ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ
ΚΑΤΕΥΘΥΝΣΗ

«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΔΙΑΣΦΑΛΙΣΗ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΜΑΝΤΕΣ ΒΑΣΙΛΕΙΟΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων/σα
Γ.ΣΤΑΜΟΥΛΗΣ

Λαμία, 2019

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο/Η ΔΗΛΩΝ/-ΟΥΣΑ

Ημερομηνία

Υπογραφή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΔΙΑΣΦΑΛΙΣΗ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ:

ΕΠΙΒΛΕΠΩΝ: Γ. ΣΤΑΜΟΥΛΗΣ

ΛΑΜΙΑ

Νοέμβριος 2018

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΔΙΑΣΦΑΛΙΣΗ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ:

ΕΠΙΒΛΕΠΩΝ: Γ. ΣΤΑΜΟΥΛΗΣ

ΛΑΜΙΑ
Νοέμβριος 2018

ΠΕΡΙΛΗΨΗ

Η διαχείριση των προσωπικών δεδομένων, και ιδιαίτερα των διακινούμενων στο Διαδίκτυο, συνιστά ένα επίκαιρο ζήτημα που έχει απασχολήσει τόσο την Ευρωπαϊκή Ένωσης όσο και την ελληνική νομοθεσία. Στην παρούσα εργασία καταγράφονται τα νομοθετικά κείμενα που στοχεύουν στη διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών, με έμφαση στον πρόσφατο Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR). Η διασφάλιση του ηλεκτρονικού απορρήτου αφορά αποφασιστικά τη διασφάλιση της ανωνυμίας στο Διαδίκτυο. Περιγράφονται μία ποικιλία τεχνολογικών εργαλείων τα οποία μπορούν να χρησιμοποιηθούν αυτόνομα ή σε συνδυασμό, ήτοι Εικονικά Ιδιωτικά Δίκτυα (VPNs), διακομιστές μεσολάβησης (proxy servers) και η δρομολόγηση Onion, με χρήση του φυλλομετρητή Tor ή του δίκτύου I2P. Τέλος, περιγράφεται το νομικό πλαίσιο της άρσης του ηλεκτρονικού απορρήτου σε ό,τι αφορά τις προϋποθέσεις και τη διαδικασία που πραγματοποιείται προς αυτή την κατεύθυνση.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ηλεκτρονικά δεδομένα

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: απόρρητο, ανωνυμία, Διαδίκτυο

ABSTRACT

Personal data management and, specifically, the management of data which is transferred via the Web, is a crucial topic that is included in several pieces of the European and Greek legislation. In the current thesis these pieces of legislation are described and emphasis is given on the recent General Data Protection Regulation. Protection of electronic privacy relates to the concept of Web anonymity. For this reason, a variety of technological tools are described, used independently or in combination, such as Virtual Personal Networks (VPNs), proxy servers and Onion routing, by the use of Tor browser of I2P network. Finally, the legal framework for the disclosure of electronic data is described in detail, relating to the causes and the relevant procedure.

SUBJECT AREA: Electronic data

KEYWORDS: privacy, anonymity, Web

Αφιερώνω την παρούσα εργασία...

ΕΥΧΑΡΙΣΤΙΕΣ

Για τη διεκπεραίωση της παρούσας πτυχιακής εργασίας, θα ήθελα να ευχαριστήσω:

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

1. ΕΙΣΑΓΩΓΗ

Πριν από κάποια έτη το Διαδίκτυο αποτελούσε ένα πολύ μικρότερο τμήμα του σημερινού του όγκου. Οι κόμβοι του ήταν διεσπαρμένοι σε ερευνητικά εργαστήρια, σε εταιρικούς φορείς και σε ακαδημαϊκά ιδρύματα. Η αλματώδης ανάπτυξη της χρήσης του Διαδικτύου κατά τα τελευταία 10-15 έτη, ιδιαίτερα δε η αμεσότερη πρόσβαση σε αυτό λόγω της χρήσης των «έξυπνων τηλεφώνων» (smartphones) η οποία έχει εξαπλωθεί ραγδαία κατά την τελευταία δεκαετία, αλλά και η προώθηση των ηλεκτρονικών συναλλαγών έχουν οδηγήσει στη μετατροπή των δεδομένων υλικής μορφής σε ηλεκτρονική μορφή που λαμβάνει χώρα σε καθημερινή βάση. Καθώς σχεδόν όλες υπηρεσίες και όλοι οι εταιρικοί οργανισμοί και ιδιώτες χρησιμοποιούν υπολογιστικά συστήματα ή/και κινητά τηλέφωνα για την ανταλλαγή και τη διαχείριση των δεδομένων τους, η αξία των πληροφοριών που συγκεντρώνονται αποκτά ιδιαίτερες διαστάσεις και καθίσταται ένα θέμα που συζητείται ολοένα και περισσότερο. Επί παραδείγματι, είναι πρόσφατος ο «θόρυβος» αναφορικά με τη διαχείριση των προσωπικών δεδομένων από γνωστό κοινωνικό δίκτυο του Διαδικτύου. Σε αρκετές περιπτώσεις το σύνολο των πληροφοριών εταιρικών και κρατικών φορέων έχει αποθηκευτεί σε ψηφιακή μορφή, χωρίς να υφίσταται η αναλογική ή η έντυπη μορφή τους.

Η διαρκής εξάρτηση του ατόμου και των συναλλαγών από τα ηλεκτρονικά συστήματα, σε συνδυασμό με την ενίσχυση της λειτουργικότητας και της φιλικότητας των συστημάτων αυτών συνεπάγονται την ενισχυμένη τους πολυπλοκότητα. Το γεγονός αυτό επιφέρει μία πληθώρα προβλημάτων και αδυναμιών αναφορικά με την ασφάλεια των δεδομένων και των συστημάτων, λόγω προγραμματιστικών λαθών, κακών ρυθμίσεων ή των σχέσεων εμπιστοσύνης που διαμορφώνονται μεταξύ των ιδιωτών ή και των οργανισμών. Επιπλέον, οι χρήστες του Διαδικτύου, αν και έχει αντιληφθεί σε κάποιες περιπτώσεις φαινόμενα κλοπής δεδομένων και παραβίασης της ασφάλειας διαφόρων συστημάτων συνεχίζει να μην έχει λάβει κάποια ιδιαίτερη εκπαίδευση σε σχέση με τα ζητήματα της ασφάλειας του διαδικτύου. Τουναντίον, η πλειοψηφία των χρηστών αγνοούν τις απειλές και τους κινδύνους που ενέχει η χρήση του Διαδικτύου, οι δε εταιρείες παροχής υπηρεσιών (λ.χ. ηλεκτρονικής αλληλογραφίας ή τραπεζικών συναλλαγών) ουσιαστικά εθίζουν σε πρακτικές που διέπονται αρκετές φορές από χαμηλά επίπεδα ασφαλείας, ενώ

παρέχουν την αίσθηση ότι αντιμετωπίζουν με αποτελεσματικό τρόπο το ζήτημα της ασφάλειας των δεδομένων προσωπικών δεδομένων των χρηστών τους.

Η ευρεία ανάπτυξη των διαδικτυακών υπηρεσιών έχει οδηγήσει στην ανάγκη διασφάλισης του απορρήτου, της ιδιωτικότητας και της ανωνυμίας σε μία σειρά εφαρμογών. Ο σκοπός της παρούσας εργασίας είναι διπλός. Από τη μία πλευρά εξέτασης του ζητήματος του απορρήτου των ηλεκτρονικών επικοινωνιών θα επιδιωχθεί να αναδειχθούν τα τεχνολογικά και τεχνικά εργαλεία που εξυπηρετούν τη διασφάλιση του απορρήτου των επικοινωνιών, ιδίως με την επίτευξη ενός ικανοποιητικού βαθμού ανωνυμίας του χρήστη κατά την διαδικτυακή του πλοήγηση. Από την άλλη, θα καταγραφούν τα νομοθετικά κείμενα της Ευρωπαϊκής Ένωσης και της Ελλάδας που στοχεύουν στη διασφάλιση των δικαιωμάτων των φυσικών και νομικών προσώπων των οποίων τα προσωπικά δεδομένα συλλέγονται και υφίστανται επεξεργασία, αλλά και τα κείμενα που επιτρέπουν την άρση του εν λόγω απορρήτου στις περιπτώσεις που αυτό κρίνεται αναγκαίο.

2. ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

2.1. Γενικές παρατηρήσεις

Η αλματώδης ανάπτυξη της Πληροφορικής και των νέων τεχνολογιών, οι νέες μορφές ηλεκτρονικών συναλλαγών και διαφήμισης, αλλά και η ανάγκη της ηλεκτρονικής οργάνωσης του δημοσίου τομέα συνεπάγονται αυξημένη ζήτηση δεδομένων προσωπικού χαρακτήρα τόσο από τον δημόσιο όσο και από τον ιδιωτικό τομέα. Κατά συνέπεια, στην ιδιωτική ζωή των πολιτών είναι δυνατόν να δημιουργηθούν προβλήματα λόγω της ανεξέλεγκτης καταχώρησης και επεξεργασίας των προσωπικών δεδομένων σε ηλεκτρονικά αρχεία εταιρειών, οργανισμών και υπηρεσιών. Οι εν λόγω κίνδυνοι αυξάνονται σε σημαντικό βαθμό με την ανάπτυξη των νέων δυνατοτήτων για την ταχύτατη μεταφορά πληροφοριών σε διεθνές επίπεδο μέσω του Διαδικτύου (World Wide Web). Συνεπώς, για τη διασφάλιση της ατομικής προστασίας στο πλαίσιο της σημερινής «κοινωνίας της πληροφορίας» δεν αρκούν οι παραδοσιακές θεσμοθετημένες ρυθμίσεις και εγγυήσεις, αλλά απαιτείται ειδική αντιμετώπιση.

Η 7η Φεβρουαρίου έχει καθιερωθεί ως η «Παγκόσμια Ημέρα Ασφαλούς Πλοήγησης στο Διαδίκτυο», μετά την πρωτοβουλία της επιτρόπου της ΕΕ Vivan Reding, ώστε να ευαισθητοποιηθούν οι χρήστες αναφορικά με τους κινδύνους του Διαδικτύου. Είναι γεγονός ότι τόσο σε διεθνές όσο και σε εθνικό επίπεδο, αλλού σε μεγαλύτερο και αλλού σε μικρότερο βαθμό, έχουν ληφθεί μέτρα που αφορούν την ασφαλή πλοήγηση στο Διαδίκτυο. Επιπλέον, έχουν διαμορφωθεί ειδικές οργανώσεις, ενώ σε ευρωπαϊκό επίπεδο η Ευρωπαϊκή Ένωση (ΕΕ) έχει θεσπίσει συγκεκριμένους νόμους που στοχεύουν στην προστασία των χρηστών του Διαδικτύου.

Σύμφωνα με εκτιμήσεις, η απώλεια διαφόρων ψηφιακών δεδομένων συνιστά μία από τα σοβαρότερα μη υπολογιζόμενα προβλήματα των σύγχρονων κοινωνιών. Η προστασία των δεδομένων αυτών από εξωτερικούς αλλά και από εσωτερικούς κινδύνους, καθώς και η διασφάλιση της κατάλληλης λειτουργίας του συνόλου των υπολογιστικών συστημάτων που μετέχουν σε ένα οικιακό ή εταιρικό δίκτυο οφείλουν να περιλαμβάνονται στις προτεραιότητες των διαφόρων χρηστών. Η «μόλυνση» ενός η παραπάνω συστημάτων από ψηφιακό ιό συνεπάγεται πολύ

συχνά την απώλεια δεδομένων ζωτικής φύσης σε σχέση με την εταιρεία ή το άτομο. Ιδιαίτερα σημαντικό θεωρείται το κόστος που αντιστοιχεί στις απολεσθείσες ώρες εργασίας μέρους ή του συνόλου του προσωπικού της επιχείρησης. Επιπροσθέτως, ένας εισβολέας των υπολογιστικών συστημάτων (hacker) είναι δυνατόν να χρησιμοποιήσει είτε εταιρικά δεδομένα είτε προσωπικά δεδομένα τα οποία παρέχουν οι πελάτες μιας εταιρείας πλήττοντας ανεπανόρθωτα τη φήμη και το κύρος της επιχείρησης και επιβαρύνοντάς την με άμεσο ή έμμεσο τρόπο.

Γενικά, οι προσωπικές πληροφορίες που σχετίζονται με κάθε είδους δραστηριότητα του ατόμου, προσωπική ή επαγγελματική, αναφέρονται ως «προσωπικά δεδομένα». Με βάση τον Ν. 2472/1997 προσωπικά δεδομένα αποκαλείται «κάθε πληροφορία που αναφέρεται στο πρόσωπο του εκάστοτε ατόμου», όπως το όνομα, το επάγγελμα, η οικογενειακή κατάσταση, οι πολιτικές πεποιθήσεις, η θρησκεία, οι φιλοσοφικές απόψεις, η συνδικαλιστική δράση, η κατάσταση της υγείας, η ερωτική ζωή και οι ενδεχόμενες ποινικές διώξεις και καταδίκες (Χρυσόγονος, 2002).

2.2. Προστασία των προσωπικών δεδομένων

Η ΕΕ αναγνώρισε για πρώτη φορά ότι η συλλογή, όπως επίσης και η επεξεργασία και ιδίως η κοινοποίηση και μετάδοση προσωπικών δεδομένων πρέπει να διέπονται από συγκεκριμένες διατάξεις περί το 1981. Τότε υπεγράφη στο Στρασβούργο η «Συνθήκη για την Προστασία του Ατόμου από την Αυτόματη Επεξεργασία Προσωπικών Δεδομένων» (Σειρά ευρωπαϊκών συνθηκών Νο 108). Έκτοτε σε ευρωπαϊκό επίπεδο έχουν δημοσιευτεί διάφορες συστάσεις που αφορούν την προστασία των δεδομένων, ιδίως η Σύσταση R(90)19, που αφορά την προστασία των προσωπικών δεδομένων τα οποία χρησιμοποιούνται για την εξόφληση λογαριασμών και την επιτέλεση άλλων συναφών εργασιών.

Με τη χρήση του Διαδικτύου από την πλευρά των χρηστών οι τελευταίοι επιφορτίζονται με ορισμένες ευθύνες που αφορούν τη δράση τους, ενώ θέτουν την ιδιωτικότητά τους σε κίνδυνο. Οι χρήστες για τη διασφάλιση αυτής της ιδιωτικότητας οφείλουν να συμπεριφέρονται με τρόπο ο οποίος τους παρέχει επαρκή βαθμό προστασίας και προάγει τις ομαλές σχέσεις με άλλα πρόσωπα. Τα παραπάνω

συνιστούν κατευθυντήριες γραμμές των θεσμοθετημένων συστάσεων, ενώ παράλληλα προτείνονται διάφοροι πρακτικοί τρόποι που διασφαλίζουν την ιδιωτικότητα. Ωστόσο, οι χρήστες οφείλουν να γνωρίζουν τόσο τις υποχρεώσεις όσο και τα δικαιώματά τους που προκύπτουν από τα επιμέρους νομικά κείμενα. Εξάλλου ο σεβασμός της ιδιωτικότητας συνιστά θεμελιώδες ατομικό δικαίωμα με βάση τόσο την ευρωπαϊκή όσο και την εθνική νομοθεσία. Παρακάτω θα περιγραφούν τα νομικά κείμενα που διέπουν τη διασφάλιση του απορρήτου στις ηλεκτρονικές επικοινωνίες (Χρυσόγονος, 2002).

2.2.1. Οδηγία 95/46/ΕΚ

Η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου αφορούσε την προστασία φυσικών προσώπων σε ό,τι αφορά την επεξεργασία προσωπικών δεδομένων και την ελεύθερη κυκλοφορία των συγκεκριμένων δεδομένων. Οι διατάξεις της Οδηγίας είχαν διπλό στόχο, ήτοι αφ' ενός την προστασία της ιδιωτικής ζωής και των θεμελιωδών δικαιωμάτων, αφ' ετέρου δε τη διασφάλιση της ελεύθερης ροής των προσωπικών δεδομένων εντός της ΕΕ, ούτως ώστε να επιτευχθούν η κοινωνική και η οικονομική συνεργασία και προόδου, καθώς και η επιστημονική και τεχνική συνεργασία στο πλαίσιο της κοινωνίας των τηλεπικοινωνιών και της πληροφορίας.

Η παραπάνω Οδηγία αποτέλεσε το ευρωπαϊκό κείμενο αναφοράς σε ζητήματα προστασίας προσωπικών δεδομένων. Ορίζει ένα κανονιστικό πλαίσιο το οποίο στοχεύει στην καθιέρωση ενός είδους ισορροπίας μεταξύ της ελεύθερης ροής των προσωπικών δεδομένων εντός των κρατών-μελών της ΕΕ και της διασφάλισης υψηλού επιπέδου προστασίας της ιδιωτικότητας των ατόμων και των εταιρικών φορέων. Στην Οδηγία ως «δεδομένο προσωπικού χαρακτήρα» ορίζεται κάθε πληροφοριακό στοιχείο το οποίο αναφέρεται σε φυσικό πρόσωπο με γνωστή ή εξακριβώσιμη ταυτότητα. Οι διατάξεις της εφαρμόζονται στην καθολικά ή εν μέρει αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων (όπως, επί παραδείγματι, μέσω πληροφοριακής βάσης δεδομένων πελατών μιας επιχείρησης). Οι διατάξεις επεκτείνονται και στη μη αυτοματοποιημένη επεξεργασία των δεδομένων αυτών τα οποία καταγράφονται σε παραδοσιακά αρχεία (σε χαρτί).

Στα κράτη-μέλη της ΕΕ εφαρμόστηκαν οι εθνικές διατάξεις που θεσπίζονται ως απόρροια της Οδηγίας 95/46/ΕΚ σε κάθε διαδικασία επεξεργασίας προσωπικών δεδομένων, εφόσον η εν λόγω επεξεργασία διενεργείται στο πλαίσιο δραστηριοτήτων ενός φορέα που είναι εγκατεστημένος στο έδαφος των κρατών-μελών. Κατά συνέπεια, η Ελλάδα, στη βάση αυτής της Οδηγίας, θεωρήθηκε υπεύθυνη για τη διασφάλιση της προστασίας των προσωπικών δεδομένων που υφίστανται επεξεργασία από τους οργανισμούς ηλεκτρονικού εμπορίου οι οποίοι έχουν εγκατασταθεί ή πρόκειται να εγκατασταθούν στα γεωγραφικά όρια της χώρας. Η Οδηγία 95/46/ΕΚ καταργήθηκε τον Μάιο του 2018 και αντικαταστάθηκε από τον Κανονισμό 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

2.2.2. Οδηγία 2002/58/ΕΚ

Η Οδηγία 2002/58/ΕΚ στοχεύει στην «επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών». Πρόκειται για αναθεώρηση της προγενέστερης Οδηγίας 97/66/ΕΚ που αφορούσε την επεξεργασία των προσωπικών δεδομένων και την προστασία της ιδιωτικότητας στον τηλεπικοινωνιακό τομέα, ούτως ώστε να ληφθούν υπ’ όψιν οι νεότερες τεχνολογικές εξελίξεις και υπηρεσίες. Η εν λόγω Οδηγία συνιστά θεμελιώδες στοιχείο του κανονιστικού πλαισίου που στοχεύει στην ανάπτυξη του τομέα των ηλεκτρονικών επικοινωνιών με τρόπο επωφελή για τους ιδιώτες και τις επιχειρήσεις οι οποίες μεταχειρίζονται τις υπηρεσίες του τομέα των ηλεκτρονικών επικοινωνιών.

Στην Οδηγία 2002/58/ΕΚ καθιερώνεται η θέσπιση ειδικών τεχνικών και νομικών διατάξεων που στοχεύουν στην προστασία βασικών ελευθεριών και δικαιωμάτων. Πιο συγκεκριμένα, η ανάπτυξη του ηλεκτρονικού εμπορίου προϋπέθετε τη δυνατότητα προστασίας των προσωπικών δεδομένων των χρηστών, ενώ διά της έκδοσης της Οδηγίας πραγματοποιήθηκε εναρμόνιση των διατάξεων των κρατών-μελών μεταξύ τους, με τρόπο ώστε να διασφαλίζονται ίσα επίπεδα προστασίας των βασικών ελευθεριών και δικαιωμάτων και η ελεύθερη ροή των προσωπικών δεδομένων και των υπηρεσιών και εξοπλισμών ηλεκτρονικών επικοινωνιών στο πλαίσιο της ΕΕ (Παπαδόπουλος, 2008).

Ως θεμελιώδεις αρχές που διέπουν την προστασία των δεδομένων προσωπικού χαρακτήρα, σύμφωνα με την Οδηγία 2002/58/ΕΚ ορίζονται οι ακόλουθες:

1. Οι διαδικασίες επεξεργασίας προσωπικών δεδομένων οφείλουν να είναι σε κάθε περίπτωση νόμιμες και θεμιτές.

2. Η συλλογή των προσωπικών δεδομένων οφείλει σε κάθε περίπτωση να ικανοποιεί νόμιμους και ρητά καθορισμένους σκοπούς, ενώ η χρήση τους πρέπει να είναι ανάλογη.

3. Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται και χρησιμοποιούνται πρέπει να μην υπερβαίνουν τα αναγκαία δεδομένα που ικανοποιούν στους σκοπούς των διαδικασιών επεξεργασίας τους.

4. Δεδομένα που μπορούν δυνάμει να αποκαλύψουν την ταυτότητα των προσώπων δεν θα πρέπει να φυλάσσονται για χρονικό διάστημα μεγαλύτερο του απολύτως απαραίτητου.

5. Τα δεδομένα πρέπει να ενημερώνονται, όπου αυτό χρειάζεται, και να είναι ακριβή.

6. Οι φορείς που κατέχουν προσωπικά δεδομένα πρέπει να παρέχουν στα πρόσωπα στα οποία αναφέρονται τα δεδομένα αυτά εύλογα μέσα για την τροποποίηση, τη δέσμευση ή τη διαγραφή ανακριβών δεδομένων.

7. Για την αποτροπή της χωρίς άδεια ή παράνομης επεξεργασίας δεδομένων προσωπικού χαρακτήρα πρέπει να λαμβάνονται τα κατάλληλα οργανωτικά και τεχνικά μέτρα.

8. Τα δεδομένα προσωπικού χαρακτήρα δεν πρέπει να προωθούνται σε χώρες εκτός του οικονομικού χώρου της ΕΕ, εκτός αν οι χώρες αυτές εγγυώνται το κατάλληλο (επαρκές) επίπεδο προστασίας των προσωπικών δεδομένων.

Επίσης, η παραπάνω Οδηγία επιβάλλει την υποχρέωση στα κράτη-μέλη της ΕΕ να συγκροτήσουν τουλάχιστον μία ανεξάρτητη εποπτική αρχή που θα είναι επιφορτισμένη με την παρακολούθηση της εφαρμογής των διατάξεών της. Η τήρηση ενημερωμένου δημοσίου μητρώου από την πλευρά των εν λόγω αρχών αποτελεί ένα από τα καθήκοντά τους, ούτως ώστε το κοινό να είναι σε θέση να

γνωρίζει τα ονόματα των κατόχων των δεδομένων, καθώς και το είδος της επεξεργασίας που χρησιμοποιούν οι τελευταίοι. Ακόμη, ο φορέας παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών οι οποίες είναι διαθέσιμες στο ευρύ κοινό πρέπει να λαμβάνει τα απαραίτητα οργανωτικά και τεχνικά μέσα που διασφαλίζουν την ασφάλεια των υπηρεσιών του από κοινού με τους παρόχους των δημοσίων δικτύων επικοινωνιών. Οι παραπάνω φορείς οφείλουν να ενημερώνουν τους συνδρομητές τους, εφόσον υφίσταται κάποιος ιδιαίτερος κίνδυνος που απειλεί την ασφάλεια του δικτύου (Χρυσόγονος, 2002).

2.2.3. Κανονισμός 2016/79

Ο Κανονισμός (ΕΕ) 2016/79 που αφορά «την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ («Γενικός Κανονισμός για την Προστασία Δεδομένων» (General Data Protection Regulation, GDPR), όπως προαναφέρθηκε, αντικατέστησε την Οδηγία 95/46/ΕΚ, η οποία θεωρήθηκε ότι δεν ήταν πλέον προσαρμοσμένη στη σύγχρονη διαδικτυακή τεχνολογική πραγματικότητα. Τέθηκε δε σε ισχύ τον Μάιο του 2018. Τα κράτη-μέλη της ΕΕ όφειλαν να ψηφίσουν διατάξεις σε τομείς όπου προβλέπονται μερικές εξειδικεύσεις ή παρεκκλίσεις από το βασικό νομοθετικό πλαίσιο. Κατά συνέπεια, άμεση συνέπεια είναι η ανάγκη κατάργησης του Ν. 2492/97, η οποία και αναμένεται (Ιγγλεζάκης, 2017).

Το νέο ρυθμιστικό πλαίσιο εδράζεται στο οικοδόμημα της παλαιότερης Οδηγίας, αλλά εισάγει επιπλέον δικαιώματα, με χαρακτηριστικά από αυτά το δικαίωμα στη λήθη και η φορητότητα των δεδομένων. Επιπλέον, καταργείται ο προληπτικός έλεγχος διά των γνωστοποιήσεων και των αδειών από την πλευρά των εποπτικών αρχών. Ο προληπτικός έλεγχος αντικαθίσταται από την ανάγκη εκπόνησης «μελέτης αντικτύπου». Επιπλέον, εισάγεται η υποχρέωση των φορέων να διορίζουν υπεύθυνο για την προστασία των προσωπικών δεδομένων. Το σύνολο των δημοσίων αρχών και των εταιρικών φορέων που διαχειρίζονται προσωπικά δεδομένα κλήθηκαν να προσαρμοστούν στο γράμμα και το πνεύμα του

νέου ευρωπαϊκού Κανονισμού. Οι καινοτομίες που εισήχθησαν με τη διαμόρφωση και την εφαρμογή του Κανονισμού είναι οι εξής:

1. Ενίσχυση της νομικής θέσης των πολιτών με θεμελίωση βασικών δικαιωμάτων

2. Επιβολή νέων υποχρεώσεων στους υπεύθυνους επεξεργασίας προσωπικών δεδομένων

3. Εφαρμογή νέων μοντέλων (“privacy by design”)

4. Περαιτέρω έμφαση στη γνωστοποίηση των παραβιάσεων που αφορούν τη διαχείριση προσωπικών δεδομένων

5. Ιδιαίτερα βαριές κυρώσεις σε περίπτωση παραβάσεων.

Αναλυτικότερα, στα δικαιώματα που θεμελιώνονται από τον Κανονισμό 2016/79 περιλαμβάνονται τα ακόλουθα:

1. Το δικαίωμα ενημέρωσης, εφόσον οι υπεύθυνοι επεξεργασίας καλούνται να λάβουν τα δέοντα μέτρα για την παροχή κάθε πληροφορίας και ανακοίνωσης στον πολίτη αναφορικά με την επεξεργασία και μάλιστα σε μορφή σαφή, κατανοητή και ευσύνοπτη, ειδικά όταν τα προσωπικά δεδομένα αφορούν παιδιά

2. Το δικαίωμα προσβάσεως στα δεδομένα, καθώς ο πολίτης δικαιούται να λαμβάνει από τους υπεύθυνους επεξεργασίας σχετική επιβεβαίωση η οποία αναφέρεται στο κατά πόσον τα προσωπικά δεδομένα που τον αφορούν υφίστανται διαδικασίες επεξεργασίας, ενώ ο πολίτης δικαιούται πρόσβαση σε ένα πλήθος πληροφοριών οι οποίες περιλαμβάνονται στο Άρθρο 15.

3. Το δικαίωμα διορθώσεως, εφόσον ο πολίτης δικαιούνται να απαιτήσει από τους υπεύθυνους επεξεργασίας την τροποποίηση (διόρθωση) ανακριβών προσωπικών δεδομένων και μάλιστα άνευ αδικαιολόγητης καθυστέρησης. Ο πολίτης δικαιούται μέσω συμπληρωματικής δήλωσης να απαιτήσει τη συμπλήρωση προσωπικών δεδομένων ελλιπούς χαρακτήρα, λαμβάνοντας πάντοτε υπ’ όψιν τους σκοπούς των διαδικασιών επεξεργασίας.

4. Το «δικαίωμα στη λήθη», καθώς ο πολίτης δικαιούται να απαιτήσει από τους υπεύθυνους επεξεργασίας να διαγραφούν προσωπικά δεδομένα που τον αφορούν, στην περίπτωση που τα τελευταία δεν θεωρούνται πλέον απαραίτητα ή αν ο πολίτης ανακαλέσει τη συγκατάθεση ή αντιτεθεί στις διαδικασίες επεξεργασίας και

δεν υφίστανται νόμιμοι και επιτακτικοί λόγοι για την επεξεργασία αυτών ή εφόσον τα προσωπικά δεδομένα έχουν υποβληθεί παρανόμως προς επεξεργασία ή για την τήρηση νομικής υποχρέωσης ή συλλέχθηκαν όταν ο πολίτης ήταν ακόμα παιδί. Επιπλέον, όσοι έχουν δημιουργήσει αντίγραφα ή συνδέσμους των δεδομένων οφείλουν να προχωρήσουν στη διαγραφή των δεδομένων.

5. Το δικαίωμα στον περιορισμό της επεξεργασίας, καθώς ο πολίτης δικαιούνται να απαιτήσει από τους υπεύθυνους επεξεργασίας να περιοριστούν οι διαδικασίες επεξεργασίας των προσωπικών δεδομένων, στην περίπτωση που είναι αμφισβητήσιμη η ακρίβεια των τελευταίων ή όταν η επεξεργασία είναι παράνομη ή εφόσον οι υπεύθυνοι επεξεργασίας δεν χρειάζονται πλέον τα συγκεκριμένα δεδομένα για τους διακηρυγμένους σκοπούς της επεξεργασίας, όμως τα δεδομένα απαιτούνται από την πλευρά του πολίτη για την άσκηση, υποστήριξη ή θεμελίωση νομικών αξιώσεων ή εφόσον ο πολίτης εκφράζει αντιρρήσεις αναφορικά με την επεξεργασία, ενώ είναι σε αναμονή διαδικασιών επαλήθευσης των νόμιμων ισχυρισμών του εκάστοτε υπεύθυνου επεξεργασίας.

6. Το δικαίωμα στη φορητότητα των προσωπικών δεδομένων, καθώς ο πολίτης μπορεί να λαμβάνει τα προσωπικά δεδομένα που έχει παράσχει στους υπεύθυνους επεξεργασίας σε μορφή ευρέως χρησιμοποιούμενη, δομημένη και αναγνώσιμη από τεχνικό εξοπλισμό, ενώ δικαιούται επίσης να προωθεί τα συγκεκριμένα δεδομένα σε άλλους υπεύθυνους επεξεργασίας.

7. Το δικαίωμα εναντιώσεως, καθώς ο πολίτης μπορεί να αντιτίθεται στην επεξεργασία των προσωπικών δεδομένων (από δημόσιους ή ιδιωτικούς φορείς) ανά πάσα στιγμή, συμπεριλαμβανομένης της διαμόρφωσης προφίλ επί τη βάσει των συγκεκριμένων διατάξεων. Επιπλέον, εφόσον τα δεδομένα υφίστανται επεξεργασία με στόχο άμεση εμπορική προώθηση, ο πολίτης μπορεί να αντιταχθεί στην επεξεργασία των προσωπικών δεδομένων ανά πάσα στιγμή, συμπεριλαμβανομένης της διαμόρφωσης προφίλ αν η τελευταία αφορά τη συγκεκριμένη εμπορική προώθηση.

2.2.4. Εθνικό πλαίσιο προστασίας προσωπικών δεδομένων

Ιδιαίτερη έμφαση στο πεδίο προστασίας των προσωπικών δεδομένων στην Ελλάδα, με έμφαση στην κατηγορία των ηλεκτρονικών δεδομένων, έχει δοθεί από τις αρχές της δεκαετίας του 2000. Πιο συγκεκριμένα, η προστασία των εν λόγω δεδομένων κατοχυρώθηκε συνταγματικά μόλις με το Ψήφισμα της Ζ' Αναθεωρητικής Βουλής (6/4/2001). Έκτοτε η εξέλιξη της τεχνολογίας και η διαμόρφωση νέων και καινοτόμων τεχνολογιών οι οποίες εξυπηρετούν την αυτοματοποιημένη συλλογή, χρήση και επεξεργασία δεδομένων προσωπικού χαρακτήρα οδήγησε σε μία σειρά ρυθμίσεων και νομοθετικών πρωτοβουλιών με εφαλτήριο την προστασία των δεδομένων αυτών επί τη βάσει αυτοτελούς συνταγματικού δικαιώματος (Χρυσόγονος, 2002).

Πιο συγκεκριμένα, στο αναθεωρημένο άρθρο 9^{A} αναφέρεται ότι κάθε πολίτης απολαμβάνει «δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη Αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει».

Επιπλέον, στην Ελλάδα λειτουργεί ως ανεξάρτητη διοικητική υπηρεσία από το 1997 η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΔΑΕ). Η ίδρυση και λειτουργία της ανεξάρτητης αρχής διέπεται από τον Ν. 2472/97. Στους στόχους της αρχής περιλαμβάνεται η εποπτεία του βαθμού εφαρμογής των νόμων και των σχετικών ρυθμίσεων που αναφέρονται στην προστασία των φυσικών προσώπων από την επεξεργασία προσωπικών δεδομένων.

Τα δεδομένα τα οποία συλλέγονται από τους οργανισμούς ηλεκτρονικού εμπορίου για την εξυπηρέτηση των πελατών τους, στο πλαίσιο των ηλεκτρονικών συναλλαγών υπόκεινται σε έλεγχο από την Αρχή, ενώ η τελευταία έχει επωμιστεί τις ακόλουθες αρμοδιότητες:

1. Την έκδοση οδηγιών και κανονιστικών πράξεων που στοχεύουν στην εφαρμογή των διατάξεων οι οποίες σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα, καθώς και την γνωμοδότηση που αφορά τα σχετικά ζητήματα

2. Το να απευθύνει υποδείξεις και συστάσεις στους υπεύθυνους των διαδικασιών επεξεργασίας των προσωπικών δεδομένων και η επιβολή και υποστήριξη των φορέων διατήρησης αρχείων σε ό,τι αφορά την κατάρτιση κωδίκων δεοντολογίας της χρήσης των προσωπικών δεδομένων

3. Την αναφορά των παραβάσεων στις αρμόδιες δικαστικές και διοικητικές αρχές και την επιβολή κυρώσεων

4. Τη διενέργεια ελέγχων σε κάθε αρχείο διατήρησης προσωπικών δεδομένων, αυτεπάγγελτα ή ύστερα από καταγγελία

Στην Ελλάδα το θεμελιώδες νομικό πλαίσιο για την προστασία των δεδομένων προσωπικού χαρακτήρα διέπεται από τους νόμους 2472/97 («Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα») και 3471/06 («Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/97»).

Πιο συγκεκριμένα, σύμφωνα με τη Σαατζίδου-Παντελιάδου (2006), στο δεύτερο κεφάλαιο του νόμου αναφέρονται οι αρχές που θα πρέπει να χαρακτηρίζουν τη διαδικασία επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, ήτοι:

1. Η αρχή της νομιμότητας του στόχου της επεξεργασίας, η οποία επιβάλλει τη νομιμότητα και τη σαφήνεια των σκοπών συλλογής και χρήσης των προσωπικών δεδομένων

2. Η αρχή της αναλογικότητας, κατά την οποία τα δεδομένα προσωπικού χαρακτήρα τα οποία υφίστανται επεξεργασία απαιτείται να είναι πρόσφορα, συναφή και όχι περισσότερα από τα απαιτούμενα για την επίτευξη των σκοπών της επεξεργασίας

3. Η αρχή της ακριβείας, κατά την οποία τα δεδομένα οφείλουν να είναι ακριβή και να ενημερώνονται, εφόσον αυτό απαιτείται

4. Η αρχή της χρονικής διάρκειας κατά την οποία τα δεδομένα διατηρούνται, σύμφωνα με την οποία η διατήρηση των δεδομένων μπορεί να υφίσταται μόνον κατά το χρονικό διάστημα το οποίο απαιτείται ούτως ώστε να υλοποιηθούν οι σκοποί της συλλογής και της επεξεργασίας αυτών.

Πλην των παραπάνω, η νομοθεσία προβλέπεται ότι η επεξεργασία των προσωπικών δεδομένων είναι επιτρεπτή και νόμιμη μόνον στην περίπτωση που το υποκείμενο το οποίο αφορούν τα συλλεχθέντα δεδομένα έχει συμφωνήσει στις διαδικασίες συλλογής και επεξεργασίας. Από τον όρο αυτόν προβλέπεται ένα πεδίο εξαιρέσεων που θεωρείται αρκετά ευρύ, όπως στην περίπτωση που η επεξεργασία είναι απαιτούμενη για την υλοποίηση κάποιας σύμβασης, αν εκπληρώνεται κάποια υποχρέωση του υπεύθυνου επεξεργασίας που επιβάλλει ο νόμος, αν η επεξεργασία απαιτείται για να διαφυλαχθούν ζωτικά συμφέροντα του υποκειμένου, αν το υποκείμενο τελεί σε νομική ή φυσική αδυναμία να συμφωνήσει με την επεξεργασία, αν απαιτείται για την υλοποίηση έργου δημοσίου συμφέροντος ή εμπίπτοντος στην άσκηση της δημόσιας εξουσίας ή αν η διαδικασία της επεξεργασίας θεωρείται απόλυτα αναγκαία για να ικανοποιηθεί το έννομο συμφέρον το οποίο επιδιώκει ο υπεύθυνος επεξεργασίας των δεδομένων ή οι τρίτοι προς τους οποίους διαβιβάζονται τα δεδομένα και μόνον εφόσον οι εν λόγω συνθήκες υπερέχουν των συμφερόντων και δικαιωμάτων των υποκειμένων και δεν θίγονται οι ελευθερίες αυτών (Κατραμάδος, 1999).

Κεντρικής σημασίας είναι το τρίτο κεφάλαιο του παραπάνω νόμου (Άρθρα 11-14) όπου περιγράφονται τα δικαιώματα των υποκειμένων και όπου θεσπίζονται οι σχετικές εγγυήσεις. Τα συγκεκριμένα δικαιώματα περιλαμβάνουν το δικαίωμα πρόσβασης, ενημέρωσης, προσωρινής δικαστικής προστασίας και αντίρρησης.

Σύμφωνα με το δικαίωμα πρόσβασης του προσώπου στα δεδομένα, κάθε υποκείμενο δικαιούται να γνωρίζει αν προσωπικά δεδομένα που το αφορούν έχουν αποτελέσει ή αποτελούν αντικείμενο επεξεργασίας. Το πρόσωπο δικαιούται σε μόνιμη βάση να απαιτεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας, άνευ καθυστέρησης, εγγράφως και κατά τρόπο σαφή ενημέρωση αναφορικά με το σύνολο των προσωπικών δεδομένων που το αφορούν, την προέλευση αυτών, τους σκοπούς και την εξέλιξη της επεξεργασίας, τις κατηγορίες των αποδεκτών των δεδομένων, τον τρόπο αυτοματοποιημένης επεξεργασίας, και, ενδεχομένως, τη δέσμευση, τη διόρθωση ή τη διαγραφή των ελλιπών ή ανακριβών δεδομένων, αλλά και την ανακοίνωση των τροποποιήσεων ή της διαγραφής σε τρίτους (Κατραμάδος, 1999).

Σε ό,τι αφορά το δικαίωμα ενημέρωσης προβλέπεται ότι ο υπεύθυνος επεξεργασίας πρέπει να ενημερώνει με σαφή τρόπο τον σκοπό επεξεργασίας των προσωπικών δεδομένων, την ταυτότητα αυτού ή του εκπροσώπου του, τους αποδέκτες των δεδομένων και την ύπαρξη δικαιώματος πρόσβασης σε αυτά. Μόνον στην περίπτωση που συντρέχουν λόγοι εθνικής ασφαλείας για την επεξεργασία των προσωπικών δεδομένων ή λόγοι διακρίβωσης πολύ σοβαρών εγκλημάτων είναι δυνατή η μερική ή καθολική άρση της υποχρέωσης ενημέρωσης του προσώπου, επί τη βάσει απόφασης της Αρχής. Στην περίπτωση που η συλλογή των δεδομένων πραγματοποιείται αποκλειστικώς για δημοσιογραφικούς σκοπούς και αναφέρεται σε δημόσια πρόσωπα δεν υφίσταται η υποχρέωση ενημέρωσης.

Το δικαίωμα δικαστικής προστασίας ορίζεται με το Άρθρο 14 στο οποίο προβλέπεται ότι κάθε πρόσωπο μπορεί να ζητήσει από την αρμόδια δικαστική αρχή τη μη εφαρμογή ή την άμεση αναστολή απόφασης ή πράξης που τον θίγει, η οποία έχει ληφθεί από διοικητική αρχή, νομικό πρόσωπο ιδιωτικού ή δημοσίου δικαίου, φυσικό πρόσωπο ή ένωση προσώπων αποκλειστικώς διά μέσου αυτοματοποιημένης επεξεργασίας στοιχείων, αν η εν λόγω επεξεργασία στοχεύει στο να αξιολογηθεί η προσωπικότητά του και ιδιαίτερα η αποδοτικότητά του στην εργασία, η οικονομική φερεγγυότητά του, η αξιοπιστία του και, γενικώς, η συμπεριφορά του.

Ιδιαίτερης σημασίας θεωρείται το δικαίωμα αντίρρησης, σύμφωνα με το οποίο το πρόσωπο το οποίο αφορούν τα συλλεχθέντα προσωπικά δεδομένα μπορεί να προβάλλει αντιρρήσεις αναφορικά με την επεξεργασία των δεδομένων. Οι αντιρρήσεις πρέπει να υποβάλλονται εγγράφως στον υπεύθυνο επεξεργασίας και θα πρέπει να αφορούν συγκεκριμένο αίτημα, όπως για τη δέσμευση, διαγραφή, τροποποίηση, μη διαβίβαση ή προσωρινή μη χρησιμοποίηση των δεδομένων. Ακολούθως, ο υπεύθυνος επεξεργασίας οφείλει να απαντήσει και να ενημερώσει εγγράφως το πρόσωπο σχετικά με τις ενέργειες στις οποίες προέβη ή σχετικά με τους λόγους μη ικανοποίησης του παραπάνω αιτήματος. Αν οι αντιρρήσεις απορριφθούν, η απάντηση του υπευθύνου επεξεργασίας πρέπει να κοινοποιείται στην Αρχή. Στην περίπτωση που ο τελευταίος δεν απαντήσει εντός δεκαπέντε ημερών το πρόσωπο μπορεί να προχωρήσει σε προσφυγή στην Αρχή και να αιτηθεί εξέτασης των αντιρρήσεών του. Η Αρχή έχει τη δυνατότητα επιβολής της

άμεσης αναστολής της επεξεργασίας των δεδομένων, εφόσον θεωρήσει ότι οι αντιρρήσεις είναι δικαιολογημένες και ότι υπάρχει κίνδυνος για σοβαρή βλάβη του προσώπου λόγω της συνέχισης της επεξεργασίας, μέχρι την έκδοση οριστικής απόφασης που να αφορά τις αντιρρήσεις (Μήτρου, 1999).

3. ΕΡΓΑΛΕΙΑ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΚΑΙ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

3.1. Πολιτικές ιδιωτικότητας

Η προστασία διά του νομικού πλαισίου, η οποία παρέχει τους όρους για τις νόμιμες διαδικασίες συλλογής, χρήσης και επεξεργασίας των προσωπικών

δεδομένων παραβιάζεται συχνότατα στον διαδικτυακό χώρο και, κατά συνέπεια, ο βέλτιστος τρόπος για την προστασία του χρήστη αφορά τη διατήρηση με όσο το δυνατόν καλύτερο τρόπο της ανωνυμίας αυτού, αλλά και τη λήψη ορισμένων μέτρων προφύλαξης. Προς την τελευταία κατεύθυνση κινείται η ανάπτυξη των κατάλληλων τεχνολογικών εργαλείων διά των οποίων επιτυγχάνεται η προστασία του χρήστη κατά την πλοήγησή του στο Διαδίκτυο. Επιπλέον, αν ο χρήστης επιθυμεί να προβεί στην καταχώρηση των προσωπικών του δεδομένων, είναι καλό να λαμβάνει αρχικά γνώση της πολιτικής ιδιωτικότητας (privacy policy) που ακολουθεί ο εκάστοτε ιστοχώρος και η εκάστοτε επιχείρηση η οποία δραστηριοποιείται στον χώρο του Διαδικτύου.

Ουσιαστικά, οι πολιτικές ιδιωτικότητας αντιστοιχούν σε κείμενα που αναρτώνται από τους οργανισμούς και τις επιχειρήσεις στους διαδικτυακούς τους τόπους, ούτως ώστε να ενημερώσουν τον χρήστη αναφορικά με τον τρόπο με τον οποίον θα χρησιμοποιηθούν τα προσωπικά τους δεδομένα, καθώς και με το χρονικό διάστημα κατά τη διάρκεια του οποίου θα διατηρηθούν, αλλά και με τις επιλογές που διαθέτουν ως προς τη χρήση και επεξεργασία των δεδομένων τους (Cavoukian & Hamilton, 2002). Ο συγκεκριμένος τρόπος πληροφόρησης στην ιδανική περίπτωση δίνει τη δυνατότητα στους χρήστες να προβαίνουν στη λήψη αποφάσεων ως προς τη διαχείριση των δεδομένων προσωπικού χαρακτήρα που τους αφορούν και την επιλογή ανάμεσα σε διαφορετικές ιστοσελίδες και επιχειρήσεις στη βάση της πολιτικής ιδιωτικότητας που εκείνες ακολουθούν.

Στη σημερινή εποχή η χρήση των συγκεκριμένων εργαλείων έχει καταστεί ιδιαίτερα κοινή, καθώς το σύνολο των δημοφιλών ιστοσελίδων αλλά και η συντριπτική πλειοψηφία των ιστοσελίδων που είναι λιγότερο δημοφιλείς μεριμνούν στην παρουσίαση εγγράφων που αφορούν πολιτικές ιδιωτικότητας. Ωστόσο, παρά την ευρεία διαθεσιμότητα των εν λόγω εγγράφων, οι χρήστες πολύ σπάνια προβαίνουν στην ανάγνωσή τους. Μάλιστα αναφέρεται ότι οι καταναλωτές θεωρούν τις πολιτικές ιδιωτικότητας δύσκολες και δυσνόητες στην μελέτη και την κατανόησή τους (Adkinson et al., 2002; Cuhan & Milne, 2004), ενώ ορισμένες από αυτές διατυπώνονται με τρόπο που απαιτεί ευρεία γνώση και πληροφόρηση (Jensen & Potts, 2004).

Πέραν της δυσκολίας κατανόησης, οι πολιτικές ιδιωτικότητας είναι δυνατόν να μεταβληθούν άνευ συγκεκριμένης προειδοποίησης και να διαφέρουν σε σημαντικό βαθμό μεταξύ διαφορετικών ιστοχώρων, γεγονός που καθιστά αρκετά δύσκολο. Καθώς τις περισσότερες φορές οι πολιτικές ιδιωτικότητας δεν διαβάζονται αρκετοί χρήστες έχουν λάθος εικόνα αναφορικά με αυτές. Έρευνα που διενεργήθηκε στις ΗΠΑ και την οποίαν αναφέρουν οι Turow et al. (2005) κατέγραψε ότι οι περισσότεροι χρήστες που έχουν αναγνώσει έγγραφα πολιτικής ιδιωτικότητας δημοφιλών ιστοσελίδων θεωρεί ότι η ύπαρξη των εγγράφων είναι ισοδύναμη με την προστασία των δεδομένων προσωπικού χαρακτήρα.

Με βάση τα παραπάνω, καθίσταται σαφές ότι παρά την ευρεία διαθεσιμότητα των πολιτικών ιδιωτικότητας, οι χρήστες του Διαδικτύου δεν ενημερώνονται αναφορικά με την προστασία των προσωπικών τους δεδομένων και, επομένως, αυτές δεν θεωρούνται αποτελεσματικό μέσο για την πρόσβαση των χρηστών στις πληροφορίες αναφορικά με ζητήματα ιδιωτικότητας.

3.2. Ανωνυμία στο Διαδίκτυο

3.2.1. Γενικές παρατηρήσεις

Οι χρήστες του Διαδικτύου που δεν εμφανίζουν ιδιαίτερες ανησυχίες αναφορικά με την ιδιωτικότητά τους μπορούν να την προστατεύσουν διά της ελεγχόμενης γνωστοποίησης προσωπικών δεδομένων. Σε αυτή την περίπτωση αποδέχονται τη γνωστοποίηση των διευθύνσεων διαδικτυακού πρωτοκόλλου (Internet Protocol address, IP address), δηλαδή των μοναδικών αριθμών που χρησιμοποιούνται από συσκευές σε ένα δίκτυο υπολογιστών το οποίο για την αναγνώριση και επικοινωνία των συσκευών χρησιμοποιεί το πρότυπο διαδικτυακού πρωτοκόλλου (Internet Protocol standard). Πέραν τούτου, αποδέχονται την αποκάλυψη και όλων των υπόλοιπων πληροφοριών που διέπουν τη μη προσωπική ταυτοποίηση, ούτως ώστε να εξασφαλίζεται η παροχή των υπηρεσιών οι οποίες δεν θα παρέχονταν στην περίπτωση πλήρους ανωνυμίας, όπως για παράδειγμα η παροχή πληροφοριών αναφορικά με το ιστορικό αναζήτησης του χρήστη σε έναν δεδομένο φυλλομετρητή (browser). Εκτός από τους παραπάνω χρήστες υπάρχουν

και εκείνοι που επιθυμούν μεγαλύτερο βαθμό προστασίας της ιδιωτικότητας και σε αυτή την περίπτωση επιχειρούν την επίτευξη «διαδικτυακής ανωνυμίας» (Internet anonymity), ώστε να εξασφαλίσουν την ιδιωτικότητά τους, χωρίς να παρέχουν τη δυνατότητα σύνδεσης των διαδικτυακών τους δραστηριοτήτων με δεδομένα και πληροφορίες που επιτρέπουν την προσωπική ταυτοποίηση σε τρίτα μέρη.

Για την επίτευξη της ανωνυμίας στο Διαδίκτυο χρησιμοποιούνται ποικίλοι τρόποι και διάφορα εργαλεία, κάθε ένα από τα οποία εμφανίζει ορισμένα πλεονεκτήματα και μειονεκτήματα. Συχνά δε αξιοποιούνται ταυτοχρόνως πολλές μέθοδοι, για την επίτευξη του βέλτιστου αποτελέσματος. Τα βασικά εργαλεία αφορούν τα Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks, VPNs), τους διακομιστές μεσολάβησης (proxy servers), τον φυλλομετρητή Tor (Tor Browser) και το I2P.

3.2.2. VPNs

Το VPN αποτελεί εικονικό δίκτυο δομημένο σε επίπεδο πάνω από τα υφιστάμενα «φυσικά» δίκτυα και το οποίο έχει τη δυνατότητα να παρέχει έναν μηχανισμό ελέγχου και επικοινωνίας που χαρακτηρίζεται από σημαντικό βαθμό ασφαλείας. Μέσω του VPN ο χρήστης μπορεί με ασφάλεια να προβεί σε σύνδεση μέσω διαδικτύου με ένα ιδιωτικό δίκτυο. Το εικονικό δίκτυο διαμορφώνει μία κρυπτογραφημένη σύνδεση που αναφέρεται ως «σήραγγα VPN» (VPN tunnel). Το σύνολο των δεδομένων που ανταλλάσσονται μπορούν να μεταφερθούν διά της συγκεκριμένης ασφαλούς σήραγγας. Κατ' αυτόν τον τρόπο διατηρούνται οι πληροφορίες προσωπικού χαρακτήρα ιδιωτικά και ασφαλή.

Τα VPNs χρησιμοποιούνται κυρίως για την προστασία των πληροφοριών που ανταλλάσσονται κατά τις επικοινωνίες που αφορούν τα δημόσια δίκτυα, όπως το Διαδίκτυο. Με τη χρήση του συγκεκριμένου εργαλείου παρέχονται διάφορα είδη προστασίας των δεδομένων, όπως ο έλεγχος πρόσβασης, η ακεραιότητα, η εμπιστευτικότητα και ο έλεγχος της ταυτότητας πηγής των δεδομένων.

Παρά το ότι τα VPNs μπορούν να περιορίσουν τους κινδύνους που απειλούν την ασφαλή πλοήγηση στο Διαδίκτυο δεν μπορούν να τους απομακρύνουν

ολοκληρωτικά. Επί παραδείγματι, μία εφαρμογή VPN ενδέχεται να εμφανίζει αδύναμα σημεία σε σχέση με το χρησιμοποιούμενο λογισμικό ή με τους εφαρμοζόμενους αλγορίθμους. Μπορεί επίσης να έχει ρυθμιστεί με τιμές διαμόρφωσης και με ρυθμίσεις που δεν είναι ασφαλείς. Τα παραπάνω γίνονται αντιληπτά από τους επιτιθέμενους χρήστες ως ελαττώματα του συστήματος τα οποία μπορούν να αξιοποιήσουν. Άλλο σοβαρό πρόβλημα αφορά την αποκάλυψη του κλειδιού κρυπτογράφησης. Ο επιτιθέμενος χρήστης που ανακαλύπτει ένα ορισμένο κλειδί όχι μόνον είναι σε θέση να αποκρυπτογραφήσει τη ροή των ανταλλασσόμενων δεδομένων, αλλά και να αποτελέσει εξουσιοδοτημένο χρήστη. Ένα άλλο ζήτημα που διέπει τη χρήση VPNs αναφέρεται στη διαθεσιμότητα. Αν και τα εικονικά δίκτυα σχεδιάζονται για την υποστήριξη της ακεραιότητας και της εμπιστευτικότητας μπορεί να ειπωθεί ότι εν γένει δεν βελτιώνουν τους όρους διαθεσιμότητας, ήτοι της ικανότητας των χρηστών με εξουσιοδότηση εισόδου στο εικονικό δίκτυο να αποκτήσουν τη δέουσα πρόσβαση στα συστήματα. Αντίθετα, αρκετές εφαρμογές VPN προσθέτοντας περισσότερες υπηρεσίες και περισσότερα στοιχεία στην υφιστάμενη δομή του δικτύου τείνουν να περιορίσουν σε έναν βαθμό τη διαθεσιμότητα. Η ύπαρξη περιορισμού ή μη της διαθεσιμότητας καθορίζεται σε έναν μεγάλο βαθμό από το μοντέλο αρχιτεκτονικής που έχει υιοθετηθεί, καθώς και από τις λεπτομέρειες της διαμόρφωσης του δικτύου.

Γενικά, οι κατηγορίες των μοντέλων αρχιτεκτονικής VPN είναι τρεις και περιλαμβάνουν τις ακόλουθες:

1. “Host-to-Gateway/End-to-Site/Remote-Access”: Η εν λόγω αρχιτεκτονική στοχεύει στην προστασία της επικοινωνίας μεταξύ κάποιου συγκεκριμένου δικτύου ενός οργανισμού και ανεξάρτητων κεντρικών υπολογιστών. Η χρήση της είναι συνακόλουθη με τη δυνατότητα να επιτρέπεται να αποκτούν πρόσβαση σε υπηρεσίες εσωτερικού χαρακτήρα (π.χ. Web διακομιστές, e-mail του οργανισμού) χρήστες μη ασφαλισμένων δικτύων.

2. “Gateway-to-Gateway/LAN-to-LAN/Site-to-Site”. Το συγκεκριμένο μοντέλο αρχιτεκτονικής στοχεύει στην προστασία των επικοινωνιών μεταξύ δύο δικτύων, όπως επί παραδείγματι το δίκτυο υποκαταστημάτων μίας επιχείρησης και το δίκτυο των κεντρικών της γραφείων, δίκτυα επιχειρηματικών εταίρων, κλπ.

3. “Host-to-host/End-to-End/Remote Desktop”, που στοχεύει στην προστασία δύο υπολογιστών. Αυτό το είδος αρχιτεκτονικής προτιμάται συχνά στην περίπτωση που ένας σχετικά μικρός αριθμός χρηστών πρέπει να διαχειρίζεται ή να χρησιμοποιεί κάποιο απομακρυσμένο σύστημα και απαιτείται η χρήση πρωτοκόλλων τα οποία δεν είναι ασφαλή.

Το πρώτο από τα παραπάνω είδη αφορά τη σύνδεση υπολογιστών φιλοξενίας (hosts) σε διάφορα δίκτυα με hosts του δικτύου ενός οργανισμού διά της ανάπτυξης μίας πύλης στο δίκτυο του οργανισμού και της δυνατότητας που δίνει σε εξωτερικούς hosts να προβούν σε συνδέσεις VPN στην πύλη αυτή. Είναι γεγονός ότι εξασφαλίζεται η προστασία της επικοινωνίας μεταξύ της πύλης και των hosts, αλλά όχι και των hosts προορισμού που μετέχουν στον οργανισμό και της πύλης. Αξιοποιείται συχνά στην περίπτωση που διάφοροι hosts εντός μη ασφαλισμένων δικτύων συνδέονται με πόρους ασφαλισμένων δικτύων. Τα VPN που έχουν αναπτυχθεί στη βάση του συγκεκριμένου μοντέλου στις περισσότερες περιπτώσεις δεν είναι διαφανή (για τους χρήστες), καθώς κάθε χρήστης, πριν την αξιοποίηση του VPN, πρέπει να προβεί σε πιστοποίηση της ταυτότητάς του, ενώ οι hosts πρέπει να διαθέτουν λογισμικό πελάτη VPN (Winkler & Zeadally, 2015).

Τα μοντέλα Gateway-to-Gateway/LAN-to-LAN/Site-to-Site αναπτύσσονται για τη διαμόρφωση μίας πύλης σε κάθε δίκτυο και μίας σύνδεσης VPN ανάμεσα στις δύο πύλες. Κατ’ αυτόν τον τρόπο, οι hosts των δύο δικτύων επικοινωνούν διά της σύνδεσης VPN, που τους παρέχει προστασία. Ωστόσο, δεν εξασφαλίζεται η προστασία μεταξύ της τοπικής πύλης κάθε host και του host αυτού καθ’ εαυτόν. Καθώς αυτό το είδος αρχιτεκτονικής χρησιμοποιείται για τη σύνδεση μέσω διαδικτύου δύο ασφαλισμένων δικτύων τα ιδιωτικά δίκτυα ευρείας περιοχής (wide area networks, WANs) καθίστανται πιο δαπανηρά. Τα VPN που διαμορφώνονται με τον παραπάνω τρόπο γενικά θεωρούνται διαφανή και η εγκατάσταση ή η διαμόρφωση λογισμικού σε διακομιστές ή πελάτες δεν θεωρείται προαπαιτούμενο.

Τέλος, στο τρίτο είδος αρχιτεκτονικής επιτυγχάνεται η σύνδεση hosts με έναν δεδομένο «στοχευμένο» host με την ανάπτυξη ενός κατάλληλου λογισμικού VPN και με τη διαμόρφωση του «στοχευμένου» host με τέτοιον τρόπο ώστε να είναι παραλήπτης συνδέσεων VPN από το σύνολο των άλλων hosts. Το συγκεκριμένο μοντέλο VPN είναι το μόνο που εξασφαλίζει την προστασία των ανταλλασσόμενων

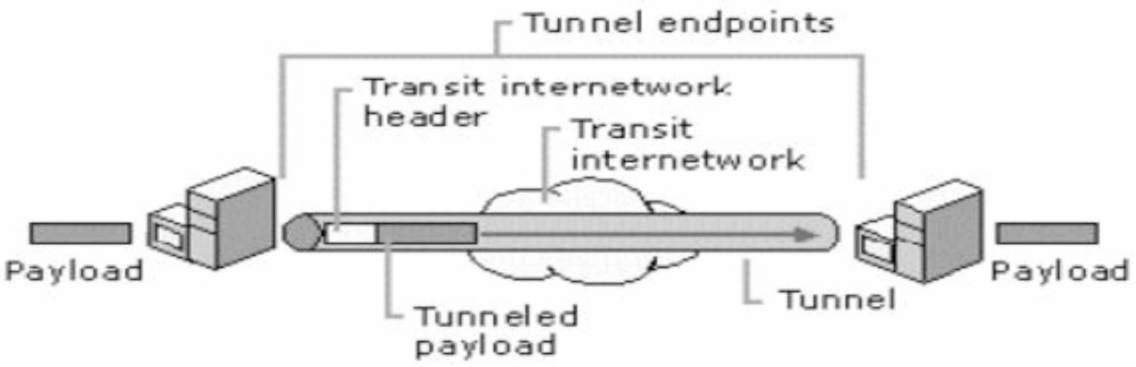
δεδομένων καθ' όλη τη διαδικασία διαβίβασης των πληροφοριών. Από την άλλη, το μοντέλο host-to-host είναι δυσκολότερο ως προς την εφαρμογή και τη συντήρησή του, καθώς η διαμόρφωση σε κάθε host είναι προαπαιτούμενο.

Στον Πίνακα 3.1 καταγράφονται οι λειτουργίες κάθε μοντέλου αρχιτεκτονικής VPN.

Πίνακας 3.1. Λειτουργίες των μοντέλων αρχιτεκτονικής VPN (Winkler & Zeadally, 2015).

Λειτουργία	**Host-to-Gateway**	**Gateway-to-Gateway**	**Host-to-host**
Παροχή προστασίας			
Μεταξύ τοπικής πύλης και πελάτη	N/A (το τελικό σημείο VPN είναι ο πελάτης)	όχι	N/A (το τελικό σημείο VPN είναι ο πελάτης)
Μεταξύ των τελικών σημείων του VPN	ναι	ναι	ναι
Μεταξύ του απομακρυσμένου διακομιστή και της απομακρυσμένης πύλης	όχι	όχι	N/A (το τελικό σημείο VPN είναι ο διακομιστής)
Διαφάνεια			
Στους χρήστες	όχι	ναι	όχι
Στα συστήματα χρηστών	όχι	ναι	όχι
Στους διακομιστές	ναι	ναι	όχι

Η χρήση μιας διαδικτυακής υποδομής που εξυπηρετεί τη μεταφορά δεδομένων που αφορούν ένα δίκτυο μέσω άλλου δικτύου στο πλαίσιο του εικονικού δικτύου αναφέρεται ως VPN Tunneling. Τα μεταφερόμενα δεδομένα είναι δυνατόν να συνιστούν πακέτα κάποιου άλλου πρωτοκόλλου. Το πλαίσιο ενσωματώνεται σε πρόσθετη κεφαλίδα από το πρωτόκολλο σήραγγας, αντί να πραγματοποιήσει την αποστολή του όπως εκείνο έχει παραχθεί από τον κόμβο προελεύσεως. Ακολούθως, τα πακέτα που έχουν «εγκλωβιστεί» διακινούνται ανάμεσα στα τελικά σημεία της σήραγγας διά του εσωτερικού δικτύου. Η διαδρομή μέσω της οποίας πραγματοποιείται η διακίνηση αυτή αποκαλείται «σήραγγα» (tunnel), όπως και έχει προαναφερθεί. Έπειτα λαμβάνει χώρα η αποκωδικοποίηση των πακέτων μόλις αυτά φτάσουν στον προορισμό, ώστε να ληφθούν τα αρχικά δεδομένα. Κατά συνέπεια, η σήραγγα αναφέρεται στις διαδικασίες της «ενθυλάκωσης», της μετάδοσης και της αποκωδικοποίησης των μεταφερόμενων πακέτων, όπως απεικονίζεται στο Σχήμα 3.1. Η όλη διαδικασία του tunneling χρησιμοποιεί πολλά πρωτόκολλα, κάθε ένα από τα οποία λειτουργεί με διαφορετικό τρόπο και στοχεύει σε διαφορετικούς σκοπούς.



Σχήμα 3.1. Σήραγγα VPN (Winkler & Zeadally, 2015).

Η συλλογή πρωτοκόλλων επικοινωνίας στο Διαδίκτυο, ήτοι Πρωτοκόλλων Ελέγχου Μετάδοσης/Διαδικτύου (Transmission Control Protocol/Internet Protocol, TCP/IP) είναι γενικά οργανωμένη σε επίπεδα (layers) κάθε ένα από τα οποία

(Application Layer, Transport Layer, Network Layer, Data Link Layer) αντιμετωπίζει συγκεκριμένα ζητήματα που διέπουν τη μεταφορά δεδομένων και εξασφαλίζει την παροχή μιας καθορισμένης υπηρεσίας στα ανώτερα επίπεδα, με τέτοιον τρόπο ώστε σε κάθε στρώμα να προστίθενται περισσότερες πληροφορίες. Κατά συνέπεια, ένας έλεγχος ασφαλείας που διενεργείται σε ανώτερο επίπεδο δεν είναι δυνατόν να παρέχει πλήρη προστασία για τα κατώτερα επίπεδα. Στην περίπτωση του στοχεύετε η διαμόρφωση μίας σήραγγας VPN, ο διακομιστής και ο πελάτης της σήραγγας απαιτείται να χρησιμοποιούν κοινό πρωτόκολλο tunneling. Ειδικότερα, η λειτουργικότητα μίας σήραγγας VPN εδράζεται στα εξής πρωτόκολλα:

1. Πρωτόκολλο Layer 2 tunneling (L2TP), το οποίο αφορά το Data Link layer και αξιοποιεί «πλαίσια» (frames) ως μονάδες ανταλλαγής δεδομένων.

2. Πρωτόκολλο Layer 3 tunneling (L3TP), το οποίο αφορά το Network layer και αξιοποιεί πακέτα δεδομένων. Το πρωτόκολλο IPSec αντιστοιχεί στο συγκεκριμένο επίπεδο και αφορά την ενσωμάτωση των πακέτων σε πρόσθετη κεφαλίδα, προτού αυτά αποσταλούν σε ένα ορισμένο δίκτυο IP.

Τα προαναφερθέντα επίπεδα/στρώματα αντιστοιχούν στο Μοντέλο Αναφοράς Διασύνδεσης Ανοιχτών Συστημάτων (Open Systems Interconnection Reference Model, OSI). Για τα πρωτόκολλα που αφορούν τα τεχνολογικά συστήματα Layer 2 Tunneling L2TP και PPTP (point-to-point tunneling protocol, παλαιότερο πρωτόκολλο Layer 2) πρέπει να επισημανθούν τα εξής:

1. Απαιτείται η «συμφωνία» των τελικών σημείων της σήραγγας με την ίδια τη σήραγγα και η «διαπραγμάτευσή» τους αναφορικά με τις μεταβλητές διαμορφώσεως

2. Η σήραγγα εμφανίζει παρόμοια χαρακτηριστικά με εκείνα της συνεδρίας

3. Τα μεταφερόμενα σε όλο το εύρος της σήραγγας δεδομένα αποστέλλονται με τη χρήση πρωτοκόλλου που βασίζεται σε διαγράμματα και πρωτοκόλλου συντήρησης της σήραγγας που αξιοποιείται για τη διαχείριση της σήραγγας

4. Συνεπώς, απαιτείται η διαμόρφωση, η συντήρηση και ο τερματισμός μίας δεδομένης σήραγγας

Επιπλέον, για τις τεχνολογίες που υιοθετούν πρωτόκολλα Layer 3 Tunneling αναφέρονται τα εξής:

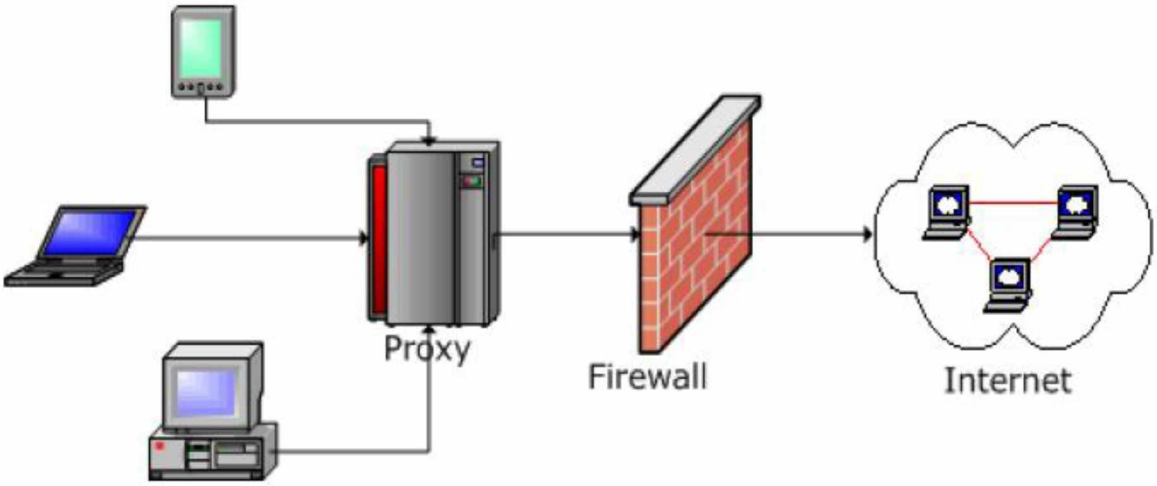
1. Δεν απαιτείται η συντήρηση της συγκεκριμένης σήραγγας

2. Λαμβάνεται ως δεδομένο ότι το σύνολο των προβλημάτων ρύθμισης των παραμέτρων έχουν επιλυθεί, συχνά δε διά χειροκίνητης διαδικασίας.

Μετά τη διαμόρφωση της σήραγγας, είναι εφικτή η αποστολή δεδομένων μέσω αυτής. Ο διακομιστής ή ο πελάτης μεταχειρίζεται ένα κατάλληλο πρωτόκολλο μεταφοράς των δεδομένων σήραγγας, ούτως ώστε να προετοιμάσει τα προς αποστολή δεδομένα. Παραδείγματος χάριν, στην περίπτωση που ο πελάτης προβαίνει στην αποστολή ωφέλιμου φορτίου στον διακομιστή (ή αντιστρόφως) πραγματοποιείται η προσθήκη της κεφαλίδας του εκάστοτε πρωτοκόλλου μεταφοράς δεδομένων στο ωφέλιμο φορτίο. Εν συνεχεία, ο πελάτης προβαίνει στην αποστολή του «εγκλωβισμένου» ωφέλιμου φορτίου στο εσωτερικό δίκτυο. Το τελευταίο μεταφέρει το ωφέλιμο φορτίο στον εξυπηρετητή (της σήραγγας), ο οποίος μετά την αποδοχή των πακέτων απομακρύνει την κεφαλίδα του πρωτοκόλλου και επιτελεί την προώθηση του ωφέλιμου φορτίου στο δίκτυο-στόχο.

3.2.3. Διακομιστές μεσολάβησης (proxy servers)

Με τον όρο «διακομιστής μεσολάβησης» ή proxy server νοείται ο ειδικός μετακομιστής ο οποίος αφορά το έβδομο επίπεδο του ISO/OSI και στοχεύει κατ' αρχήν στο να καταστεί εφικτή η πρόσβαση στο Διαδίκτυο κάποιου χρήστη εντός του τείχους προστασίς (Firewall). Ο εν λόγω διακομιστής αναμένει τη λήψη αιτήματος εντός του τείχους προστασίας, ούτως ώστε να το προωθήσει με κατεύθυνση έναν απομακρυσμένο διακομιστή που βρίσκεται εκτός του τείχους προστασίας (Σχήμα 3.2). Ακολούθως, διαβάζει την απάντηση που έχει λάβει και την αποστέλλει πίσω στον χρήστη.



Σχήμα 3.2. Λειτουργία διακομιστή μεσολάβησης (Sysel & Dolezal, 2014).

Επιμέρους στόχοι των διακομιστών μεσολάβησης είναι οι εξής:

1. Παρακολούθηση-φιλτράρισμα, με το να καθιστούν δυνατή την πραγματοποίηση ενός είδους φιλτραρίσματος, όπως παράκαμψης, κρυπτογραφημένων δεδομένων, περιεχομένου και την καταγραφή.

2. Βελτίωση της απόδοσης, καθώς εφόσον αναζητείται κάποιο περιεχόμενο που ευρίσκεται αποθηκευμένο στην προσωρινή μνήμη (“cache”), πραγματοποιείται άμεσα η προώθησή του στον χρήστη, χωρίς να διαμεσολαβήσει για την αίτηση αποστολής η εξωτερική επικοινωνία για την αίτηση αποστολής με έναν διακομιστή.

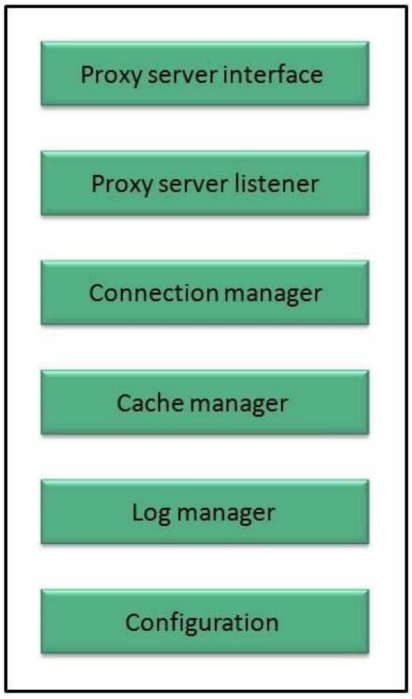
3. Μετάφραση, καθώς συντελεί στην προσαρμογή των ιστοτόπων προέλευσης, ώστε να είναι αντιληπτοί από τους κατά τόπους χρήστες, αφού εξαιρεθεί ο πηγαίος κώδικας ή αντικατασταθεί με το αρχικό (τοπικό) περιεχόμενο.

4. Ανώνυμη πρόσβαση σε ορισμένες υπηρεσίες, αφού από την πλευρά του διακομιστή η επερώτηση δεν λαμβάνεται από τον χρήστη αλλά από τον proxy server. Με άλλα λόγια, ο διακομιστής μεσολάβησης αποστέλλει την προσωπική του διεύθυνση IP και κατ’ αυτόν τον τρόπο δεν απεικονίζεται η διεύθυνση IP του αρχικού χρήστη.

5. Ασφάλεια, καθώς ο διακομιστής μεσολάβησης εξυπηρετεί την απόκρυψη της διεύθυνσης IP του χρήστη, προστατεύει τον τελευταίο από ανεπιθύμητο

περιεχόμενο (spam), από επιτιθέμενους χρήστες (π.χ. hackers), εφόσον η μόνη ανιχνεύσιμη διεύθυνση IP είναι εκείνη του proxy server.

Πιο συγκεκριμένα, η γενική αρχιτεκτονική ενός διακομιστή μεσολάβησης διακρίνεται στα τμήματα που αναφέρονται στο Σχήμα 3.3.



Σχήμα 3.3. Αρχιτεκτονική proxy server (Tutorialspoint, 2018).

Με βάση το Σχήμα 3.3, οι κύριοι τομείς της αρχιτεκτονιής ενός proxy server είναι οι ακόλουθοι:

1. Proxy Server Interface, όπου πραγματοποιείται η διαχείριση και ο έλεγχος της διεπαφής χρήστη, ο οποίος και έρχεται σε επαφή με ένα γραφικό περιβάλλον διεπαφής που είναι εύχρηστο, παράθυρο και menu με τις επιλογές της έναρξης του διακομιστή μεσολάβησης, τον τερματισμό του διακομιστή μεσολάβησης, την έξοδο, τον αποκλεισμό μιας διαδικτυακής τοποθεσίας ιστοτόπου η αρχείου (URL), τον αποκλεισμό χρηστών, τη διαχείριση προσωρινής μνήμης, την τροποποίηση των ρυθμίσεων και τη διαχείριση του αρχείου όπου καταγράφονται τα δεδομένα.

2. Proxy Server Listener, που αντιστοιχεί στη θύρα όπου λαμβάνονται νέα αιτήματα από την πλευρά του χρήστη στη βάση μιας διεργασίας συνεχούς παρακολούθησης. Πέραν τούτου, μπορεί να πραγματοποιηθεί αποκλεισμός χρηστών που περιλαμβάνονται στη λίστα που έχει δώσει ο εκάστοτε χρήστης.

3. Connection Manager: Στον τομέα αυτόν περιέχεται η βασική λειτουργία του διακομιστή μεσολάβησης. Πιο συγκεκριμένα, εκτελούνται οι εξής διαδικασίες:

α. Διαβάζονται τα αιτήματα της κεφαλίδας του χρήστη

β. Πραγματοποιείται η ανάλυση της URL και καθορίζεται αν η URL είναι αποκλεισμένη ή όχι

γ. Καθίσταται εφικτή η σύνδεση επικοινωνίας με άλλον διαδικτυακό (Web) διακομιστή

δ. Διαβάζεται η απάντηση που έχει ληφθεί από άλλον Web server με τον οποίον ο proxy server έχει επικοινωνήσει

ε. Εφόσον δεν είναι διαθέσιμο κάποιο αντίγραφο κάποιας σελίδας στην προσωρινή μνήμη, ο proxy server έχει τη δυνατότητα να λάβει τη συγκεκριμένη σελίδα από τον Web server. Ειδάλλως, διενεργείται έλεγχος από την κεφαλίδα της τελευταία τροποποιημένης ημερομηνίας και η ανάγνωση πραγματοποιείται από τον Web server ή την προσωρινή μνήμη

στ. Ελέγχεται αν επιτρέπεται η αποθήκευση δεδομένων προσωρινής μνήμης και αποθηκεύεται προσωρινά η εκάστοτε σελίδα.

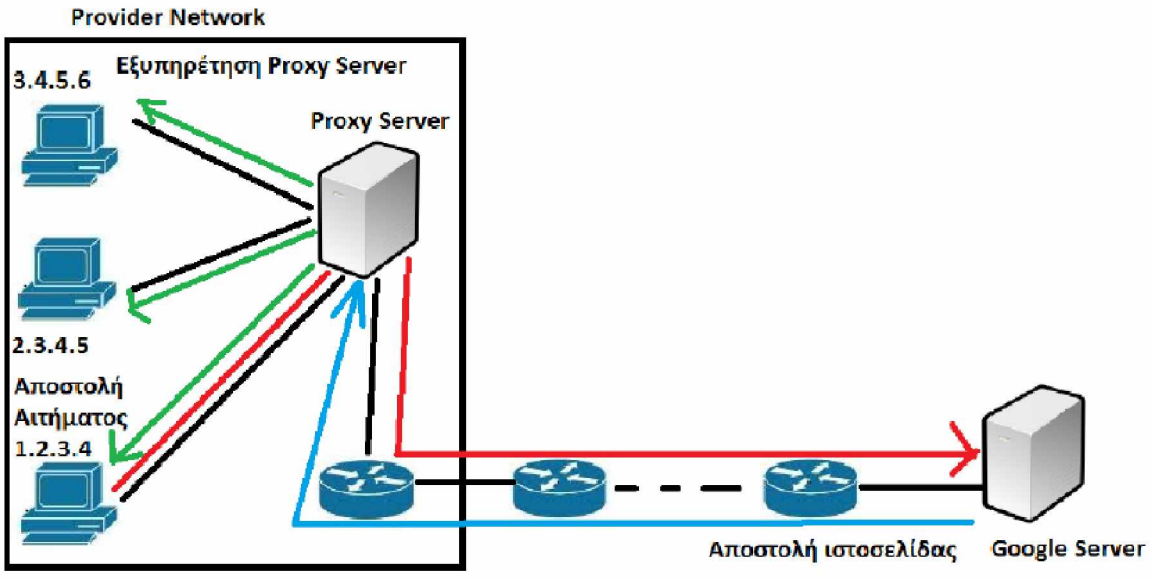
4. Cache Manager, που αφορά την αποθήκευση, την εκκαθάριση, την αναζήτηση και τη διαγραφή ιστοσελίδων που περιέχονται στην προσωρινή μνήμη.

5. Log Manager, που ευθύνεται για την ενημέρωση, την προβολή και την εκκαθάριση των αρχείων καταγραφής (τα Logs).

6. Configuration, που αφορά τις ρυθμίσεις διαμόρφωσης που καθιστούν εφικτή τη λειτουργία άλλων τομέων της αρχιτεκτονικής, με στόχο την πραγματοποίηση ενεργειών, όπως λ.χ. την προσωρινή αποθήκευση.

Ακολούθως, θα περιγραφεί αναλυτικότερα η λειτουργία ενός διακομιστή μεσολάβησης. Για τη σύνδεση ενός χρήστη σε έναν τέτοιον διακομιστή απαιτείται ο

αριθμός θύρας TCP και η διεύθυνση IP του. Ο διακομιστής μεσολάβησης ευρίσκεται στον τομέα του τοπικού δικτύου (Local Area Network, LAN) του παρόχου. Έτσι, ο πελάτης του παρόχου (ο χρήστης) μπορεί να αποκτήσει ταχεία πρόσβαση στον διακομιστή, ενώ δεν αντιλαμβάνεται ότι προστέθηκε ένας επιπλέον σταθμός στο μονοπάτι προώθησης του αιτήματος. Όταν ο χρήστης προβεί στην προώθηση του αιτήματός του προς τον proxy server, λ.χ. για την πρόσβαση σε μία ιστοσελίδα, στην περίπτωση που ενδιαφέρονται περισσότεροι χρήστες να αποκτήσουν πρόσβαση στη συγκεκριμένη ιστοσελίδα, ο διακομιστής μεσολάβησης διατηρεί αντίγραφα των ιστοσελίδων οι οποίες έχουν αποτελέσει το αντικείμενο της προώθησης των αιτημάτων από την πλευρά του. Κατά συνέπεια, είναι δυνατόν να προβεί στην απευθείας αποστολή της ιστοσελίδας στους χρήστες, χωρίς να απαιτηθεί να λάβει χώρα προώθηση του αιτήματος έως τον Web server διά μέσου επιπλέον κόμβων. Έτσι, με τη χρήση του ιδιαίτερα συντομότερου μονοπατιού, οι χρήστες λαμβάνουν πολύ ταχύτερα την ιστοσελίδα την οποίαν πληκτρολόγησαν. Από την άλλη, ο πάροχος κατορθώνει να εξοικονομήσει αρκετά χρήματα και να περιορίσει την κίνηση (Σχήμα 3.4).



Σχήμα 3.4. Λειτουργία του proxy server, στην περίπτωση που ζητείται η πρόσβαση στην ιστοσελίδα www.google.com (Ikits & Hansen, 2006).

Όπως έγινε αντιληπτό, βασικό πλεονέκτημα των διακομιστών μεσολάβησης που ενδιαφέρει τη διασφάλιση του απορρήτου στο Διαδίκτυο είναι η δυνατότητα παροχής ενός βαθμού ανωνυμίας στον εκάστοτε χρήστη, αφού χρησιμοποιούν την διεύθυνση IP τους για την πραγματοποίηση διαφόρων αιτήσεων. Όταν ο χρήστης προωθήσει ένα πακέτο δεδομένων στον διαδικτυακό χώρο χρησιμοποιώντας έναν proxy server αποστέλλει στον τελευταίο και τη διεύθυνση IP του. Ωστόσο, μετά την έξοδο του πακέτου από το δίκτυο του παρόχου, χρησιμοποιείται για την προώθησή του η διεύθυνση του διακομιστή μεσολάβησης. Όταν ληφθεί η απάντηση (π.χ. η ιστοσελίδα) από τον proxy server, αποστέλλει στον χρήστη την αιτούμενη ιστοσελίδα, καθώς έχει καταγράψει τη διεύθυνση IP του. Στην περίπτωση που περισσότεροι χρήστες αιτηθούν την ίδια ιστοσελίδα και εκείνη έχει αποθηκευτεί στον διακομιστή μεσολάβησης, δεν πραγματοποιείται η μετάδοση κάποιας IP διεύθυνσης σε τελικό διακομιστή ή σε κόμβους εκτός δικτύου και κατ' αυτόν τον τρόπο ο τελικός διακομιστής δεν θα ενημερωθεί ότι ο μεγάλος αριθμός των χρηστών εισήλθαν στην εξυπηρετούμενη από αυτόν ιστοσελίδα, καθώς οι χρήστες χρησιμοποίησαν τον proxy server για την πρόσβαση. Έτσι, αυτομάτως εκείνοι επιτυγχάνουν έναν βαθμό ανωνυμίας, καθώς η διεύθυνση IP τους μέσω των πακέτων IP δεν αποστέλλεται στον τελικό διακομιστή.

Πρέπει ωστόσο να σημειωθεί ότι η ανωνυμία του χρήστη περιορίζεται στο πεδίο της κίνησης που αφορά το Πρωτόκολλο Μεταφοράς Υπερκειμένου (HyperText Transfer Protocol, HTTP), ήτοι στην επικοινωνία κατά την οποία χρησιμοποιείται η θύρα 80. Στην περίπτωση που ο χρήστης εισέλθει σε ιστότοπο που περιέχει πολυμέσα, το πρόσθετο Flash του φυλλομετρητή δεν αποκτά πρόσβαση με τη βοήθεια του διακομιστή μεσολάβησης, αλλά, μέ την αποστολή αιτήματος στον διακομιστή του ιστοτόπου, μέσω του χρήστη και με αξιοποίηση επιπλέον ενδιάμεσων κόμβων. Το γεγονός αυτό συνεπάγεται ότι δεν χρησιμοποιείται ο proxy server και, επομένως, αποστέλλεται η διεύθυνση IP που αντιστοιχεί στον χρήστη. Κατά συνέπεια, ο βαθμός της ανωνυμίας χρήσει απλού διακομιστή μεσολάβησης, η αξιοποίησή του οποίου δεν περιλαμβάνει ορισμένες ειδικές ρυθμίσεις, δεν είναι μεγάλος.

Εν γένει, μπορούν να διακριθούν τρία κύρια είδη διακομιστών μεσολάβησης, τα οποία είναι τα εξής:

1. Reverse Proxies, δηλαδή διακομιστές μεσολάβησης που εμφανίζονται ως τελικοί διακομιστές στους χρήστες. Η εξυπηρέτηση κάθε αίτησης μεταφέρεται σε έναν ή περισσότερους τελικούς διακομιστές. Οι χρήστες λαμβάνουν απάντηση με τέτοιον τρόπο, ώστε θεωρούν ότι την έλαβαν από τον ίδιο τον διακομιστή μεσολάβησης. Με άλλα λόγια, το συγκεκριμένο είδος διακομιστή χρησιμοποιείται για την απόκρυψη της διεύθυνσης IP τελικών διακομιστών σε ένα δίκτυο διακομιστών.

2. Forward Proxies, οι οποίοι ονομάζουν τον τελικό διακομιστή με τον οποίον θα συνδεθούν. Η εύρεσή τους μπορεί να πραγματοποιηθεί από έναν μεγάλο αριθμό ιστοσελίδων μέσω δικτύου.

3. Open Proxies, που πρόκειται για forward proxies προσβάσιμους από το σύνολο των χρηστών. Το Διαδίκτυο περιλαμβάνει εκατοντάδες χιλιάδες διακομιστές αυτής της κατηγορίας. Ένας τέτοιος διακομιστής που ονομάζεται “Anonymous Open Proxy” καθιστά δυνατή την απόκρυψη της διεύθυνσης IP οποιουδήποτε χρήστη κατά την διαδικτυακή πλοήγηση.

Είναι ευνόητο ότι η ανωνυμία του τελικού χρήστη εξασφαλίζεται από τους Forward Proxies, ενώ, αντιθέτως, οι Reverse Proxies εξυπηρετούν την επίτευξη ανωνυμίας από τους τελικούς διακομιστές. Ειδικότερα, μπορούν να διακριθούν τα ακόλουθα είδη Open Proxies:

1. Anonymous Proxy, ο οποίος συνεργάζεται με άλλους διακομιστές μεσολάβησης και δεν καθιστά προσβάσιμη για το σύνολο των χρηστών την διεύθυνση IP του. Ο εν λόγω διακομιστής είναι σε έναν βαθμό ανιχνεύσιμος, αλλά εξασφαλίζει έναν σημαντικό βαθμό ασφαλείας στην πλειοψηφία των χρηστών.

2. Transparent Proxy, ο οποίος καθιστά εφικτή με την κεφαλίδα HTTP την πρόσβαση στην IP και χρησιμοποιείται συχνά, κυρίως στη βάση της ικανότητας προσωρινής αποθήκευσης ιστοσελίδων που διαθέτει, εξασφαλίζοντας κατ’ αυτόν τον τρόπο την ανωνυμία στους χρήστες. Η διεύθυνση IP του Transparent Proxy είναι ορατή στο σύνολο των χρηστών. Πολλές φορές οι χρήστες του δεν γνωρίζουν ότι χρησιμοποιούν το συγκεκριμένο είδος διακομιστή.

3. Distorting Proxy, που επιτρέπει να ληφθεί μέσω της κεφαλίδας HTTP μία εσφαλμένη διεύθυνση IP.

4. High Anonymity/Elite Proxy, του οποίου η διεύθυνση IP δεν είναι προσβάσιμη από κανέναν χρήστη.

Καθώς το είδος των Transparent Proxies αξιοποιείται στις απλούστερες περιπτώσεις, για παράδειγμα αν ένας χρήστης επιθυμεί να παρακάμψει τον αποκλεισμό μίας διεύθυνσης IP, δεν απαιτείται ιδιαίτερος σχολιασμός στον τρόπο λειτουργίας τους, γι' αυτό η βιβλιογραφική αναφορά θα περιοριστεί στα άλλα τρία είδη Open Proxies.

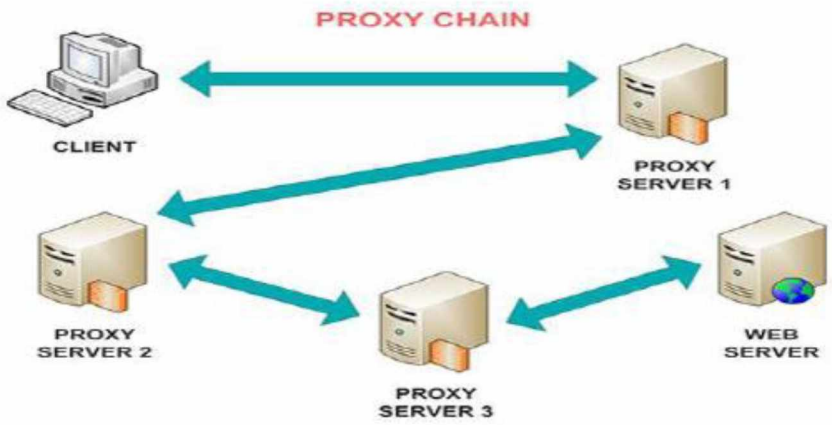
Οι διακομιστές Anonymous Proxies μεταχειρίζονται ειδικά λογισμικά που καθιστούν δυνατή την απόκρυψη της διεύθυνσης IP ενός χρήστη. Το κύριο πρόβλημα που διέπει τη χρήση τους είναι η επεξεργασία μεγάλου όγκου δεδομένων και η δραστική μείωση της ταχύτητας πρόσβασης των χρηστών σε ιστοσελίδες. Επίσης, καθώς παράλληλα επιχειρείται η διαγραφή ή η παράκαμψη αρκετών «ύποπτων» δεδομένων, συχνά ο χρήστης δεν κατορθώνει να αποκτήσει πρόσβαση στον επιθυμητό ιστότοπο και, ως εκ τούτου, λαμβάνει ένα μήνυμα σφάλματος. Επιπλέον, υφίσταται ο κίνδυνος συλλογής δεδομένων ανύποπτων χρηστών. Ουσιαστικά, οι Anonymous Proxies στη μεταβλητή της κεφαλίδας HTTP "HTTP_X_FORWARDED_FOR" δεν μεταφέρουν την πραγματική IP του χρήστη, αλλά εκείνη του ίδιου του διακομιστή μεσολάβησης. Εναλλακτικά, αποστέλλεται κενή κεφαλίδα. Ο διακομιστής μεσολάβησης αποστέλλει τα επιπρόσθετα πεδία, κανένα εκ των οποίων δεν περιλαμβάνει την πραγματική IP του χρήστη (Li et al., 2013).

Οι Distorting Proxies (Gateway Proxies) μεταβάλλουν την κεφαλίδα HTTP ενός χρήστη με στόχο την απόκρυψη της διεύθυνσης IP του. Πιο συγκεκριμένα, οι εν λόγω διακομιστές αποκρύπτουν την αρχική IP ενός χρήστη με το να καθιστούν διαθέσιμη μία εσφαλμένη IP διά της κεφαλίδας HTTP. Με άλλα λόγια, η μόνη διαφορά ανάμεσα στους υπόλοιπους proxy servers και στους Distorting Proxies αντιστοιχεί στον τρόπο με βάση τον οποίον τροποποιούνται οι κεφαλίδες HTTP των διευθύνσεων IP των χρηστών. Παράλληλα έχουν τη δυνατότητα να «παρουσιάσει» τους χρήστες ως διακομιστές (servers). Παρ' όλ' αυτά, υπάρχει ο κίνδυνος εντοπισμού αυτών, με αποτέλεσμα να γίνει γνωστό ότι χρησιμοποιούν έναν διακομιστή μεσολάβησης. Έχει αναφερθεί ότι επιτιθέμενοι χρήστες έχουν τη δυνατότητα να αποκτήσουν πρόσβαση σε εταιρείες παροχής των σχετικών

υπηρεσιών, στις οποίες οι χρήστες βασίζονται τις περισσότερες φορές ούτως ώστε να διασφαλίσουν την ανωνυμία τους. Κατά συνέπεια, η χρήση ενός Distorting Proxy δεν συνοδεύεται από 100% βαθμό ασφάλειας, αφού υφίσταται ο κίνδυνος εντοπισμού ενός χρήστη από διαχειριστές ιστοχώρων και επιτιθέμενους χρήστες. Η χρήση ενός Distorting Proxy αφορά το σύνολο των διαδικτυακών υπηρεσιών, ούτως ώστε να επιταχυνθεί η ροή των δεδομένων και να διασφαλισθεί το απόρρητο των χρηστών. Πρέπει, ωστόσο, να σημειωθεί ότι παρέχει στους χρήστες τη δυνατότητα παράκαμψης ιστοχώρων μπλοκαρισμένων στην χώρα τους ή στα τοπικά δίκτυα ενός γραφείου και άλλων εγκαταστάσεων. Επιπλέον, η χρήση του επιτρέπει την προστασία του υπολογιστή ενός χρήστη από κακόβουλο λογισμικό (malware) κατά την διαδικτυακή τους πλοήγηση (Edman & Yener, 2009).

Τέλος, οι High Anonymity Proxies (Elite/L1 Proxies) αποτελούν διακομιστές μεσολάβησης που δεν μεταφέρουν πληροφορίες όχι μόνο αναφορικά με την πραγματική διεύθυνση IP του, αλλά και με το ότι ο εκάστοτε χρήστης αξιοποιεί τις υπηρεσίες ενός proxy server. Πιο συγκεκριμένα, πραγματοποιεί την αποστολή μόνον της μεταβλητής “REMOTE_ADDR” της κεφαλίδας HTTP, ενώ τα υπόλοιπα τμήματα της κεφαλίδας παραμένουν κενά. Το γεγονός αυτό συνεπάγεται ιδιαίτερα αυξημένη ζήτηση των υπηρεσιών των High Anonymity Proxies, καθώς εξασφαλίζουν μεγάλο βαθμό ανωνυμίας κατά την διαδικτυακή πλοήγηση (Li et al., 2013).

Πέραν της χρήστης μόνον ενός διακομιστή μεσολάβησης, είναι δυνατή η χρήση μίας σειράς διακομιστών στο πλαίσιο μίας αλυσίδας (proxy chain). Η αλυσίδα διακομιστών μεσολάβησης συνιστά μία αλληλουχία proxies συνδεδεμένων μεταξύ τους με την οποία και συνδέεται ο εκάστοτε χρήστης που επιθυμεί να εισέλθει σε κάποιον ιστότοπο (Σχήμα 3.5).



Σχήμα 3.5. Αλυσίδα διακομιστών μεσολάβησης (proxy chain) (Edman & Yener, 2009).

Μέχρι να αποκτήσει πρόσβαση στον τελικό προορισμό ο χρήστης συνδέεται με διαδοχικό τρόπο στους διάφορες διακομιστές μεσολάβησης. Απαιτείται η διασφάλιση της λειτουργικότητας του συνόλου της αλυσίδας κατά τη χρήση αυτής, δηλαδή η επιτυχής υλοποίηση των διαδοχικών συνδέσεων. Εφόσον δεν λειτουργεί κάποια IP του proxy server, η σύνδεση είναι αδύνατη. Αυτό σημαίνει ότι ο ανενεργός διακομιστής πρέπει να αντικατασταθεί με νέο ή να αποκλειστεί ο ανενεργός διακομιστής και να συνδεθούν οι υπόλοιποι με στόχο τον σχηματισμό μιας νέας αλυσίδας. Ορισμένες φορές η ανίχνευση ενός ή περισσότερων ανενεργών διακομιστών είναι ιδιαίτερα δύσκολη, αναλόγως και με τον αριθμό των proxies που ανήκουν στην εκάστοτε αλυσίδα.

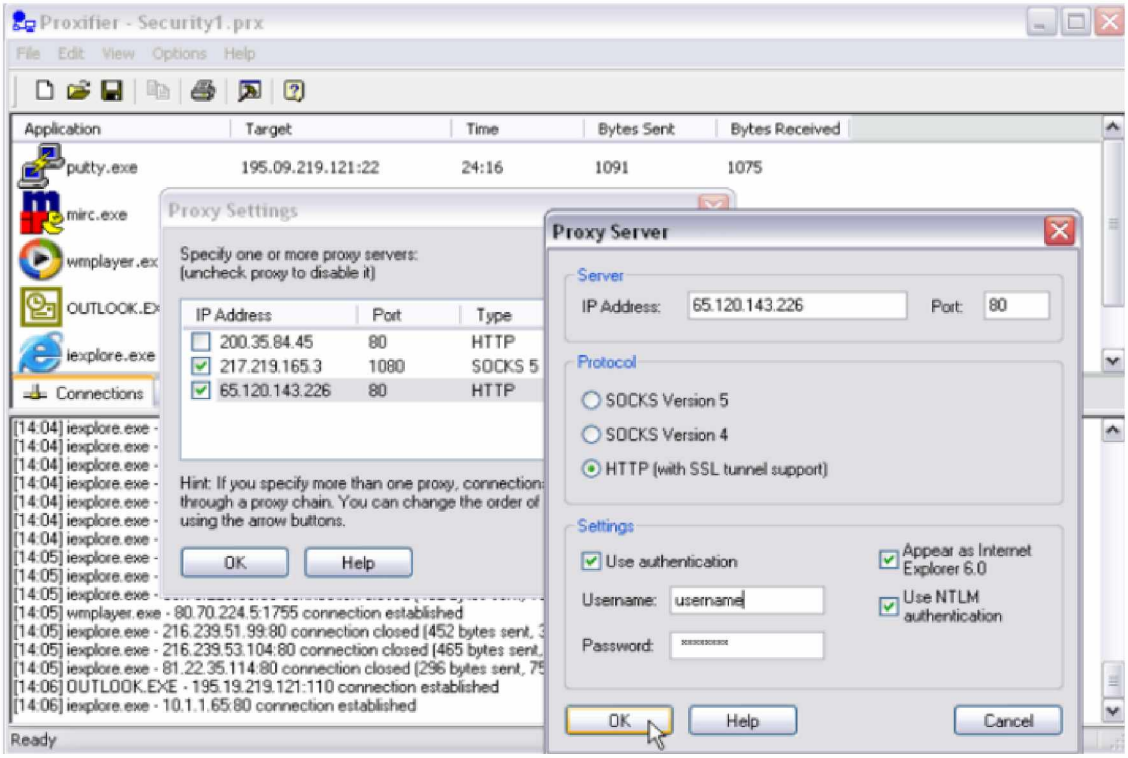
Μια proxy chain αξιοποιείται συχνά για την πραγματοποίηση διαδικτυακών επιθέσεων, ενώ η χρήση της είναι απαραίτητη αν ένας χρήστης επιθυμεί να αποκτήσει πρόσβαση μη εξουσιοδοτημένη σε έναν δεδομένο διακομιστή. Διά της συγκεκριμένης τεχνικής ο χρήστης μπορεί να απολαμβάνει ανωνυμία υψηλού επιπέδου. Αυτό δεν σημαίνει ότι η ανωνυμία είναι απόλυτη. Για τον προσδιορισμό της ταυτότητας ενός χρήστη μιας αλυσίδας διακομιστών μεσολάβησης προϋποτίθεται η συλλογή των logs του συνόλου των proxy servers του διαχειριστή οι οποίοι χρησιμοποιούνται, διαδικασία ιδιαίτερα επίπονη και χρονοβόρα. Μάλιστα, με την πάροδο του χρόνου η ανίχνευση καθίσταται ολοένα και πιο δύσκολη, καθώς

οι διαχειριστές προβαίνουν σε διαγραφή των logs μετά από σχετικά σύντομο χρονικό διάστημα. Έκτοτε η ανίχνευση της διεύθυνσης IP του δεδομένου χρήστη είναι αδύνατη. Η χρήση της αλυσίδας proxies από κράτη τα οποία δεν συνεργάζονται με τη Δύση αναφορικά με ζητήματα παραχωρήσεως πληροφοριών (π.χ. Ρωσία, Κίνα) είναι συνήθης και περιλαμβάνει την αξιοποίηση τουλάχιστον 5 διαδοχικών διακομιστών μεσολάβησης.

Το κύριο πρόβλημα που διέπει την αξιοποίηση μίας αλυσίδας proxy servers αφορά την παρεχόμενη ταχύτητα, καθώς στις περισσότερες περιπτώσεις υπάρχει μεγάλη καθυστέρηση, το μέγεθος της οποίας εξαρτάται από τις επιμέρους ρυθμίσεις των διακομιστών μεσολάβησης. Η (συνολική) καθυστέρηση μπορεί να ειδωθεί ως το άθροισμα των επιμέρους καθυστερήσεων ανάμεσα στις διαφορετικές συνδέσεις των διακομιστών. Είναι, λοιπόν, ευνόητο ότι η συνολική καθυστέρηση αυξάνεται με την αύξηση του αριθμού των proxy servers της αλυσίδας, αλλά μια τέτοια αύξηση έχει ως συνέπεια μεγαλύτερο βαθμό ανωνυμίας του χρήστη, οπωσδήποτε πολύ μεγαλύτερο σε σχέση με την ανωνυμία που παρέχεται από έναν απλό διακομιστή μεσολάβησης.

Η αλυσίδα proxy chain μπορεί να χρησιμοποιηθεί από κατάλληλο λογισμικό, όπως το Proxifier. Πρόκειται για απλό λογισμικό που παρέχεται δωρεάν και εγκαθίσταται εύκολα στον υπολογιστή ενός χρήστη. Όπως παρατηρείται στο Σχήμα 3.6, ο χρήστης προβαίνει απλά στην εισαγωγή της διεύθυνσης IP του διακομιστή μεσολάβησης, του αριθμού της θύρας και του είδους της υποδοχής (socket). Στο πεδίο συνδέσεων εμφανίζεται το σύνολο των συνδέσεων που δημιουργεί το εν λόγω σύστημα. Με τη χρήση του Proxifier τα ανταλλασσόμενα δεδομένα, ο συνολικός χρόνος και άλλοι παράμετροι της διαδικασίας είναι δυνατόν να κατηγοριοποιηθούν με εύκολο τρόπο. Οι πραγματοποιημένες συνδέσεις είναι εφικτό να κρυπτογραφηθούν κατά τις απαιτήσεις του εκάστοτε χρήστη. Ο τελευταίος μπορεί να προχωρήσει στη δημιουργία ενός αριθμού αλυσίδων αναλόγως των απαιτήσεών του. Σε μία λίστα που μπορεί να τροποποιηθεί από τον χρήστη καθορίζεται η σειρά της αλυσίδας, ενώ παρέχεται η δυνατότητα της ενεργοποίησης και της απενεργοποίησης διαφόρων διακομιστών μεσολάβησης. Πριν τεθεί σε λειτουργία η proxy chain θα πρέπει να ελεγχθεί ο κάθε διακομιστής, δυνατότητα που παρέχεται από το Proxifier, καθώς αρκετοί διαχειριστές απενεργοποιούν για

διάφορους λόγους διαθέσιμους διακομιστές. Με βάση τα παραπάνω, παρέχεται άμεσος έλεγχος στον χρήστη για τη λειτουργία μίας proxy chain και με βάση τις παρεχόμενες πληροφορίες του επιτρέπεται η επιλογή των διακομιστών που εμφανίζουν τη μικρότερη καθυστέρηση, εξασφαλίζοντας παράλληλα υψηλά επίπεδα ανωνυμίας.



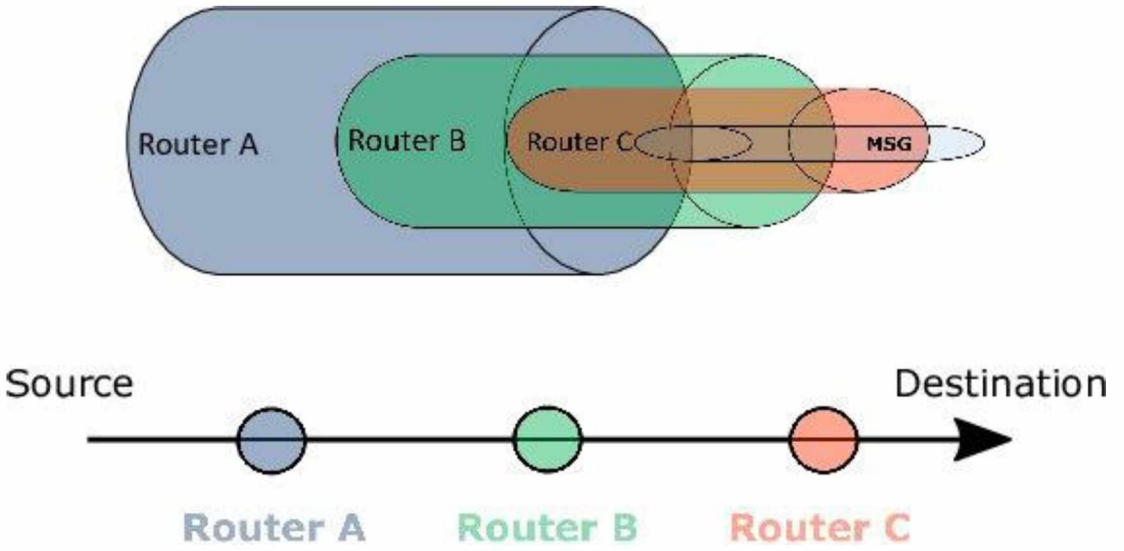
Σχήμα 3.6. Φόρμα εισαγωγής IP proxy server, θύρας και υποδοχής στο λογισμικό Proxifier (QP Download, 2018).

3.2.4. Δρομολόγηση Onion

3.2.4.1. Γενικές παρατηρήσεις

Το δίκτυο Onion αποτελεί ένα δίκτυο επικαλύψεως που είναι σχεδιασμένο για εφαρμογής εξασφάλισης διαδικτυακής ανωνυμίας και εδράζονται στο TCP, όπως το ασφαλές «κέλυφος», η άμεση αποστολή μηνυμάτων και η περιήγηση στο Διαδίκτυο. Οι πελάτες μπορούν να επιλέξουν μία διαδρομή μέσω του συγκεκριμένου δικτύου και να δημιουργήσουν ένα κύκλωμα στη διαδρομή του οποίου κάθε κόμβος (εναλλακτικά, «δρομολογητής Onion/κρεμμυδιού») δεν

γνωρίζει κανέναν άλλον κόμβο του κυκλώματος πλην του προηγούμενου και του διαδοχικού του. Η ροή της πληροφορίας «κατέρχεται» σε κυψέλες που έχουν σταθερό μέγεθος και οι οποίες μπορούν να ξεκλειδωθούν σε κάθε κόμβο από συμμετρικό κλειδί και να αναμεταδοθούν, σε μια διαδικασία που προσιδιάζει τα επικαλυπτόμενα στρώματα ενός κρεμμυδιού (Σχήμα 3.7).



Σχήμα 3.7. Αρχή λειτουργίας της δρομολόγησης Onion (Shirazi et al., 2016).

Αναλυτικότερα, κατά τη δρομολόγηση Onion, αντί να πραγματοποιείται η απευθείας σύνδεση των εφαρμογών εκκίνησης σε μία αποκρινόμενη μηχανή, οι συνδέσεις πραγματώνονται μέσω μίας ορισμένης σειράς μηχανών που αποκαλούνται «δρομολογητές Onion/ORs». Το συγκεκριμένο δίκτυο δρομολόγησης καθιστά εφικτή την ανωνυμία της σύνδεσης μεταξύ ανταποκριτή και εκκινητή, με άλλα λόγια την απόκρυψη της πληροφορίας «ποιος είναι συνδεδεμένος με ποιον», όπως επίσης και την απόκρυψη του σκοπού της σύνδεσης, τόσο από τους εξωτερικούς υπολογιστές όσο και από τους «συμβιβασμένους» δρομολογητές Onion. Στην περίπτωση που ο εκκινητής επιθυμεί επιπλέον να παραμείνει ανώνυμος ακόμη και στον αποστολέα, πρέπει να αφαιρεθεί το σύνολο των πληροφοριών ταυτοποίησης από τη ροή των δεδομένων πριν την εκκίνηση της ανώνυμης σύνδεσης.

Οι ORs συνδέονται στο δίκτυο με μόνιμες (μακροχρόνιες) συνδέσεις υποδοχών, στις οποίες εμπλέκονται οι ανώνυμες συνδέσεις. Η ακολουθία των ORs για την εκάστοτε ανώνυμη σύνδεση είναι καθορισμένη αυστηρά κατά τη διαδικασία της ρύθμισης της σύνδεσης. Εν τούτοις, κάθε OR έχει τη δυνατότητα αναγνώρισης μόνον του προηγούμενου και του επόμενου κόμβου κατά μήκος μιας δεδομένης διαδρομής. Σε κάθε OR τα διαβιβαζόμενα δεδομένα εμφανίζονται διαφορετικά και, κατά συνέπεια, δεν μπορούν να εντοπιστούν κατά μήκος της διαδρομής, ενώ οι «συμβιβασμένοι» ORs δεν είναι σε θέση να «συνεργαστούν» αναφορικά με τη συσχέτιση της ροής που αναγνωρίζει ο κάθε ένας από αυτούς. Επιπροσθέτως, οι εν λόγω δρομολογητές δεν μπορούν να χρησιμοποιήσουν επαναλαμβανόμενους ORs ή αναπαραγόμενα δεδομένα (Li et al., 2013).

Η πρόσβαση στο δίκτυο δρομολόγησης Onion πραγματοποιείται με τη βοήθεια μιας σειράς από διακομιστές μεσολάβησης. Μία εφαρμογή εκκίνησης προβαίνει σε σύνδεση υποδοχής με proxy server εφαρμογής. Ο συγκεκριμένος τύπος μηνύματος σύνδεσης, σε γενική μορφή, είναι σε θέση να διαδοθεί μέσω του εν λόγω δικτύου δρομολόγησης. Στη συνέχεια πραγματοποιείται σύνδεση με διακομιστή μεσολάβησης Onion (Onion proxy), ώστε διαμορφώνεται μία διαδρομή μέσω του δικτύου δρομολόγησης onion και κατασκευάζεται μία δομή δεδομένων ονόματι “Onion”. Η δομή αυτή διαβιβάζεται στη γέφυρα εισόδου που καταλαμβάνει μία εκ των μακροχρόνιων συνδέσεων σε έναν OR και εμπλέκει τις συνδέσεις του δικτύου Onion στον συγκεκριμένο δρομολογητή. Ο τελευταίος αντιστοιχεί σε εκείνον για τον οποίον το εξωτερικό περίβλημα του Onion προορίζεται. Κάθε περίβλημα/στρώμα σε μία διαδρομή ορίζει το επόμενο «άλμα» (hop). Ένας OR που λαμβάνει κάποιο Onion αναγνωρίζει το άλμα και αποστέλλει το ενσωματωμένο Onion στον επόμενο OR. Ο τελευταίος OR επιτελεί την προώθηση δεδομένων εκτελώντας μία «διοχέτευση εξόδου» που αποσκοπεί στη μεταφορά δεδομένων ανάμεσα στο δίκτυο δρομολόγησης Onion και τον αποστολέα. Πέραν της μεταφοράς των πληροφοριών με κάθε «επόμενο άλμα», κάθε στρώμα Onion περιλαμβάνει κύριες πληροφορίες εκ των οποίων παράγονται τα κλειδιά κρυπτογράφησης που αποστέλλονται είτε προς τα εμπρός είτε προς τα πίσω και κατά μήκος της διαδρομής της ανώνυμης σύνδεσης. Με τη δημιουργία της ανώνυμης σύνδεσης είναι δυνατή η μεταφορά δεδομένων και πριν από την

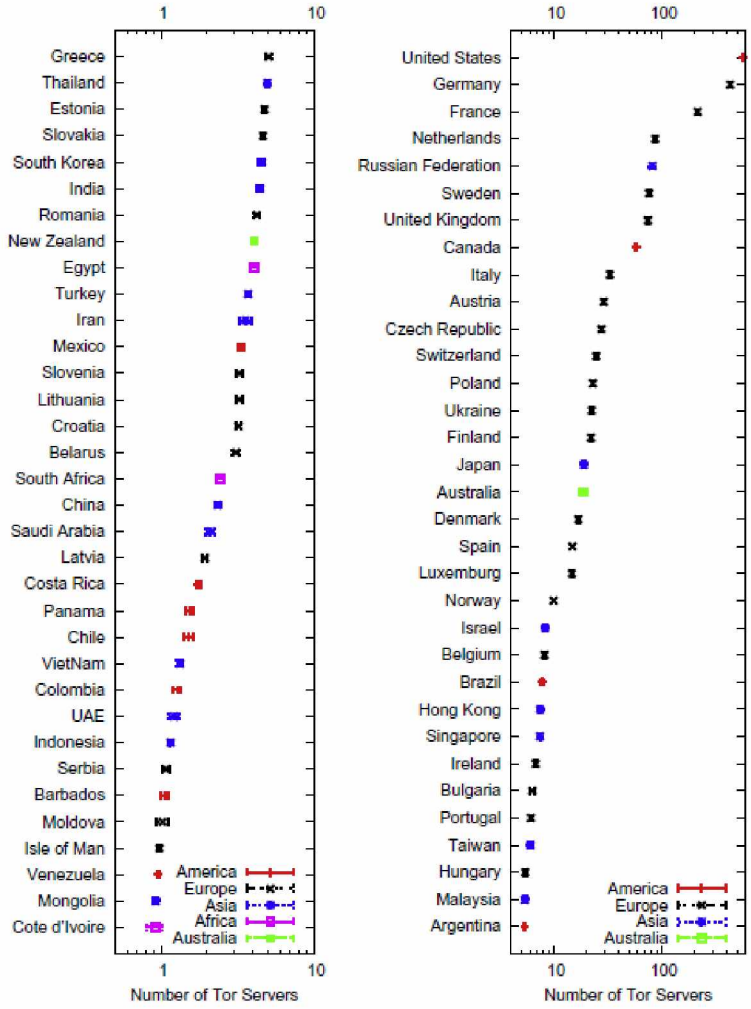
αποστολή τους ο OR προσθέτει για κάθε OR μιας διαδρομής ένα επιπλέον επίπεδο κρυπτογράφησης. Καθώς τα δεδομένα διαβιβάζονται διά της ανώνυμης σύνδεσης κάθε OR πραγματοποιεί την αφαίρεση ενός επιπέδου κρυπτογράφησης και καταλήγει ως απλό κείμενο στον ανταποκριτή. Το συγκεκριμένο είδος στρωματοποίησης λαμβάνει χώρα με αντίστροφη σειρά, ώστε τα δεδομένα να διαβιβαστούν πίσω στον εκκινητή. Συνεπώς, τα δεδομένα που έχουν διαβιβαστεί προς τα «πίσω» πρέπει μετά την κρυπτογράφηση να επαναλαμβάνονται για να ανακτηθεί το απλό κείμενο (Shirazi et al., 2016).

Είναι γεγονός ότι η στρωματοποίηση των κρυπτογραφικών δραστηριοτήτων πλεονεκτεί έναντι της κρυπτογράφησης της σύνδεσης, αφού τα διακινούμενα μέσω του δικτύου Onion παρουσιάζονται διαφορετικά σε κάθε OR. Κατ' αυτόν τον τρόπο, η αξιοπιστία μίας ανώνυμης σύνδεσης είναι αντίστοιχη της αξιοπιστίας του ισχυρότερου συνδέσμου (Li et al., 2013).

3.2.4.2. Φυλλομετρητής Tor

Η χρήση της δρομολόγησης Onion ταυτίζεται για πολλούς με την αξιοποίηση του φυλλομετρητή Tor (Tor browser). Συχνά μάλιστα το δίκτυο Onion αποκαλείται και «δίκτυο Tor» (Tor Network). Στον τομέα της ανωνυμίας στο Διαδίκτυο λίγες μόνον τεχνολογικές εφαρμογές συνεχίζουν να έχουν μεγαλύτερο αντίκτυπο από τον φυλλομετρητή Tor, που αντιστοιχεί σε έναν περιηγητή Διαδικτύου τροποποιημένο με βάση τον κοινό φυλλομετρητή Mozilla Firefox. Ο συγκεκριιμένος δωρεάν παρεχόμενος φυλλομετρητής συνδυάζει την ευχρηστία με τον μεγάλο βαθμό ανωνυμίας, ο οποίος μπορεί να αποκτηθεί χωρίς ιδιαίτερες τεχνικές οδηγίες και προαπαιτούμενες γνώσεις. Ο Tor browser αναπτύχθηκε ούτως ώστε να επιτραπεί η ανώνυμη και απρόσκοπτη διαδικτυακή επικοινωνία, καθιστώντας εφικτή τη σύνδεση με ιστοτόπους η πρόσβαση στους οποίους απαγορεύεται από αυταρχικά καθεστώτα, ενώ παρέχεται η δυνατότητα επικοινωνίας μεταξύ ιδιωτών και επιχειρήσεων που επιθυμούν έναν μεγάλο βαθμό ανωνυμίας και ιδιωτικότητας των πληροφοριών που ανταλλάσσουν (Muller et al., 2012). Στο Σχήμα 3.8 απεικονίζεται σε λογαριθμική κλίμακα η γεωγραφική κατανομή των διακομιστών σε διεθνές επίπεδο οι οποίοι χρησιμοποιούν τον φυλλομετρητή Tor. Παρά το ότι το συγκεκριμένο τεχνολογικό εργαλείο αναπτύχθηκε σε πρώτη φάση από την

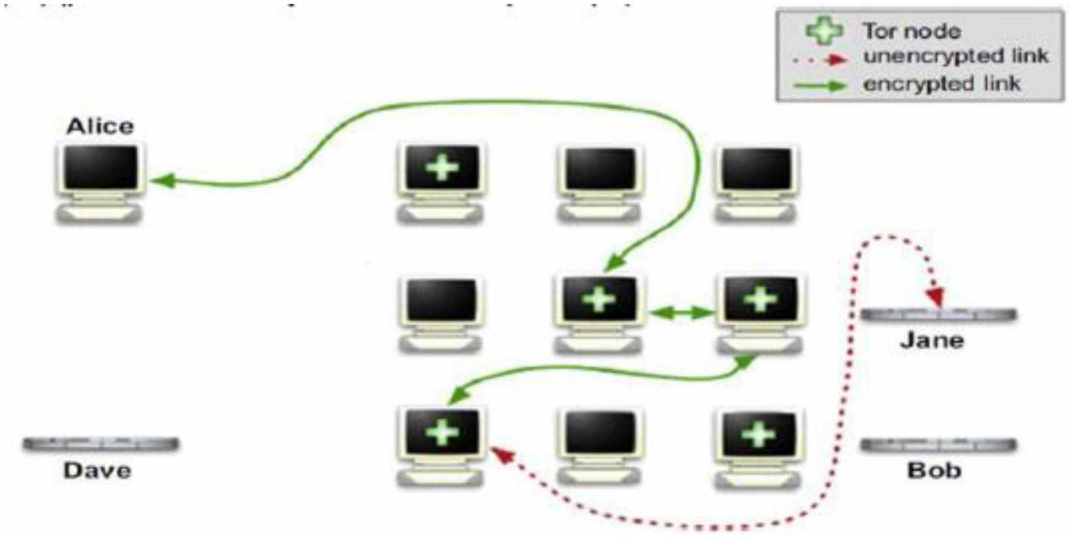
κυβέρνηση των ΗΠΑ το 2002 επί του παρόντος δεν ελέγχεται από αυτή. Η αλήθεια είναι ότι ο Tor browser δεν ελέγχεται από κάποια συγκεκριμένη οντότητα, αλλά σχεδόν το σύνολο όσων διαθέτουν την ανάλογη τεχνική ικανότητα μπορούν να προβούν σε βελτιώσεις του.



Σχήμα 3.8. Γεωγραφική κατανομή των διακομιστών που χρησιμοποιούν τον φυλλομετρητή Tor (Li et al., 2013).

Η ουσιαστική διαφορά του Tor browser έναντι των παραδοσιακών φυλλομετρητών αφορά την απόκρυψη της διεύθυνσης IP του χρήστη όταν αυτός αποστέλλει μηνύματα ηλεκτρονικού ταχυδρομίου ή όταν επισκέπτεται ιστότοπους. Η αρχή λειτουργίας του συνοψίζεται στο ότι κατευθύνει τη διαδικτυακή ροή των δεδομένων ενός χρήστη στη βάση τυχαίων αναμεταδόσεων. Αρχικά, τα δεδομένα

στοιβάζονται με τη βοήθεια κρυπτογράφησης ελλειπτικής καμπύλης, η οποία δεν μπορεί επί του παρόντος να παραβιαστεί μέσω επιθέσεων «βίαιης δύναμης» (brute force). Ενώ τα δεδομένα που έχουν κρυπτογραφηθεί εισέρχονται στον πρώτο κόμβο αναμετάδοσης (relay), ένα κρυπτογραφικό στρώμα αφαιρείται και τα δεδομένα αποστέλλονται στον «μεσαίο» κόμβο αναμετάδοσης. Η τελευταία διαγράφει ένα επιπλέον στρώμα και αποστέλλει τα δεδομένα στον τελευταίο κόμβο αναμετάδοσης («εξόδου»). Ο τελευταίος συνδέεται πλέον με τον στόχο που επιθυμεί ο χρήστης διά μέσου μίας μη κρυπτογραφημένης σύνδεσης, ενώ δεν «γνωρίζει» κανένα στοιχείο αναφορικά με τη διαδρομή κυκλοφορίας, αλλά μόνον για την προηγούμενη καταχώρηση. Μία επιπλέον σημαντική ιδιότητα της χρήσης του Tor browser είναι το γεγονός ότι στην τυχαία διαδρομή επιλέγεται ένας διαφορετικος κόμβος αναμετάδοσης εισόδου, ένας διαφορετικός μεσαίος κόμβος αναμετάδοσης και ένας διαφορετικός κόμβος αναμετάδοσης εξόδου περίπου κάθε 10 λεπτά (Σχήμα 3.9).



Σχήμα 3.9. Σχηματική απεικόνιση της λειτουργίας του δικτύου Tor (Le Blond et al., 2011).

Μία αναλογία της λειτουργίας του δικτύου Tor που μπορεί να γίνει πιο εύκολα αντιληπτή στον μη ειδικό αντιστοιχεί στην αποστολή επιστολής η οποία παραλαμβάνεται και ανακατευθύνεται από διαφορετικά άτομα. Για παράδειγμα ο Α

επιθυμεί να αποστείλει μία επιστολή στον Β, αλλά δεν επιθυμεί να πληροφορηθεί ο Β την προέλευση της επιστολής. Τα βήματα που θα μπορούσε να ακολουθήσει ο Α για τη διασφάλιση της ανωνυμίας του είναι τα ακόλουθα:

1. Ο Α συντάσσει επιστολή την οποία τοποθετεί σε φάκελο που απευθύνεται στον Β στην πόλη 1

2. Ο Α τοποθετεί τον φάκελο σε άλλον και τον απευθύνει στον Γ στην πόλη 2

3. Ο Α τοποθετεί τον παραπάνω φάκελο σε έναν άλλον και τον απευθύνει στον Δ στην πόλη 3

4. Ο Α τοποθετεί τον παραπάνω φάκελο σε έναν άλλον και τον απευθύνει στον Ε στην πόλη 4

5. Ο Α τοποθετεί την επιστολή σε γραμματοκιβώτιο που βρίσκεται έξω από την οικία του στην πόλη 5.

Με βάση την παραπάνω αναλογία, κάθε φάκελος αντιστοιχεί σε ένα διαφορετικό επίπεδο κρυπογράφησης. Αν κάθε άτομο ανοίξει μόνον τον πρώτο φάκελο, το μήνυμα της επιστολής παραμένει κρυμμένο στον πλέον εσωτερικό φάκελο. Ο Ε (relay εισόδου) παραλαμβάνει την επιστολή, και αφού αφαιρέσει τον εξωτερικό φάκελο την τοποθετεί σε γραμματοκιβώτιο για αποστολή στον Δ. Ο Ε δεν ενημερώθηκε ποτέ για το μήνυμα της επιστολής, ενώ γνωρίζει μόνον ότι προήλθε από την πόλη 5 και κατευθύνεται στην πόλη 3. Αντίστοιχη είναι η διαδικασία μέχρι την αποστολή της επιστολής στην πόλη 2. Ο Γ (relay εξόδου) αφαιρεί τον εξωτερικό φάκελο της επιστολής και την αποστέλλει στον Β. Στο σημείο αυτό το περιεχόμενο μήνυμα μπορεί να διαβαστεί από τον Β. Εάν ο Α επιθυμεί να αποστείλει μία άλλη επιστολή στον Β διασφαλίζοντας την ανωνυμία του, θα την αποστείλει σε τρία διαφορετικά άτομα μέσω της ίδιας διαδικασίας (Le Blond et al., 2011; Li et al., 2013).

Το δίκτυο Tor διαμορφώνεται επί της ουσίας σε «εθελοντική» βάση, γεγονός που συνεπάγεται ότι οποιοσδήποτε χρήστης μπορεί να διαμορφώσει έναν server ούτως ώστε να συνιστά έναν από τους χιλιάδες κόμβους αναμετάδοσης που χρησιμοποιούνται από έναν μεγάλο αριθμό χρηστών του φυλλομετρητή. Η ιδιότητα του εθελοντή δηλώνει ότι ο διακομιστής του χρήστη θα «αφαιρέσει τον εξωτερικό φάκελο» και θα προωθήσει τα δεδομένα στον αμέσως επόμενο προορισμό.

Ο κόμβος αναμετάδοσης εισόδου αναφέρεται και ως «φρουρός». Ο χρήστης του Tor browser προβαίνει σε τυχαία επιλογή των «φρουρών», ώστε να χρησιμοποιηθούν μόνον για την αποστολή του πρώτου κρυπτογραφημένου πακέτου. Εφόσον υπάρχει η υποψία ότι ένας δεδομένος «φρουρός» είναι ανεπαρκής, δεν χρησιμοποιείται. Κατόπιν, επιλέγεται τυχαίος μεσαίος κόμβος αναμετάδοσης για τη διαβίβαση του μεσαίου κρυπτογραφημένου πακέτου και κατόπιν τα κρυπτογραφημένα δεδομένα αποστέλλονται στον κόμβο αναμετάδοσης εξόδου, ο οποίος και αποστέλλει τα μη κρυπτογραφημένα δεδομένα στον επιθυμητό στόχο. Μετά την πάροδο 10 λεπτών το κύκλωμα Tor θα μεταβάλει τους κόμβους ανάμεσα στους χιλιάδες που μπορούν να επιλεγούν. Κάθε ένας από τους μεσαίους κόμβους αναμετάδοσης δημοσιεύεται δημόσια στο Διαδίκτυο, ούτως ώστε να αξιοποιηθεί από τους χρήστες του Tor browser. Εν τούτοις, υφίστανται μεσαίοι relays που συνήθως δεν δημοσιεύονται («γέφυρες») και για αυτόν τον λόγο δεν μπορούν να αποκλειστούν από τους παρόχους διαδικτυακών υπηρεσιών ή από τις κυβερνήσεις.

3.2.4.3. Δίκτυο I2P

Το δίκτυο I2P ή το Αόρατο Έργο Διαδικτύου (Invisible Internet Project) εμφανίζει παρόμοια χαρακτηριστικά με το κύκλωμα Tor, διαμορφώνοντας ένα δίκτυο επικάλυψης «εθελοντικών» συστημάτων και παρέχοντας υπηρσίες ανωνυμίας. Ουσιαστικά, πρόκειται για ένα διαδικτυακό τεχνολογικό μέσο ανοιχτού κώδικα που αφορά τη λειτουργία ενός ανώνυμου δικτύου όπου ένας χρήστης μπορεί να αποκτήσει πρόσβαση διά μέσου των συνηθισμένων περιηγητών ιστού. Το I2P δρα ως στρώμα που παρέχει τη δυνατότητα ανώνυμης ανταλλαγής δεδομένων χωρίς να διαθέτει κάποιο κεντρικό σημείο επικοινωνίας, γεγονός που συνεπάγεται ότι δεν υπάρχει ένα κεντρικό σημείο βάσει του οποίου η ανωνυμία και η ασφάλεια των χρηστών μπορούν να τεθούν σε κίνδυνο. Πρέπει ωστόσο να τονιστεί για ακόμη μία φορά ότι δεν υφίσταται απόλυτη διαδικτυακή ανωνυμία, ενώ μάλιστα η προστασία της ασφάλειας είναι ανάλογη της υπολογιστικής ισχύος που συνιστά το προαπαιτούμενο για την παραβίαση ενός συστήματος παροχής της ανώνυμης διαδικτυακής περιήγησης. Αναφορικά δε με το δίκτυο I2P οι χρήστες

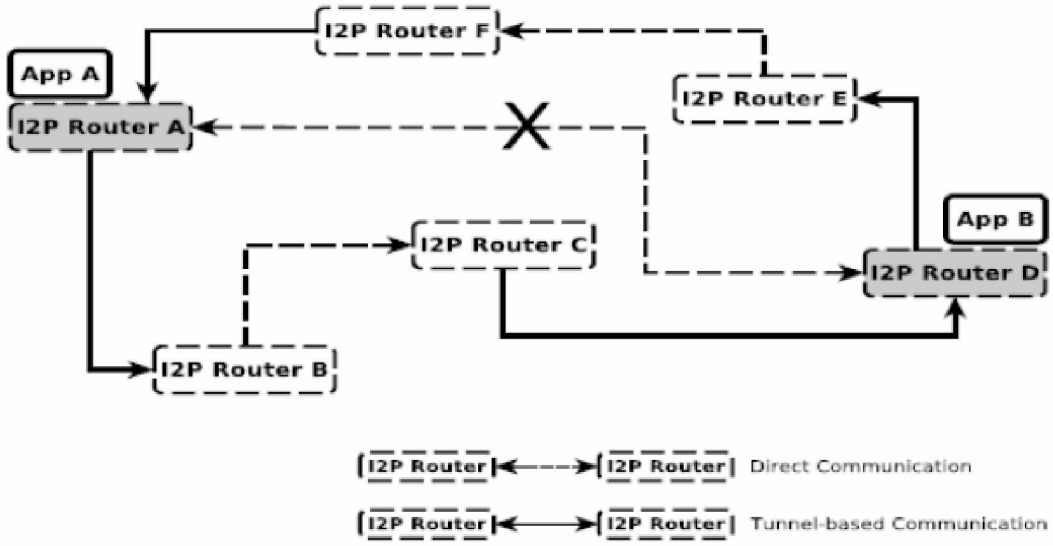
διαθέτουν τον έλεγχο του βαθμού ασφαλείας και βαθμού ανωνυμίας που εξυπηρετούν την κάλυψη των ιδιαίτερων αναγκών τους.

Το δίκτυο I2P συγκροτείται στη βάση μιας ομάδας εικονικών δρομολογητών (λογισμικών που καθιστούν δυνατή την επικοινωνία των εφαρμογών μέσω δικτύου). Ο δέκτης και ο αποστολέας δεν επικοινωνούν άμεσα μεταξύ τους, αλλά με τη βοήθεια άλλων δρομολογητών. Κάθε χρήστης που συμμετέχει στο δίκτυο λειτουργεί και ως δρομολογητής και, κατά συνέπεια, κάθε δρομολογητής λαμβάνει και αποστέλλει σε συνεχή βάση έναν αριθμό μηνυμάτων. Κάποια μηνύματα ενδέχεται να προέρχονται ή να κατευθύνονται από τον δεδομένο χρήστη, αλλά στην πλειοψηφία των περιπτώσεων οι χρήστες συνιστούν απλώς κόμβους διά των οποίων αναμεταδίδονται τα δεδομένα των υπόλοιπων χρηστών (Kosinski, 2015).

Το κύριο χαρακτηριστικό το οποίο διαφοροποιεί το δίκτυο I2P έναντι του φυλλομετρητή Tor αφορά τον σχεδιασμό του ως δικτύου ανωνύμου επιπέδου που καθιστά εφικτή στους χρήστες την ανάπτυξη των δικών του εφαρμογών και παράλληλα τον σχεδιασμό του για ανώνυμη και κοινή χρήση αρχείων και ανώνυμη φιλοξενία ιστοχώρων. Αντιθέτως, στο κύκλωμα Tor, λαμβάνει χώρα ο επαναπροσανατολισμός της πληροφορίας και η έξοδός της από το «κανονικό» Διαδίκτυο. Η κίνηση του δικτύου I2P παραμένει εντός αυτού και, ως εκ τούτου, θεωρείται ένα κλειστό δίκτυο, ενώ το κύκλωμα/δίκτυο Tor θεωρείται ένα είδος διακομιστή μεσολάβησης Διαδικτύου.

Ακολούθως, θα περιγραφεί η αρχιτεκτονική του δικτύου I2P. Κάθε χρήστης/κόμβος του συγκεκριμένου δικτύου αναπτύσσει εντός του συστήματος έναν ορισμένο δρομολογητή I2P και κατ' αυτόν τον τρόπο διαμορφώνει την «επικάλυψη δικτύου I2P». Η σύνδεση των δρομολογητών I2P μεταξύ τους συνεπάγεται τον σχηματισμό «σηράγγων», ήτοι διαδρομών πολλών αλμάτων ανάμεσα σε διάφορους δρομολογητές I2P (Σχήμα 3.10). Ο εκάστοτε δρομολογητής I2P αποστέλλει δεδομένα με τη χρήση μιας σήραγγας ενός άλματος που αξιοποιεί έναν δρομολογητή I2P B (το τελικό σημείο), ενώ λαμβάνει δεδομένα τα οποία επίσης χρησιμοποιούν σήραγγα κενός άλματος που αξιοποιεί τον δρομολογητή F I2P. Επίσης, ο δρομολογητής I2P αξιοποιεί σήραγγες ενός άλματος κατά το οποίο αποστέλλονται δεδομένα διά του δρομολογητή C I2P. Σε μια σήραγγα του δικτύου I2P ο αριθμός των αλμάτων περιλαμβάνεται μεταξύ του 0 και του 7. Περισσότερα

άλματα κατά μήκος μιας σήραγγας συνεπάγονται αύξηση του βαθμού ανωνυμίας, αλλά μείωση της απόδοσης, καθώς τα δεδομένα απαιτείται να διασχίζουν περαιτέρω ενδιάμεσους κόμβους.



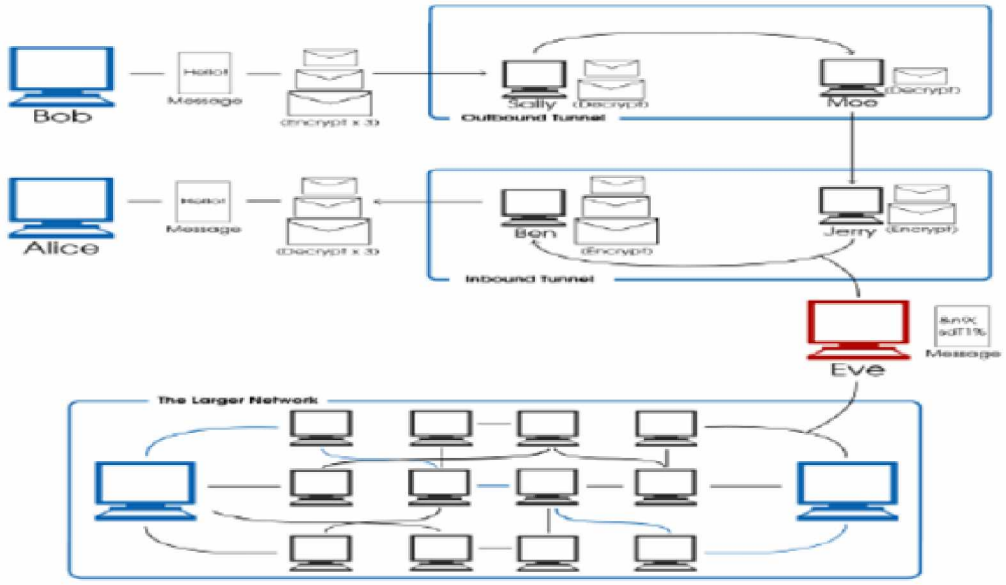
Σχήμα 3.10. Αρχιτεκτονική δικτύου I2P (Li et al., 2011).

Οι χρήστες μπορούν να αναπτύξουν εφαρμογές I2P «πάνω» από τους δρομολογητές I2P. Οι εν λόγω εφαρμογές έχουν τη δυνατότητα ανώνυμης επικοινωνίας με κάποιες άλλες, απομακρυσμένες εφαρμογές του δικτύου I2P. Στο Σχήμα απεικονίζεται ένα κλασικό σενάριο, στο οποίο οι εφαρμογές (A και B) αναπτύσσουν επικοινωνία μέσω των σηράγγων I2P, χωρίς να διαμεσολαβήσει κάποια άμεση επικοινωνία ανάμεσα στους δρομολογητές I2P τους. Ως πύλη λήψης δεδομένων η εφαρμογή A αξιοποιεί τη σήραγγα που περιλαμβάνει τον δρομολογητή I2P F και η εφαρμογή B αξιοποιεί τη σήραγγα που περιλαμβάνει τον δρομολογητή I2P C. Με παρόμοιο τρόπο, η εφαρμογή A αξιοποιεί τη σήραγγα που περιλαμβάνει ως τελικό σημείο αποστολής τον δρομολογητή I2P B, η δε εφαρμογή B αξιοποιεί τη σήραγγα που ενέχει τον δρομολογητή I2P E. Οι επικοινωνίες με τη βοήθεια των σηράγγων αποτελούν τον πυρήνα του ανώνυμου χαρακτήρα του δικτύου I2P, η λειτουργία του οποίου επιτρέπει την αποσύνδεση της ταυτότητας ενός χρήστη του συγκεκριμένου δικτύου (την οποία αντιπροσωπεύει ο δρομολογητής I2P) από την ταυτότητα κάποιας εφαρμογής I2P (Li et al., 2013).

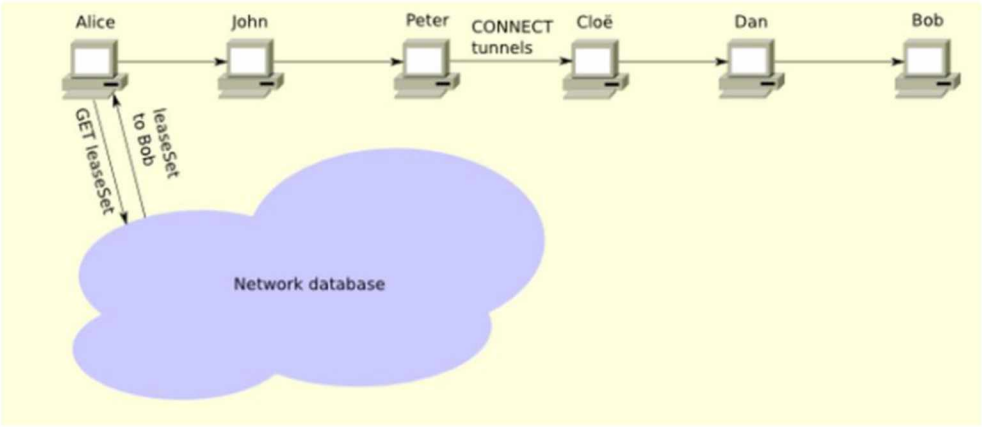
Κατά τη δρομολόγηση μηνυμάτων με τη χρήση του δικτύου I2P τα μεταδιδόμενα μηνύματα ενδέχεται να είναι αρκετά μεγαλύτερα σε σχέση με τα πακέτα IP. Κάθε δρομολογητής σχετίζεται με πολλές εξερχόμενες και εισερχόμενες σήραγγες, που είναι στην ουσία μονοκατευθυντικές διαδρομές μέσω ποικίλων δρομολογητών. Η εξερχόμενη σήραγγα αφορά τη διαδρομή που αξιοποιείται αποκλειστικά για την αποστολή δεδομένων από τον δημιουργό της σήραγγας, η δε εισερχόμενη σήραγγα αφορά μια αντίστοιχη διαδρομή που εξυπηρετεί την αποστολή δεδομένων προς τον δημιουργό της συγκεκριμένης σήραγγας. Στο Σχήμα 3.11 περιγράφεται ευσύνοπτα ο τρόπος μεταφοράς ενός μηνύματος από έναν χρήστη σε κάποιον άλλο με τη χρήση του δικτύου I2P. Για να αποσταλεί το μήνυμα από τον A (Bob) στον B (Alice) το μήνυμα διέρχεται κατ' αρχάς από την εξερχόμενη σήραγγα του χρήστη A. Στο τέλος της παραπάνω σήραγγας εισέρχεται στην εισερχόμενη σήραγγα του χρήστη B, ενδεχομένως αφού διέλθει διά μέσου περαιτέρω δρομολογητών). Κατά συνέπεια, με τη χρήση ξεχωριστών σηράγγων για τα εισερχόμενα και τα εξερχόμενα μηνύματα, τόσο ο A όσο και ο B έχουν τη δυνατότητα να καθορίσουν το ελάχιστο πλήθος των αλμάτων τα οποία επιθυμούν να χρησιμοποιήσουν για τη διαβίβαση του μηνύματος. Το γεγονός αυτό εξασφαλίζει ότι θα παρέχεται πάντοτε το απαιτούμενο ελάχιστο επίπεδο ασφαλείας, ενώ η διαβίβαση θα πραγματοποιείται σε κατάσταση ανωνυμίας (Kosinski, 2015).

Ακολούθως, θα περιγραφεί αναλυτικά η μέθοδος διασφάλισης της ανωνυμίας χρήσει ενός δικτύου I2P. Οι πληροφορίες που αναφέρονται σε έναν δρομολογητή τύπου I2P συγκεντρώνονται στη δομή δεδομένων "routerinfo". Η αναγνώριση μίας εφαρμογής I2P δεν πραγματοποιείται μέσω της κανονικής πλειάδας (διεύθυνση IP και αριθμός θύρας), αλλά διά μέσου ενός «προορισμού I2P», ανεξάρτητου της τοποθεσίας. Ο συγκεκριμένος προορισμός I2P, σε συνδυασμό με κάποια κλειδιά κρυπτογράφησης, ένα ορισμένο κλειδί υπογραφής και με έναν κατάλογο των χρησιμοποιούμενων πυλών για την παραλαβή των δεδομένων εμπεριέχονται στη δομή "leaseset". Με βάση το σενάριο που περιγράφηκε παραπάνω, λοιπόν, το leaseset που αφορά την εφαρμογή A εμπεριέχει ως την ενιαία πύλη τον δρομολογητή I2P F και το αντίστοιχο leaseset της εφαρμογής B ως ενιαία πύλη τον δρομολογητή I2P C. Έτσι, ένας δρομολογητής I2P μπορεί να αναγνωριστεί από κάποιο routerinfo, μία εφαρμογή I2P δε από ένα σύνολο leasesets. Οι leasesets και

routerinfos αντιστοιχούν στα «μεταδεδομένα δικτύου» του I2P τα οποία χρειάζονται για την ορθή λειτουργία του δικτύου (Σχήμα 3.12).



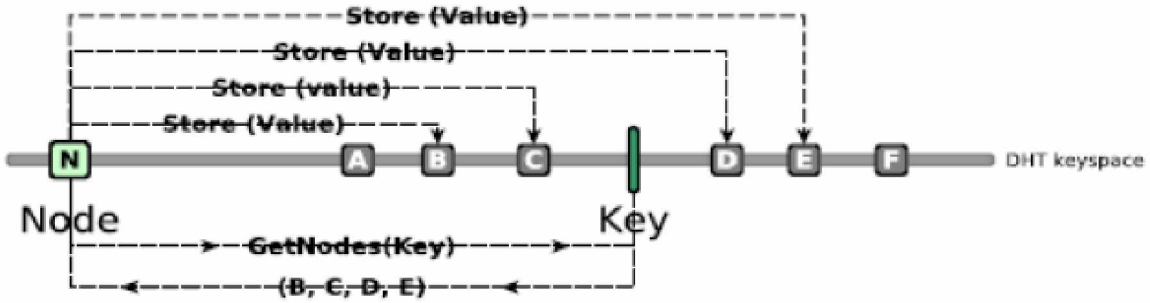
Σχήμα 3.11. Αποστολή δεδομένων διά μέσου του δικτύου I2P (Le Blond et al., 2011).



Σχήμα 3.12. Χρήση leaseset για πρόσβαση σε συγκεκριμένο προορισμο εντός του δικτύου I2P (GetI2P.net, 2018).

Το δίκτυο I2P αξιοποιεί έναν κατανεμημένο κατάλογο, ούτως ώστε να αποθηκευθεί το σύνολο των μεταδεδομένων δικτύου και να καταστούν προστιά σε

όλο το δίκτυο. Η σχετική βάση δεδομένων αναφέρεται ως “netDB” και πρόκειται ουσιαστικά για έναν κατανεμημένο πίνακα «κατακερματισμού» (distributed hash table, DHT) βάσει του αλγορίθμου Kademlia, ο οποίος και αποτελείται από ορισμένους «κόμβους πλημμύρας». Οι τελευταίοι συνιστούν κανονικούς δρομολογητές I2P ταχυτήτων που ανήκουν σε υψηλό εύρος ζώνης. Το γεγονός αυτό συνεπάγεται ότι το netDB δεν απαρτίζεται από το σύνολο του δικτύου, αλλά από υποσύστημα του συνόλου των δρομολογητών I2P. Η βάση δεδομένων netDB δρα ως ένας συνήθης κατανεμημένος πίνακας κατακερματισμού κατά την ανάκτηση και την αποθήκευση δεδομένων. Στο Σχήμα 3.13 περιγράφεται μία απλοποιημένη εκδοχή της εν λόγω διαδικασίας, στην οποία κάποιος κόμβος N προβαίνει στην αποθήκευση δεδομένων χρήσει μιας συγκεκριμένης τιμής κλειδιού. Αρχικά, πραγματοποιείται η ανάκτηση των κόμβων κοντά στην τιμή κλειδιού (set replica), έστω των κόμβων B, C, D, E (των αντιγράφων των κόμβων). Ακολούθως, αποστέλλεται το μήνυμα (το οποίο σε περίπτωση που ζητηθεί η εύρεση δεδομένων θα αντιστοιχεί σε ένα μήνυμα αναζήτησης) στους συγκεκριμένους κόμβους και η τιμή αποθηκεύεται. Η λειτουργία του netDB πραγματοποιείται με παρόμοιο τρόπο. Κάθε κόμβος πλημμύρας έχει τη δυνατότητα να αποθηκεύει ένα τμήμα του συνόλου των μεταδεδομένων του δικτύου (routerinfos ή leasesets) (Egger et al., 2013).



Σχήμα 3.13. Διαδικασία αποθήκευσης και ανάκτησης με βάση τον αλγόριθμο Kademlia (Egger et al., 2013) .

Όπως κάθε κατανεμημένος πίνακας κατακερματισμού που διαμορφώνεται με βάση τον Kademlia, ο netDB, με στόχο τον προσδιορισμό του κόμβου όπου θα πρέπει να εξαχθεί ή να δημοσιευθεί μία τιμή με τη σύγκριση του αναγνωριστικού

τιμής με το αναγνωριστικό κόμβου, αξιοποιεί την πύλη XOR. Κατά την πρώτη εκτέλεση προσδιορίζεται το ανανγωριστικό κόμβου και η τιμή σε ολόκληρη τη διάρκεια ζωής του κόμβου παραμένει αμετάβλητη. Εν τούτοις, από το netDB χρησιμοποιείται ένα προσωρινό αναγνωριστικό για να υπολογιστεί η απόσταση XOR. Η χρήση του προσωρινού αναγνωριστικού (αναγνωριστικού δρομολογήσεως) κατορθώνεται διά της προσάρτησης του αναγνωριστικού κόμβου στην τρέχουσα ημερομηνία και της «εκτόξευσης» του αποτελέσματος (Σχέση 1). Κατά συνέπεια, το χρησιμοποιούμενο από το netDB αναγνωριστικό αντιστοιχεί στο αναγνωριστικό δρομολογήσεως, που μεταβάλλεται καθημερινά. Το αναγνωριστικό κόμβου διατηρείται σταθερό.

(αναγνωριστικό δρομολογήσεως)= SHA256(κόμβος idjjyyyyMMdd) [1]

Τα μεσάνυχτα πρέπει να πραγματοποιηθεί η αναδημοσίευση κάθε τιμής σε άλλη τοποθεσία DHT, αφού μεταβάλλεται το αναγνωριστικό δρομολογήσεως. Η συγκεκριμένη λειτουργία χρησιμοποιείται για την αύξηση του υπολογιστικού κόστους της εκάστοτε εντοπισμένης επίθεσης Sybil, κατά την οποία ένας επιτιθέμενος χρήστης διαμορφώνει έναν μεγάλο αριθμό «πλαστών ταυτοτήτων», ούτως ώστε να τις τοποθετήσει πέριξ του DHT. Το σύνολο των πλαστών αυτών ταυτοτήτων βρίσκεται κοντά σε συγκεκριμένο στόχο, κατά τη διάρκεια μιας επίθεσης Sybil, με στόχο την απόκτηση ελέγχου συγκεκριμένου μέρους του DHT (Egger et al., 2013).

Αναφορικά δε με τη χρήση του δικτύου I2P οι διαθέσιμες εφαρμογές είναι παρόμοιες με τις συνήθειες διαδικτυακές εφαρμογές, όπως με τους διάφορους φυλλομετρητές, την κοινή χρήση αρχείων, την ηλεκτρονική αλληλογραφία, κλπ. Πρέπει δε να αναφερθεί ότι καθώς το δίκτυο I2P αποτελεί ένα αυτόνομο και αποκεντρωμένο σύστημα δικτύου δεν μπορεί να προσεγγιστεί εξωτερικά το σύνολο του περιεχομένου του (και αντιστρόφως). Με άλλα λόγια, μπορεί να εκτελέσει σχεδόν το σύνολο των διαδικτυακών λειτουργιών με παράλληλη διαφάλιση της ανωνυμίας. Οι εφαρμογές που χρησιμοποιούνται εντός του δικτύου διαμορφώνονται ειδικά για το δίκτυο I2P. Συγκριτικά με τη χρήση υπηρεσιών Tor η εν λόγω μέθοδος είναι αρκετά ταχύτερη αναφορικά με την πρόσβαση στις εφαρμογές αυτού του είδους. Στο δίκτυο I2P οι σήραγγες μικρού «μήκους» περιορίζουν το πλήθος των δειγμάτων τα οποία μπορούν να χρησιμοποιηθούν από

τον εκάστοτε εισβολέα για τη διενέργεια μίας ενεργού επίθεσης. Η ανωνυμοποίηση τύπου “peer-to-peer” (P2P) διασφαλίζει τη λειτουργία του συνόλου των δικτυακών πελατών ως δρομολογητών, οι οποίοι αναλόγως του μεγέθους της βάσεως χρηστών παρέχουν ένα υψηλό επίπεδο ανωνυμίας (Timpanaro et al., 2015).

Η χρήση μιας αποκεντρωμένης και ασφαλούς υπηρεσίας ηλεκτρονικού ταχυδρομείου εντός του δικτύου I2P δεν επιτρέπει την αποστολή μηνυμάτων σε λογαριασμούς χρηστών που δεν συμμετέχουν στο I2P. Το δίκτυο αξιοποιεί ιδιαίτερα ισχυρές τεχνικές κρυπτογράφησης και ο βαθμός αποκέντρωσης που επιτυγχάνεται είναι τόσο μεγάλος, ούτως ώστε στην περίπτωση που χαθεί ένας κώδικος πρόσβασης αυτός δεν μπορεί να επαναφερθεί ούτε να ανακτηθεί. Η κοινή δε χρήση αρχείων (torrents) στο πλαίσιο του δικτύου I2P είναι περισσότερο ανώνυμη και ασφαλής από τις υπηρεσίες των VPNs, ενώ δεν είναι εφικτή με τη χρήση του δικτύου Tor. Τα διαθέσιμα torrents συνιστούν κατά βάση αντίγραφα του “Piratebay”, αντίγραφα κυβερνητικών εγγράφων τα οποία έχουν διαρρεύσει και απαγορευμένων βιβλίων. Αξίζει να σημειωθέι ότι αν ορισμένα νομικά μέτρα ή μία επίθεση απαγόρευαν την ύπαρξη των torrents στο συμβατικό Διαδίκτυο, οι χρήστες θα μπορούσαν να προσφύγουν στα περιεχόμενα στο I2P torrents, αν και με χαμηλή ταχύτητα. Τέλος, μία εκ των βασικότερων υπηρεσιών που παρέχονται διά μέσου του δικτύου I2P αφορά τη φιλοξενία ιστοχώρων. Η μεταγλώττιση των κρυμμένων υπηρεσιών πραγματοποιείται με τη χρήση «επιγραφών». Ο χρήστης (πελάτης) του δικτύου έρχεται σε επαφή με προεγκατεστημένο διακομιστή που αποκαλείται “Jetty”. Την εκκίνηση του τελευταίου ακολουθεί η εμφάνιση μίας σελίδας δείγματος που περιέχει τις οδηγίες οργάνωσης. Ωστόσο, ο συγκεκριμένος διακομιστής χαρακτηρίζεται από περιορισμένη μόνο λειτουργικότητα, καθώς επί παραδείγματι δεν υποστηρίζει SQL ή PHP (Timpanaro et al., 2015).

Στο τελευταίο αυτό τμήμα της παρουσίασης των εργαλείων που παρέχουν έναν βαθμό ανωνυμίας κατά την διαδικτυακή πλοήγηση και ειδικότερα σε ό,τι αφορά τη σύγκριση μεταξύ της χρήσης και της λειτουργίας του φυλλομετρητή Tor και του δικτύου I2P και οι δύο μέθοδοι εν γένει καθιστούν εφικτή την ανώνυμη πρόσβαση σε διαδικτυακό περιεχόμενο, τη χρήση κρυπτογράφησης πολλών επιπέδων και τη χρήση ενός τύπου δρομολόγησης του είδους “peer-to-peer”. Η κυριότερη δε διαφορά αφορά το ότι το δίκτυο/κύκλωμα Tor δημιουργήθηκε ως υπηρεσία

μεσολάβησης που αναφέρεται στην ανώνυμη πρόσβαση στο συμβατικό Διαδίκτυο, το δίκτυο I2P από την άλλη διαμορφώθηκε για τη δημιουργία ενός δικτύου στο Διαδίκτυο, ενώ περιλαμβάνει τις εφαρμογές που ανήκουν στα δικά του όρια. Το κύκλωμα Tor πλέον αξιοποιεί τις λεγόμενες «κρυφές υπηρεσίες» που καθιστούν δυνατό να χρησιμοποιείται ένα δίκτυο μέσα στο συμβατικό Διαδίκτυο. Επιπροσθέτως, το δίκτυο I2P έχει προχωρήσει στην ενσωμάτωση εφαρμογής η οποία επιτρέπει τη σύνδεση των χρηστών με το συμβατικό Διαδίκτυο. Κατά συνέπεια, και τα δύο εργαλεία εξασφάλισης της ανωνυμίας μπορούν να χρησιμοποιηθούν από θεωρητική άποψη για τις ίδιες εφαρμογές, αλλά η πρακτική διδάσκει πως τόσο το δίκτυο I2P όσο και το κύκλωμα Tor είναι πολύ αποδοτικότερα στην περίπτωση που χρησιμοποιούνται με βάση την αρχική μέθοδο. Μία επιμέρους διαφορά αντιστοιχεί στο ότι το σύνολο των χρηστών του I2P αποτελούν κόμβους για τη μεταφορά των δεδομένων, ενώ στο κύκλωμα Tor οι χρήστες προβαίνουν στην επιλογή μιας τέτοιας λειτουργίας. Επίσης, το δίκτυο I2P έχει διαμορφωθεί βάσει της γλώσσας προγραμματισμού Java, ενώ το Tor βάσει της γλώσσας C (Shirazi et al., 2016).

4. ΝΟΜΙΚΕΣ ΠΡΟΫΠΟΘΕΣΕΙΣ ΓΙΑ ΤΗΝ ΑΡΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΑΠΟΡΡΗΤΟΥ

4.1. Ευρωπαϊκή νομοθεσία

Το ζήτημα της δυνατότητας των κρατικών φορέων και των φορέων παρακολούθησης του ηλεκτρονικού εγκλήματος για άρση του απορρήτου των ηλεκτρονικών επικοινωνιών συνήθως εντάσσεται στο πλαίσιο της άρσης του

απορρήτου των επικοινωνιών εν συνόλω, αν και μόλις στα τέλη της δεκαετίας του 1990 και στις αρχές της δεκαετίας του 2000 πραγματοποιούνται ρητές αναφορές στις ηλεκτρονικές επικοινωνίες στα νομοθετικά κείμενα της ΕΕ και των κρατών-μελών της.

Από την άποψη των κειμένων που έχουν δημοσιευτεί σε επίπεδο ΕΕ ενδιαφέρον αναφορικά με το υπό συζήτηση θέμα εμφανίζει το Άρθρο 8 της Ευρωπαϊκής Σύμβασης για τα Δικαιώματα του Ανθρώπου και ειδικότερα η κατοχύρωση των θεμελιωδών δικαιωμάτων, όπως του σεβασμού της οικογενειακής ζωής, της ιδιωτικής ζωής, της κατοικίας και της αλληλογραφίας. Στη δεύτερη παράγραφο του Άρθρου απαριθμούνται οι προϋποθέσεις υπό τις οποίες είναι δυνατή η επέμβαση των δικαστικών αρχών σε ό,τι αφορά την άσκηση των παραπάνω δικαιωμάτων. Ειδικότερα, η εν λόγω επέμβαση θα πρέπει να προβλέπεται από την εθνική νομοθεσία των κρατών-μελών και να συνιστά αναγκαίο μέτρο για την εξασφάλιση της τάξης, της εθνικής τάξης, της οικονομικής ευημερίας του κράτους, την προστασία της ηθικής και της υγείας, την πρόληψη ποινικών παραβάσεων και για τη διασφάλιση άλλων ελευθεριών (Χρυσόγονος, 2002).

Στην Οδηγία 2002/58/ΕΚ αναφέρεται ρητά ότι τα κράτη-μέλη μπορούν να προβαίνουν σε νομοθετικές πρωτοβουλίες που αποσκοπούν στον περιορισμό των προβλεπόμενων δικαιωμάτων και υποχρεώσεων που προκύπτουν από την ενσωμάτωση και εφαρμογή της συγκεκριμένης Οδηγίας, αν ο περιορισμός αυτός συνιστά αναγκαίο, αλλά και κατάλληλο μέτρο για να διαφυλαχθεί η εθνική ασφάλεια, η εθνική άμυνα, η δημόσια ασφάλεια και για να διωχθούν ποινικά αδικήματα και η χρησιμοποίηση του συστήματος ηλεκτρονικών επικοινωνιών χωρίς άδεια, όπως αναφέρεται στο Άρθρο 13, παρ. 1 της Οδηγίας 95/46/ΕΚ. Στο πλαίσιο αυτό οι χώρες που συναποτελούν την ΕΕ έχουν τη δυνατότητα να λαμβάνουν τα κατάλληλα νομοθετικά μέτρα που καθιστούν εφικτή τη διατήρηση δεδομένων για ένα ορισμένο χρονικό διάστημα, αποκλειστικά για τους προαναφερθέντες λόγους. Στην αιτιολογική έκθεση της Οδηγίας 2002/58/ΕΚ, που αφορά την ενσωμάτωση

4.2. Ελληνική νομοθεσία

Σύμφωνα με το Άρθρο 19 του ελληνικού Συντάγματος, «νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφαλείας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων». Το βασικό νομοθετικό κείμενο συνιστά ο εκτελεστικός νόμος Ν. 2254/1994, όπως αυτός έχει τροποποιηθεί από τον Ν. 3115/2003. Ειδικότερα δε στα Άρθρα 3-5 περιγράφονται αναλυτικά οι διαδικασίες άρσης του απορρήτου των επικοινωνιών όταν εκείνη διατάσσεται με επίκληση λόγων ασφαλείας και οι αντίστοιχες διαδικασίες που αφορούν την άρση απορρήτου βάσει της διακρίβωσης σοβαρών εγκλημάτων.

Αναλυτικότερα, στο Άρθρο 3 του Ν. 2225/1994 ορίζεται ότι η αίτηση για την άρση του απορρήτου μπορεί να υποβληθεί μόνον από την πλευρά δικαστικής, πολιτικής, στρατιωτικής ή αστυνομικής αρχής στης οποίας την αρμοδιότητα υπάγεται το ζήτημα εθνικής ασφαλείας το οποίο και επιβάλλει την αρχή. Στο Άρθρο 2 του ίδιου νόμου ορίζεται ότι η αίτηση πρέπει να υποβληθεί προς τον Εισαγγελέα Εφετών που εδρεύει στον τόπο της αιτούσας αρχής ή στον τόπο όπου πρόκειται να υλοποιηθεί η άρση. Ακολουθεί η μέσα σε 24 ώρες απόφαση του Εισαγγελέα Εφετών για την άρση ή μη του απορρήτου. Η διάταξη του Εισαγγελέα Εφετών περιέχει τα στοιχεία που περιγράφονται στο Άρθρο 5 και στην περίπτωση που, σύμφωνα με την κρίση του, κατόπιν εισήγησης της αιτούσας αρχής, ιδιαίτερες συνθήκες εθνικής ασφαλείας υποχρεώνουν τη συνοπτική παράθεση ή και την παράλειψη ορισμένων εξ' αυτών των στοιχείων στη διάταξη πραγματοποιείται ειδική μνεία. Το στενό χρονικό περιθώριο δικαιολογείται από το γεγονός ότι ο τομέας της εθνικής ασφαλείας συνιστά ζήτημα υψίστης σημασίας. Μία χρονοτριβή είναι δυνατόν να καταστεί επιζήμια για τα συμφέροντα της εκάστοτε χώρας. Εν τούτοις, πρέπει να παρατηρηθεί ότι η «εθνική ασφάλεια» συνιστά έναν αρκετά γενικό όρο και, κατά συνέπεια, ο εν λόγω περιορισμός του δικαιώματος του απορρήτου των επικοινωνιών θα πρέπει να συνοδεύεται από τις κατάλληλες εγγυήσεις οι οποίες περιορίζουν τη διαδικασία και τα αποτελέσματά της στο μέτρο του αναγκαίου, ενώ ιδίως αποτρέπουν την πρόσβαση στα δεδομένα επικοινωνίας ιδιωτών ή εταιρικών και δημοσίων φορέων διαφορετικών από τα φυσικά και νομικά

πρόσωπα που περιλαμβάνονται στη σχετική δικαστική απόφαση (Παπαδόπουλος, 2008).

Κατά το Άρθρο 5 του παραπάνω νόμου, στο οποίο περιγράφεται η διαδικασία άρσης του απορρήτου, όπως καθορίζεται μετά τη δημοσίευση του Ν. 3606/2007, η διάταξη του Εισαγγελέα Εφετών, στην περίπτωση άρσης του απορρήτου με επίκληση λόγων ασφαλείας, είναι αναγκαίο να αναφέρονται τα ακόλουθα στοιχεία:

1. Το όργανο το οποίο διατάσσει την άρση, ήτοι τον Εισαγγελέα Εφετών που εδρεύει στον τόπο της αιτούσας αρχής ή στον τόπο όπου πρόκειται να υλοποιηθεί η άρση

2. Τον εισαγγελέα, τον ανακριτή ή τη δημόσια αρχή που προέβησαν στο αίτημα της επιβολής της άρσης

3. Τον σκοπό επιβολής της άρσης ο οποίος πρέπει να εμπίπτει στο πεδίο της «εθνικής ασφαλείας»

4. Τα μέσα επικοινωνίας ή ανταπόκρισης στα οποία η συγκεκριμένη άρση επιβάλλεται

5. Το εδαφικό εύρος της εφαρμογής, την ημερομηνία έκδοσης και τη χρονική διάρκεια της άρσης

Σε ό,τι αφορά τη διακρίβωση σοβαρών εγκλημάτων ιδιαίτερα σοβαρών (κακουργημάτων), ορίζεται ότι η άρση επιτρέπεται αποκλειστικά στην περίπτωση που αιτιολογείται επαρκώς η διαπίστωση του δικαστικού συμβουλίου ότι η περαιτέρω διερεύνηση της υπόθεσης ή το ζήτημα εξακρίβωσης της διαμονής του εκάστοτε κατηγορουμένου δεν μπορεί να προχωρήσει ή αναμένεται να προχωρήσει με δυσχέρεια χωρίς την άρση του απορρήτου. Στο Άρθρο 4 διευκρινίζεται ότι η άρση στρέφεται αποκλειστικά μόνον εναντίον συγκεκριμένων προσώπων που σχετίζονται με την υπόθεση ή εναντίον προσώπων που με βάση συγκεκριμένες ενδείξεις μεταφέρουν ή λαμβάνουν μηνύματα ειδικού περιεχομένου που προέρχονται από τον κατηγορούμενο ή αφορούν αυτόν ή στην περίπτωση που τα πρόσωπα χρησιμοποιούνται ως σύνδεσμοι αυτού. Επιπλέον, κατά το Άρθρο 4 του Ν. 2225/1994 σύμφωνα με τις παραπάνω περιπτώσεις η επιβολή της άρσης πραγματοποιείται με τη χρήση διάταξης του Συμβουλίου Πλημμελειοδικών ή

Εφετών στο πεδίο αρμοδιότητας στο οποίο υπάγεται η διακρίβωση του σχετικού εγκλήματος. Η αίτηση άρσης υποβάλλεται στο Συμβούλιο από τον αρμόδιο εισαγγελέα που διενεργεί ή εποπτεύει προκαταρκτική εξέταση ή προανάκριση, καθώς και από τον υπεύθυνο ανακριτή που πραγματοποιεί τακτική ανάκριση αναφορικά με τα εγκλήματα τα οποία περιλαμβάνονται στην πρώτη παράγραφο του παραπάνω άρθρου. Εν συνεχεία, εντός 24 ωρών το Συμβούλιο αποφασίζει την άρση ή μη του απορρήτου με σχετική διάταξη όπου περιέχονται όλα τα προαναφερθέντα στοιχεία. Επιπροσθέτως, πέραν των τελευταίων, περιέχονται το όνομα του προσώπου ή τα ονόματα των προσώπων εναντίον των οποίων το εν λόγω μέτρο λαμβάνεται, καθώς και η διεύθυνση στην οποίαν διαμένουν, στην περίπτωση που αυτή είναι γνωστή, αλλά και η αιτιολογίας της απόφασης.

Κατά την παρ. 6 του Άρθρου 4 μόνον σε περιπτώσεις που θεωρούνται εξαιρετικά επείγουσες ο διενεργών την προκαταρκτική εξέταση ή την προανάκριση εισαγγελέας και ο ανακριτής ο οποίος διενεργεί την τακτική ανάκριση έχουν τη δυνατότητα να αιτηθούν της άρσης του απορρήτου. Εν τούτοις, σε κάθε περίπτωση ο ανακριτής ή ο εισαγγελέας οφείλουν να προβούν στην εισαγωγή του ζητήματος βάσει σχετικής αίτησης εντός τριών ημερών στο Συμβούλιο. Η ισχύς της διάταξης του ανακριτή ή του εισαγγελέα αναφορικά με την άρση παύει αυτοδικαίως άμα τη λήξει της τριήμερης προθεσμίας ή στην περίπτωση που το ζήτημα έχει εισαχθεί εμπρόθεσμα (από την έκδοση της διάταξης του Συμβουλίου) (Παπαδόπουλος, 2008).

Στο ΠΔ 47/2005 συσχετίζονται ρητά οι ηλεκτρονικές επικοινωνίες με τις παραπάνω διατάξεις. Επιπλέον, στο Άρθρο 8 που σχετίζεται με τις υποχρεώσεις των παρόχων υπηρεσιών και δικτύων αναφέρεται ότι οι πάροχοι των δικτύων και των υπηρεσιών έχουν την υποχρέωση να ανταποκρίνονται άμεσα στο εκάστοτε αίτημα για άρση του απορρήτου το οποίο και κοινοποιείται από τις αρχές. Στην περίπτωση δε που απαιτείται η συμμετοχή ή συνεργασία άλλων παρόχων κατά την εφαρμογή του παραπάνω αιτήματος ο πάροχος πρέπει να ενημερώνει την αρμόδια αρχή και την ΑΔΑΕ, ενώ στη συνέχεια να επεμβαίνει ανάλογα με τις υποδείξεις των εν λόγω φορέων.

Σε ό,τι αφορά τη χρονική διάρκεια άρσης του απορρήτου στο Άρθρο 5 του υπό ανάλυση νόμου ορίζεται πως αυτή δεν μπορεί να είναι μεγαλύτερη των δύο μηνών.

Τυχόν παρατάσεις του συγκεκριμένου χρονικού διαστήματος, εκ των οποίων η κάθε μία από αυτές δεν υπερβαίνει τους δύο μήνες, είναι δυνατόν να διαταχθούν βάσει της προβλεπόμενης κάθε φορά διαδικασίας, εφόσον τα αίτια της άρσης του απορρήτου εξακολουθούν να υπάρχουν. Παρ' όλ' αυτά, η χρονική διάρκεια των παρατάσεων δεν είναι δυνατόν να υπερβαίνει εν συνόλω τους δέκα μήνες. Ωστόσο, αναφέρεται ότι το συγκεκριμένο χρονικό όριο δεν υφίσταται σε εκείνες τις περιπτώσεις όπου η άρση έχει διαταχθεί επί τη βάσει ζητημάτων εθνικής ασφαλείας, αντίθετα με τις περιπτώσεις διακρίβωσης των σοβαρών εγκλημάτων. Αν είναι απορριπτική η διάταξη του Εισαγγελέα, αυτή περιλαμβάνει, κατά το Άρθρο 5, μόνον τη δημόσια αρχή που είχε προβεί στο αίτημα επιβολής της άρσης, το όργανο που αποφασίζει και την ημερομηνία έκδοσης της συγκεκριμένης διάταξης.

Αναφορικά με την άρση του απορρήτου λόγω ζητημάτων εθνικής ασφαλείας θα πρέπει να σημειωθεί ότι το αίτημα διατάσσεται εναντίον πρακτόρων, οι οποίοι είναι δυνατόν να εναλλάσσονται, κάποιας άλλης χώρας που θέτει την εθνική ασφάλεια σε κίνδυνο, αλλά όχι εναντίον συγκεκριμένων προσώπων. Στην περίπτωση που θεωρηθεί ότι η εθνική ασφάλεια τίθεται σε κίνδυνο από συγκεκριμένο πρόσωπο και επί μακρό χρονικό διάστημα, θα πρέπει να εφαρμοστεί εναντίον αυτού όχι η διαδικασία της άρσης του απορρήτου λόγω ζητημάτων εθνικής ασφαλείας, αλλά η προβλεπόμενη διαδικασία άρσης για τη διακρίβωση εγκλημάτων σοβαρής φύσης (Παπαδόπουλος, 2008).

Στην περίπτωση της αιτιολόγησης με βάση ζητήματα εθνικής ασφαλείας, όπως προαναφέρθηκε, ο όρος «εθνική ασφάλεια» είναι υπερβολικά αόριστη και γενική και, κατά συνέπεια, επιδεικτική για καταχρηστικές εφαρμογές της διάταξης, καθώς δεν συνδέεται με ενέργειες εγκληματικής φύσης. Όπως υποστηρίζεται από τον Μάνεση (1982) από το Σύνταγμα ανατίθεται στις δικαστικές αρχές «κατ' αποκλειστικότητα» η συνδρομή τους και η πραγματοποίηση της διαδικασίας άρσης του απορρήτου. Εν τούτοις, η υλοποίηση της διαδικασίας θα πρέπει να υποστηρίζεται, υποχρεωτικά, από τα δεδομένα των υπηρεσιών πληροφοριών, που δεν είναι εύκολα ελέγξιμα, ως άκρως απόρρητα, ιδιαίτερα σε ό,τι αφορά τις πηγές αυτών των δεδομένων. Επομένως, οι λειτουργοί της Δικαιοσύνης θα περιβάλλουν

τις ενέργειες και τις εκτιμήσεις των υπηρεσιών πληροφοριών απλά με το κύρος τους (Μάνεσης, 1982).

Στην περίπτωση διακρίβωσης σοβαρών εγκλημάτων αναφέρεται το Άρθρο 12 του Ν. 3658/2008 («Περί μέτρων προστασίας των πολιτιστικών αγαθών και άλλες διατάξεις»). Η διαδικασία άρσης του απορρήτου επιβάλλεται με διάταξη του Συμβουλίου Πλημμελειοδικών ή Εφετών στην κατά τόπον αρμοδιότητα του οποίου εντάσσεται η διακρίβωση του εν λόγω εγκλήματος. Η αίτηση υποβάλλεται στο Συμβούλιο από τον αρμόδιο Εισαγγελέα που ενεργεί προκαταρκτική εξέταση ή προανάκριση, καθώς και από τον ανακριτή που διενεργεί την τακτική ανάκριση η οποία αφορά τα αναφερόμενα εγκλήματα. Και σε αυτή την περίπτωση το Συμβούλιο εκδίδει απόφαση εντός 24 ωρών περί της άρσης ή μη του απορρήτου με συγκεκριμένη διάταξη στην οποίαν περιέχονται τα απαραίτητα στοιχεία που αναφέρθηκαν παραπάνω. Σε ιδιαίτερα επείγουσες περιπτώσεις, ισχύει η δυνατότητα του Εισαγγελέα και του ανακριτή να εισαγάγουν το ζήτημα εντός τριών ημερών με υποβολή αίτησης στο Συμβούλιο. Στην παρ. 1β που προστέθηκε στον Ν. 3658/2008 αναφέρεται ότι «επιτρέπεται η άρση του απορρήτου για τη διακρίβωση των κακουργημάτων που προβλέπονται από τον Ν. 3028/2002 Για την προστασία των Αρχαιοτήτων και εν γένει της Πολιτιστικής Κληρονομιάς, όπως ο νόμος αυτός εκάστοτε ισχύει» και, επομένως, στους λόγους άρσης που θα αναφερθούν παρακάτω προστέθηκαν και οι διατάξεις που σχετίζονται με τα προβλεπόμενα στον Ν. 3028/2002 κακουργήματα.

Σε ό,τι αφορά τα ιδιαίτερα σοβαρά εγκλήματα που εμπίπτουν στον παραπάνω νόμο αυτά αναφέρονται περιοριστικά και αυτά προβλέπονται από τις εξής διατάξεις, σύμφωνα με τον Λυντέρη (1995):

1. Τα Άρθρα του Ποινικού Κώδικα 134, 135 (παρ. 1-2), 135Α, 137Α, 138, 139, 140, 143, 144, 146, 148 (παρ. 2), 150, 151, 157 (παρ. 1), 168 (παρ. 1), 187 (παρ. 1-2), 207, 208 (παρ. 1), 264 (περ. β'-γ'), 270, 272, 275 (περ. β'), 291 (παρ. 1, εδ. β'-γ'), 299, 322, 324 (παρ. 2-3), 374, 380, 385

2. Τα Άρθρα του Στρατιωτικού Ποινικού Κώδικα 26, 27, 28, 29, 31, 32, 33, 34, 35, 39, 40, 41, 63, 64, 76, 93, 97

3. Το Άρθρο 15, παρ. 1 του Ν. 2168/1993

4. Τα Άρθρα 5, 6, 7, 8 του Ν. 1729/1987.

5. Τα Άρθρα 89, 90, 93 του Ν. 1165/1968.

Επιπλέον, στην ίδια παράγραφο ορίζεται πως είναι επιτρεπτή η άρση του απορρήτου ώστε να διακριβωθούν τυχόν προπαρασκευαστικές πράξεις για το έγκλημα της παραχάραξης νομίσματος, σύμφωνα με το Άρθρο 211 του Ποινικού Κώδικα, ενώ συνεχίζει, αναφορικά με τις περιπτώσεις άρσης: «για τη διακρίβωση παραβάσεων των Άρθρων 3 έως 7, 29 και 30 του Ν. 3340/2005, Για την προστασία της κεφαλαιαγοράς από πράξεις προσώπων που κατέχουν προνομιακές πληροφορίες και πράξεις χειραγώγησης της αγοράς».

Στο σύνολο των παραπάνω περιπτώσεων, κατά το Άρθρο 5, η άρση μπορεί να επιβληθεί μόνον στην περίπτωση που το αρμόδιο δικαστικό συμβούλιο διαπιστώσει στη βάση επαρκούς αιτιολόγησης πως η διερεύνηση της υπόθεσης ο προσδιορισμός του τόπου διαμονής ενός κατηγορουμένου δεν είναι εφικτές ή είναι δυσχερείς άνευ της άρσης. Σε όλες τις περιπτώσεις επίσης είτε μετά την πάροδο της χρονικής διάρκειας της άρσης είτε αφού λήξει το ανώτατο επιτρεπτό χρονικό όριο αυτής, η άρση του απορρήτου των επικοινωνιών διακόπτεται αυτοδικαίως. Η παύση της μπορεί να διαταχθεί και πριν από τη λήξη της χρονικής διάρκειας, με διάταξη που καταρτίζει το όργανο επιβολής της άρσης, στην περίπτωση που ο σκοπός της διαδικασίας υλοποιήθηκε ή αν οι λόγοι για την επιβολή του μέτρου έχουν εκλείψει.

Στο παρόν σημείο αξίζει να επισημανθεί πως πέραν των διαδικαστικών προϋποθέσεων που καταγράφονται στα Άρθρα 3 και 4 του Ν. 2225/1994 στο Άρθρο 5 αναφέρονται ορισμένες επιπλέον εγγυήσεις των οποίων η παρουσία απαγορεύει την επιβολή της διαδικασίας άρσης του απορρήτου με τρόπο που θεωρείται καταχρηστικός και οι οποίες περιγράφονται παρακάτω.

Κατ’ αρχάς, το απόσπασμα της διάταξης στο οποίο περιλαμβάνεται το διατακτικό αυτής (ή το σύνολο του κειμένου) παραδίδεται στον πρόεδρο ή τον γενικό διευθυντή ή το διοικητικό συμβούλιο ή τον εκπρόσωπο του εκάστοτε νομικού προσώπου όπου υπάγεται το μέσο επικοινωνίας ή ανταπόκρισης, στην περίπτωση

δε ατομικής επιχείρησης παραδίδεται στον επιχειρηματία. Αν το νομικό πρόσωπο υπάγεται στην αρμοδιότητα του κράτους παραδίδεται στον αρμόδιο προϊστάμενο Υπουργό ή τον αρμόδιο Υπουργό. Επιπλέον, αφού εκτελεστεί η διάταξη συντάσσεται έκθεση από την υπηρεσία η οποία προέβη στις διαδικασίες άρσης του απορρήτου. Στη συγκεκριμένη έκθεση (ή στις συγκεκριμένες εκθέσεις), υπογεγραμμένες από το αρμόδιο όργανο της αιτούσας αρχής, περιέχονται το σύνολο των ενεργειών, η ημερομηνία, ο τρόπος και ο τόπος εκτέλεσής τους, ακόμη και τα στοιχεία των υπεύθυνων υπαλλήλων. Σε κλειστό φάκελο διαβιβάζονται στη δικαστική αρχή και την αιτούσα αρχή αντίγραφα των εκθέσεων, καθώς και στην ΑΔΑΕ.

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα προσωπικά δεδομένα, και ιδιαίτερα τα διακινούμενα στο Διαδίκτυο, συνιστούν ένα επίκαιρο ζήτημα που έχει απασχολήσει το πεδίο των ανθρωπίνων δικαιωμάτων και ειδικότερα τα όργανα της Ευρωπαϊκής Ένωσης αλλά και την ελληνική νομοθεσία. Προς αυτή την κατεύθυνση έχουν συνταχθεί μία σειρά νομοθετικών κειμένων που επιχειρούν να διασφαλίσουν τα δικαιώματα των φυσικών και νομικών προσώπων των οποίων τα δεδομένα προσωπικού χαρακτήρα συλλέγονται και υφίστανται επεξεργασία. Η νεότερη προσπάθεια αφορά τη δημοσίευση του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) που εκδόθηκε το 2016 και τέθηκε σε εφαρμογή τον Μάιο του 2018.

Η διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών στη σύγχρονη εποχή συνιστά ζήτημα που αφορά καίρια και αποφασιστικά το πεδίο της ανωνυμίας στο Διαδίκτυο. Στην παρούσα εργασία περιγράφηκε μία ποικιλία τεχνολογικών εργαλείων τα οποία μπορούν να χρησιμοποιηθούν αυτόνομα ή σε συνδυασμό, ώστε να διασφαλιστεί ο εκάστοτε ζητούμενος βαθμός ανωνυμίας του χρήστη κατά την πλοήγησή του στο Διαδίκτυο. Ο χρήστης μπορεί να χρησιμοποιήσει Εικονικά Ιδιωτικά Δίκτυα (VPNs), ορισμένες κατηγορίες διακομιστών μεσολάβησης (proxy servers) ή να αξιοποιήσει την τεχνική δρομολόγησης Onion, χρησιμοποιώντας τον φυλλομετρητή Tor και το αντίστοιχο δίκτυο ή αξιοποιώντας το αποκεντρωμένο δίκτυο I2P. Κάθε μία από τις προαναφερθείσες τεχνικές εμφανίζει την δική της αρχιτεκτονική και τα δικά της πλεονεκτήματα και μειονεκτήματα και για αυτόν τον λόγο σε κάθε περίπτωση η διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών συνιστά ζήτημα που μπορεί να αξιοποιηθεί με μία ποικιλία συνδυασμού των τεχνικών αυτών, ανάλογα με τον επιθυμητό βαθμό ανωνυμίας.

Στον Ν. 2225/1994 περιγράφονται οι λόγοι άρσης του απορρήτου των επικοινωνιών, συμπεριλαμβανομένων των ηλεκτρονικών επικοινωνιών, όπως ευκρινώς παραπέμπει το ΠΔ 47/2005 και οι οποίοι αντιστοιχούν σε ζητήματα εθνικής ασφαλείας και διακρίβωσης πολύ σοβαρών εγκλημάτων. Εξάλλου, οι προϋποθέσεις με βάση τις οποίες μπορεί να πραγματοποιηθεί η αναστολή του ατομικού δικαιώματος οφείλουν να είναι ειδικές και καθορισμένες με σαφήνεια, κατά τις θεμελιώδεις αρχές του κράτους δικαίου. Αν και η σχετική νομοθεσία ανταποκρίνεται σε μεγάλο βαθμό στο παραπάνω αίτημα, σημείο προβληματισμού αποτελεί η επίκληση των λόγων «εθνικής ασφαλείας» για την άρση του απορρήτου των ηλεκτρονικών επικοινωνιών. Επομένως, απαιτείται λεπτομερέστερη αναφορά σε αυτές τις περιπτώσεις.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Adkinson, W.F., Eisenach, J.A., Lenard, T.M., 2002. “Privacy online: A report on the information practices and policies of commercial websites”. The Progress & Freedom Foundation. [διαδικτυακά] Διαθέσιμο στο: <http://www.pff.org/issues-pubs/books/020301privacyonlinereport.pdf> [Ανακτήθηκε στις 18 Νοεμβρίου 2018].

Cavoukian, A., Hamilton, T.J., 2002. The Privacy Payoff: How Successful Businesses Build Customer Trust. Whitby: McGraw-Hill Ryerson.

Cuhan, M.J., Bies, R.J., 2003. Consumer Privacy: Balancing economic and Justice Considerations. Journal of Social Issues 59(2), 323-342.

Edman, M. Yener, B. 2009. On anonymity in an electronic society: A survey of anonymous communication systems. ACM Comput. Surv. 42(1), 5.

Egger, C., Schlumberger, J., Kruegel, C., Vigna, G., 2013. Practical Attacks against the I2P Network. International Workshop on Recent Advances in Intrusion Detection, RAID 2013, Research in Attacks, Intrusions, and Defenses, 432-451.

GetI2P.net, 2018. Operation. [διαδικτυακά] Ανακτήθηκε από: <https://geti2p.net/en/docs/how/tech-intro#intro> [Προσπελάστηκε 25.11.2018].

Jensen, C., Potts, C., 2004. Privacy policies as decision-making tools: an evaluation of online privacy notices. Στο: Proceedings of the SIGCHI conference on Human Factors in Computing systems, Vienna, pp. 471-478.

Ikits, M., Hansen, C.D., 2006. The Proxy Chain Method and Its Application to Scientific Visualization. In: HAPTICS 2006 - 14th International Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems 25-26 March, 2006, Arlington, VA, USA., pp. 79.

Kosinski, J., 2015. Deepweb and Darknet-Police View, Archibald Reiss Days, Belgrade: March 2015.

Le Blond, S., Manils, P., Chaabane, A., Ali Kaafar, M., Castelluccia, C., Legout, A.,

Dabbous, W., (2011). One bad apple spoils the bunch: exploiting p2p applications to trace and profile TOR users. National Institute for Research in Computer Science and Control, p. 550.

Li, B., Erin, E., Gunes, M.H., Bebis, G., Shipley, T., 2011. An analysis of anonymity technology usage. Στο: Proceedings of the Third International Conference on Traffic Monitoring and Analysis, TMA'11, Springer-Verlag, Berlin, Heidelberg, pp. 108–121.

Li, B., Erdin, E., Gunes, M.H., Bebis, G., Shipley, T., 2013. An overview of anonymity technology usage. Computer Communications 36, 1269-1283.

QP Download, 2018. Proxifier Description. [διαδικτυακά] Διαθέσιμο στο: <https://qpdownload.com/proxifier> [Ανακτήθηκε στις 18.11.2018].

Shirazi, F., Simeonovski, M., Asghar, M.R., Backes, M., Diaz, C., 2016. A Survey on Routing in Anonymous Communication Protocols. ACM Computing Surveys 51(3), 51.

Sysel, M., Dolezal, O., 2014. An Educational HTTP Proxy Server. Procedia Engineering 69, 128-132.

Timpanaro, J.P., Cholez, T., Chrisment, I., Festor. O., 2015. Evaluation of the Anonymous I2P Network's Design Choices Against Performance and Security. ICISSP 2015 – Proceedings of the 1st International Conference on Information Systems Security and Privacy, February 2015, Angers: France, 46-55.

Turow, J., Feldman, L., Meltzer, K., 2005. Open to Exploitation: American Shoppers Online and Offline. Report from the Annenberg Public Policy Center of the University of Pennsylvania.

Tutorialspoint, 2018. Proxy Server [διαδικτυακά] Διαθέσιμο στο: <https://www.tutorialspoint.com/internet_technologies/proxy_servers.htm> [Ανακτήθηκε στις 18.11.2018].

Winkler, S., Zeadally, S., 2015. An analysis of tools for online anonymity. International Journal of Pervasive Computing and Communications 11(4), 436-453.

Ιγγλεζάκης, Ι., Εισαγωγή στον Κανονισμό Προστασίας Δεδομένων (GDPR). [διαδικτυακά] Διαθέσιμο στο: <https://www.slideshare.net/iglezakis/ss-83511848> [Ανακτήθηκε στις 18.11.2018].

Κατραμάδος, Δ., 1999. Προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων (ν. 2472/1997). ΔτΑ 3, 578.

Μάνεσης Α., Συνταγματικά Δικαιώματα- Α΄ Ατομικές ελευθερίες, 4η Έκδοση, Πανεπιστημιακές Παραδόσεις: Θεσσαλονίκη, 1982.

Λυντέρης, Χ., 1995. Η άρση του απορρήτου της επικοινωνίας ως μέσο αντεγκληματικής πολιτικής: Μια παρουσίαση και κριτική των σχετικών διατάξεων του Ν. 2225/1994. Ποιν. Χρ., 126.

Μήτρου, Λ., 1999. Η Αρχή Προστασίας Προσωπικών Δεδομένων. Αθήνα: Σάκκουλα.

Παπαδόπουλος, Ν., 2008. Προστασία του απορρήτου της επικοινωνίας: Ερμηνευτική προσέγγιση του Άρθρου 19 του Συντάγματος της Ελλάδας. Θεσσαλονίκη: Νομική βιβλιοθήκη.

Σαατζίδου-Παντελιάδου, Ε., 2006. Νέοι κανόνες δικαίου στο πλαίσιο της νέας οικονομίας: το παράδειγμα της νομικής ρύθμισης της ηλεκτρονικής επεξεργασίας των προσωπικών δεδομένων με έμφαση στην επεξεργασία των δεδομένων οικονομικής συμπεριφοράς. Διδακτορική διατριβή. Θεσσαλονίκη: Πανεπιστήμιο Μακεδονίας.

Χρυσόγονος, Κ., 2002. Ατομικά και Κοινωνικά Δικαιώματα, 2η έκδοση. Αθήνα: Σάκκουλα.