέπουν ότι ο υπεύθυνος της επεξεργασίας πρέπει να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα 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. Τα μέτρα αυτά πρέπει να εξασφαλίζουν, λαμβανομένης υπόψη της τεχνολογικής εξέλιξης και του κόστους εφαρμογής τους, επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που απορρέουν από την επεξεργασία και τη φύση των δεδομένων που απολαύουν προστασίας. »

¹⁴⁹ Σύμφωνα με το άρθρο 17 της οδηγίας 2002/58, τα κράτη μέλη όφειλαν να προβούν στις σχετικές ενέργειες για την ενσωμάτωση της οδηγίας στο εθνικό δίκαιο μέχρι την 31 Οκτωβρίου 2003.

¹⁵⁰ Βλ. *Ιωάννη Ηγγλεζάκη*, ό.π., σελ. 256.

¹⁵¹ Ομοίως, στην υπ' αρ. 10 αιτιολογική σκέψη του προοιμίου της οδηγίας 2002/58/ΕΚ προβλέπεται ότι 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.

¹⁵² Βλ. άρθρο 3 παρ. 2 ν. 3471/2006.

¹⁵³ Βλ. άρθρο 3 παρ. 1 εδ. β' ν. 3471/2006.

¹⁵⁴ Βλ. άρθρο 1 ν. 3471/2006.

αυτολεξεί την ανωτέρω αναφερόμενη ευρωπαϊκή ρύθμιση, στην οποία και παραπέμπουμε προς αποφυγή άσκοπων επαναλήψεων.

Συνοψίζοντας, υπό τις διατάξεις της οδηγίας 2002/58/EΚ και του ν. 3471/2006, η υποχρέωση ασφαλείας κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες προσδιορίζεται ενόψει των κριτηρίων του υπάρχοντος κινδύνου, των πλέον πρόσφατων τεχνικών δυνατοτήτων και του κόστους. Πέραν των ανωτέρω υποστηρίχθηκε και η άποψη¹⁵⁵ ότι οι εν λόγω ρυθμίσεις εντάσσονται στο γενικότερο πλαίσιο της ενθάρρυνσης χρήσης κρυπτογραφίας και άλλων ανάλογων τεχνολογικών εφαρμογών για την προστασία των δεδομένων προσωπικού χαρακτήρα. Ο νομοθέτης και στα ανωτέρω κείμενα, δεν εξειδικεύει εάν κάποιο από τα παραπάνω κριτήρια έχει μεγαλύτερη βαρύτητα και ως εκ τούτου δημιουργείται η εντύπωση ότι όλα έχουν την ίδια σημασία για τον προσδιορισμό της έκτασης της υποχρέωσης ασφαλείας. Ωστόσο, από μία προσεκτικότερη ανάγνωση της διατύπωσης, μπορεί κανείς να συμπεράνει ότι το κόστος ανάγεται σε παράγοντα με μάλλον «πρωταγωνιστικό ρόλο», που καλείται να εξισορροπήσει το μέτρο της ευθύνης, το οποίο άλλως θα εκτινασσόταν σε πολύ υψηλή κλίμακα, καθώς θα ακολουθούσε την αλματώδη εξέλιξη των πλέον πρόσφατων τεχνικών δυνατοτήτων. Έτσι, το κόστος όχι μόνο καθορίζει το μέτρο της ασφαλείας για τον φορέα παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, αλλά ακόμα, εάν παρίσταται αναγκαίο να ληφθούν, λαμβάνονται από κοινού με τον φορέα παροχής του δημοσίου δικτύου, οπότε και επιμερίζονται τα σχετικά έξοδα.

Περαιτέρω, η νομοθετική εξάρτηση των ληπτέων μέτρων ασφαλείας από το κόστος τους, δηλαδή, εν τέλει, από το ύψος των τελών σύνδεσης με το δίκτυο, προσφέρει στο φορέα παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών τη δυνατότητα να προσπεράσει πολύ εύκολα οιαδήποτε υποχρέωση λήψης μέτρων ασφαλείας, απλά προσφέροντας φθηνότερες υπηρεσίες στον πελάτη του. Πολλώ, δε, μάλλον, καθόσον ο νόμος δεν περιέχει οιαδήποτε διατίμηση των ληπτέων μέτρων, με αποτέλεσμα να καταλείπεται η δυνατότητα αυτή στον ίδιο τον υπόχρεο για τη λήψη των

¹⁵⁵ Βλ. Γεώργιο Γεωργιάδη, Ο ν. 3471/2006 για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, ΧρΙΔ 2007, σελ. 26.

μέτρων ασφαλείας, υπό την επιφύλαξη, βέβαια των γενικών ρητρών του αστικού κώδικα¹⁵⁶.

Ως εκ τούτου, η όλη ρύθμιση τείνει να εκφυλίζει την βαρύνουσα και κύρια για τον φορέα παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών υποχρέωση λήψης μέτρων ασφαλείας και προστασίας του πελάτη του σε απλή παρεπόμενη υποχρέωση ενημέρωσης. Εξάλλου, ο εκάστοτε κίνδυνος του δικτύου ποικίλλει ανάλογα με τα δεδομένα που θέλουν να εισάγουν σε αυτό οι χρήστες, οπότε το μόνο σταθερό μέτρο που μπορεί να λάβει προς τούτο ο φορέας είναι να ενημερώνει τους πελάτες του για τον κίνδυνο που διατρέχουν.

2. ΟΙ ΝΕΕΣ ΡΥΘΜΙΣΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2009/136/EK ΚΑΙ ΤΟΥ Ν. 4070/2012.

Το κανονιστικό πλαίσιο για την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες μεταβλήθηκε με την έκδοση της νέας οδηγίας 2009/136/EK¹⁵⁷. Ειδικότερα, υπό την πίεση των τεχνολογικών εξελίξεων και των αλλαγών στην αγορά των τηλεπικοινωνιών, η Επιτροπή προώθησε το σχέδιό της για την αναθεώρηση των κανονιστικών ρυθμίσεων της Ευρωπαϊκής Ένωσης σχετικά με δίκτυα ηλεκτρονικών επικοινωνιών¹⁵⁸. Συγκεκριμένα, μέσα από τη διαδικασία του άρθρου 251 ΣυνθΕΚ προχώρησε στην αναθεώρηση και ενίσχυση και ορισμένων σημείων της Οδηγίας 2002/58/EK με σημαντικότερες, τις προσθήκες στο άρθρο 4 που αφορά στην ασφάλεια των υπηρεσιών ηλεκτρονικών επικοινωνιών¹⁵⁹ και την υποχρέωση

¹⁵⁶ Βλ. ιδίως 288, 371-372, 379 ΑΚ, άρθρο 2 παράγραφος 6 ν. 2251/1994.

¹⁵⁷ Οδηγία 2009/136/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2009, για την τροποποίηση της οδηγίας 2002/22/EK για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/EK σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του Κανονισμού (ΕΚ) αρ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών.

¹⁵⁸ Βλ. *Πάνο Κίτσο, Παναγιώτα Παππά*, Ενίσχυση της πληροφορικής και της διαφάνειας στις υπηρεσίες ηλεκτρονικών επικοινωνιών υπό το πρίσμα της οδηγίας 2009/136/EK, ΔΙΜΕΕ 2010, σελ. 211.

¹⁵⁹ Βλ. άρθρο 2 παρ. 4 της Οδηγίας 2009/136/EK.

γνωστοποίησης των κινδύνων ασφαλείας και της παραβίασης προσωπικών δεδομένων¹⁶⁰. Στο επίπεδο του εθνικού δικαίου, ο Έλληνας νομοθέτης προέβη στην ενσωμάτωση των νέων ρυθμίσεων με το ν. 4070/2012¹⁶¹, ο οποίος τροποποίησε το άρθρο 12 του ν. 3471/2006.

Αναλυτικότερα, με το άρθρο 2 της Οδηγίας 2009/136/EK, τροποποιείται το άρθρο 4 της Οδηγίας 2002/58/EK με την προσθήκη μίας εμβόλιμης παραγράφου της 1α και των παραγράφων 3, 4 και 5. Η τροποποίηση αυτή ξεκινά από τον τίτλο του ανωτέρω άρθρου, καθόσον αυτός αντικαθίσταται και προστίθεται ο όρος της «επεξεργασίας». Ο νέος τίτλος του άρθρου θα είναι «Ασφάλεια της επεξεργασίας», ο οποίος αντανακλά το σταθερό προσανατολισμό του ευρωπαϊού νομοθέτη για την καθιέρωση μίας πολιτικής ασφάλειας σε σχέση με την επεξεργασία προσωπικών δεδομένων και τον εντοπισμό των τρωτών σημείων του συστήματος. Ο στόχος είναι η παρακολούθηση των παραβιάσεων αυτών, ούτως ώστε να δίνεται η δυνατότητα να λαμβάνονται τακτικά μέτρα πρόληψης, διόρθωσης και μετριασμού τους¹⁶². Ακολούθως, ο νομοθέτης παραθέτει τις κατευθύνσεις στις οποίες θα πρέπει να κατατείνουν τα τεχνικά και οργανωτικά μέτρα της παραγράφου 1 του άρθρου 4 της Οδηγίας 2002/58/EK, τα οποία θα πρέπει τουλάχιστον: α) να εξασφαλίζουν ότι πρόσβαση σε προσωπικά δεδομένα μπορεί να έχει μόνον εξουσιοδοτημένο προσωπικό για αυστηρά νομίμως εγκεκριμένους σκοπούς, β) να προστατεύουν τα αποθηκευμένα ή διαβιβασθέντα δεδομένα προσωπικού χαρακτήρα από τυχαία ή παράνομη

¹⁶⁰ Σημειωτέον ότι σχετικές υποχρεώσεις έχουν ήδη εισαχθεί στις Η.Π.Α σε επίπεδο πολιτειακό βλ. ειδικότερα *Πάνο Κίτσο, Παναγιώτα Παππά*, ό.π., υποσ. 6, <http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx>. (14.01.10) ενώ σε διαδικασία κύρωσης βρίσκεται και ο ομοσπονδιακός νόμος H.R. 2221: Data Accountability and Trust Act βλ. <http://www.govtrack.us/congress/bill.xpd?bill=h111-2221&tab=summary> (14.01.10). Επίσης η Γερμανία μόλις πρόσφατα με την αναθεώρηση τον Ιούλιο του 2009, του Ομοσπονδιακού Νόμου για την Προστασία των προσωπικών Δεδομένων (Bundesdatenschutzgesetz ή "BDSG") περιέλαβε διατάξεις σχετικές με τη γνωστοποίηση παραβίασης προσωπικών δεδομένων. Βλ. αγγλική μετάφραση του νόμου στην ιστοσελίδα της Γερμανικής Αρχής Προσωπικών Δεδομένων, <http://www.bfdi.bund.de/cae/servlet/contentblob/844438/publicationFile/51350/aktualisiertesBDSG>

¹⁶¹ Βλ. άρθρο 173 ν. 4070/2012 «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις » (ΦΕΚ Α' 82/10-4-2012).

¹⁶² Βλ. υπ' αρ. 57 αιτιολογική σκέψη του προοιμίου της οδηγίας 2009/136/EK.

καταστροφή, τυχαία απώλεια ή αλλοίωση, και από μη εγκεκριμένη ή παράνομη αποθήκευση, επεξεργασία, πρόσβαση ή αποκάλυψη και γ) να διασφαλίζουν την εφαρμογή πολιτικής ασφάλειας σε σχέση με την επεξεργασία προσωπικών δεδομένων. Επίσης, προβλέπεται ότι τα μέτρα αυτά θα ελέγχονται από τις αρμόδιες εθνικές αρχές, οι οποίες θα εκδίδουν συστάσεις σχετικά με βέλτιστες πρακτικές όσον αφορά το επίπεδο ασφάλειας, το οποίο θα πρέπει να επιτυγχάνεται με τα ανωτέρω μέτρα.

Επιπροσθέτως, προστίθεται η παράγραφος 3 στο άρθρο 4 της Οδηγίας 2002/58/EK, σύμφωνα με την οποία προβλέπονται οι υποχρεώσεις των παροχών των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε περίπτωση παραβίασης προσωπικών δεδομένων. Ιδιαίτερα σημαντικός είναι ο προσδιορισμός των υπόχρεων να κοινοποιήσουν τις σχετικές παραβιάσεις ασφαλείας, οι οποίοι είναι αυτοί που επεξεργάζονται δεδομένα στο πλαίσιο της παροχής των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών¹⁶³. Η διάταξη αυτή αποτέλεσε εξ αρχής πεδίο διαβούλευσης¹⁶⁴ μεταξύ των μερών που συμμετείχαν στη διαδικασία αναθεώρησης της Οδηγίας 2002/58/EK. Αρχικά, αντικείμενο διαφωνιών αποτέλεσε το φάσμα των φορέων που θα υπάγονται στη απαίτηση κοινοποίησης. Προβλήθηκε το επιχείρημα ότι θα έπρεπε οι υποχρεώσεις αυτές να εκτείνονται και στους παρόχους υπηρεσιών της κοινωνίας της πληροφορίας, όπως τις on-line τράπεζες, τις on-line δραστηριότητες των επιχειρήσεων, τους on-line παρόχους υπηρεσιών υγείας, κ.λπ.¹⁶⁵, καθώς η διεύρυνση του πεδίου

¹⁶³ Η έννοια "Υπηρεσίες ηλεκτρονικών επικοινωνιών" προσδιορίζεται στην Οδηγία 2002/21/EK ως «... οι υπηρεσίες που παρέχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοηλεκτρονικές μεταδόσεις». Όπως αναφέρεται δεν περιλαμβάνονται σε αυτές οι «υπηρεσίες που παρέχουν περιεχόμενο μεταδιδόμενο με χρήση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών ή που ασκούν έλεγχο επί του περιεχομένου· δεν περιλαμβάνουν επίσης τις υπηρεσίες της κοινωνίας της πληροφορίας, όπως αυτές ορίζονται στο άρθρο 1 της Οδηγίας 98/34/EK». Οδηγία 2002/21/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (Οδηγία πλαίσιο) (ΕΕ L 108 της 24.04.2002, σελ. 33).

¹⁶⁴ Βλ. Πάνο Κίτσο, Παναγιώτα Παππά, ό.π., σελ. 212.

¹⁶⁵ Βλ. Γνώμη 2/2008 για την αναθεώρηση της οδηγίας 2002/58/EK σχετικά με την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία «προστασία της ιδιωτικής ζωής

εφαρμογής θα συμβάλει στη μεγαλύτερη ευαισθητοποίηση του κοινού και θα μειωθούν οι κίνδυνοι στον τομέα της ασφάλειας¹⁶⁶. Όπως, μάλιστα, παρατηρεί και στη δεύτερη σχετική γνωμοδότησή του ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων¹⁶⁷, οι παραβιάσεις ασφαλείας έχουν σαν στόχο, όχι μόνο τις εταιρίες τηλεπικοινωνιών, αλλά και άλλους τύπους εταιριών/παροχών, όπως οι on-line επιχειρήσεις λιανικής πώλησης, οι on-line τράπεζες, τα on-line φαρμακεία με αποτέλεσμα η παραβίαση των διαφόρων τύπων δεδομένων προσωπικού χαρακτήρα να έχει σοβαρές επιπτώσεις στην ιδιωτική ζωή ενός προσώπου.

Ως εκ τούτου, παρόλο που στην οδηγία 2009/136/EK αναφέρεται ότι οι διατάξεις αυτές ισχύουν για τους παρόχους των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, χωρίς να γίνεται καμία αναφορά στους παρόχους υπηρεσιών της κοινωνίας της πληροφορίας, στο προοίμιο της αναφέρεται ρητά ότι θεωρείται προτεραιότητα σε κοινοτικό επίπεδο η σχετική υποχρέωση ρητής και υποχρεωτικής κοινοποίησης σε όλους τους τομείς, καθώς και στους παρόχους υπηρεσιών της κοινωνίας της πληροφορίας¹⁶⁸. Εκφράζεται, έτσι, εν αναμονή της αναθεώρησης που αναμένεται να πραγματοποιηθεί για το σύνολο της νομοθεσίας στο συγκεκριμένο τομέα, μία γενική επιθυμία η οποία θα οδηγήσει σε νέα κοινοτική νομοθεσία που να περιλαμβάνει και τους υπόχρεους κοινοποιήσεων

στις ηλεκτρονικές επικοινωνίες») σελ. 3, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_el.pdf (14.01.2010).

¹⁶⁶ Όπως αναφέρεται στη δεύτερη γνωμοδότηση του Ε.Ε.Π.Δ. «Στις Ηνωμένες Πολιτείες για παράδειγμα, όλες σχεδόν οι πολιτείες (περισσότερες από 40 στην παρούσα συγκυρία) έχουν θεσπίσει νόμους για την κοινοποίηση των παραβιάσεων της ασφάλειας, το πεδίο εφαρμογής των οποίων είναι ευρύτερο και συμπεριλαμβάνει όχι μόνο τους PPECS αλλά και όποια οντότητα κατέχει τα σχετικά δεδομένα προσωπικού χαρακτήρα».

¹⁶⁷ Βλ. σημείο 23 της δεύτερης γνωμοδότησης του Ευρωπαίου Επόπτη Προστασίας Δεδομένων για την αναθεώρηση της Οδηγίας 2002/58/EK σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία για την ιδιωτική ζωή και τις Ε.Ε (2009/C 128/04).

¹⁶⁸ Βλ. υπ' αρ. 59 αιτιολογική σκέψη της οδηγίας 2009/136/EK, σύμφωνα με την οποία «... η ανάγκη για την απαίτηση ρητής και υποχρεωτικής κοινοποίησης σε όλους τους τομείς, καθώς και στους παρόχους υπηρεσιών της κοινωνίας της πληροφορίας, θα πρέπει να θεωρείται προτεραιότητα σε κοινοτικό επίπεδο οι οποίες δεν συνίστανται, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών υπηρεσία».

και τους παρόχους υπηρεσιών της κοινωνίας της πληροφορίας¹⁶⁹. Ταυτόχρονα και ανεξάρτητα από την πορεία των ρυθμίσεων αυτών σε κοινοτικό επίπεδο, ενθαρρύνονται οι εθνικές νομοθεσίες να λάβουν άμεσα κατάλληλα μέτρα, για την εφαρμογή των αρχών που διέπουν τους κανόνες για την παραβίαση των δεδομένων στην Οδηγία 2002/58/EK ανεξάρτητα από τομέα ή τύπο δεδομένων¹⁷⁰.

Περαιτέρω, για τους σκοπούς του νόμου έγινε προσθήκη του ορισμού της παραβίασης των προσωπικών δεδομένων που θεωρείται ως «...η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση προσωπικών δεδομένων που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία, σε συνδυασμό με την παροχή διαθέσιμης στο κοινό ηλεκτρονικής υπηρεσίας επικοινωνιών στην Κοινότητα»¹⁷¹. Η ανάγκη συγκεκριμενοποίησης της έννοιας της παραβίασης των προσωπικών δεδομένων βλέπουμε ότι οδήγησε τελικά στη σύνταξη ενός ορισμού, το εύρος του οποίου είναι αρκετό για να συμπεριλάβει τις περισσότερες από τις σχετικές καταστάσεις όπου δικαιολογείται η κοινοποίηση παραβιάσεων της ασφάλειας, όπως οι περιπτώσεις όπου συνέβη αναρμόδια πρόσβαση τρίτου σε δεδομένα προσωπικού χαρακτήρα όπως η αθέμιτη παρείσφρηση σε διακομιστή που περιέχει προσωπικά δεδομένα και η ανάκτηση τέτοιων δεδομένων¹⁷².

Επίσης, στο πλαίσιο της εισαγωγής του συστήματος υποχρεωτικής κοινοποίησης, προβλέπεται πρώτα ότι ο ενδιαφερόμενος πάροχος διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών θα πρέπει να γνωστοποιεί, χωρίς περιττή καθυστέρηση, την παραβίαση προσωπικών δεδομένων στην αρμόδια εθνική αρχή¹⁷³¹⁷⁴, καθώς η παραβίαση που αφορά τα δεδομένα

¹⁶⁹ Βλ. Πάνο Κίτσο, *Παναγιώτα Παππά*, ό.π., σελ. 212.

¹⁷⁰ Βλ. παράγραφο 4 του άρθρου 4 της οδηγίας 2002/58/EK που προστέθηκε με το άρθρο 2 παράγραφος γ, περίπτωση 4 της οδηγίας 2009/136/EK.

¹⁷¹ Βλ. άρθρο 2 παρ. 2 εδ η της οδηγίας 2009/136/EK.

¹⁷² Βλ. δεύτερη γνωμοδότηση του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων, ό.π., υποσ. 167.

¹⁷³ Βλ. άρθρο 2 παρ. 4 γ εδ α' της οδηγίας 2009/136/EK.

προσωπικού χαρακτήρα μπορεί να επιφέρει, εάν δεν αντιμετωπιστεί κατάλληλα και εγκαίρως, σημαντική οικονομική απώλεια και κοινωνική ζημία στο συνδρομητή ή στο μεμονωμένο άτομο¹⁷⁵. Ο έλεγχος και η εποπτεία των παρόχων έχει ανατεθεί στις αρμόδιες εθνικές αρχές, οι οποίες, κατ' αυτόν τον τρόπο, αποσκοπούν στην εξασφάλιση υψηλού επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής. Για το λόγο αυτό, οι εθνικές αρχές θα πρέπει να είναι εξοπλισμένες με τα απαραίτητα μέσα για την εκτέλεση των καθηκόντων που τους έχουν ανατεθεί, στα οποία μέσα συμπεριλαμβάνεται η διάθεση πλήρων και αξιόπιστων δεδομένων σχετικά με περιστατικά ασφάλειας που έχουν λάβει χώρα, ώστε να καθίσταται δυνατή η περαιτέρω ανάλυση και αξιολόγησή τους από τις αρμόδιες εθνικές αρχές¹⁷⁶.

Προς το σκοπό της αποτελεσματικότερης παρέμβασης και του άμεσου εντοπισμού των παραβιάσεων ασφαλείας, ο Ευρωπαίος Επόπτης Προσωπικών¹⁷⁷ Δεδομένων παρατηρεί ότι θα πρέπει να καταρτιστεί από τους αρμόδιους φορείς ένας ακριβής ορισμός των μέτρων ασφαλείας που θα χρησιμοποιούνται, και θα βρίσκεται στη διάθεση των αρχών. Με αυτό τον τρόπο σε περίπτωση που υπάρχει παραβίαση της ασφαλείας, θα είναι ευκολότερο τόσο για τους αρμόδιους φορείς όσο και για τις ελεγκτικές αρχές να κρίνουν αν η έκθεση των δεδομένων αυτών σε κίνδυνο μπορεί να έχει αρνητικές συνέπειες ή να προξενήσει βλάβη σε φυσικά πρόσωπα¹⁷⁸.

Περαιτέρω, σχετικά με τη διευκρίνιση της έννοιας της περιττής καθυστέρησης δεν προκύπτει από το κείμενο της οδηγίας πώς ακριβώς αυτή θα πρέπει να προσδιορίζεται, αλλά απολείπεται κενό αναφορικά με την οριοθέτηση των χρονικών περιθωρίων της. Ο κοινοτικός νομοθέτης προφανώς αφήνει στις εθνικές νομοθεσίες να θεσπίσουν χρονικά όρια, με βάση το είδος της

¹⁷⁴ Σε εθνικό επίπεδο προβλέπεται σύμφωνα με τη νέα παράγραφο αρ. 5 του ν. 3471/2006 ότι ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών γνωστοποιεί αμελλητί την παραβίαση στην ΑΠΔΠΧ και στην ΑΔΑΕ.

¹⁷⁵ Βλ. υπ' αρ. 61 αιτιολογική σκέψη της οδηγίας 2009/136/EK.

¹⁷⁶ Βλ. υπ' αρ. 58 αιτιολογική σκέψη της οδηγίας 2009/136/EK.

¹⁷⁷ Βλ. δεύτερη γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ό.π., σημείωση υπ' αρ. 55.

¹⁷⁸ Ωστόσο, μέχρι σήμερα οι αρμόδιες εθνικές αρχές δεν έχουν καταρτίσει ένα τέτοιου κατάλογο που θα περιέχει τα ελάχιστα μέτρα ασφαλείας που θα πρέπει να λαμβάνονται από τους παρόχους.

παραβίασης και την ποιότητα και ποσότητα των δεδομένων που παραβιάστηκαν. Όμως, αυτή η επιλογή του δεν παύει να αποτελεί σημείο που θα δημιουργήσει πιθανόν ερμηνευτικά προβλήματα¹⁷⁹. Σε επίπεδο, δε, εθνικού δικαίου ο νομοθέτης επέλεξε τον όρο «αμελλητί», που αποτελεί συνήθη αόριστη νομική έννοια, η οποία εξειδικεύεται κάθε φορά ενόψει των ειδικών συνθηκών που συνοδεύουν την κάθε περίπτωση.

Ανάλογη υποχρέωση γνωστοποίησης, βέβαια, δεν θα μπορούσε να μην προβλέπεται και για τα φυσικά πρόσωπα των οποίων τα προσωπικά δεδομένα υπόκεινται σε επεξεργασία και στα οποία πρέπει να γνωστοποιείται τυχόν παραβίασή τους. Ειδικότερα, προβλέπεται ότι η γνωστοποίηση των παραβιάσεων πρέπει να γίνεται προς τον ενδιαφερόμενο συνδρομητή ή στο ενδιαφερόμενο πρόσωπο χωρίς αδικαιολόγητη καθυστέρηση, όταν η παραβίαση προσωπικών δεδομένων ενδέχεται να έχει επιπτώσεις στα προσωπικά δεδομένα του συνδρομητή ή ενός προσώπου και στην ιδιωτική ζωή του. Έτσι, το κριτήριο που ενεργοποιεί το μηχανισμό κοινοποιήσεων είναι οι αρνητικές επιπτώσεις που μπορούν να επιφέρουν σημαντική οικονομική απώλεια και κοινωνική ζημία στο συνδρομητή ή στο μεμονωμένο άτομο¹⁸⁰. Η καινοτομία που εισάγεται στο συγκεκριμένο σημείο είναι η χρήση της λέξης «ενδιαφερόμενα πρόσωπα», με την οποία διευρύνεται το πεδίο των αποδεκτών στους οποίους κοινοποιείται η παραβίαση της ασφάλειας, ούτως ώστε να συμπεριλαμβάνονται όλα τα ενδιαφερόμενα πρόσωπα και όχι μόνο τους «συνδρομητές».

Μάλιστα, όπως παρατηρεί ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων, η έννοια αυτή συμπεριλαμβάνει προφανώς ως αποδέκτες των κοινοποιήσεων, όχι μόνο τους σημερινούς συνδρομητές, αλλά και πρώην συνδρομητές ή τρίτους, όπως χρήστες που συνεργάζονται με ορισμένους υπόχρεους φορείς δίχως να είναι συνδρομητές τους¹⁸¹. Στην κατεύθυνση αυτή, η ομάδα

¹⁷⁹ Βλ. *Πάνο Κίτσο, Παναγιώτα Παππά*, ό.π., σελ. 213.

¹⁸⁰ Μία παραβίαση θεωρείται ότι επηρεάζει αρνητικά τα δεδομένα και την ιδιωτική ζωή των συνδρομητών ή των ιδιωτών αν συνεπάγεται π.χ. κλοπή ή απάτη, σωματική ή υλική βλάβη, σημαντικό εξευτελισμό ή προσβολή της υπόληψης σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών επικοινωνιών στην Κοινότητα. Βλ. *Πάνο Κίτσο, Παναγιώτα Παππά*, ό.π..

¹⁸¹ Βλ. δεύτερη γνωμοδότηση του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων, ό.π., σημείωση υπ' αρ. 167.

εργασίας του άρθρου 29 σε σχετική γνώμη της¹⁸² είχε προτείνει τη σχετική τροποποίηση, διευκρινίζοντας ότι ο όρος «ενδιαφερόμενα πρόσωπα» συμπεριλαμβάνει όλα τα πρόσωπα των οποίων τα δεδομένα έχουν πράγματι θιγεί από την παραβίαση της ασφάλειας. Συγκεκριμένα, τα πρόσωπα που έχουν ακυρώσει την εγγραφή τους σε μια υπηρεσία δεν είναι πλέον «συνδρομητές», πλην όμως τα δεδομένα προσωπικού χαρακτήρα φυλάσσονται από τον υπεύθυνο επεξεργασίας δεδομένων¹⁸³. Σε κάθε περίπτωση, όμως, οι πάροχοι θα πρέπει να τηρούν λεπτομερή και εκτεταμένο ιστορικό εσωτερικού ελέγχου όπου θα καταγράφονται όσες τυχόν παραβιάσεις έχουν διαπιστωθεί και οι σχετικές με αυτές κοινοποιήσεις καθώς και τα μέτρα που ελήφθησαν προς αποφυγή μελλοντικών παραβιάσεων, το οποίο θα πρέπει να βρίσκεται στη διάθεση των αρχών για επανεξέταση και ενδεχόμενη έρευνα¹⁸⁴.

Πέραν, δε των ανωτέρω, προβλέπεται ότι η κοινοποίηση παραβίασης προσωπικών δεδομένων σε ενδιαφερόμενο συνδρομητή ή άλλο άτομο δεν είναι αναγκαία, εάν ο πάροχος έχει αποδείξει κατά ικανοποιητικό τρόπο στην αρμόδια αρχή, ότι έχει εφαρμόσει τα κατάλληλα τεχνολογικά μέτρα προστασίας, τα οποία πρέπει να κάνουν τα δεδομένα ακατανόητα για όσους δεν είναι εξουσιοδοτημένοι να έχουν πρόσβαση σε αυτά και ότι τα μέτρα αυτά εφαρμόστηκαν για τα δεδομένα που αφορούσε η παραβίαση της ασφάλειας. Επισημαίνεται, όμως, ότι σε περίπτωση που ο πάροχος δεν έχει ήδη γνωστοποιήσει στο συνδρομητή ή στο άλλο άτομο την παραβίαση των

¹⁸² Βλ. Γνώμη 2/2008 για την αναθεώρηση της οδηγίας 2002/58/EK σχετικά με την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία «προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες»), ό.π., σελ. 3.

¹⁸³ Όπως αναφέρει η ομάδα του άρθρου 29, όταν οι πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών κατέχουν πληροφορίες για ένα πρόσωπο Α, που δεν είναι εγγεγραμμένος συνδρομητής στις υπηρεσίες τους, αποτελεί μια άλλη υποθετική κατάσταση που υποστηρίζει την ανάγκη να διευρυνθεί η κατηγορία των αποδεκτών της υποχρέωσης κοινοποίησης. Αυτό μπορεί να συμβεί αν οι πληροφορίες έχουν διαβιβαστεί από έναν συνδρομητή της υπηρεσίας που κάλεσε τον Α να εγγραφεί στην υπηρεσία αυτή. Αν οι πληροφορίες που αφορούν τον Α δημοσιοποιούνται μετά από παραβίαση της ασφάλειας, τότε η παραβίαση αυτή πρέπει να κοινοποιηθεί προφανώς στον Α. Βλ. Γνώμη 2/2008 για την αναθεώρηση της οδηγίας 2002/58/EK σχετικά με την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία «προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες»).

¹⁸⁴ Βλ. δεύτερη γνωμοδότηση του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων, ό.π., σημείωση υπ' αρ. 56.

προσωπικών δεδομένων, η αρμόδια εθνική αρχή, αφού εξετάσει τις πιθανές επιπτώσεις της παραβίασης, έχει τη δυνατότητα να του ζητήσει να το πράξει. Και στο σημείο αυτό, επίσης, δεν εξειδικεύεται ποιος είναι ο «ικανοποιητικός τρόπος» απόδειξης της συμμόρφωσης με τις υποδείξεις της αρμόδιας αρχής, γεγονός που δημιουργεί, ομοίως, ερμηνευτικά προβλήματα¹⁸⁵.

Η ανωτέρω γνωστοποίηση στο φυσικό πρόσωπο του οποίου τα προσωπικά δεδομένα παραβιάστηκαν, θα πρέπει να περιέχει τουλάχιστον περιγραφή της φύσης της παραβίασης των προσωπικών δεδομένων και τα σημεία επαφής όπου μπορούν να αποκτηθούν περισσότερες πληροφορίες, καθώς επίσης και να συνιστά μέτρα για να μετριαστούν ενδεχόμενα δυσμενή αποτελέσματα της παραβίασης προσωπικών δεδομένων. Περαιτέρω, στην κοινοποίηση προς την αρμόδια εθνική αρχή θα πρέπει να περιγράφονται επιπροσθέτως οι συνέπειες της παραβίασης και τα μέτρα που προτάθηκαν ή λήφθηκαν από τον πάροχο για την αντιμετώπιση της παραβίασης προσωπικών δεδομένων¹⁸⁶.

Όσον αφορά, ειδικότερα, στις αρμοδιότητες που απονέμονται στις εθνικές αρχές, η νέα παράγραφος 4 που προστίθεται στο άρθρο 4 της Οδηγίας 2002/58/EK περιγράφει τις αρμοδιότητες που θα έχουν οι εθνικές αρχές, οι οποίες θα πρέπει να διαθέτουν τα αναγκαία μέσα για την εκτέλεση των καθηκόντων τους, συμπεριλαμβανομένων πλήρων και αξιόπιστων δεδομένων σχετικά με πραγματικά περιστατικά ασφάλειας, τα οποία έχουν οδηγήσει στο να διακυβευθούν τα δεδομένα προσωπικού χαρακτήρα κάποιων ατόμων. Στο πλαίσιο αυτό, θα πρέπει να παρακολουθούν τα μέτρα που λαμβάνονται και να διαδίδουν βέλτιστες πρακτικές μεταξύ παρόχων διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών και συγκεκριμένα: (α) να καθορίζουν κατευθυντήριες γραμμές, (β) να εκδίδουν οδηγίες σχετικά με τις περιστάσεις κατά τις οποίες απαιτείται από τον πάροχο η γνωστοποίηση των παραβιάσεων προσωπικών δεδομένων, το μορφότυπο της εν λόγω γνωστοποίησης καθώς και τον τρόπο με τον οποίο πρέπει να γίνεται η γνωστοποίηση αυτή, (γ) να έχουν τη δυνατότητα να παρακολουθούν εάν οι

¹⁸⁵ Βλ. *Πάνο Κίτσο, Παναγιώτα Παππά, ό.π.*

¹⁸⁶ Βλ. άρθρο 2 παρ. 4 γ) της οδηγίας 2009/136/EK.

πάροχοι υπηρεσιών έχουν εκπληρώσει τις υποχρεώσεις τους όσον αφορά τη γνωστοποίηση της παραβίασης των προσωπικών δεδομένων και δ. να επιβάλλουν κατάλληλες κυρώσεις σε περίπτωση αμέλειας των παρόχων να το πράξουν. Επισημαίνεται ότι, προς αρωγή των αρμοδιοτήτων των εθνικών αρχών οι πάροχοι θα πρέπει να τηρούν αρχείο παραβιάσεων δεδομένων προσωπικού χαρακτήρα. Το αρχείο αυτό θα περιλαμβάνει την περιγραφή των σχετικών περιστατικών, τα αποτελέσματά τους και τα ένδικα μέσα που έχουν ληφθεί, σε επίπεδο που να επιτρέπει στις αρμόδιες εθνικές αρχές να διαπιστώνουν τη συμμόρφωση των φορέων με τις υποχρεώσεις τους.

Τέλος, η ρύθμιση συμπληρώνεται με αναφορά στα τεχνικά εκτελεστικά μέτρα που μπορεί να λαμβάνει η Επιτροπή όσον αφορά τις συνθήκες, το μορφότυπο και τις διαδικασίες που εφαρμόζονται στις απαιτήσεις πληροφόρησης και κοινοποίησης της παραβίασης προσωπικών δεδομένων¹⁸⁷. Αναλυτικότερα, προκειμένου να διασφαλιστεί η συνοχή κατά την εφαρμογή των μέτρων αυτών η Επιτροπή μπορεί, κατόπιν διαβούλευσης με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια δικτύων και Πληροφοριών (ENISA), με την Ομάδα Εργασίας για την προστασία των ατόμων κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, που συστάθηκε με βάση το άρθρο 29 της Οδηγίας 95/46/EK, και με τον Ευρωπαϊκό Επόπτη Προστασίας Δεδομένων¹⁸⁸, να λαμβάνει τεχνικά εκτελεστικά μέτρα σχετικά με τις συνθήκες το μορφότυπο και τις διαδικασίες που εφαρμόζονται στις απαιτήσεις πληροφόρησης και κοινοποίησης. Κατά τη θέσπιση των μέτρων αυτών, η Επιτροπή θα πρέπει να εξασφαλίζει τη συμμετοχή όλων των άμεσα ενδιαφερομένων, έτσι ώστε «να ενημερώνονται σχετικά με τα βέλτιστα διαθέσιμα τεχνικά και οικονομικά μέσα για την εφαρμογή του παρόντος άρθρου».

¹⁸⁷ Ibid.

¹⁸⁸ Εντύπωση προκαλεί το γεγονός ότι δεν συμπεριλαμβάνονται στους φορείς διαβούλευσης οι αρμόδιες εθνικές αρχές παρά τις σημαντικές αρμοδιότητες ελέγχου και εποπτείας που τους έχουν ανατεθεί με την οδηγία 2009/136/EK.

3. ΣΥΓΚΡΙΣΗ ΤΩΝ ΡΥΘΜΙΣΕΩΝ ΤΗΣ ΟΔΗΓΙΑΣ 2002/58/ΕΚ ΚΑΙ ΤΟΥ Ν. 3471/2006 ΜΕ ΤΙΣ ΤΡΟΠΟΠΟΙΗΣΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2009/136/ΕΚ ΚΑΙ ΤΟΥ Ν. 4070/2012

Οι παραπάνω ρυθμίσεις, αν και δεν αλλάζουν την ουσία των μέχρι τώρα ρυθμίσεων της Οδηγίας 2002/58/ΕΚ, είναι ιδιαίτερα σημαντικές, καθόσον αναδεικνύουν τη σημασία της ασφάλειας των υποδομών των ηλεκτρονικών επικοινωνιών για τη λειτουργία των υπολοίπων διατάξεων που αναφέρονται στην προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής¹⁸⁹.

Τη νέα αυτή διάσταση της σημασίας της ασφάλειας των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες υπογραμμίζει και ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων, ο οποίος, μάλιστα, αναφέρει¹⁹⁰ ότι οι κοινοποιήσεις των παραβιάσεων ασφαλείας «μπορούν ενδεχομένως να βοηθήσουν τα φυσικά πρόσωπα να λάβουν μέτρα για τον μετριασμό της πιθανής ζημιάς που οφείλεται στην έκθεση των δεδομένων σε κίνδυνο». Είναι, όμως, ιδιαίτερα σημαντική και για τις επιχειρήσεις που παρέχουν υπηρεσίες ηλεκτρονικών επικοινωνιών, γιατί η υποχρέωσή τους αυτή «θα παρακινήσει τις εταιρείες να βελτιώσουν την ασφάλεια των δεδομένων και να αντιμετωπίζουν πιο υπεύθυνα τα δεδομένα προσωπικού χαρακτήρα που χειρίζονται».

Έτσι, σε μία περίοδο που ζητείται η εμπιστοσύνη του καταναλωτή στην ανάπτυξη του εμπορίου, αλλά και άλλων υπηρεσιών που παρέχονται μέσω των νέων τεχνολογιών των ηλεκτρονικών επικοινωνιών, οι εταιρίες θα πρέπει να αντιμετωπίσουν τα μέτρα αυτά όχι μόνο ή – τουλάχιστον – όχι κυρίως από την πλευρά του κόστους, αλλά και από την πλευρά της συμβολής τους στην ανάπτυξη των υπηρεσιών που προσφέρουν. Άλλωστε, «αυτοί που επεξεργάζονται προσωπικά δεδομένα και επωφελούνται από την πληροφορική επανάσταση πρέπει να επωμιστούν τις ευθύνες που απορρέουν από τη χρήση και τα οφέλη των νέων αυτών τεχνολογιών και να λάβουν τα

¹⁸⁹ Βλ. *Πάνο Κίτσο, Παναγιώτα Παππά, ό.π.*

¹⁹⁰ Βλ. δευτέρα γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ό.π., σημείωση υπ' αρ. 167.

απαραίτητα μέτρα ασφαλείας για την αντιμετώπιση των κινδύνων στα δεδομένα αυτά»¹⁹¹.

Περαιτέρω, ήδη αναμένεται νέα τροποποίηση της σχετικής νομοθεσίας με την ψήφιση του νέου Κανονισμού «E – Privacy Regulation», που θα ρυθμίζει την επεξεργασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες, αντικαθιστώντας την Οδηγία 2002/58/EK. Η σχετική διαδικασία βρίσκεται στο στάδιο επεξεργασίας της υφιστάμενης πρότασης της Ευρωπαϊκής Επιτροπής από τα αρμόδια όργανα της ΕΕ και αναμένεται η οριστικοποίηση και η ψήφισή της από το Ευρωπαϊκό Κοινοβούλιο¹⁹². Ειδικότερα, στην πρόταση του νέου Κανονισμού, όπως έχει διαμορφωθεί μέχρι τώρα, γίνεται παραπομπή για το θέμα της ασφάλειας στο νέο Κανονισμό ΕΕ 2016/679¹⁹³ για την προστασία των προσωπικών δεδομένων. Συγκεκριμένα προβλέπεται¹⁹⁴ ότι, στο πλαίσιο του εν λόγω κανονισμού, η έννοια της ασφάλειας εξετάζεται υπό το πρίσμα του άρθρου 32 του Κανονισμού ΕΕ 2016/679 και δη λαμβανομένων υπόψη των τελευταίων εξελίξεων, του κόστους εφαρμογής, καθώς και της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών της επεξεργασίας, όπως επίσης και των κινδύνων διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Στο πλαίσιο αυτό, τόσο ο υπεύθυνος επεξεργασίας, όσο και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα, προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των υφιστάμενων κινδύνων. Στα μέτρα αυτά, περιλαμβάνονται κατά περίπτωση, ιδίως η ψευδωνυμοποίηση και η κρυπτογράφηση δεδομένων προσωπικού

¹⁹¹ Βλ. Reding V., Securing personal data and fighting data breaches, ομιλία στο σεμινάριο «Responding to Data Breaches» που διοργάνωσε ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων με τον ENISA, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/09-10-23_Speech_Reding_EN.pdf, Βλ. Πάνο Κίτσο, Παναγιώτα Παππά, ό.π.

¹⁹² Για την πρόταση του Κανονισμού «E – Privacy Regulation», βλ. ιστοσελίδα Ευρωπαϊκής Επιτροπής <https://ec.europa.eu/digital-single-market/en/proposal-privacy-regulation>.

¹⁹³ Κανονισμός ΕΕ 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/EK (Γενικός Κανονισμός για την Προστασία Δεδομένων – GDPR).

¹⁹⁴ Βλ. Αιτιολογική σκέψη υπ' αρ. 37 της πρότασης του Κανονισμού «E – Privacy Regulation» της Ευρωπαϊκής Επιτροπής.

χαρακτήρα, η δυνατότητα διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση, η δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος και η διαδικασία για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

Επιπροσθέτως, κατά την εκτίμηση του ενδεδωγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία. Επίσης, η τήρηση εγκεκριμένου κώδικα δεοντολογίας, όπως αναφέρεται στο άρθρο 40 του Κανονισμού 2016/679 ή εγκεκριμένου μηχανισμού πιστοποίησης, όπως αναφέρεται στο άρθρο 42 αυτού, δύναται να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις απαιτήσεις της ασφαλούς επεξεργασίας. Τέλος προβλέπεται ότι, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία λαμβάνουν μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους.

Ενόψει των ανωτέρω, καταλήγουμε ότι σύμφωνα με το σχέδιο του νέου Κανονισμού «E – Privacy Regulation», το θέμα της ασφάλειας δεν αντιμετωπίζεται κατά τρόπο ενιαίο, αλλά κατά περίπτωση, σύμφωνα με τα κριτήρια των τελευταίων τεχνολογικών εξελίξεων, του κόστους εφαρμογής τους, του είδους και των σκοπών της επεξεργασίας, του υπάρχοντος κινδύνου, αλλά και των συνεπειών για το υποκείμενο σε περίπτωση παραβίασης των κανόνων ασφαλούς επεξεργασίας. Ομοίως, όπως είδαμε, με το άρθρο 12 του ν. 3471/2006, τα κριτήρια με βάση τα οποία κρίνεται το

ενδεδειγμένο σε κάθε περίπτωση επίπεδο ασφαλούς επεξεργασίας είναι ο υπάρχον κίνδυνος, οι πλέον προσφάτες τεχνικές δυνατότητες και το κόστος εφαρμογής τους. Συνεπώς, τόσο με την υπάρχουσα, όσο και με την υπό διαβούλευση νομοθεσία, το ζητούμενο επίπεδο της ασφάλειας αποτιμάται ενόψει των ειδικών συνθηκών που συνοδεύουν την υπό κρίση περίπτωση, ενώ φαίνεται να μετριάζεται και να απομακρύνεται ξεκάθαρα από την οιονεί αντικειμενική ευθύνη του άρθρου 37 του ν. 4070/2012. Έτσι, είναι πιθανόν να δημιουργηθούν προβλήματα, στο βαθμό που οι δύο ρυθμίσεις αλληλεπικαλύπτονται, ενώ μία τέτοια απόκλιση δεν εμφανίζεται δικαιολογημένη.

Είναι, δε, βέβαιο ότι, ο νέος Κανονισμός που θα αντικαταστήσει την Οδηγία 2002/58/EK («E – Privacy Regulation»), θα συμβάλλει σίγουρα στην ενδυνάμωση και την επέκταση της προστασίας προσωπικών δεδομένων των πολιτών στην Ευρωπαϊκή Ένωση. Αυτό που απομένει, είναι να δούμε αν, ενόψει της πληθώρας των ανωτέρω κριτηρίων που χρησιμοποιεί για τον προσδιορισμό του αναγκαίου επιπέδου ασφάλειας, η ερμηνεία του νέου Κανονισμού από τις εθνικές νομοθεσίες θα γίνει με τρόπο ομοιόμορφο ή αν θα οδηγηθούμε και πάλι σε αποκλίσεις, οι οποίες δεν εξυπηρετούν τη σύγκλιση, εντός του ευρωπαϊκού χώρου, προς ένα ομοιογενές επίπεδο ασφαλούς επεξεργασίας των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες.

VI. ΣΥΜΠΕΡΑΣΜΑΤΑ

Όπως προκύπτει από την προεκτεθείσα ανάλυση για το ζήτημα της ευθύνης του παρόχου ηλεκτρονικού δικτύου λόγω των προβλημάτων ασφάλειας του δικτύου, η ύπαρξη της πολυνομίας, η οποία συνίσταται στην απουσία μίας γενικής ρυθμίσεως και στην ύπαρξη ποικίλων διατάξεων που ρυθμίζουν το ζήτημα, έχει ως αποτέλεσμα την επίταση της ανασφάλειας δικαίου περί το πρόβλημα. Ως εκ τούτου, παρίσταται αναγκαία η οριοθέτηση της εφαρμογής των ανωτέρω διατάξεων, προκειμένου να δοθεί απάντηση στο ερώτημα της ευθύνης του παρόχου για προβλήματα ασφάλειας του δικτύου και της έκτασης

αυτής. Έτσι, υπό τα ως άνω δεδομένα, εκ πρώτης όψεως η ρύθμιση της ευθύνης του παρόχου φαίνεται να τριχοτομείται.

Ειδικότερα, ο πάροχος υπηρεσιών της ΚτΠ (πάροχος υπηρεσιών διαδικτύου σύμφωνα με την οδηγία 2000/31/EK και το π.δ. 131/2003), ο οποίος δεν είναι πάροχος δημοσίου δικτύου θα πρέπει να ευθύνεται μόνο για δόλο σύμφωνα με τις διατάξεις των άρθρων 15 της οδηγίας 2000/31/EK και 14 του π.δ. 131/2003, καθόσον δεν υπέχει καμία γενική υποχρέωση ελέγχου ή δραστήριας αναζήτησης του παρανόμου των πληροφοριών. Ωστόσο, σύμφωνα με την ορθότερη άποψη, η οποία ερμηνεύει τις εν λόγω διατάξεις χρησιμοποιώντας το γραμματικό, το ιστορικό και το τελολογικό κριτήριο, υποστηρίζεται ότι ο πάροχος θα πρέπει να ευθύνεται τουλάχιστον και για τις περιπτώσεις βαρείας αμέλειάς του. Την ίδια αντιμετώπιση και τη μείωση του μέτρου της ευθύνης μόνο για τις περιπτώσεις δόλου και βαρείας αμέλειας, φαίνεται να επιφυλάσσει ο Έλληνας νομοθέτης και για τους παρόχους υπηρεσιών ηλεκτρονικού δικτύου, ακόμα και αν πρόκειται για δημόσιο δίκτυο, οι οποίοι ανήκουν στην κυριαρχική διοίκηση¹⁹⁵. Εντούτοις, η ευνοϊκότερη μεταχείριση που επιφυλάσσεται για τους τελευταίους, αποτελεί μάλλον μία πρωτοβουλία του Έλληνα νομοθέτη, η οποία παρίσταται να αντίκειται στο ενωσιακό δίκαιο και συγκεκριμένα στο άρθρο 13α της οδηγίας 2009/140/EK που αυξάνει τον πήχη του καθήκοντος ασφάλειας για όλους τους παρόχους δημοσίων¹⁹⁶ δικτύων επικοινωνιών ή υπηρεσιών ηλεκτρονικών επικοινωνιών, υποχρεώνοντάς τους στη λήψη μέτρων ανάλογα αφενός με τον υπάρχοντα κίνδυνο, αφετέρου με τις πλέον πρόσφατες τεχνολογικές εξελίξεις.

Περαιτέρω, σε σχέση με την ασφάλεια των μη κρατικών δημοσίων δικτύων τη μη αφορώσα σε προσωπικά δεδομένα, η οποία μπορεί να αφορά είτε σε δεδομένα νομικών προσώπων, είτε γενικά στην ακεραιότητα των δικτύων έναντι κακόβουλων ενεργειών τρίτων μη εξουσιοδοτημένων προσώπων, ο πάροχός τους θα ευθύνεται για κάθε αμέλεια και μάλιστα, με μέτρο τις

¹⁹⁵ Βλ. ανωτέρω κεφάλαιο IV, ενότητα 3 της παρούσας.

¹⁹⁶ Χωρίς να γίνεται διάκριση εάν πρόκειται για κρατικά ή ιδιωτικά δίκτυα, αλλά το μόνο κριτήριο είναι εάν πρόκειται για δημόσιο δίκτυο, δηλαδή διαθέσιμο στο κοινό, βλ. ανωτέρω κεφάλαιο IV, ενότητες 2 και 3.

τελευταίες τεχνολογικές εξελίξεις σύμφωνα με τη ρύθμιση του άρθρου 37 του ν. 4070/2012. Μάλιστα, υποστηρίζεται¹⁹⁷ ότι υπό τις νέες αυτές νομοθετικές ρυθμίσεις, δεν πρόκειται πλέον για απλώς παρεπόμενη υποχρέωση του παρόχου, που εξαντλείται στην υποχρέωση ενημέρωσης του χρήστη-πελάτη περί ανασφάλειας του δικτύου, αλλά καθιερώνεται ένα είδος «οιονεί αντικειμενικής ευθύνης» του παρόχου να τηρεί τις διατάξεις του νόμου, ώστε να διασφαλίζεται ικανοποιητικό επίπεδο ασφάλειας του δικτύου.

Όσον αφορά στην ασφάλεια των προσωπικών δεδομένων στα ηλεκτρονικά δίκτυα, προβλέπεται κατ' άρθρο 12 ν. 3471/2006 η υποχρέωση των παρόχων τόσο των κρατικών όσο και των μη κρατικών παρόχων δημοσίων δικτύων για τη λήψη των κατάλληλων μέτρων, ώστε να διασφαλίζεται επίπεδο ασφάλειας ανάλογο με τον υπάρχοντα κίνδυνο και ειδικότερα με κριτήρια αφενός τις τεχνολογικές εξελίξεις, αφετέρου το κόστος εφαρμογής τους. Σε περίπτωση, δε, συνδρομής ιδιαίτερου κινδύνου για την ασφάλεια, ο πάροχος οφείλει απλώς να ενημερώσει σχετικά τον χρήστη-πελάτη, ενώ εάν πρόκειται για κίνδυνο πέραν του πεδίου των μέτρων που ο πάροχος οφείλει να λαμβάνει, τότε υπάρχει υποχρέωση ενημέρωσης του χρήστη-πελάτη και για τις δυνατότητες αποτροπής του κινδύνου και για το κόστος αυτών.

Συγκρίνοντας τις ανωτέρω διατάξεις, διαπιστώνουμε ότι, η ρύθμιση του άρθρου 12 ν. 3471/2006 είναι ειδικότερη του άρθρου 37 ν. 4070/2012 κατά το ότι αφορά μόνο την επεξεργασία προσωπικών δεδομένων στα ηλεκτρονικά δίκτυα και ως εκ τούτου, δεν μπορεί να θεωρηθεί ότι έχει σιωπηρώς καταργηθεί από αυτό. Εξάλλου, η εν λόγω ρύθμιση του άρθρου 12 ν. 3471/2006, τροποποιήθηκε με το άρθρο 173 του ίδιου νόμου, δηλαδή του 4070/2012, οπότε δεν μπορεί να θεωρηθεί ότι καταργήθηκε από τη μεταγενέστερη διάταξη του άρθρου 37, καθώς ταυτόχρονα τροποποιήθηκε με το άρθρο 173 του ίδιου νόμου. Σε κάθε περίπτωση, δε, θέματα που άπτονται

¹⁹⁷ Βλ. Γιώργο Ν. Γιαννόπουλο, ό.π., σελ. 60.

με την επεξεργασία δεδομένων προσωπικού χαρακτήρα εξαιρούνται ρητά από το πεδίο εφαρμογής της οδηγίας 2000/31/EK και του π.δ. 131/2003¹⁹⁸.

Ενόψει της προαναφερόμενης ανάλυσης, καταλήγουμε στα ακόλουθα συμπεράσματα σχετικά με την ευθύνη του παρόχου ηλεκτρονικού δικτύου για λόγους που σχετίζονται με την παραβίαση ασφάλειας του δικτύου:

- Αρχικά θα πρέπει να διακρίνουμε στην ευθύνη από δόλο ή από αμέλεια.
- Στην περίπτωση του δόλου, ο πάροχος θα πρέπει να δράσει αυτοβούλως, συμμορφούμενος στο καθήκον λήψης των πρόσφορων τεχνικών και οργανωτικών μέτρων προς το σκοπό της κατάλληλης διαχείρισης του κινδύνου όσον αφορά στην ασφάλεια των δικτύων και των υπηρεσιών, σύμφωνα με τις επιταγές του άρθρου 37 του ν. 4070/2012.
- Στην περίπτωση της αμέλειας του παρόχου θα πρέπει να προβούμε σε περαιτέρω διάκριση της ευθύνης και δη με κριτήριο το σε ποιο σημείο έγκειται η ανασφάλεια του δικτύου, εάν δηλαδή πρόκειται για ανασφάλεια που συνίσταται στο παράνομο περιεχόμενο των πληροφοριών που διακινούνται στο δίκτυο ή εάν πρόκειται για ανασφάλεια που προκαλείται από κακόβουλες ενέργειες τρίτων προσώπων, μη εξουσιοδοτημένων (π.χ. από τη δράση των γνωστών «hackers»). Ενόψει της τελευταίας διακρίσεως, καθίσταται σαφές ότι εάν το πρόβλημα ανασφάλειας του δικτύου έγκειται στο παράνομο περιεχόμενο των διακινούμενων σε αυτό πληροφοριών, τότε κατά την ορθότερη ανωτέρω άποψη, ο πάροχος θα πρέπει να ευθύνεται ακόμα και για βαρεία αμέλεια και να απαλλάσσεται για κάθε περίπτωση ελαφράς αμέλειας, καθόσον, σύμφωνα με τις διατάξεις των άρθρων 15 της οδηγίας 2000/31/EK και 14 του π.δ. 131/2003, δεν υπέχει καμία γενική υποχρέωση ελέγχου των αποθηκευμένων ή μεταδιδόμενων πληροφοριών, ούτε υποχρέωση δραστήριας αναζήτησης γεγονότων ή περιστάσεων που δείχνουν ότι πρόκειται για παράνομες δραστηριότητες. Ωστόσο, δεν αποκλείεται σε ειδικές περιπτώσεις να

¹⁹⁸ Βλ. άρθρο 1 παράγραφος 5 οδηγίας 2000/31/EK και άρθρο 20 παράγραφος 1 π.δ. 131/2003.

επιβάλλονται υποχρεώσεις ελέγχου σύμφωνα με την εθνική νομοθεσία και κατόπιν εντολής των εθνικών αρχών¹⁹⁹.

- Σχετικά με την δεύτερη περίπτωση, κατά την οποία λόγω των προβλημάτων ελλείψεων ασφάλειας του δικτύου λαμβάνουν χώρα κακόβουλες ενέργειες τρίτων μη εξουσιοδοτημένων προσώπων, τότε φαίνεται καταρχήν να συγκρούονται η διάταξη του άρθρου 37 του ν. 4070/2012 με αυτή του άρθρου 12 του ν. 3471/2006. Ως εκ τούτου, εάν οι ανωτέρω ενέργειες έχουν ως αποτέλεσμα την παράνομη επεξεργασία των προσωπικών δεδομένων του χρήστη στο πεδίο των ηλεκτρονικών επικοινωνιών, τότε ως ειδικότερο, θα εφαρμόζεται το άρθρο 12 ν. 3471/2006. Έτσι, ο πάροχος θα έχει αντικειμενική ευθύνη²⁰⁰ για κάθε περιουσιακή ή ηθική βλάβη. Βέβαια, θα πρέπει να λάβουμε υπόψη ότι το ζήτημα της απόδειξης της περιουσιακής βλάβης είναι πιθανόν να εμφανίζει σημαντικές αποδεικτικές δυσκολίες. Σχετικά, δε, με την ηθική βλάβη, ορίζεται ως κατώτατο όριο το ποσό των δέκα χιλιάδων ευρώ (10.000€), εκτός εάν ζητηθεί από τον ζημιωθέντα μικρότερο ποσό²⁰¹. Ωστόσο, εάν ο πάροχος έχει ενημερώσει το χρήστη-πελάτη για την ύπαρξη ιδιαίτερου κινδύνου παραβίασης της ασφάλειας του δικτύου, απαλλάσσεται από την προαναφερόμενη αντικειμενική ευθύνη του. Συνεπώς, το σημαντικό προνόμιο για τον χρήστη του δικτύου της θέσπισης αντικειμενικής ευθύνης του παρόχου ουσιαστικά «εκφυλίζεται» σε απλό καθήκον ενημέρωσής του για τους ιδιαίτερους κινδύνους ασφάλειας του δικτύου. Έτσι, αντί να διευκολύνεται η θέση του χρήστη του δικτύου, όπως είναι η βούληση του νομοθέτη, αυτός επιβαρύνεται ουσιαστικά με την απόδειξη ότι ο κίνδυνος ασφάλειας δεν είναι «ιδιαίτερος», στην περίπτωση που ήθελε κινηθεί κατά του παρόχου, επιδιώκοντας την αποκατάσταση της ζημίας του. Επίσης, θα πρέπει εδώ να γίνει δεκτό, κατ' ανάλογη εφαρμογή του

¹⁹⁹ Βλ. π.χ. την πρόσφατη υπ' αρ. 4658/2012 ΜΠΑ, ό.π.

²⁰⁰ Βλ. άρθρο 14 ν. 3471/2006.

²⁰¹ Οι εν λόγω αγωγές με τις οποίες ζητείται η αποκατάσταση της περιουσιακής και της ηθικής βλάβης εκδικάζονται με τη διαδικασία των εργατικών διαφορών σύμφωνα με το άρθρο 14, παράγραφος 3 ν. 3471/2006.

άρθρου 579 ΑΚ ότι η ως άνω ενημέρωση του παρόχου προς το χρήστη-πελάτη του για την ύπαρξη ιδιαίτερου κινδύνου θα πρέπει να λάβει χώρα κατά το προσυμβατικό στάδιο, άλλως σε περίπτωση που γίνει μεταγενέστερα ο χρήστης-πελάτης θα πρέπει να έχει δικαίωμα να καταγγείλει αζημίως τη σύμβαση παροχής υπηρεσιών δικτύου λόγω πραγματικού ελαττώματος, ή να ζητήσει τη μείωση της αντιπαροχής του κατ' ανάλογη εφαρμογή του άρθρου 576 παράγραφος 1 ΑΚ.

- Περαιτέρω, σε κάθε άλλη περίπτωση, κατά την οποία λόγω των προβλημάτων της ελλείψεως ασφάλειας του δικτύου λαμβάνουν χώρα κακόβουλες ενέργειες τρίτων μη εξουσιοδοτημένων προσώπων, οι οποίες, όμως δε σχετίζονται με την επεξεργασία προσωπικών δεδομένων, τότε χωρεί εφαρμογή των διατάξεων του άρθρου 37 του ν. 4070/2012. Έτσι, ο πάροχος θα ευθύνεται ενδοσυμβατικά έναντι του χρήστη σε περίπτωση που δεν έχει λάβει όλα τα απαιτούμενα μέτρα για την θωράκιση του δικτύου με κριτήρια τον υφιστάμενο κίνδυνο και τις πλέον πρόσφατες τεχνολογικές εξελίξεις. Μάλιστα, ο νόμος 4070/2012 δεν καθιερώνει κάποιου είδους αντικειμενική ευθύνη, όπως κατά τα ανωτέρω ο ν. 3471/2006. Αντιθέτως, εκτός από τις διοικητικές κυρώσεις που τυχόν υποβληθούν στον πάροχο από την Α.Δ.Α.Ε. δεν προβλέπεται καμία ειδικότερη θεμελίωση της ευθύνης του, οπότε είναι αναγκαία η προσφυγή στις γενικές διατάξεις του ΑΚ. Συνεπώς, ο χρήστης-πελάτης θα πρέπει να επικαλεστεί και να αποδείξει την κατάρτιση της σύμβασής του με τον πάροχο, τη ζημία του και τον αιτιώδη σύνδεσμο αυτής ένεκα της πλημμελούς εκτέλεσης της σύμβασης, η οποία εν προκειμένω θα συνίσταται στην έλλειψη ασφάλειας του δικτύου. Ο πάροχος, δε, θα πρέπει να επικαλεστεί και να αποδείξει ότι είχε πράγματι προβεί στη λήψη όλων των απαιτούμενων μέτρων σύμφωνα με το άρθρο 37 του ν. 4070/2012 και της υπό έκδοση απόφασης της Α.Δ.Α.Ε. και ότι ως εκ τούτου δεν βαρύνεται με πταίσμα ως την ασφάλεια του δικτύου του.
- Ενόψει των ανωτέρω, καταλήγουμε ότι παρόλο που ο νόμος θέτει ψηλά τον πήχη του καθήκοντος επιμέλειας του παρόχου σχετικά με τη λήψη των απαιτούμενων μέτρων ασφαλείας για την ασφάλεια του

δικτύου, η προστασία του χρήστη- πελάτη λόγω παραβίασης της εν λόγω υποχρέωσης του παρόχου κάθε άλλο εκτός από ικανοποιητική δεν μπορεί να χαρακτηριστεί. Ειδικότερα, είναι εύλογο οι περισσότερες περιπτώσεις κακόβουλων ενεργειών τρίτων μη εξουσιοδοτημένων προσώπων να συνεπάγονται την παράνομη επεξεργασία προσωπικών δεδομένων, οπότε ο πάροχος θα απαλλάσσεται με την απλή ενημέρωση του χρήστη-πελάτη για την ύπαρξη ιδιαίτερου κινδύνου ασφάλειας του δικτύου. Στις υπόλοιπες περιπτώσεις, που δεν άπτονται παράνομης επεξεργασίας προσωπικών δεδομένων και οι οποίες συγκριτικά θα είναι πολύ λιγότερες, αφενός ο θιγόμενος χρήστης – πελάτης θα πρέπει να έχει υποστεί περιουσιακή ζημία, καθόσον δε χωρεί ευθύνη για αποκατάσταση ηθικής βλάβης λόγω παράβασης συμβατικής υποχρέωσης²⁰², αφετέρου, ακόμα και στην περίπτωση της περιουσιακής ζημίας, η απόδειξη του αιτιώδους συνδέσμου μεταξύ αυτής και της πλημμελούς εκτέλεσης της σύμβασης, η οποία έγκειται στην ύπαρξη «κενών» ασφαλείας του δικτύου είναι αν όχι εξαιρετικά δυσχερής, σχεδόν αδύνατη, διότι είναι λογικό ο χρήστης να μην γνωρίζει τα κενά ασφαλείας του δικτύου, τα οποία μπορεί να τα γνωρίζει μόνο ο πάροχος.

VII. ΕΠΙΛΟΓΟΣ

Από την προηγηθείσα ανάλυση προκύπτει πράγματι ότι η μη εκπλήρωση του καθήκοντος επιμέλειας του παρόχου ηλεκτρονικού δικτύου ως προς τη λήψη των απαιτούμενων μέτρων για την ασφάλεια του δικτύου του έχει κυρίως διοικητικές συνέπειες που άπτονται στην επιβολή κυρώσεων από την εποπτεύουσα αρχή, εν προκειμένω από την Α.Δ.Α.Ε. και την Ε.Ε.Τ.Τ. Αντιθέτως, σε επίπεδο αστικής ευθύνης του παρόχου λόγω παραβίασης του ανωτέρω καθήκοντος επιμέλειας, η αποκατάσταση της ζημίας του πελάτη-χρήστη παρίσταται εξαιρετικά δυσχερής αφενός λόγω της δυνατότητας του παρόχου να απαλλαγεί προβαίνοντας σε προηγούμενη ενημέρωση του παρόχου, αφετέρου λόγω των σοβαρών προβλημάτων απόδειξης που

²⁰² Βλ. άρθρο 299 ΑΚ σε συνδυασμό με άρθρα 59, 932 ΑΚ.

υπογραμμίζονται ανωτέρω. Όμως, με τον τρόπο αυτό, η υποχρέωση του παρόχου για τη λήψη των απαιτούμενων μέτρων για την ασφάλεια του δικτύου του καθίσταται ουσιαστικά «ατελής», καθόσον ο αντισυμβαλλόμενός του δεν μπορεί εν τοις πράγμασι να ικανοποιηθεί αποτελεσματικά σε περίπτωση παράβασης της εν λόγω υποχρέωσης του παρόχου. Το γεγονός, δε, αυτό κάθε άλλο παρά συνάδει με την αναγκαιότητα για αυξημένη ασφάλεια στο τομέα των ηλεκτρονικών δικτύων, η οποία αποτελεί «αίτημα των καιρών μας» και ταυτόχρονα πρόκληση, ιδίως ενόψει της συνεχούς ανάπτυξης των ηλεκτρονικών δικτύων σε όλες τις εκφάνσεις της καθημερινής μας ζωής.

VIII. ΒΙΒΛΙΟΓΡΑΦΙΑ – ΠΗΓΕΣ

1. ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ - ΑΡΘΡΟΓΡΑΦΙΑ

- Γεωργιάδης Γεώργιος, Ο ν. 3471/2006 για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, ΧρΙΔ 2007.
- Γιαννόπουλος Γιώργος, Η ευθύνη των παρόχων υπηρεσιών στο Internet, Η ανατροπή της ασυλίας τους από τη νομοθεσία για: ηλεκτρονικές επικοινωνίες (μετά το ν. 4070/2012), προστασία προσωπικών δεδομένων, απόρρητο επικοινωνιών, πνευματική ιδιοκτησία, εκδόσεις Νομική Βιβλιοθήκη, Αθήνα 2013,
- Θεοδωρίδης Κωνσταντίνος, European Network and Information Security Agency, Η εξασφάλιση της ΕΕ ξεκινά από το Ηράκλειο, ΔΙΜΕΕ 2005.
- Ιγγλεζάκης Ιωάννης, Δίκαιο της Πληροφορικής, εκδόσεις Σάκκουλα Αθήνα – Θεσσαλονίκη, 2008.
- Ιγγλεζάκης Ιωάννης, Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου, εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη 2003.

- Καλλινίκου Διονυσία, σχόλια σε υπ' αρ. 4658/2012 ΜΠΑ, ΧρΙΔ 2012.
- Καράκωστας Ιωάννης, Δίκαιο και Internet, Νομικά ζητήματα του διαδικτύου, εκδόσεις Δίκαιο & Οικονομία. Π. Ν. Σάκκουλας, Αθήνα 2003.
- Καράκωστας Ιωάννης, Το δίκαιο του internet, ΝοΒ 1998.
- Κατσανάκη Φαίνη, Ευθύνη παρόχων υπηρεσιών Internet κατά τη διαμεσολάβηση στη διακίνηση παράνομου υλικού, ΧρΙΔ 2008.
- Κάτσικας Σωκράτης, Ασφάλεια Υπολογιστών, Τόμος α', σελ. 49-50, Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα 2001.
- Κίτσος Πάνος - Παππά Παναγιώτα, Ενίσχυση της πληροφορικής και της διαφάνειας στις υπηρεσίες ηλεκτρονικών επικοινωνιών υπό το πρίσμα της οδηγίας 2009/136/ΕΚ, ΔΙΜΕΕ 2010.
- Κοτσαλής Λεωνίδα, Προσωπικά Δεδομένα, σελ. 383-384, Νομική Βιβλιοθήκη, έκδοση 2016.
- Μαργαρίτης Μιχαήλ, σχόλια σε υπ' αρ. 4658/2012 ΜΠΑ, ΝοΒ 2012.
- Πιτσιρίκος Ιωάννης, Δεδομένα προσωπικού χαρακτήρα στο Διαδίκτυο υπό το πρίσμα του ν. 3471/2006 (όπως τροποποιήθηκε από τους ν. 3917/2001, 4070/2012), Πειραϊκή Νομολογία 2012.
- Σπυρόπουλος Στέργιος, Η διάκριση των παρόχων υπηρεσιών στο διαδίκτυο και η οριοθέτηση της ευθύνης τους με βάση την κοινοτική Οδηγία 2000/31/ΕΚ σχετικά με το ηλεκτρονικό εμπόριο, ΔΙΜΕΕ 2005.
- Χριστοδούλου Κωνσταντίνος, Επιτομή Ηλεκτρονικού Αστικού Δικαίου, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή 2013.

- Χριστοδούλου Κωνσταντίνος, Ευθύνη του παρόχου δικτύου για προσβολές της ιδιωτικής σφαίρας, ΔΙΜΕΕ 2010.
- Χριστοδούλου Κωνσταντίνος, Προστασία της προσωπικότητας και της συμβατικής ελευθερίας στα κοινωφελή δίκτυα, εκδόσεις Αντ. Ν. Σάκουλα, Αθήνα – Κομοτηνή 2007.
- Χριστοδούλου Κωνσταντίνος, Αστική Ευθύνη του παρόχου δικτύου ως μεσάζοντος στην παροχή υπηρεσιών της κοινωνίας της πληροφορίας, ΔΙΜΕΕ 2004.

2. ΞΕΝΟΓΛΩΣΣΗ ΒΙΒΛΙΟΓΡΑΦΙΑ – ΑΡΘΡΟΓΡΑΦΙΑ

- Gollman Dieter, Computer Security, Wiley, 1999.
- Krutz Ronald - Russell Dean Vines, The CISSP Pre Guide: Mastering the Ten Domains of Computer Security, Willey, 2001.
- Reed Chris, Internet Law: Text and Materials, second edition, Cambridge University Press 2004.
- Stoneburner Gary, NIST, SP 800-33:Computer Security, NIST, December 2001.

3. ΛΟΙΠΕΣ ΠΗΓΕΣ

- Ιστοσελίδα Ευρωπαϊκής Επιτροπής www.ec.europa.eu
- Ιστοσελίδα Ευρωπαίου Επόπτη Προστασίας Δεδομένων www.edps.europa.eu
- Ιστοσελίδα της Γερμανικής Αρχής Προσωπικών Δεδομένων, www.bfdi.bund.de
- Ιστοσελίδα ENISA www.enisa.europa.eu/
- Ιστοσελίδα Α.Δ.Α.Ε. www.adae.gr/
- Ιστοσελίδα Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα www.dpa.gr