Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά Συστήματα

Μια Επισκόπηση των Τεχνολογιών Ελέγχου Προσπέλασης με Βάση το Περιεχόμενο

Γρηγόριος Χρυσομαλίδης

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Μάιος 2013

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μια Επισκόπηση των Τεχνολογιών Ελέγχου Προσπέλασης με Βάση το Περιεχόμενο

Γρηγόριος Χρυσομαλίδης

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2013

Περίληψη

Σήμερα, περισσότερο από ποτέ το Διαδίκτυο αποτελεί πλέον όχι ένα ακαδημαϊκό, επιστημονικό εργαλείο αλλά ένα μέσο μαζικής ενημέρωσης και κοινωνικοποίησης. Η τεράστια εξάπλωση του το καθιστά ένα δυναμικό βήμα ελεύθερης έκφρασης και πολιτικής δραστηριοποίησης, αλλά παράλληλα και ιδανικό περιβάλλον για τη διάδοση πληροφοριών, που σχετίζονται με παιδική πορνογραφία, βίαιη συμπεριφορά, και αμφισβήτηση ανθρωπίνων δικαιωμάτων. Η πρωτόγνωρη διάδοση των πολιτισμικών αγαθών που συνεπάγεται η ψηφιακή επανάσταση δημιουργεί τις προϋποθέσεις περιορισμού και έλεγχου της ροής της πληροφορίας για διαφόρους λόγους, από την προστασία ευαίσθητων κοινωνικών ομάδων ως την επιβολή της δημόσιας τάξης, ορισμένης πάντα σύμφωνα με τις κατά τόπους επικρατούσες συνθήκες.

Η παρούσα μεταπτυχιακή διατριβή περιλαμβάνει μια ολοκληρωμένη βιβλιογραφική μελέτη και μια «state-of-the-art» αναφορά των σύγχρονων τεχνολογιών που χρησιμοποιούνται για το φιλτράρισμα στο Διαδίκτυο, δηλαδή την απαγόρευση προσπέλασης σε διαδικτυακές θέσεις, με κριτήριο το περιεχόμενο τους. Παρουσιάζονται και αξιολογούνται οι διαφορές τεχνολογίες σε σχέση με την κλίμακα, το επίπεδο και τον τρόπο εφαρμογής τους. Ακόμη γίνεται μια παρουσίαση των ανταγωνιστικών τους τεχνολογιών που σχετίζονται με την παράκαμψη του ελέγχου.

Πέρα από το τεχνολογική διάσταση θίγονται και τα σημαντικά κοινωνικά ηθικά και νομικά ζητήματα που προκύπτουν, με κρισιμότερο αυτό των επιπτώσεων της διαδικτυακής λογοκρισίας στα ανθρώπινα δικαιώματα. Παρουσιάζονται επιπλέον οι αντιπαραθέσεις που προκύπτουν από την δημόσια διαβούλευση που πραγματοποιείται σε διεθνές νομικό επίπεδο. Επίσης περιγράφεται η επικρατούσα κατάσταση σε ένα πλήθος κρατών που παρουσιάζουν ενδιαφέρον είτε λόγω της βαρύτητας τους στο διεθνές τεχνολογικό και πολιτικό γίγνεσθαι, είτε λόγω των ιδιαιτέρων πολιτικών που εφαρμόζουν σε θέματα ελέγχου του Διαδικτύου.

Τέλος παρουσιάζεται σαν μελέτη περίπτωσης το μεγαλύτερο δημόσιο ελληνικό δίκτυο το Πανελλήνιο Σχολικό Δίκτυο και η επιλογή φιλτραρίσματος που εφαρμόζεται σε αυτό.

Summary

Today more than ever, the Internet is no longer an academic, scientific tool but a mass media of information and socialization. Its huge spread makes it a dynamic area for the freedom of expression and political activity, but at the same time an ideal environment for the dissemination of information related to child pornography, violent behavior and doubt of human rights. The unprecedented spread of cultural goods as a consequence of the digital revolution creates the conditions for limiting and controlling the flow of information for various reasons, from protecting vulnerable social groups to the enforcement of public order, nominated according to the local circumstances.

This M.Sc. dissertation includes a comprehensive bibliographical study and a state-of-the-art reference of modern technologies used to filter the Internet, with the meaning of the denial of access to web sites, based on their content. Various technologies are presented and evaluated in relation to the scale, the level and the method that is used to implement them. There is also a presentation of the competing technologies related the bypassing of control.

Beyond the technological dimension many important social, ethical and legal issues are raised with the most critical of them the impact of the Internet censorship in human rights. Moreover, the controversies arising from the public debate that carried out in international legal terms are presented. It is also described the situation for a number of states, which is relevance either due to their gravity in international technological and political affairs or due to the particular policies that are adopted for control of the Internet.

Finally the case study that is presented is the greatest Greek public network, the Greek School Network and the method of filtering that is applied there.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα Καθηγητή κ. Στέφανο Γκρίτζαλη για την ουσιαστική καθοδήγηση του, την ομάδα της Υπηρεσίας Ελέγχου του Πανελλήνιου Σχολικού Δικτύου και ιδιαίτερα τον κ. Παναγιώτη Χριστιά για τη παροχή σημαντικών πληροφοριών που συνέβαλλαν στη συγγραφή του 6ου κεφαλαίου και την Ελένη, την Κυριακή και τον Σίμο, την οικογένεια μου, για την υπομονή τους και τον χρόνο που τους στέρησα.

Περιεχόμενα

Κεφάλαιο 1
Έλεγχος Προσπέλασης με Βάση το Περιεχόμενο

Το Διαδίκτυο αναδείχθηκε αρχικά ως ένα σημαντικό εργαλείο επικοινωνίας για τους ερευνητές στον ακαδημαϊκό κόσμο, αλλά γρήγορα εξελίχτηκε, ιδιαίτερα μετά την εμφάνιση του Παγκόσμιου Ιστού, σε ένα εξαιρετικά πολύτιμο μέσο στο χώρο των επιχειρηματικών δραστηριοτήτων, της πολιτικής έκφρασης, της ψυχαγωγίας, των καταναλωτικών συνηθειών και της κοινωνικής ζωής των σύγχρονων ανθρώπων [29].

Στο Δυτικό κόσμο γενικά θεωρείται δεδομένο, με βάση τα ανθρώπινα δικαιώματα, τα κατά τόπους συντάγματα και νομικά συστήματα και τις ηθικές αξίες, ότι η πρόσβαση στο Διαδίκτυο παρέχεται ελεύθερα, απεριόριστα και το πιο σημαντικό χωρίς αλλοιώσεις [93]. Η δημοτικότητα του Παγκόσμιου Ιστού, ο δημοκρατικός χαρακτήρας του Διαδικτύου, μια που ο κάθε χρήστης μπορεί θεωρητικά να δημοσιεύσει ελεύθερα και εύκολα το δικό του περιεχόμενο σε αυτό, καθώς και η αποκεντρωμένη φύση του, δημιουργούν μεταξύ άλλων, από τη μία ένα πεδίο πρόσφορο για καταχρήσεις και από την άλλη ένα στόχο για τα πάσης φύσεως κέντρα εξουσίας που επιδιώκουν να ρυθμίσουν οτιδήποτε δύναται να τα αμφισβητήσει. Προκύπτει έτσι η ανάγκη, ή επιβάλλεται η επιλογή, ανάλογα με την περίπτωση, του ελέγχου της προσπέλασης στο

περιεχόμενο που διακινείται στα δίκτυα ανά τον κόσμο καθημερινά. Η απαίτηση για προστασία διαφόρων κοινωνικών ομάδων, όπως οι ανήλικοι, από ακατάλληλο περιεχόμενο που σχετίζεται για παράδειγμα με βία, πορνογραφία, ναρκωτικά κ.α., αλλά και η επιθυμία κάποιων να περιορίσουν ή να χειραγωγήσουν την ελεύθερη έκφραση, αποτελούν τις δύο αντιφατικές αλλά παράλληλα συμπληρωματικές συνιστώσες που συνέβαλλαν στη δημιουργία ενός ολόκληρου τομέα της τεχνολογίας των επικοινωνιών που σχετίζεται με το φιλτράρισμα του περιεχομένου.

Πολλές τεχνικές έχουν προταθεί και εφαρμοστεί προκειμένου να προστατευτούν ή να καταπιεστούν ή απλά να ελεγχθούν οι χρήστες του Διαδικτύου. Η μελέτη των τεχνολογιών αυτών αποτελεί πάντα μια πρόκληση, δεδομένου της συνεχούς εξέλιξης της, λόγω της εξαιρετικά δυναμικής μορφής του Διαδικτύου. Σε μια τέτοια θεώρηση των τεχνολογιών ελέγχου περιεχομένου, σημαντικό είναι να περιλαμβάνονται πάντα οι νομικές ηθικές και κοινωνικές παράμετροι και επιπτώσεις από την εφαρμογή τους.

1.1 Ορισμός του Ελέγχου Πρόσβασης με Βάση το Περιεχόμενο

Ο έλεγχος του περιεχομένου στο Διαδίκτυο (διαφορετικά το φιλτράρισμα) δεν είναι μια νέα δραστηριότητα, είναι κάτι που εφαρμόζεται εδώ και χρόνια. Ωστόσο, ο όρος καλύπτει ένα ευρύ φάσμα πολιτικών, υλικοτεχνικής υποδομής, λογισμικού και υπηρεσιών. Όλοι οι τύποι του αποκλεισμού στο Διαδίκτυο δεν είναι το ίδιο αποτελεσματικοί, νομικά ισοδύναμοι και ακόμη ένα σύστημα ελέγχου δεν μπορεί εύκολα να χρησιμοποιηθεί σε όλους τους τύπους περιεχομένου.

Ο πρωταρχικός στόχος του ελέγχου είναι το προς αποκλεισμό περιεχόμενο να μη παραληφθεί από τον υπολογιστή του τελικού χρήστη με τη βοήθεια ενός προϊόντος λογισμικού ή υλικού το οποίο εξετάζει όλες τις διαδικτυακές επικοινωνίες και καθορίζει αν πρέπει να εμποδίσει ή όχι την προβολή συγκεκριμένου υλικού. Για παράδειγμα, ένα μήνυμα ηλεκτρονικού ταχυδρομείου μπορεί να αποκλειστεί, διότι υπάρχει υποψία να είναι spam, ένας ιστότοπος ενδέχεται να αποκλειστεί, διότι υπάρχει υποψία ότι περιέχει κακόβουλο λογισμικό ή μια σύνδεση ομότιμων δικτύων μπορεί να διακοπεί επειδή είναι ύποπτη για ανταλλαγή περιεχόμενου παιδικής πορνογραφίας [13].

Πρόκειται ουσιαστικά για μιας μορφής λογοκρισίας στο Διαδίκτυο. Ο όρος λογοκρισία περιγράφει τον περιορισμό ιδεών, έγγραφων, επιστολών, φωτογραφιών, ταινιών, ή

οποιουδήποτε άλλου είδους πληροφορίας και ανθρώπινης έκφρασης. Η λέξη προέρχεται από την αρχαία Ρώμη, όπου δύο δικαστές, που ονομάζονταν, λογοκριτές ήταν υπεύθυνοι για την διαφύλαξη του δημόσιου ήθους [27].

Το φιλτράρισμα στο Διαδίκτυο άρχισε πριν από δύο δεκαετίες περίπου με το μπλοκάρισμα ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου (spam) κυρίως, μεταξύ άλλων λόγων, για να αποφευχθεί η υπερφόρτωση του δικτύου. Είναι αλήθεια ότι μετά από τόσα χρόνια ο έλεγχος των spam δεν έχει επιτευχτεί σε απόλυτο βαθμό [13].

1.1.1 Κατηγορίες Περιεχομένου προς Αποκλεισμό

Το πρώτο κριτήριο που μπορεί να παρατηρηθεί για την διαφοροποίηση μεταξύ των προσεγγίσεων αποκλεισμού περιεχομένου, είναι ο στόχος του μηχανισμού ελέγχου. Γενικά υπάρχουν τέσσερα διαφορετικά σημεία που είναι δυνατό να επικεντρωθεί [13]:

- Βασισμένη στην υπηρεσία προσέγγιση, π.χ. ηλεκτρονικό ταχυδρομείο.

- Βασισμένη στο περιεχόμενο προσέγγιση, π.χ. ομιλίες μίσους, παιδική πορνογραφία, τζόγος.

- Βασισμένη στον χρήστη προσέγγιση, π.χ. χρήστες που παράνομα ανακτούν υλικό προστατευμένο με πνευματικά δικαιώματα ή που αποστέλλουν spam.

- Βασισμένη στις μηχανές αναζήτησης προσέγγιση, π.χ. παρεμπόδιση αναζήτησης αποτελεσμάτων για παράνομους ιστότοπους.

Περιεχόμενο που ακόμη, μεταξύ άλλων, αποτελεί αντικείμενο του φιλτραρίσματος στο Internet είναι [13]:

- Ανεπιθύμητη ηλεκτρονική αλληλογραφία (spam). Οι πάροχοι υπηρεσιών ηλεκτρονικής αλληλογραφίας αναφέρουν ότι επί του παρόντος το 85 με 90 τοις εκατό από όλα τα ηλεκτρονικά μηνύματα είναι spam. Η συνηθέστερη περίπτωση είναι τα spam να φιλτράρονται με τη συγκατάθεση του πελάτη, δηλαδή του τελικού αποδέκτη.

- Ερωτικό και πορνογραφικό υλικό. Αυτό που συνήθως επιδιώκεται είναι η πρόληψη της πρόσβασης ανηλίκων σε περιεχόμενο που θεωρείται επιβλαβές. Σε ορισμένες χώρες έχουν αναπτυχθεί συστήματα επαλήθευσης ηλικίας, ενώ κάποιες άλλες ποινικοποιούν οποιαδήποτε ανταλλαγή πορνογραφικού υλικού, ακόμη και μεταξύ των ενηλίκων.

- Παιδική πορνογραφία. Καταδικάζεται σε παγκόσμιο επίπεδο και αδικήματα που σχετίζονται με αυτήν αναγνωρίζονται διεθνώς ως εγκληματικές πράξεις. Παρά τις σημαντικές προσπάθειες που έχουν γίνει προκειμένου να ελεγχθεί το δίκτυο διανομής υλικού παιδικής πορνογραφίας, αυτό δε κατέστη δυνατό σε ικανοποιητικό βαθμό.

- Αμφιλεγόμενα πολιτικά θέματα, θέματα μίσους, ξενοφοβίας. Ορισμένες χώρες ποινικοποιούν τη δημοσιοποίηση θεμάτων φυλετικού μίσους, βίας και ξενοφοβίας, ενώ σε κάποιες άλλες με ιδιαίτερη ευαισθησία σε θέματα προστασίας της ελευθερίας της έκφρασης, όπως οι ΗΠΑ, μπορεί να επιτραπεί η ανεμπόδιστη δημοσίευση τους.

- Παράνομα τυχερά παιχνίδια. Το Διαδίκτυο επιτρέπει στους ανθρώπους να παρακάμψουν τους περιορισμούς στα τυχερά παιχνίδια με απευθείας συνδέσεις με διαδικτυακά καζίνο, τα περισσότερα εκ των οποίων φιλοξενούνται σε χώρες με ανοικτή νομοθεσία σε σχέση με τον τζόγο στο Διαδίκτυο.

- Δυσφήμηση και δημοσίευση ψευδών πληροφοριών. Κάποιες ιστοσελίδες μπορούν να προβάλουν ψευδείς ή δυσφημιστικές και συκοφαντικές πληροφορίες, ειδικά σε φόρουμ και chat rooms, όπου οι χρήστες μπορούν να δημοσιεύσουν μηνύματα χωρίς άμεσο έλεγχο από κάποιους διαχειριστές.

- Περιεχόμενο που δημοσιεύεται από τρομοκρατικές οργανώσεις. Η δημοσίευση της προπαγάνδας και των πληροφοριών που σχετίζονται με τη διάπραξη εγκλημάτων και τρομοκρατικών ενεργειών.

- Παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας (copyright). Περιλαμβάνει την ανταλλαγή τραγουδιών, κινηματογραφικών ταινιών, λογισμικού και γενικότερα αρχείων που προστατεύοντα με δικαιώματα πνευματικής ιδιοκτησίας, μέσω συστημάτων διαμοιρασμού αρχείων. Η τεχνολογία ομότιμων δικτύων (Peer to Peer–P2P) διαδραματίζει σημαντικό ρόλο στην περίπτωση αυτή.

1.2 Κατηγορίες Τεχνολογιών και Τεχνικών Αποκλεισμού

Υπάρχουν δύο βασικές επιλογές στον αποκλεισμό περιεχομένου στο Διαδίκτυο, ο κεντρικός αποκλεισμός σε επίπεδο δικτύου και ο προσωπικός σε επίπεδο τελικού χρήστη, συχνά με βαθμονόμηση του περιεχομένου και αυτοκαθορισμό. Υπάρχει πάντα η δυνατότητα εφαρμογής υβριδικών συστημάτων που συνδυάζουν τις παραπάνω επιλογές.

Ο αποκλεισμός σε επίπεδο τελικού χρήστη επιτρέπει σε αυτόν να αποφασίσει τον τύπο του περιεχομένου που θα απορριφτεί, βασιζόμενος σε κριτήρια τα οποία μπορούν να ρυθμιστούν και να καθοριστούν ξεχωριστά για διαφορετικές κατηγορίες χρηστών (γονείς, παιδιά, δάσκαλοι, φοιτητές κτλ). Η επιλογή αυτή μπορεί να είναι η πιο εξειδικευμένη και «πελατοκεντρική», αλλά ενέχει πάντα τον κίνδυνο της πραγματικής αδυναμίας αποκλεισμού ακατάλληλου περιεχομένου, μια που ο χρήστης έχοντας διαχειριστικά δικαιώματα, αποφασίζει τελικά σε τι θα έχει πρόσβαση και σε τι όχι [13].

Με το βασισμένο στο κεντρικό δίκτυο αποκλεισμό, ο πάροχος της υπηρεσίας (Πάροχος Υπηρεσιών Διαδικτύου, εργοδότης, οργανισμός κτλ), μπορεί να καθορίσει το τύπο του περιεχομένου ή της δραστηριότητας που θα απαγορεύσει για όλους τους χρήστες της υπηρεσίας. Ο πάροχος είναι υπεύθυνος για να επιλέξει και τον μηχανισμό που θα λειτουργήσει προκειμένου να επιτύχει το σκοπό του [27].

Υπάρχουν τρία θέματα κλειδιά, τρία κρίσιμα ερωτήματα, στη διαδικασία καθορισμού του περιεχόμενου που πρόκειται να αποκλειστεί [13] :

- Πως τεχνολογικά καθορίζεται το περιεχόμενο ;
- Ποιος επιλέγει αυτό το περιεχόμενο ;
- Πως θα πραγματοποιηθεί ο αποκλεισμός τελικά ;

1.2.1 Βασικές Τεχνικές Καθορισμού του Περιεχομένου

Η διαδικασία κατά την οποία συλλέγεται, εξετάζεται και αξιολογείται το διακινούμενο στο δίκτυο περιεχόμενο είναι πολύπλοκη και πολλές φορές απαιτητική σε κατανάλωση πόρων. Υπάρχουν τρεις βασικές στρατηγικές [13] :

- Οι λίστες αποκλεισμού είναι η πιο συνηθισμένη μέθοδος. Πρόκειται για «μαύρες» λίστες, καταλόγους δηλαδή που περιέχουν οτιδήποτε θεωρείται ακατάλληλο ή «άσπρες» λίστες που περιέχουν το περιεχόμενο στο οποίο μόνο θα επιτρέπεται η πρόσβαση. Ο λίστες αυτές παράγονται με αυτοματοποιημένους ή όχι τρόπους και πολλές φορές ελέγχονται από εκπαιδευμένους επαγγελματίες. Υπάρχουν διαφορετικοί τύποι λιστών με διευθύνσεις, λέξεις κλειδιά κ.α. και το περιεχόμενο τους θεωρείται τις περισσότερες φορές εμπιστευτικό.

- Μια δεύτερη μέθοδος προσδιορισμού του περιεχομένου που πρόκειται να μπλοκαριστεί περιλαμβάνει την αυτόματη επιθεώρηση της εικόνας, του κείμενου ή του βίντεο που διακινείται με τη χρήση σύγχρονου εξελιγμένου λογισμικού για τον προσδιορισμό του επίπεδου του ακατάλληλου ή παράνομου υλικού που περιέχεται.

- Η χρήση του αυτοκαθορισμού με τη βοήθεια μιας προκαθορισμένης από τρίτους βαθμονόμησης και σήμανσης του περιεχομένου είναι μια τρίτη επιλογή για το διαχωρισμό του διακινούμενου υλικού σε επιβλαβές και μη επιβλαβές.

1.2.2 Ποιος Καθορίζει το Περιεχόμενο

Σε χώρες όπου η δικαστική εξουσία είναι ανεξάρτητη από τη νομοθετική και την εκτελεστική, δηλαδή στις σύγχρονες φιλελεύθερες δημοκρατίες, μόνο ο δικαστής θα πρέπει να έχει την αρμοδιότητα να χαρακτηρίσει ένα περιεχόμενο, μια κατάσταση ή μια ενέργεια ως παράνομη. Το ζήτημα αυτό δημιουργεί μία από τις σημαντικότερες προκλήσεις για τα συστήματα ελέγχου της διακίνησης της πληροφορίας στο Διαδίκτυο. Οι ισχύουσες εθνικές και διεθνείς νομικές διαδικασίες σπάνια είναι συμβατές με τις διασυνοριακές προκλήσεις του Διαδικτύου ή με την ταχύτητα λειτουργίας του. Ως αποτέλεσμα, δεν είναι πάντα οι δικαστικές αρχές αυτές οι οποίες αποφασίζουν [13].

Η εστίαση στον ρόλο αυτών που παίρνουν τις αποφάσεις για το τι είναι παράνομο ή μη αποδεκτό περιεχόμενο και επομένως πρέπει να αποκλειστεί, οδηγεί και στην αναγνώριση και κατηγοριοποίηση τους σε [76]:

- Μεμονωμένα άτομα, όπως για παράδειγμα είναι οι γονείς που επιθυμούν να προστατευόσουν τα παιδιά τους.

- Οργανισμούς και ιδρύματα δημόσια και ιδιωτικά, όπως σχολειά και βιβλιοθήκες, που επιδίωξη τους είναι να προστατεύσουν βασικά το κοινό στο οποίο απευθύνονται αλλά και τη διαδικασία ή τη λειτουργία την οποία καλούνται να επιτελέσουν.

- Επιχειρήσεις και εμπορικές εταιρίες, με στόχο κυρίως την προστασία των δικών τους συμφερόντων και της απόδοσης των οικονομικών δραστηριοτήτων τους.

- Κυβερνήσεις και κρατικοί οργανισμοί, όταν απειλείται η υπόσταση τους ως κέντρα εξουσίας ή τα δικαιώματα αυτών που αντιπροσωπεύουν.

- Δικαστές και νομοθέτες σαν οι κατά βάση αρμόδιοι σε μια ευνομούμενη πολιτεία.

1.2.3 Εφαρμογή του Αποκλεισμού

Μετά τον καθορισμό του ακαταλλήλου υλικού από αυτούς που επέλεξαν να εφαρμόσουν τον έλεγχο περιεχόμενου, ακολουθεί ο αποκλεισμός του. Αν και απόλυτα ακριβές φιλτράρισμα είναι σχεδόν αδύνατό να υπάρξει, υπάρχει μια ευρεία ποικιλία μεθόδων που χρησιμοποιείται για τον έλεγχο της ροής της ψηφιακής πληροφορίας. Τέτοιες μέθοδοι είναι η ανακατεύθυνση των χρηστών σε διακομιστές μεσολάβησης, η αλλαγή δρομολόγησης στα πακέτα δεδομένων που προορίζονται για μια συγκεκριμένη IP διεύθυνση που περιέχεται στην «μαύρη» λίστα, η υποκλοπή, η παρακολούθηση συνομιλιών, οι απαγορευτικές πολιτικές τιμολόγησης, η εισβολή (hacking) σε ιστοσελίδες και διάδοση κακόβουλου λογισμικού, οι επιθέσεις άρνησης υπηρεσιών(DoS), η διακοπτόμενη παροχή διασύνδεσης κ.α..

Ανάμεσα στις επιλογές αποκλεισμού διακρίνονται και λιγότερο τεχνικές και περισσότερο κοινωνικές μέθοδοι. Η τροποποίηση της νομοθεσίας ώστε να λειτουργεί εκφοβιστικά, η αυστηρή αστυνόμευση, η φυσική επέμβαση και πολλές φορές η διακοπή λειτουργίας των εξυπηρετητών που φιλοξενούν το περιεχόμενο, είναι κάποιοι από τους μηχανισμούς ελέγχου που σχετίζονται περισσότερο με την επιθυμία για φιλτράρισμα παρά με την τεχνολογία που θα εφαρμοστεί.

Οι περισσότερες μορφές φιλτραρίσματος είναι δύσκολο να ανιχνευθούν τεχνικά, έτσι ο χρήστης μπορεί να μην γνωρίζει καν ότι λογοκρίνεται. Οι περισσότεροι πάροχοι δεν έχουν την ικανότητα να εφαρμόσουν αποκλεισμό σε επίπεδο ατόμου ή μοναδικής IP διεύθυνσης [90].

Οι μηχανισμοί αποκλεισμού περιεχομένου είναι πολλές φορές αρκετά πολύπλοκοι, παρόλα αυτά συχνά μπορούν να παρακαμφθούν με μικρή σχετικά προσπάθεια. Υπάρχουν διάφοροι λόγοι για αυτό, ο πιο βασικός είναι ότι το Internet έχει σχεδιαστεί για να είναι αποκεντρωμένο, με ενσωματωμένη τη δυνατότητα εξασφάλισης της ροής των δεδομένων πέρα από τυχόν εμπόδια.

Σημαντικό είναι να σημειωθεί ότι πολλές φορές οι προσπάθειες ελέγχου λειτουργούν με μειωμένη αποτελεσματικότητα, είτε αποκλείοντας περιεχόμενο που δε θα έπρεπε, δείχνοντας «υπερβάλλοντα ζήλο» (over-blocking), είτε αποτυγχάνοντας να αποκλείσουν περιεχόμενο ακατάλληλο με βάση τα τεθέντα κριτήρια (under-blocking). Αυτό είναι και το βασικό πρόβλημα αλλά και η πρόκληση για τις τεχνολογίες ελέγχου πρόσβασης[13].

1.3 Διαβούλευση, Κίνητρα και Προκλήσεις

Υπάρχουν πολλά κίνητρα για τη λογοκρισία στο Διαδίκτυο, για αυτό και μπορεί να πάρει διάφορες μορφές, συμπεριλαμβανομένης της πολιτικής καταστολής αντιφρονούντων και ακτιβιστών για τα ανθρώπινα δικαιώματα, θρησκευτικού περιεχομένου ελέγχους που αναστέλλουν τη διάδοση ιδεών που θεωρούνται αιρετικές ή ιερόσυλες, προστασία της πνευματικής ιδιοκτησίας, πολιτιστικούς περιορισμούς που υπάρχουν ως μέρος της καταπίεσης εθνικών μειονοτήτων (π.χ. άρνηση να επιτρέψει σε κυβερνητικές ιστοσελίδες ορισμένες γλώσσες) ή σεξουαλικές μειονότητες (ομοφυλόφιλοι). Συνήθως, οι κυβερνήσεις που επιδιώκουν να επιβάλουν λογοκρισία δεν χρησιμοποιούν τόσο τη δικαιολογία της προστασίας της δημόσιας ηθικής από κινδύνους, όπως η πορνογραφία ή τα τυχερά παιχνίδια, αλλά την καταπολέμηση της τρομοκρατίας [90].

Η συζήτηση για το φιλτράρισμα στο Διαδίκτυο δεν μπορεί να περιοριστεί σε ένα συγκεκριμένο θέμα, είναι πολύπλοκή όπως η τεχνολογία που χρησιμοποιείται. Υπάρχουν πολλά διαφορετικού είδους θέματα τα οποία πρέπει να συζητηθούν μια που οι προκλήσεις που αντιμετωπίζουν οι φορείς χάραξης των πολιτικών ελέγχου είναι πολυδιάστατες.

Υπάρχουν πολλοί λόγοι για τους οποίους πιστεύει (ή σε ορισμένες περιπτώσεις ελπίζει), σήμερα η κοινωνία ότι οι απόπειρες αποκλεισμού περιεχομένου μπορούν να καθησυχάσουν κάποιες σημαντικές κοινωνικές ανησυχίες, που κάποιες άλλες προσεγγίσεις δεν φαίνεται να τις αντιμετωπίζουν με επιτυχία. Πολλές διαφορετικές οντότητες σήμερα εφαρμόζουν τον αποκλεισμό, με ένα ευρύ φάσμα υλικού να είναι ο στόχος της εν λόγω εφαρμογής. Οι

προσπάθειες μπλοκαρίσματος του Διαδικτύου μπορούν να προσεγγιστούν με πολλούς διαφορετικούς τρόπους, ανάλογα με ποιος θα είναι ο επιθυμητός στόχος τους. Αρκετές χώρες έχουν ήδη υιοθέτησε τέτοιου είδους συστήματα.

Το Διαδίκτυο είναι ένα τεράστιο περίπλοκο δίκτυο δικτύων, με μεγάλο πλήθος συσκευών υλικοτεχνικής υποδομής, πρωτόκολλων και υπηρεσιών. Το πρώτο βήμα στην προσπάθεια ελέγχου της πρόσβασης με βάση το περιεχόμενο είναι η επιλογή της θέσης εγκατάστασης του. Ένα δεύτερο βασικό μέλημα είναι να καθοριστεί ποιος είναι αυτός που επιλέγει τι θα αποκλειστεί, διαβαθμίζοντας τη δυνατότητα αυτή ανάμεσα στους διαφορετικούς χρηστές και οργανισμούς. Ένα ευρύ φάσμα περιεχομένου μπορεί να προκαλέσει διαφορετικές ανησυχίες σε διαφορετικές κοινωνίες και κάθε μέτρο αποκλεισμού είναι αναγκαίο να περιγράφει την ποικιλία του περιεχομένου που στοχεύει. Ο αποκλεισμός περιεχομένου στο Διαδίκτυο εφαρμόζεται είτε στους παραγωγούς είτε στους καταναλωτές του παράνομου περιεχομένου και έχει διαφορετικά επίπεδα αποτελεσματικότητας, ανάλογα με την επιλογή αυτή.

Το φιλτράρισμα στο Διαδίκτυο συζητείται ως μια τεχνική λύση σε σχέση με ένα ευρύ φάσμα παράνομων δραστηριοτήτων. Σε ένα μεγάλο βαθμό, χωρίς αυτό να είναι απαραίτητο, οι πράξεις αυτές ποινικοποιούνται στη χώρα που προτίθεται να εφαρμόσει ή έχει ήδη υλοποιήσει τη τεχνολογία ελέγχου, αλλά δεν ποινικοποιούνται πάντα με τον ίδιο τρόπο στη χώρα όπου το περιεχόμενο φιλοξενείται. Η παιδική πορνογραφία είναι μια από αυτές τις κατηγορίες περιεχομένου που εμπίπτει στις διατάξεις ποινικού δικαίου.

Η επιβολή του αποκλεισμού είναι δύσκολή μια που συχνά υλικό διατίθενται νόμιμα από εξυπηρετητές στο εξωτερικό. Αυτή είναι μια άμεση συνέπεια των διαφορετικών εθνικών προτύπων που υφίστανται σε σχέση με την δημοσίευση περιεχομένου. Είναι σα να γίνεται προσπάθεια να διατηρηθούν εθνικά πολιτιστικά πρότυπα στην εποχή της παγκόσμιας διαδικτυακής ενοποίησης [13].

1.3.1 Λόγοι που Προκαλούν τον Αποκλεισμό Περιεχομένου

Ένας βασικός λόγος που οδηγεί στον έλεγχο του περιεχομένου είναι η απουσία οργάνων ελέγχου στο Διαδίκτυο. Δεδομένου ότι το Διαδίκτυο έχει πρωταρχικά σχεδιαστεί με βάση μια αποκεντρωμένη αρχιτεκτονική, ευέλικτο σε σφάλματα και δυσλειτουργίες, είναι ανθεκτικό στις προσπάθειες εξωτερικού ελέγχου. Οι δυνατότητες αποκλεισμού περιεχομένου είναι κάτι το οποίο δε είχε σίγουρα ληφθεί υπόψη στον αρχικό σχεδιασμό του.

Η διεθνής διάσταση του Διαδικτύου αποτελεί μια ακόμη αφορμή για αυτούς που θέλουν κατά καιρούς να ελέγξουν την ροή της πληροφορίας σε αυτό. Η διεθνής συνεργασία που βασίζεται στις αρχές της παραδοσιακής αμοιβαίας δικαστικής συνδρομής, είναι συχνά πολύ αργή και χρονοβόρα. Οι τυπικές προϋποθέσεις και ο χρόνος που απαιτείται για τη συνεργασία ξένων μεταξύ τους υπηρεσιών επιβολής του νόμου, συχνά εμποδίζουν τις απαιτούμενες έρευνες να εξελιχθούν αποτελεσματικά. Οι απόπειρες αποκλεισμού περιεχομένου είναι δυνατό να θεωρηθούν κάποιες φορές ως μια προσπάθεια αποτελεσματικότερης δράσης, ακόμα και σε αυτές τις περιπτώσεις όπου οι περιορισμοί της τρέχουσας διεθνούς συνεργασίας εμποδίζουν τη λήψη μέτρων έγκαιρα.

Η μείωση της σημασίας των υποδομών που φιλοξενούν περιεχόμενο στα όρια της επικυριαρχίας μια χώρας είναι ένα σημαντικό κίνητρο επιβολής μηχανισμών φιλτραρίσματος. Η δημοσίευση περιεχομένου που είναι απόλυτα νόμιμο σε μια χώρα μπορεί να είναι εγκληματική πράξη σε κάποια άλλη. Η προσπάθεια επομένως, να αποκλειστεί περιεχόμενο μπορεί να χαρακτηριστεί ως πράξη επαναπροσδιορισμού της εδαφικής κυριαρχίας και του κρίσιμου πολιτικού, κοινωνικού, οικονομικού και πολιτισμικού ζωτικού χώρου, όπου οι κυβερνήσεις επιδιώκουν να εξασφαλίσουν ότι εφαρμόζονται τα εθνικά πρότυπα σε σχέση με το παγκοσμιοποιημένο περιεχόμενο που είναι διαθέσιμο στους χρήστες του Διαδικτύου στο εσωτερικό της χώρας [13].

Το κίνητρο για την επιλογή του ελέγχου της πληροφορίας που διακινείται στο Διαδίκτυο, συνδέεται άμεσα με το ποιος τον εφαρμόζει. Αυτό μπορεί να είναι κοινωνικό ή ηθικό, όπως στην περίπτωση των γονιών που επιθυμούν την προστασία των παιδιών τους. Υπάρχει περίπτωση να είναι πολιτικό όταν αφορά κυβερνήσεις που επιδιώκουν τη διατήρηση της έννομης τάξης, όπως ορίζεται κάθε φορά με τα δικά τους κριτήρια. Στην περίπτωση εξάλλου των επιχειρήσεων, κίνητρο μπορεί να αποτελέσει η διαφύλαξη της παραγωγικότητας των εργαζομένων τους, ο περιορισμός της κατασπατάλησης πόρων όπως το εύρος ζώνης, η διασφάλισης της προστασίας ευαίσθητων εταιρικών δεδομένων και αποφυγή νομικών επιπλοκών όταν υπάρχει παράνομη δραστηριότητα εργαζομένων [76].

1.3.2 Ποιον Αφορά ο Αποκλεισμός Περιεχομένου

Ο αποκλεισμός του παράνομου περιεχομένου στο Διαδίκτυο δεν μπορεί να θεωρηθεί μόνο ως ένα μέσο που σχετίζεται με τους παραβάτες που διαθέτουν το περιεχόμενο (παραγωγοί), αλλά και ως το μέσο που αποσκοπεί στην αποτροπή του χρήστη από τη λήψη του παράνομου περιεχομένου (καταναλωτές).

Από την πλευρά του παραγωγού ή του παρόχου του παράνομου περιεχομένου το Διαδίκτυο έχει γίνει ένα σημαντικό εργαλείο για τη διανομή ακατάλληλου υλικού, όπως για παράδειγμα υλικού παιδικής πορνογραφίας, καθώς προσφέρει μια σειρά από πλεονεκτήματα για τους δράστες που κάνουν την αντιμετώπιση τους δύσκολη. Η διευκόλυνση στην διανομή του παράνομου υλικού, για παράδειγμα στην περίπτωση της παιδικής πορνογραφίας, είναι ανάλογη με τη διευκόλυνση στην παράγωγή του, που προσφέρεται από τη σύγχρονη ψηφιακή φωτογραφική μηχανή και την ψηφιακή βιντεοκάμερα. Ο λόγος για την εφαρμογή της τεχνολογίας φιλτραρίσματος είναι επομένως παρόμοιος με τους λόγους της ποινικοποίησης της ανταλλαγής υλικού παιδικής πορνογραφίας, δηλαδή να μειωθεί η εγκληματική δραστηριότητα και να προστατευτούν τα παιδιά.

Ο καταναλωτής του παράνομου περιεχομένου έχει και αυτός ευθύνη. Εκτός από την παραγωγή, έκδοση και διάθεση υλικού παιδικής πορνογραφίας, ένας σημαντικός αριθμός χωρών ποινικοποιεί την κατοχή υλικού παιδικής πορνογραφίας. Οι ζήτηση για το εν λόγω υλικό θα μπορούσε να προωθήσει την παραγωγή του δημιουργώντας έναν κύκλο με βάση το νόμο της προσφοράς και της ζήτησης. Επιπλέον, μια σειρά από χώρες προχωρούν στην ποινικοποίηση όχι μόνο της κατοχής υλικού παιδικής πορνογραφίας αλλά και της απλή πρόσβασης σε τέτοιο περιεχόμενο.

Παρά το γεγονός ότι το φιλτράρισμα στο Διαδίκτυο δεν αφαιρεί το περιεχόμενο στην πηγή του, επιτυγχάνει την παρεμπόδιση των όποιων βλαβερών συνεπειών από την επικοινωνία του. Η επιτυχία αυτή εξαρτάται από την αποτελεσματικότητα των τεχνολογιών αποκλεισμού, τα κίνητρα και το επίπεδο γνώσης του χρήστη [13].

1.4 Συμπεράσματα

Από όλους τους μύθους που σχετίζονται με το Διαδίκτυο, αυτός που παρουσιάζει την μεγαλύτερη πρόκληση είναι ότι πρόκειται για ένα εγγενώς απελευθερωτικό εργαλείο, μια υποδομή που αναπόφευκτα προωθεί τη δημοκρατία δίνοντας φωνή σε όσους δεν έχουν πολιτική εξουσία και με τον τρόπο αυτό υπονομεύει τις αυταρχικές και καταπιεστικές κυβερνήσεις. Με βάση νεωτεριστικές θεωρίες ανάπτυξης, η βελτίωση του επιπέδου εκπαίδευσης και οι περισσότερες ευκαιρίες πρόσβασης σε πληροφορίες οδηγούν αναπόφευκτα σε μια απελευθέρωση της δημόσιας σφαίρας μέσω ενός καλά ενημερωμένου κοινού που αυτοκαθορίζεται πολιτικά και μορφωτικά. Στις Δυτικές ιδιαίτερα κοινωνίες έχει γίνει πεποίθηση

ότι η παγκοσμία κοινότητα των ανθρώπων που καθημερινά πλοηγούνται στο Διαδίκτυο πρέπει να είναι αυτοδιοικούμενη χωρίς την παρέμβαση οπουδήποτε κράτους [90]. Το Διαδίκτυο έχει ριζικά αλλάξει τον τρόπο με τον οποίο διαδίδεται η πληροφορία σε ολόκληρο τον κόσμο, προσφέροντας άμεση πρόσβαση σε σχεδόν κάθε είδος ψηφιακό πόρο. Δυστυχώς, αυτό ισχύει εξίσου, τόσο για το νόμιμο όσο και για το παράνομο περιεχόμενο [26].

Το Διαδίκτυο χτίστηκε εξ' αρχής ως ένα αποκεντρωμένο δίκτυο με την ικανότητα να αναδρομολογείται, ξεπερνώντας φυσικές καταστροφές και προσπάθειες ελέγχου. Αυτό αποτελεί μια σημαντική πρόκληση για εκείνους που επιδιώκουν την αστυνόμευση του, ακόμη και στην περίπτωση της διακίνησης παράνομου υλικού. Οι βασικοί υποστηρικτές του φιλτραρίσματος περιεχομένου στο Διαδίκτυο είναι συνήθως κυβερνήσεις, αν και μερικοί πάροχοι της υπηρεσίας έχουν εφαρμόσει εθελοντικά σχετικά προγράμματα. Η συντριπτική πλειοψηφία των χωρών έχουν νόμους κατά εγκλημάτων, όπως η παιδική πορνογραφία και η συκοφαντική δυσφήμιση. Όσες κυβερνήσεις προσπάθησαν ενεργά να αποκλείσουν αυτό το είδος της παράνομης λειτουργίας αντιμετώπισαν σημαντικά προβλήματα στην προσπάθεια τους να επιβάλουν νόμους στο Διαδίκτυο. Το Διαδίκτυο δεν έχει όρια νομικής δικαιοδοσίας, έτσι ώστε είναι πολλές φορές αδύνατο για τις υπηρεσίες επιβολής του νόμου να επέμβουν αποτελεσματικά εναντίων των δικτυακών τόπων που τον παραβιάζουν [26].

Οι τεχνικές που εφαρμόζονται για τον έλεγχο περιεχομένου καλύπτουν ένα ευρύ φάσμα τεχνολογιών, αλλά και κοινωνικών και πολιτικών επιλογών. Η αποτελεσματικότητα τους ποικίλει, όπως ποικίλουν και οι τρόποι παράκαμψης τους .

Κεφάλαιο 2
Το Διαδίκτυο Σήμερα - Ένα Τοπίο που Συνεχώς Αλλάζει

Σε μια επισκόπηση των τεχνολογιών που αποσκοπούν να δώσουν αποτελεσματικές λύσεις σε αυτούς που επιδιώκουν να ελέγξουν την πρόσβαση στο διαδίκτυο με βάση το περιεχόμενο, είναι σημαντικό να προσδιοριστούν τα σύγχρονα χαρακτηριστικά αυτού του τόσο δυναμικά μεταβαλλόμενου μέσου. Κατά τη διάρκεια των τελευταίων ετών το Διαδίκτυο αναδείχθηκε ως το κυρίαρχο μέσο επικοινωνίας, παρέχοντας μια πλατφόρμα που επιτρέπει στον κάθε χρήστη να παράγει αλλά και να δημοσιεύσει εύκολα, γρήγορα και με χαμηλό κόστος, το δικό του περιεχόμενο. Οι πρώτες βασικές τεχνολογίες επικοινωνίας όπως το ηλεκτρονικό ταχυδρομείο, τα άμεσα μηνύματα (instant messaging – IM) και οι ομάδες συζήτησης (newsgroups) εξελίχθηκαν, συμπεριλαμβάνοντας βασισμένα στον Παγκόσμιο Ιστό (web) εργαλεία με φιλικό περιβάλλον διεπαφής, τα οποία προσελκύουν συνεχώς περισσότερους χρήστες. Η αύξηση των ευρυζωνικών συνδέσεων έχει διευκολύνει την διάδοση πολυμεσικού περιεχομένου όπως αρχεία ήχου, εικόνας και βίντεο και την σε πραγματικό χρόνο επικοινωνία. Επιπλέον αναδείχτηκαν ένα πλήθος από

βασισμένα στο web εργαλεία όπως τα κοινωνικά δίκτυα, τα ιστολόγια και τα online (σε απευθείας σύνδεση) παιχνίδια, τα οποία επιτρέπουν μεγαλύτερη διαδραστικότητα μεταξύ των χρηστών του Διαδικτύου [01].

Τα οφέλη που προκύπτουν από αυτή τη ραγδαία εξέλιξη της επικοινωνίας και του διαμοιρασμού της πληροφορίας, συνδυάζονται με νέες προκλήσεις και ενίοτε κινδύνους, για τους χρήστες και την κοινωνία γενικότερα. Σε αυτές τις προκλήσεις καλείται πολλές φορές να δώσει απάντηση η τεχνολογία ελέγχου της πρόσβασης με βάση το περιεχόμενο, προσαρμοζόμενη στο νέο δυναμικά μεταβαλλόμενο περιβάλλον.

2.1 Διείσδυση του Διαδικτύου

Τα τελευταία χρόνια η διείσδυση του Διαδικτύου τείνει να προσεγγίσει τη διείσδυση της τηλεόρασης και της τηλεφωνίας, στις βιομηχανικές τουλάχιστον χώρες. Οι συσκευές με δυνατότητα διασύνδεσης στο Internet, συμπεριλαμβανομένων προσωπικών συσκευών, οχημάτων και οικιακών συσκευών δεν είναι κάτι σπάνιο [86]. Περισσότερα από δυόμιση δισεκατομμύρια άνθρωποι, δηλαδή ένα ποσοστό διείσδυσης άνω του 35%, έχουν σήμερα την δυνατότητα να συνδεθούν με κάποιον τρόπο στο Διαδίκτυο. Το ποσοστό διείσδυσης ποικίλει σημαντικά από χώρα σε χώρα και γενικότερα από περιοχή σε περιοχή, αντικατοπτρίζοντας σε μεγάλο βαθμό την τεχνολογική αλλά και οικονομική και κοινωνικοπολιτική ανάπτυξη της [54].

Οι χώρες με τη μεγαλύτερη διείσδυση είναι η Ισλανδία και η Νορβηγία όπου σχεδόν όλος ο πληθυσμός έχει πρόσβαση στο Internet. Η περιοχή του κόσμου που παρουσιάζει κατά μέσο όρο τα μεγαλύτερα ποσοστά είναι η Βόρεια Αμερική, πατρίδα αλώστε των σημαντικότερων ίσως σήμερα παρεχόμενων διαδικτυακών υπηρεσιών [54].

Η πρόσβαση στο Διαδίκτυο είναι ιδιαίτερα διαδεδομένη στην Ευρωπαϊκή Ένωση μια που τους τελευταίους μήνες του 2012, περισσότερο από τα τρία τέταρτα των νοικοκυριών εμφανιζόταν να έχουν αυτή τη δυνατότητα. Παρόλα αυτά και εδώ παρουσιάζεται μεγάλη ανομοιογένεια με χώρες όπως η Ολλανδία, η Δανία και η Σουηδία να έχουν ένα ποσοστό διείσδυσης άνω του 90% ενώ άλλες, όπως η χώρα μας, μόλις τον τελευταίο καιρό να ξεπερνούν το 50%. Η Ελλάδα παρότι παρουσιάζει συνεχώς έναν από τους μεγαλύτερους ρυθμούς αύξησης του ποσοστού του πληθυσμού που έχει πρόσβαση σε διαδικτυακές υπηρεσίες, εξακολουθεί να έχει να καλύψει σημαντικό δρόμο προκειμένου να προσεγγίσει τις υπόλοιπες αναπτυγμένες χώρες [10, 83].

Όταν γίνεται αναφορά στο τμήμα του πληθυσμού μιας χώρας που έχει πρόσβαση στο Διαδίκτυο, η χρήση μόνο ποσοστών σε κάποιες περιπτώσεις δεν αρκεί, αλλά απαιτείται η μελέτη απόλυτων μεγεθών. Έτσι αν και στην Κίνα το ποσοστό διείσδυσης κυμαίνεται περίπου στο 40%, με ιδιαίτερα αυξητικές τάσεις βέβαια, το νούμερο αυτό αντιπροσωπεύει περίπου μισό δισεκατομμύριο χρήστες, σχεδόν το ένα πέμπτο του παγκόσμιου πληθυσμού του κυβερνοχώρου, γεγονός που την καθιστά σημαντικό παράγοντα στις εξελίξεις του. Στην Κίνα άλλωστε, είναι εγκατεστημένος ο μεγαλύτερος και σημαντικότερος από κάθε άποψη μηχανισμός ελέγχου περιεχομένου στον κόσμο [20].

2.1.1 Ανήλικοι Χρηστές του Διαδικτύου

Στην μελέτη των ποσοστών διείσδυσης της χρήσης του Internet θα πρέπει να συνεκτιμηθούν και άλλα ποιοτικά χαρακτηριστικά, ιδιαίτερα όταν αναφερόμαστε στον έλεγχο προσπέλασης με βάση το περιεχόμενο. Ένα από αυτά τα χαρακτηριστικά είναι η διείσδυση ανά ηλικιακή ομάδα. Τα ποσοστά διείσδυσης στου ανήλικους χρήστες αυξάνονται συνεχώς σε όλο τον κόσμο, φτάνοντας σε ορισμένες ηλικίες και περιοχές, όπως οι έφηβοι στον δυτικό κόσμο, σχεδόν σε απόλυτη συμμετοχή. Ακόμη σημαντική παράμετρος είναι η συνεχώς μικρότερη ηλικία αυτών που για πρώτη φορά έχουν πρόσβασης το διαδίκτυο. Με βάση το γεγονός, ότι τα παιδιά είναι η κατεξοχήν ευαίσθητη ομάδα που χρειάζεται προστασία από την όποια παραβατικότητα στο Internet, τα δεδομένα αυτά παίζουν σημαντικό ρόλο στην επιλογή και την εφαρμογή του φιλτραρίσματος στο περιεχόμενο στο οποίο έχουν πρόσβαση [01, 55].

2.1.2 Περισσότερος Χρόνος Online – Διαφορετικές Συνήθειες

Όχι μόνο περισσότεροι άνθρωποι συνδέονται καθημερινά στο Διαδίκτυο, αλλά περνούν και περισσότερο χρόνο σε αυτό. Για μεγάλο κομμάτι του παγκόσμιου πληθυσμού η διασύνδεση είναι μια καθημερινότητα η οποία πολλές φορές έχει διάρκεια αρκετών ωρών [01].

Οι κοινωνικές, οικονομικές, πολιτικές, και πολιτισμικές συνθήκες καθορίζουν συχνά και το περιεχόμενο ή τις υπηρεσίες που ένας χρήστης αναζητά από το Διαδίκτυο. Οι online συνήθειες διαφέρουν από περιοχή σε περιοχή και είναι αυτές που σε κάποιο βαθμό μπορούν να καθορίσουν τη στρατηγική του ενδεχόμενου ελέγχου. Έτσι ενώ για παράδειγμα στη Γαλλία υπάρχει ένα μεγάλο ποσοστό διείσδυση της χρήσης του Internet, της τάξης του 80%, μόνο ένα μικρό σχετικά ποσοστό των χρηστών, 38%, διαβάζει εφημερίδες και ενημερώνεται κυρίως από

το Διαδίκτυο, τη στιγμή που το σχετικό ποσοστό σε χώρες όπως η Λιθουανία και η Εσθονία ξεπερνάει το 90% [10].

2.2 Βελτίωση Συνθηκών Διασύνδεσης

Το Διαδίκτυο γίνεται συνεχώς ταχύτερο και περιέχει μεγαλύτερη ποσότητα πληροφορίας. Οι τρόποι και οι συσκευές διασύνδεσης βελτιώνονται δίνοντας μεγαλύτερη ευελιξία. Παρόλα αυτά το μέσο κόστος σύνδεσης συνεχώς μειώνεται [56], καθιστώντας το Internet όλο και πιο ελκυστικό και εύχρηστο για τον τελικό χρήστη.

2.2.1 Αύξηση Ταχύτητας Διασύνδεσης και Όγκου Δεδομένων

Αν και οι ταχύτητες σύνδεσης του Διαδικτύου επιβραδύνθηκαν συγκυριακά, εντός του 2012, η μέση παγκόσμια ταχύτητα σύνδεσης κατά το τρίτο τρίμηνο του 2012 διαμορφώθηκε στα 2,8 Mbps. Η Νότια Κορέα είναι η χώρα με την μεγαλύτερη μέση ταχύτητα παγκοσμίως (14,7 Mbps), ακολουθούμενη από την Ιαπωνία (10,7 Mbps) και το Χονγκ Κονγκ (8,9 Mbps). Στην Ελλάδα, η μέση ταχύτητα ήταν 4 Mbps και ήταν η δεύτερη χαμηλότερη στην Ευρώπη, μετά την Ιταλία (3,9 Mbps) [55].

Σε παγκόσμιο επίπεδο, η εφαρμογή υψηλών ευρυζωνικών ταχυτήτων σύνδεσης (άνω των 10 Mbps) αυξήθηκε 8,8% κατά μέσο όρο στο τρίτο τρίμηνο του 2012, ενώ η υιοθέτηση απλών ευρυζωνικών ταχυτήτων (άνω των 4 Mbps) αυξήθηκε κατά 4,8%, με αποτέλεσμα η ευρυζωνική διείσδυση στον παγκόσμιο πληθυσμό να διαμορφωθεί σε 11% και 41% αντίστοιχα [94]. Σε ορισμένες χώρες, όπως η Νότια Κορέα και η Ιαπωνία, οικιακές συνδέσεις της τάξης των 100 megabit ή 1 gigabit είναι πλέον συνηθισμένες, ενώ σε όλο και περισσότερες χώρες δημιουργούνται υποδομές για «fiber to the home» (οπτική ίνα στο σπίτι) συνδέσεις, με ταχύτητες ως 1 gigabit.

Λόγω της κατανεμημένης φύσης του Διαδικτύου, δεν υπάρχει ένα ενιαίο σημείο μέτρησης για τη συνολική κίνηση σε αυτό. Παρόλα αυτά, δεδομένα κίνησης από διάφορα δημόσια σημεία ροής της πληροφορίας, μπορούν να δώσουν μια ένδειξη του όγκου των δεδομένων στο Διαδίκτυο Έτσι προκύπτει ότι παράλληλα με τη ταχύτητα διασύνδεσης αυξάνει και ο συνολικός όγκος της διακινούμενης πληροφορίας στο Διαδίκτυο, ξεπερνώντας στα τέλη του 2011 τα 20 PetaByte ανά μήνα [14].

2.2.2 Μεγαλύτερη Ποικιλία Συσκευών Διασύνδεσης

Τα τελευταία χρόνια οι συσκευές που χρησιμοποιούνται για την πρόσβαση στο Διαδίκτυο έχουν αλλάξει. Ενώ στο παρελθόν η πλειοψηφία των χρηστών συνδεόταν στο Διαδίκτυο μέσω επιτραπέζιων (desktop) ή φορητών (laptop) προσωπικών υπολογιστών, αυξάνεται συνεχώς ο αριθμός αυτών που έχουν πρόσβαση μέσω άλλων, κυρίως φορητών συσκευών, όπως κινητά τηλέφωνα, υπολογιστές παλάμης (PDA), ταμπλέτες (tablet computers) και κονσόλες παιχνιδιών [86]. Όσο το κόστος της μεταφοράς δεδομένων σε δίκτυα κινητής τηλεφωνίας με τεχνολογίες μεταγωγής πακέτων τρίτης ή και τέταρτης γενιάς (3G, 4G) μειώνεται παράλληλα με την αύξηση της ταχύτητας της, τόσο περισσότεροι χρήστες κάνουν την επιλογή της ασύρματης διασύνδεσης. Μια επιλογή που υποστηρίζεται και από την ευρύτατη αποδοχή πρωτοκόλλων ασύρματης δικτύωσης όπως το Wi-Fi και WiMAX. Αξιοσημείωτο είναι ότι το 2011 ήταν η πρώτη χρονιά που οι πωλήσεις των έξυπνων τηλεφώνων (smart phones), ξεπέρασαν αυτές των προσωπικών υπολογιστών [09].

2.3 Η Μεταβαλλόμενη Φύση της Κυκλοφορίας στο Διαδίκτυο

Η φύση του περιεχόμενου που κυκλοφορεί στο Διαδίκτυο έχει αλλάξει σημαντικά από τις αρχές του εικοστού πρώτου αιώνα. Ενώ αρχικά οι χρήστες του Διαδικτύου το χρησιμοποιούσαν κατά βάση για επικοινωνία μέσω ηλεκτρονικών μηνυμάτων και αναζήτηση πληροφοριών σε στατικές ιστοσελίδες, στην πορεία εξελίχθηκε σε ένα πιο δυναμικό μέσο επικοινωνίας, ενημέρωσης, κοινωνικοποίησης, ψυχαγωγίας και γενικότερα παροχής ποικίλων τύπων υπηρεσιών.

Από τη μια η καθιέρωση του web 2.0 [74], με το χρήστη του Διαδικτύου να λειτουργεί διαδραστικά, με συνεργασίες σε απευθείας σύνδεση και διαμοιρασμό πληροφοριών μέσα από εφαρμογές όπως τα κοινωνικά μέσα, τα wikis και τα ιστολόγια. Από την άλλη ή τάση προς τον Σημασιολογικό Ιστό (Semantic Web ή web 3.0) [57], όπου νέες τεχνολογίες και μέθοδοι επιτρέπουν στους υπολογιστές να αντιλαμβάνονται τη σημασία της πληροφορίας που διαχειρίζονται απελευθερώνοντας πλήθος δυνατοτήτων στο Διαδίκτυο για την πιο ευφυή εκμετάλλευση της πληροφορίας αυτής, δημιουργούν ένα σκηνικό όπου το περιεχόμενο που καλούνται να ελέγξουν οι τεχνολογίες φιλτραρίσματος αποκτά πολυδιάστατα και δυναμικά χαρακτηριστικά.

2.3.1 Κοινωνικά Μέσα (Social Media)

Τα κοινωνικά μέσα είναι αυτά που επιτρέπουν την αλληλεπίδραση μεταξύ των ανθρώπων μέσω της δημιουργίας και του διαμοιρασμού πληροφοριών και ιδεών σε εικονικές κοινότητες με την βοήθεια των δικτύων. Πρόκειται ουσιαστικά για μια ομάδα από διαδικτυακές εφαρμογές που επιτρέπουν τη δημιουργία και την ανταλλαγή περιεχόμενου, δημιουργημένου από τον χρήστη (user-generated). Τα μέσα αυτά βασίζονται σε φορητές και βασισμένες στον Παγκόσμιο Ιστό τεχνολογίες για τη δημιουργία άκρως διαδραστικών πλατφόρμων, μέσω των οποίων άτομα και κοινότητες μοιράζονται, συνδημιουργούν, συζητήσουν και τροποποιούν περιεχόμενο [88].

Οι πιο γνωστές κατηγορίες κοινωνικών μέσων είναι [71] :

- Τα κοινωνικά δίκτυα, που επιτρέπουν στους χρήστες να δημιουργήσουν προσωπικές ιστοσελίδες και στη συνέχεια να διασυνδεθούν με φίλους τους, επικοινωνώντας και διαμοιράζοντας πληροφορίες. Το μεγαλύτερο και πιο επιτυχημένο κοινωνικό δίκτυο στις μέρες μας είναι το Facebook.

- Τα ιστολόγια (blogs), τα διαδικτυακά δηλαδή ημερολόγια, όπου ο καθένας μπορεί να εκφράσει τις απόψεις του σε οποιαδήποτε θεματολογία επιθυμεί.

- Τα wikis, τους ιστότοπους που επιτρέπουν στους χρήστες να συνδιαμορφώσουν ένα κοινό κείμενο ή μια βάση δεδομένων, με χαρακτηριστικότερη περίπτωση τη Wikipedia την μεγαλύτερη on line εγκυκλοπαίδεια στο Διαδίκτυο.

- Τα φόρουμ (forum), ιστοθέσεις για απευθείας συζήτηση γύρω από συγκεκριμένα θέματα.

- Τα Podcast, την κατά αίτηση και εγγραφή συνήθως, διάθεση αρχείων βίντεο και ήχου από υπηρεσίες όπως το iTunes της εταιρίας Apple.

- Οι κοινότητες περιεχομένου, όπου ταξινομείται και διαμοιράζεται συγκεκριμένου είδους περιεχόμενο, όπως για παράδειγμα φωτογραφίες (Flickr, Instagram), βίντεο (You tube) κ.α..

- Τα μικροιστολόγια (micro blogging), ένας συνδυασμός κοινωνικών δικτύων και ιστολογίων όπου μικρού μεγέθους συνήθως, περιεχόμενο ενημερώνεται και διανέμεται σε μια τακτική βάση, με το Twitter να κυριαρχεί στο χώρο.

- Οι υπηρεσίες άμεσων μηνυμάτων (Instant Messaging – IM), αλλά και chat, αν και δεν αποτελούν την αιχμή της άμεσης επικοινωνίας μεταξύ των χρηστών, εξακολουθούν να παίζουν σημαντικό ρόλο στην παραγωγή πληροφορίας σε πραγματικό χρόνο.

- Τα On line παιχνίδια, τα οποία επιτρέπουν την διαδραστική επικοινωνία των διαφόρων παικτών μέσα από το περιβάλλον του παιχνιδιού, που πολλές φορές τους δίνει και τη δυνατότητα της σε πραγματικό χρόνο συνομιλίας.

2.3.2 Διαμοιρασμός Αρχείων Μέσω Ομότιμων Δικτύων

Ένα ομότιμο δίκτυο υπολογιστών (Peer to Peer ή P2P) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Με τα P2P δίκτυα δίνεται η δυνατότητα στους χρήστες να ανακτήσουν αρχεία πολυμέσων, όπως μουσική, ταινίες, παιχνίδια, χρησιμοποιώντας μόνο ένα λογισμικό P2P που αναζητά άλλους διασυνδεδεμένους υπολογιστές. Είναι γενικά αποδεκτό ότι η χρήση τέτοιων δικτύων ενώνει χρήστες από όλο τον κόσμο λειτουργώντας χωρίς λογοκρισία, ελέγχους ή φραγμούς προάγοντας τη βασική ιδέα της δημιουργίας του παγκοσμίου ιστού, που δεν είναι άλλη από την ελεύθερη διακίνηση ιδεών και τη δωρεάν παροχή υπηρεσιών και πληροφοριών.

Η απλή δομή, το μηδαμινό κόστος και η άναρχη ροή πληροφορίας είναι τα στοιχεία που καθιστούν τη λειτουργία των P2P δικτύων μοναδική. Η φιλοσοφία τους δίνει τη δυνατότητα στους συμμετέχοντες, της δημιουργίας δυναμικά αναπτυσσόμενων χώρων, το περιεχόμενο των οποίων καθορίζεται από τους ίδιους τους χρήστες.

Από την άλλη τα δίκτυα P2P καθιστούν δυνατή την αντιγραφή και διανομή αρχείων μεταξύ χρηστών, τα οποία προστατεύονται από πνευματικά δικαιώματα, όπως τραγούδια, ταινίες και λογισμικό, χωρίς τη συναίνεση του κατόχου των πνευματικών δικαιωμάτων. Η ευρεία χρήση των δικτύων P2P για αυτόν τον σκοπό συνετέλεσε ώστε τα δίκτυα να ταυτιστούν με έννοιες όπως «παρανομία» και να υποστούν πόλεμο τόσο τα ίδια και οι δημιουργοί τους, όσο και οι χρήστες τους [58].

Μια άλλη παράμετρος πολύ σημαντική, που δεν αφορά άμεσα τον έλεγχο του περιεχομένου, αφορά όμως την ομαλή λειτουργία των δικτύων, είναι το σημαντικό τμήμα του εύρους ζώνης που καταλαμβάνουν σήμερα τέτοιου είδους διασυνδέσεις.

2.3.3 Τηλεφωνία Μέσω Διαδικτύου (VoIP)

Η τηλεφωνία μέσω Διαδικτύου (Voice over IP) έχει γίνει μια πολύ δημοφιλής υπηρεσία. Υπάρχει ένα ευρύ φάσμα παροχής υπηρεσιών VoIP που κυμαίνονται από δωρεάν συνομιλία από υπολογιστή σε υπολογιστή, μέσω κάποιας εφαρμογής όπως το Skype, έως την εμπορική διάθεση της υπηρεσίας από παρόχους τηλεφωνίας που επιδιώκουν να μειώσουν το κόστος εκμεταλλευόμενοι τις διαδικτυακές υποδομές. Εξαιτίας της εκτεταμένης χρήσης της υπηρεσίας αυτής σήμερα, ο διακινούμενος όγκος πληροφορίας, όχι τόσο από πλευράς κατανάλωσης εύρους ζώνης όσο από πλευράς περιεχομένου, είναι σημαντικός και αποτελεί πρόκληση για τα συστήματα που έχουν σαν σκοπό να ελέγξουν την διακινούμενο στο Internet περιεχόμενο[86].

2.3.4 Οικονομικές Δραστηριότητες στο Διαδίκτυο

Είναι πολύ σημαντική η διείσδυση του Διαδικτύου σε τομείς που σχετίζονται με οικονομικές δραστηριότητες. Το ηλεκτρονικό εμπόριο (e-commerce), η αγοραπωλησία δηλαδή αγαθών και υπηρεσιών με την βοήθεια ηλεκτρονικών μέσων και οι διαδικτυακές τραπεζικές (e banking), χρηματιστηριακές και γενικότερα οικονομικές συναλλαγές συνθέτουν σήμερα μια οικονομία πολλών δισεκατομμυρίων ευρώ και μια ροή πληροφορίας πολλών δισεκατομμυρίων Byte [86].

Δύο βασικά χαρακτηριστικά της οικονομικής διαδικτυακής δραστηριότητας είναι καθοριστικά για την προσπάθεια ελέγχου του περιεχομένου που παράγεται από αυτήν. Είναι πολύ συνηθισμένο, αν όχι κανόνας, οι ηλεκτρονικές οικονομικές συναλλαγές να είναι κρυπτογραφημένες, γεγονός που καθιστά δύσκολη την επιθεώρηση και κατά συνέπεια τον έλεγχο, των δεδομένων που παράγονται κατά την εκτέλεση τους. Μια δεύτερη παράμετρος είναι η διεθνής τους διάσταση και οι επιπλοκές στις διεθνείς συναλλαγές που μπορεί να προκαλέσει οποιαδήποτε προσπάθεια περιορισμού τους [30].

2.3.5 Παραδοσιακά Μέσα Μαζικής Ενημέρωσης στο Διαδίκτυο

Όλα τα παραδοσιακά Μέσα Μαζικής Ενημέρωσης (ΜΜΕ), χρησιμοποιούν το Διαδίκτυο προκειμένου να αναμεταδοθούν, σύγχρονα ή ασύγχρονα σε ένα ευρύτερο κοινό. Οι περισσότερες εφημερίδες διαθέτουν πέρα από ιστότοπους, που λειτουργούν ως πύλες (portal) ενημέρωσης και ηλεκτρονικές εκδόσεις των εντύπων τους, που διανέμονται μέσω του Παγκόσμιου Ιστού. Το διαδικτυακό ραδιόφωνο δίνει τη δυνατότητα σε ραδιοφωνικούς σταθμούς να αναμεταδοθούν σε περιοχές που θα ήταν αδύνατη ή κάλυψη τους μέσω των ερτζιανών, αλλά και σε ακροατές να έχουν πρόσβαση στην άμεση ενημέρωση που παρέχεται από προγράμματα που εκπέμπονται σε απομακρυσμένα σημεία του πλανήτη. Η τηλεόραση μέσω του Διαδικτύου, είτε με την μορφή της ζωντανής αναμετάδοσης των προγραμμάτων (live streaming), είτε με τη μορφή μετάδοσης ετεροχρονισμένων (time shifting) προγραμμάτων είτε ακόμη με την μορφή των βίντεο κατά παραγγελία (video on demand), αποτελεί μια ακόμη πηγή δυναμικού, ελκυστικού και πολύ μεγάλου σε όγκο, περιεχομένου [59, 69] .

2.4 Cloud Computing

Το Cloud Computing είναι ο διαμοιρασμός μέσω των υποδομών του διαδικτύου και η χρήση και χρέωση ανάλογα με τη ζήτηση, υπολογιστικών πόρων, λογισμικού και πληροφοριών, που είναι συγκεντρωμένα σε μεγάλα και κατά περίπτωση απομακρυσμένα κέντρα δεδομένων. Ο όρος cloud (σύννεφο) χρησιμοποιήθηκε για πρώτη φορά στα τηλεπικοινωνιακά δίκτυα και το Διαδίκτυο, επειδή αυτά σχεδιάζονταν σε τεχνολογικά διαγράμματα που έμοιαζαν με clouds, υποδεικνύοντας περιοχές όπου οι πληροφορίες μετακινούνται και υποβάλλονται σε επεξεργασία. Ο μέσος χρήστης, ωστόσο, δεν χρειάζεται να γνωρίζει επακριβώς πώς συμβαίνει αυτό. Αυτό είναι άλλωστε, ένα από τα βασικά χαρακτηριστικά του Cloud Computing.

Ο καταναλωτής έχει θεωρητικά άπειρη διαθέσιμη υπολογιστική ισχύ, μπορεί να χρησιμοποιήσει μόνο όση χρειάζεται κάθε φορά και να χρεωθεί για αυτήν και μόνο. Αυτό του επιτρέπει να είναι πιο ευέλικτος και αποδοτικός στις όποιες δραστηριότητες του απαιτούν υπολογιστές, αφού του δίνει τη δυνατότητα να αποφύγει ριψοκίνδυνες προβλέψεις, όσο αφορά τους υπολογιστικούς πόρους που θα χρειαστεί, απομακρύνοντας τον από υπερεκτιμήσεις που οδηγούν σε σπατάλη κεφαλαίου ή υποεκτιμήσεις που οδηγούν σε επιχειρηματικούς κινδύνους και αποτυχίες.

Οι πάροχοι του Cloud Computing μπορούν να κερδίσουν μεγάλα ποσά απευθυνόμενοι σε μια τεράστια πελατειακή βάση. Οι μεγάλες εταιρίες του χώρου της πληροφορικής μεταβαίνοντας στη δραστηριότητα του παρόχου Cloud Computing επιτυγχάνουν καλύτερη εκμετάλλευση της ήδη εγκατεστημένης μεγάλης υλικοτεχνικής υποδομής τους. Επιπλέον αποκτούν δυνατότητα για μεγαλύτερη σχέση εμπιστοσύνης ή και δέσμευσης με τους πελάτες τους και καλύτερη προώθηση των όποιων άλλων προϊόντων τους. Αυτή όμως η απομακρυσμένη και κάποιες φορές συγκεντρωμένη σε μια τοποθεσία διαχείριση μπορεί να απολέσει κρίσιμη παράμετρο σε μια προσπάθεια ελέγχου του περιεχομένου [03].

2.5 Ο Κρυφός Ιστός

Ο Κρυφός ή Αόρατος Ιστός (επίσης γνωστός και ως Deep Web ή κρυμμένο Web) αναφέρεται στο περιεχόμενο του Παγκοσμίου Ιστού που δεν ανήκει στο Επιφανειακό Web (Surface Web), το οποίο δεικτοδοτείται από μία συνηθισμένη μηχανή αναζήτησης. Οι περισσότερες πληροφορίες του Web είναι θαμμένες μέσα σε ιστότοπους με δυναμικά παραγόμενες ιστοσελίδες και οι συνηθισμένες μηχανές αναζήτησης δεν μπορούν να τις εντοπίσουν. Το Deep Web είναι αρκετές τάξεις μεγέθους μεγαλύτερο από το επιφανειακό Web [84].

2.6 Συμπεράσματα

Μια ολοκληρωμένη θεώρηση των τεχνολογιών φιλτραρίσματος του Διαδικτύου απαιτεί μια αποτύπωση όλων των διαστάσεων των δυναμικών χαρακτηριστικών του· της εξάπλωσης του, του πλήθους και της ποιότητας των υπηρεσιών που παρέχει, αλλά κυρίως της φύσης και του όγκου του περιεχομένου του.

Σήμερα σε όλο τον κόσμο, πάνω από 2 δισεκατομμύρια άνθρωποι έχουν πρόσβαση στο Διαδίκτυο, χρησιμοποιώντας ένα πλήθος διαφορετικών και όλο και συχνότερα, φορητών συσκευών. Ο κάθε χρήστης, με τη βοήθεια των σύγχρονων διαδικτυακών υποδομών και εργαλείων είναι εν δυνάμει καταναλωτής, δημιουργός και διακινητής περιεχομένου. Ενός περιεχομένου που μπορεί να έχει διαφορετικές μορφές, κλιμακούμενης πολυπλοκότητας και ρευστότητας, από απλό κείμενο έως βίντεο ή και διαδραστικό on line παιχνίδι.

Οι νέες υπηρεσίες και κυρίως τα διαδικτυακά κοινωνικά μέσα, δρουν καθοριστικά στην κοινωνική ζωή, στην πολιτική δράση, στις καταναλωτικές συνήθειες, στο τρόπο διασκέδασης

ενημέρωσης και επικοινωνίας του σύγχρονου ανθρώπου. Ο όγκος, η πολυπλοκότητα της δομής και η βαρύτητα της πληροφορίας που παράγεται και διακινείται καθημερινά είναι συνεχώς αυξανόμενα. Το τοπίο αυτό αποτελεί σίγουρα πρόκληση για όποιον θέλει και πιστεύει πως μπορεί, να εφαρμόσει μηχανισμούς ελέγχου της πρόσβασης στο Διαδίκτυο με βάση το περιεχόμενο.

Κεφάλαιο 3
Τεχνολογίες Ελέγχου Προσπέλασης με Βάση το Περιεχόμενο

Ένα φίλτρο είναι μία «συσκευή ή ένα εργαλείο για την καταστολή ή την ελαχιστοποίηση κυμάτων ή ταλαντώσεων συγκεκριμένων συχνοτήτων», ενώ ένα φίλτρο περιεχομένου ορίζεται ως «ένα ή περισσότερα κομμάτια λογισμικού ή υλικού που συνεργάζονται για να αποτρέψουν τους χρήστες από το να έχουν πρόσβαση σε συγκεκριμένη πληροφορία στο Διαδίκτυο. Η φιλοδοξία των τεχνολογιών ελέγχου πρόσβασης είναι να επιτύχουν το διαχωρισμό της πληροφορίας που διακινείται στα δίκτυα σε «καλή» και «κακή» και να επιτρέψουν ή όχι τη μετάδοση της σε συγκεκριμένες ομάδες ανθρώπων [27]. Δύο είναι δηλαδή οι βασικές λειτουργίες τους [01]:

- Η αναγνώριση του περιεχόμενου.

- Ο αποκλεισμός του περιεχομένου.

Υπάρχουν διαφορετικές στρατηγικές για τον περιορισμό της πρόσβασης σε διαφόρους ιστότοπους οι οποίες είναι δυνατό να εφαρμοστούν σε διαφορετικές φυσικές θέσεις στην τοπολογία του δικτύου ξεκινώντας από το κορμό του σε εθνικό επίπεδο και καταλήγοντας στο τελικό χρήστη. Στη καρδιά ενός τέτοιου συστήματος υπάρχουν συχνά κατάλογοι με διευθύνσεις IP ή URL ή λέξεις ή κατηγορίες περιεχομένου και αλγόριθμοι οι οποίοι αντικατοπτρίζουν τις επιδιώξεις των σχεδιαστών ή των διαχειριστών του, οι οποίες συνήθως συνοψίζονται στο να:

- Περιορίσουν την πρόσβαση σε τόπους του Διαδικτύου που περιλαμβάνονται σε μια εσωτερική βάση του προϊόντος.

- Περιορίσουν την πρόσβαση σε τόπους του Διαδικτύου που περιλαμβάνονται σε βάση δεδομένων που διατηρείται εξωτερικά από το ίδιο το προϊόν.

- Περιορίσουν την πρόσβαση σε ιστοσελίδες που φέρουν αξιολογήσεις που έχουν ανατεθεί σε αυτές από τρίτους.

- Σαρώσουν το περιεχόμενο των δικτυακών τόπων που ένας χρήστης προσπαθεί να δει και να περιορίζουν την πρόσβαση με βάση την εμφάνιση συγκεκριμένων λέξεων, φράσεων ή εικόνων σε αυτούς.

Οι τεχνικές λύσεις που έχουν προταθεί για τη λογοκρισία/φιλτράρισμα του περιεχομένου χωρίζονται σε δύο κύριες κατηγορίες· αποτροπή πρόσβασης στο περιεχόμενο, κεντρικά από κάποιον οργανισμό και διαβάθμιση του περιεχομένου και αυτοέλεγχος με συμμετοχή του τελικού χρήστη [27]. Οι τεχνολογίες αυτές εφαρμόζονται στα διάφορα σταδία δημιουργίας διακίνησης και ανάγνωσης του περιεχομένου και λειτουργούν σε διαφορετικά επίπεδα του μοντέλου αναφοράς Ανοικτής Διασύνδεσης Συστημάτων (OSI). Η διάταξη των μηχανισμών ελέγχου μπορεί να βρίσκεται σε διαφορετικές θέσεις της διαδικασίας μεταφοράς της πληροφορίας και η λειτουργία τους να είναι είτε στατική, βασισμένη σε λίστες είτε δυναμική βασισμένη σε συνεχή ανάλυση [01].

Αξίζει να σημειωθεί ότι η ταχεία εξέλιξη της τεχνολογίας και ιδιαίτερα η κοινή χρήση ευρυζωνικών συνδέσεων στο Διαδίκτυο, καθώς και η δυναμική φύση του περιεχομένου του,

αποτελούν μια σοβαρή τεχνολογική πρόκληση για όποιον προσπαθεί να ελέγχει τη πρόσβαση πληροφοριών [93].

3.1 Θέση στην Τοπολογία Δικτύου

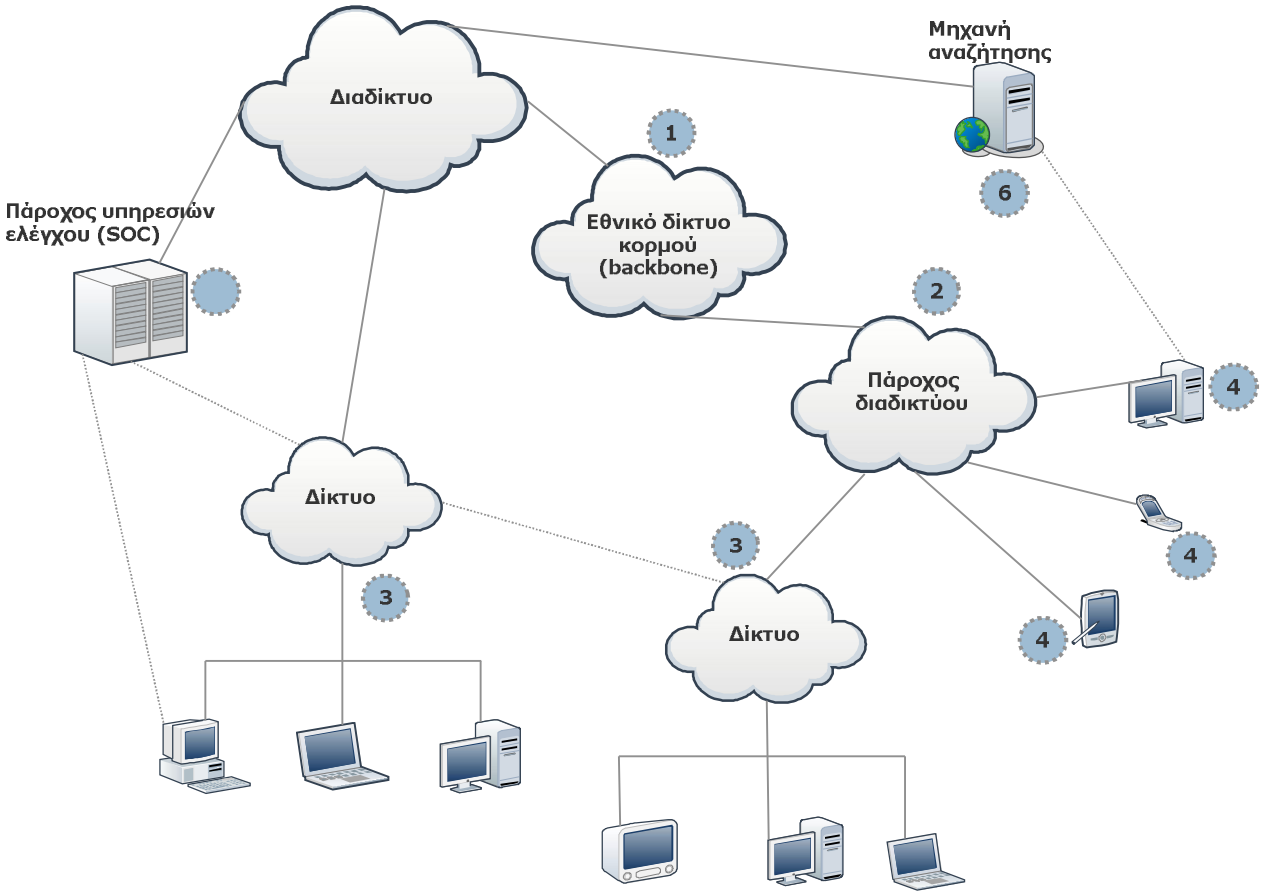
Υπάρχουν πολλές επιλογές για τη θέση ανάπτυξης του λογισμικού ή των συσκευών φιλτραρίσματος. Το λογισμικό μπορεί να εγκατασταθεί στην συσκευή η οποία χρησιμοποιείται για την πρόσβαση στο διαδίκτυο, όπως ένας προσωπικός υπολογιστής, ή να τοποθετηθεί σε απομακρυσμένη τοποθεσία, όπως οι εξυπηρετητές δικτύου μιας εταιρίας ή ενός παρόχου υπηρεσιών σταθερής ή κινητής επικοινωνίας. Ανάλογα, η υλικοτεχνική υποδομή φιλτραρίσματος, μπορεί να τοποθετηθεί στον τελικό χρήστη ή να είναι τμήμα του δικτυακού εξοπλισμού ενός οργανισμού.

Η επιλογή της τοποθεσίας λειτουργίας της τεχνολογίας φιλτραρίσματος καθορίζει, λίγο έως πολύ, τη μέθοδο αποκλεισμού που θα χρησιμοποιηθεί, τις δυνατότητες και τους περιορισμούς της, αλλά και τον τρόπο με τον οποίο μπορεί να παρακαμφθεί [01].

Η απόφαση σχετικά με τη θέση εξαρτάται από διάφορους παράγοντες, για παράδειγμα ένας γονέας που επιθυμεί να ελέγξει ένα ή δύο υπολογιστές στο σπίτι μπορεί να επιλέξει τοπική εγκατάσταση, διότι παρέχει στοχευμένο και πιο λεπτομερή έλεγχο για τις κατηγορίες που επιδιώκει να φιλτράρει. Ένας διαχειριστής ασφάλειας μιας επιχείρησης μπορεί να βρει ότι τα επιμέρους τοπικά φίλτρα προκαλούν μεγάλη διαχειριστική δαπάνη και επομένως να επιλέξει να εφαρμοστούν πολιτικές ελέγχου σε επίπεδο δικτύου οργανισμού. Οι πάροχοι συχνά παρέχουν προστιθέμενη αξία στους συνδρομητές τους, προσφέροντας υπηρεσίες φιλτραρίσματος περιεχομένου με ανάλογο τρόπο που προσφέρουν υπηρεσίες φιλτραρίσματος ηλεκτρονικού ταχυδρομείου.. Εν ολίγοις κάθε θέση έχει πλεονεκτήματα και μειονεκτήματα [87].

Παρότι η μέθοδος φιλτραρίσματος που χρησιμοποίει η κάθε εταιρία παροχής τέτοιου είδους υπηρεσιών είναι συνήθως εμπιστευτική, από εμπορικής απόψεως, πληροφορία, προϊόντα φιλτραρίσματος εγκατεστημένα σε διαφορετικούς κόμβους του δικτύου, μοιράζονται πολλά κοινά χαρακτηριστικά. Οι προμηθευτές φίλτρων συχνά παρέχουν παρόμοιες λύσεις για γονικούς έλεγχους σε οικιακούς υπολογιστές, σε διαχειριστές εταιρικών δικτύων ακόμη και σε διαχειριστές παρόχων υπηρεσιών Διαδικτύου. Σε όλες τις περιπτώσεις ο διαχειριστής (ή γονέας) μπορεί να καθορίσει την πρόσβαση στην πληροφορία. Προϊόντα που έχουν σχεδιαστεί για

οργανισμούς ή για παρόχους υπηρεσιών Διαδικτύου ενσωματώνουν δυνατότητες διαχείρισης της πρόσβασης στο Διαδίκτυο μεγάλου αριθμού χρηστών, αλλά επιτρέπουν διαχειριστικές δυνατότητες και σε ανεξάρτητους χρήστες [01].



Σχήμα 3.1: Θέσεις στο δίκτυο όπου εφαρμόζεται ο έλεγχος περιεχομένου: 1. Εθνικό δίκτυο κορμού 2. Πάροχος υπηρεσιών Διαδικτύου 3. Δίκτυο οργανισμού 4. Τελικός χρήστης 5. Τρίτα μέρη. 6. Μηχανές αναζήτησης.

3.1.1 Εθνικό Επίπεδο/Επίπεδο Χώρας

Το φίλτρο τοποθετείται σε επίπεδο εθνικού δικτύου κορμού (backbone), στις πύλες επικοινωνίας του δικτύου της χώρας με το παγκόσμιο Διαδίκτυο. Πολλές χώρες, όπως η Κίνα, η Σαουδική Αραβία κ.α., κάνουν την επιλογή φιλτραρίσματος περιεχομένου σε εθνικό επίπεδο. Ο καθορισμός του φιλτραρίσματος αποτελεί σε αυτήν την περίπτωση κεντρική πολιτική επιλογή. Οι χρήστες δεν έχουν καμία δυνατότητα προσαρμογής στους μηχανισμούς επιλογής του περιεχομένου οι οποίοι ελέγχονται ως προς την ασφάλεια και την απόδοση που παρέχουν κεντρικά από την κυβέρνηση [04].

3.1.2 Επίπεδο Παρόχου Υπηρεσιών Διαδικτύου (ISP)

Τα φίλτρα στην περίπτωση αυτή εγκαθίστανται στο επίπεδο του παρόχου της υπηρεσίας διασύνδεσης στο Διαδίκτυο (ISP), στις πύλες επικοινωνίας του με το εσωτερικό ή εξωτερικό δίκτυο [04], είτε υπό μορφή λογισμικού στους εξυπηρετητές του [01] επηρεάζοντας όλους του πελάτες του.

Σε διαφορές χώρες, όπως ο Καναδάς και το Ηνωμένο Βασίλειο, επίσημες ή ανεπίσημες κυβερνητικές πιέσεις οδηγούν τους παρόχους, σε «εθελοντικό» φιλτράρισμα περιεχομένου που σχετίζεται με παιδική κακοποίηση και πορνογραφία. Οι δικαστικές αρχές στη Γαλλία, τη Γερμανία και το Βέλγιο απαίτησαν από τους παρόχους να περιορίσουν την πρόσβαση σε περιεχόμενο λόγων μίσους και το διαμοιρασμό παράνομων αρχείων μέσω ομότιμων δικτύων.

Τα φίλτρα αυτά παρουσιάζουν σημαντικά πλεονεκτήματα σε σχέση με τα εγκατεστημένα σε επίπεδο τελικού χρήστη. Η πρόσβαση στα σημεία εφαρμογής των μηχανισμών και κατά συνέπεια η μη εξουσιοδοτημένη τροποποίηση τους είναι πιο δύσκολη. Οι πάροχοι έχουν δυνατότητες να δεσμεύσουν πόρους για τον έλεγχο σε μεγαλύτερη κλίμακα ακόμη και να λειτουργήσουν υπολογιστές, διακομιστές (proxies), αποκλειστικά για αυτό το σκοπό [67]. Ανάλογα με το προϊόν που επιλέγει να χρησιμοποιήσει ο κάθε πάροχος, δίνονται ή όχι κάποιες δυνατότητες στους πελάτες να καθορίσουν αυτοί το περιεχόμενο των υπηρεσιών στις οποίες θα έχουν πρόσβαση. Υπάρχει δηλαδή η δυνατότητα ο έλεγχος του περιεχόμενου να παρέχεται ή να πωλείται σαν πρόσθετη υπηρεσία στους καταναλωτές [29]. Σε κάποιες περιπτώσεις, έχουμε υβριδική εφαρμογή και είναι απαραίτητο να εγκατασταθεί κάποιο λογισμικό και στην πλευρά του τελικού χρήστη.

Παραδοσιακά τα φίλτρα σε αυτό το επίπεδο είναι συνήθως βασισμένα σε καταλόγους (indexes), όπου αναφέρεται αν επιτρέπεται κάτι ή όχι, μια που δεδομένου του μεγάλου όγκου της προς διαχείριση πληροφορίας, αυτές οι τεχνικές απαιτούν λιγότερη υπολογιστική ισχύ [01]. Επιπλέον η διαχείριση και ενημέρωση των καταλόγων αυτών κεντρικά είναι πιο εύκολη, άμεση και αποτελεσματική [67]. Τα τελευταία χρόνια με την αύξηση της υπολογιστικής ισχύος στον βασικό κορμό των δικτύων των παρόχων, επιλέγονται και τεχνικές βασισμένες στην ανάλυση του περιεχομένου.

3.1.3 Επίπεδο Οργανισμού

Ο οργανισμός μπορεί να είναι επιχείρηση, εταιρία, εκπαιδευτικός οργανισμός, σχολείο, βιβλιοθήκη, κάποια υπηρεσία ή ίδρυμα. Το φίλτρο παρεμβάλλεται συνήθως, μεταξύ του δικτύου του οργανισμού και της πύλης πρόσβασης προς το Διαδίκτυο. Σε όλους του χρήστες του δικτύου π.χ. εργαζόμενους ή μαθητές, παρέχεται Διαδίκτυο με φιλτραρισμένο περιεχόμενο [01]. Ο έλεγχος ρυθμίζεται από το διαχειριστή του εσωτερικού δικτύου, σύμφωνα με την πολιτική ορθής χρήσης του οργανισμού. Πολλές φορές ο παραπάνω έλεγχος συνδυάζεται με περιορισμούς στον χρόνο πρόσβασης αλλά και στο εύρος ζώνης [04].

Τα προϊόντα που χρησιμοποιούνται για τον έλεγχο σε αυτή την κλίμακα συχνά συμπεριλαμβάνουν και την αποκλειστική χρήση hardware, ανάλογα όπως περιγράφτηκε και για τους ISP, με την προοπτική της αποφυγής χρήσης λογισμικού πολύ απαιτητικού σε υπολογιστικούς πόρους [01]. Συχνά η εγκατάσταση γίνεται σε εξυπηρετητές οι οποίοι μπορεί να παρεμβάλλονται μεταξύ του εσωτερικού δικτύου και του Διαδικτύου ή να λειτουργούν ως δρομολογητές ή ακόμη και ως διακομιστές (proxies), στο ίδιο επίπεδο με τους άλλους υπολογιστές του δικτύου [29].

3.1.4 Επίπεδο Τελικού Χρήστη

Ο τελικός χρήστης μπορεί να προσδιοριστεί στο επίπεδο ενός οικιακού προσωπικού υπολογιστή ή μιας φορητής συσκευής πρόσβασης στο διαδίκτυο (κινητό τηλέφωνο, tablet κα). Ο μηχανισμός ελέγχου σε αυτή την περίπτωση μπορεί να είναι ανεξάρτητος ή τμήμα ενός ολοκληρωμένου πακέτου προστασίας που συμπεριλαμβάνει Firewall, πρόγραμμα προστασίας από υιούς κτλ. Τα φίλτρα των οικιακών υπολογιστών συνδυάζονται όλο και περισσότερο με επιπρόσθετες λειτουργίες, όπως λογισμικό γονικού ελέγχου ή λογισμικό ασφαλείας και για αυτό το εύρος του μεγέθους τους μπορεί να ποικίλει από ένα απλό πρόσθετο στο πρόγραμμα πλοήγησης που αποσκοπεί στο να μπλοκάρει συγκεκριμένους ιστότοπους, έως ένα ολοκληρωμένο πρόγραμμα γονικού ελέγχου που συμπεριλαμβάνει περιορισμό πρόσβασης σε συγκεκριμένο περιεχόμενο και εφαρμογές παρακολούθησης, αποστολή αναφορών και χρονικό περιορισμό [01].

Φίλτρα σχεδιασμένα για προσωπικούς υπολογιστές εγκαθίστανται κατευθείαν σε αυτούς και μπορούν να ρυθμιστούν ώστε να προσφέρουν διαφορετικά επίπεδα ελέγχου για διαφορετικούς χρήστες. Είναι μια επιλογή που γίνεται συνήθως από οικιακούς χρήστες ή μικρούς οργανισμούς μια που η τοπική εγκατάσταση καθιστά δύσκολη την εφαρμογή μιας ευρύτερης πολιτικής

ελέγχου σε μεγαλύτερη κλίμακα. Οι απαιτήσεις σε υπολογιστικούς πόρους σε αυτή την περίπτωση είναι συνήθως μικρότερες.

Η κύρια αδυναμία της προσέγγισης αυτής είναι η ευκολία παράκαμψης του ελέγχου, που προκύπτει από την δυνατότητα τοπικής διαχείρισης του. Δεδομένου ότι ο έλεγχος εκτελείται στο τοπικό σταθμό εργασίας ο ελεγχόμενος, εργαζόμενος ή ανήλικος μπορεί συχνά να βρει τρόπους απενεργοποίησης των μηχανισμών και πρόσβασης στο αποκλεισμένο περιεχόμενο [29].

Κινητές Συσκευές Πρόσβασης

Στο επίπεδο του τελικού χρήστη ιδιαίτερη αναφορά αξίζει να γίνει στην πρόσβαση με χρήση κινητών συσκευών όπως τηλέφωνα και ταμπλέτες. Εξαιτίας της ραγδαία αυξανόμενης χρήσης των κινητών συσκευών για την πλοήγηση στο διαδίκτυο, φίλτρα που προορίζονται για τέτοιου είδους συσκευές αποτελούν μια ιδιαίτερα αναπτυσσόμενη περιοχή αυτής της τεχνολογίας.

Πολλοί πάροχοι υπηρεσιών κινητής επικοινωνίας [05] εγκαθιστούν φίλτρα κεντρικά προκειμένου να αποτρέψουν την πλοήγηση σε περιεχόμενο χαρακτηρισμένο ως ακατάλληλο, υπάρχει όμως και η απαίτηση για τοπική λειτουργία ελέγχου στην συσκευή. Οι συσκευές αυτές έχουν κάποιους περιορισμούς στην εγκατάσταση του έλεγχου όπως [06]:

- περιορισμένη υπολογιστική ισχύ και ενέργεια (μπαταρία) προκειμένου να λειτουργήσουν το απαραίτητο λογισμικό
- περιορισμένη μνήμη προκειμένου να αποθηκεύσουν καταλόγους με περιεχόμενα
- συστήματα ελέγχου για τη διασφάλιση μη απενεργοποίησης από τον κάθε χρήστη

δημιουργώντας νέες προκλήσεις σε αυτόν το τομέα. Πολλές φορές επιλέγεται η υβριδική λύση, κεντρικού ελέγχου και τοπικής εφαρμογής, προκειμένου να υπάρχουν πιο αξιόπιστα αποτελέσματα.

3.1.5 Τρίτα Μέρη

Οι υπηρεσίες ελέγχου πρόσβασης μπορούν να παρέχονται και ως υπηρεσίες SaaS (Software as a Service) από τρίτα έμπιστα μέρη, χωρίς να είναι απαραίτητη η αγορά λογισμικού ή υλικού. Τρίτα

μέρη χαρακτηρίζονται με την έννοια ότι δεν είναι ούτε πάροχοι ούτε καταναλωτές υπηρεσίας επικοινωνίας, αλλά παρέχουν μέσω Διαδικτύου υπηρεσίες ελέγχου πρόσβασης διαθέτοντας τους πόρους τους στο σύννεφο (cloud). Στην περίπτωση αυτή ο πάροχος, το τρίτο μέρος, της υπηρεσίας λειτούργει σε διαφορετικές τοποθεσίες ανά τον κόσμο κέντρα ασφαλείας, SOC (Security Operation Center), με εξυπηρετητές ή δρομολογητές να παρεμβάλλονται είτε στη διαδρομή της αίτησης για κάποιο περιεχόμενο, είτε στη διαδρομή της αποστολής αυτού του περιεχομένου. Η παρεμβολή αυτή γίνεται με διαφόρους τρόπους, όπως τη ρύθμιση του προγράμματος πλοήγησης από τον χρήστη, ή αλλάζοντας τις πολιτικές δρομολόγησης του τοπικού παρόχου [01, 04].

Η λύση του ελέγχου από τρίτους χρησιμοποιείται ιδιαίτερα από εταιρίες που απασχολούν εργαζόμενους που ταξιδεύουν συχνά ή από παρόχους που επιθυμούν να αναθέσουν σε άλλους το φιλτράρισμα για τους πελάτες τους. Το πλεονέκτημα της εφαρμογής αυτής είναι η μεταφερσιμότητα της λειτουργίας ελέγχου παντού στον κόσμο, αν και είναι συνηθισμένη η επιλογή της τοποθέτησης των εξυπηρετητών φιλτραρίσματος κοντά στον τελικό χρήστη για την αποφυγή της υποβάθμισης της υπηρεσίας [29].

3.1.6 Μηχανές Αναζήτησης

Αν και οι μηχανές αναζήτησης δεν είναι κόμβος της τοπολογίας του ευρύτερου δικτύου, αντιμετωπίζονται σαν ξεχωριστή κατηγορία και εδώ, λόγω της εκτεταμένης χρήσης τους. Οι περισσότερες μεγάλες μηχανές αναζήτησης προσφέρουν δυνατότητες φιλτραρίσματος που επιτρέπουν στους πελάτες τους να διαχειριστούν μόνοι τους την πρόσβαση σε περιεχόμενο. Τα φίλτρα είναι σχεδιασμένα να αφαιρούν παράνομο περιεχόμενο ή περιεχόμενο ακατάλληλο για παιδιά, στα πλαίσια μια προκαθορισμένης δικαιοδοσίας, από τα αποτελέσματα της αναζήτησης, αν και οι ίδιες, οι πάροχοι των υπηρεσιών αναζήτησης, δηλώνουν ότι αυτό δεν είναι εφικτό κατά απόλυτο ποσοστό. Μερικές μηχανές αναζήτησης επιτρέπουν στους χρήστες να θέτουν τις επιλογές φιλτραρίσματος στην κεντρική σελίδα αναζήτησης, αποτρέποντας την πρόσβαση σε εικόνες, βίντεο κ.α. ή να φιλτράρουν όλες τις αναζητήσεις στον παγκόσμιο ιστό. Άλλες μηχανές αναζήτησης προσφέρουν σελίδες αναζήτησης ειδικά σχεδιασμένες για παιδία.

Οι προμηθευτές των φίλτρων συχνά ενσωματώνουν αυτές τις ασφαλείς αναζητήσεις στα προϊόντα τους. Πολλά πακέτα γονικού ελέγχου δίνουν στους γονείς τη δυνατότητα να καθορίζουν την ασφαλή πλοήγηση ώστε τα παιδιά να μην μπορούν να την απενεργοποιήσουν όταν το φίλτρο λειτουργεί [01].

3.2 Έλεγχος Περιεχομένου στα Διαφορετικά Στάδια της Λειτουργιάς του

Ο έλεγχος και το φιλτράρισμα της πληροφορίας μπορεί να εφαρμοστεί σε ολόκληρο τον «κύκλο ζωής» της πληροφορίας, στα διάφορα σταδία δηλαδή δημιουργίας διακίνησης και κατανάλωσης του περιεχομένου. Η επιλογή του σταδίου που θα εφαρμοστεί ο έλεγχος του περιεχομένου εξαρτάται από τις τεχνικές δυνατότητες, του διαθέσιμους πόρους, αλλά και την πολιτική που ακολουθείται από αυτόν που τον επιδιώκει.

Σχήμα 3.2: Έλεγχος περιεχομένου στα διαφορετικά στάδια της λειτουργιάς του: 1. Δημιουργός περιεχομένου 2. Μηχανισμός διανομής περιεχομένου 3. Συνδρομητής.

3.2.1 Δέσμευση από το Δημιουργό του Περιεχομένου

Δεδομένου ότι κάθε χρήστης του διαδικτύου, κάνοντας χρήση μια προσωρινής για αυτόν IP διεύθυνσης, έχει τη δυνατότητα να είναι και δημιουργός περιεχομένου, η δέσμευση από τον ίδιο το δημιουργό καθίσταται δύσκολη πρώτα από όλα για λόγους περιορισμένης δυνατότητας επόπτευσης, εξαιτίας του πολύ μεγάλου πλήθους δημιουργών. Οι δημιουργοί περιεχομένου δεν μπορούν εύκολα να ομαδοποιηθούν σε κατηγορίες στις οποίες να εφαρμοστεί μια συγκεκριμένη πολιτική. Υπάρχει η ανάγκη ύπαρξης κατάλληλου φορέα για τον έλεγχο του περιεχομένου που

δημοσιεύεται στο διαδίκτυο. Ακόμη πάντως και αν υπάρξει τέτοιος φορέας, θα υπήρχαν πολλά νομικά ζητήματα που θα είχαν να κάνουν κυρίως με την παγκόσμια δικαιοδοσία του [72].

Επιπλέον οι δημιουργοί του περιεχομένου δεν έχουν στη διάθεση τους κάποιο μηχανισμό για να αναγνωρίσουν αν οι αιτούμενοι την πληροφορία δικαιούνται με βάση το νόμο, την ηλικία ή τις προτιμήσεις τους να έχουν πρόσβαση σε αυτή. Η μόνη λύση, που εναπόκειται στην καλή θέληση των δημιουργών περιεχομένου, είναι η σήμανση του περιεχομένου τους σύμφωνα με ένα προσυμφωνημένο τρόπο, ο οποίος θα επιτρέψει στους παραλήπτες τον έλεγχο. Οι χρήστες θα πρέπει στην περίπτωση αυτή να στέλνουν στους διακομιστές περιεχομένου μαζί με το αίτημα για πληροφορία ένα σύνολο κανόνων, που θα επιτρέπουν να καθοριστεί και να εφαρμοστεί η πολιτική του ελέγχου. Σημαντικά νομικά και οικονομικά ζητήματα τίθενται και στην περίπτωση αυτή [64].

3.2.2 Δέσμευση στο Μηχανισμό Διανομής του Περιεχομένου

Είναι η περιοχή στην οποία εφαρμόζονται οι περισσότερες και πιο αποτελεσματικές μέθοδοι φιλτραρίσματος. Το παράνομο ή προσβλητικό περιεχόμενο δεσμεύεται είτε σε επίπεδο πακέτου είτε σε επίπεδο εφαρμογής [27].

Η πληροφορία στο διαδίκτυο μεταφέρεται μέσω απρόβλεπτων διαδρομών, καθορισμένων συνεχώς από δρομολογητές. Η δέσμευση περιεχομένου στο επίπεδο μεταγωγής πακέτου, απαιτεί δρομολογητές φιλτραρίσματος (screening routers), οι οποίοι εξετάζουν την IP διεύθυνση της προέλευσης του εισερχόμενου πακέτου, τη συγκρίνουν με μια «μαύρη λίστα» (black list) ή με μια «λευκή λίστα» (white list) και είτε προωθούν το πακέτο, είτε το απορρίπτουν [64].

Η δέσμευση περιεχομένου στο επίπεδο εφαρμογής, απαιτεί την ύπαρξη πυλών εφαρμογών (application gateways) και διακομιστών διαμεσολάβησης (proxy servers) που εξετάζουν τις πηγές ή πληροφορίες για τις πηγές, με σκοπό να αποφασίσουν αν το αίτημα του αντιστοίχου πρωτοκόλλου της εφαρμογής επιτρέπεται. Για παράδειγμα, μια κοινή προσέγγιση είναι ο προσδιορισμός των διευθύνσεων URL που δεν θα πρέπει να είναι προσβάσιμες και η τοποθέτησή τους σε μια «μαύρη λίστα» που είναι βρίσκεται στον διακομιστή διαμεσολάβησης.

3.2.3 Δέσμευση από τον Συνδρομητή

Είναι λογικό μια υπηρεσία προστιθέμενης αξίας όπως είναι ο έλεγχος περιεχομένου να μπορεί να εφαρμοστεί στο τελικό «καταναλωτή» του περιεχομένου. Η επιλογή αυτή δεν επιφορτίζει το διανομέα της πληροφορίας να αποτρέπει την κυκλοφορία της συνολικά στο δίκτυο, αλλά στοχευόμενα μόνο εκεί που απαιτείται σε συγκεκριμένους χρήστες, οι οποίοι είναι δυνατό να είναι μεμονωμένα άτομα, ολόκληροι οργανισμοί ή και το σύνολο των πελατών ενός παρόχου [64].

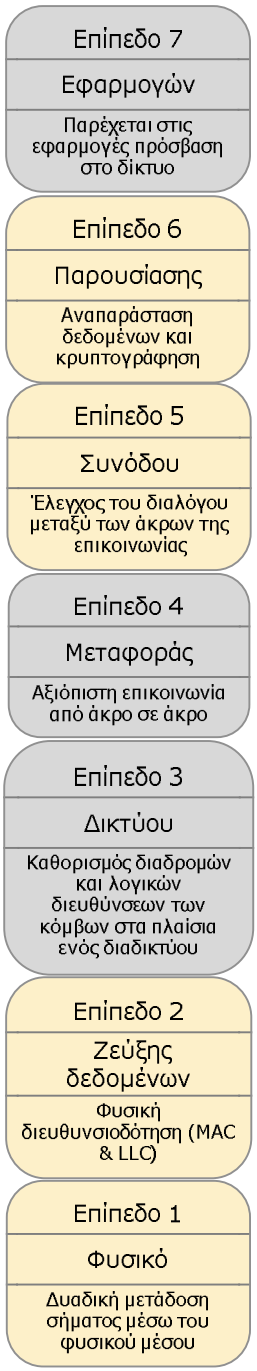
Η προσέγγιση με βαθμονόμηση του περιεχομένου και η αυτό-οριοθέτηση, καθιστά τους συνδρομητές υπευθύνους για την επιλογή του περιεχομένου στο οποίο θέλουν ή όχι να έχουν πρόσβαση. Στην περίπτωση αυτή οι πάροχοι του περιεχομένου, ή τρίτοι οργανισμοί, πρέπει να έχουν αξιολογήσει και κατατάξει το υλικό και οι τελικοί χρήστες προστατεύουν τους εαυτούς τους ρυθμίζοντας τις εφαρμογές πλοήγησης ώστε να μην επιτρέπεται η λήψη ακατάλληλου περιεχομένου. Η σήμανση παρέχει στο χρήστη αρκετές πληροφορίες για να αποφασίσει αν θα έχει πρόσβαση ή όχι, ενώ η αξιολόγηση και η κατάταξη εισάγουν πληροφορίες και τιμές στα δεδομένα βασισμένες σε καθορισμένες υποθέσεις και κριτήρια.

3.3 Λειτουργία σε Διαφορετικά Επίπεδα του Μοντέλου Αναφοράς Ανοικτής Διασύνδεσης Συστημάτων (OSI)

Ξεχωριστές τεχνολογίες ελέγχου και δέσμευσης περιεχομένου μπορούν να λειτουργήσουν σε διαφορετικά επίπεδα του μοντέλου αναφοράς Ανοικτής Διασύνδεσης Συστημάτων (OSI), με μεγάλη διαφοροποίηση σε θέματα κόστους και αποτελεσματικότητας [93]. Τα φίλτρα λειτουργούν είτε στο επίπεδο 3, Επίπεδο Δικτύου του μοντέλου OSI, ή στο επίπεδο 4, Επίπεδο Μεταφοράς, ή και στο επίπεδο 7, Επίπεδο Εφαρμογής.

Φίλτρα που εγκαθίστανται στο επίπεδο 3 ή στο επίπεδο 4, αναφέρονται ως φίλτρα Επιπέδου Δικτύου και αυτά που εγκαθίστανται στο επίπεδο 7 αποκαλούνται φίλτρα Επιπέδου Εφαρμογής [28]. Στον έλεγχο στο επίπεδο δικτύου κάθε πακέτο καθώς διέρχεται μέσω της συσκευής φιλτραρίσματος (πχ δρομολογητής), επιθεωρείται και με βάση το περιεχόμενο της κεφαλίδας του είτε προωθείται είτε σιωπηλά απορρίπτεται. Η απόρριψη σε χαμηλό επίπεδο, στερεί τη δυνατότητα ενημέρωσης του χρήστη σχετικά με το περιεχόμενο της πληροφορίας, γεγονός που συχνά οδηγεί σε υπερβάλλουσα απόρριψη δεδομένων. Αυτός ο τύπος ελέγχου είναι από τους

παλιότερα γνωστούς και ευρύτερα εφαρμοσμένους, μια που θεωρητικά τουλάχιστον δεν υπάρχει ανάγκη για νέο εξοπλισμό ή τεχνολογία προκειμένου να λειτουργήσει. Παρόλα αυτά αξίζει να αναφερθεί ότι στον έλεγχο στο επίπεδο δικτύου υπάρχει συχνά σημαντική διαφοροποίηση σε απαιτήσεις πόρων και δυνατότητα κλιμάκωσης ανάλογα με το αν λειτουργεί στο επίπεδο 3 ή το επίπεδο 4 [93].



Σχήμα 3.3: Μοντέλο αναφοράς OSI.

3.3.1 Επίπεδο 3

Το επίπεδο 3 (Επίπεδο Δικτύου) του μοντέλου OSI είναι πρωταρχικά υπεύθυνο για τη λογική διευθυνσιοδότηση και δρομολόγηση των δεδομένων και περιέχει πληροφορίες (πχ IP διευθύνσεις) για την πηγή και τον προορισμό του πακέτου [21]. Χρησιμοποιώντας αυτές τις πληροφορίες είναι δυνατό να καθοριστούν κανόνες για το μπλοκάρισμα συγκεκριμένων πακέτων, βασισμένοι στην ενσωματωμένη διεύθυνση του αποστολέα ή/και του παραλήπτη, αποτρέποντας επικοινωνία από ή προς συγκεκριμένες θέσεις.

Το πλεονέκτημα, θεωρητικά, του ελέγχου στο επίπεδο 3 είναι ότι η διαχείριση των εντολών απόρριψης των πακέτων μπορεί να γίνει αποτελεσματικά και με μικρή διαχειριστική επιβάρυνση σε δικτυακές συσκευές όπως οι δρομολογητές. Στη πράξη, αυτό που συνήθως συμβαίνει είναι ότι λόγω του μεγάλου πλήθους των κανόνων ελέγχου, αυξάνεται πολύ το φορτίο, μειώνεται σημαντικά η απόδοση και δημιουργούνται προβλήματα συγχρονισμού μεταξύ των δικτυακών συσκευών που εμπλέκονται.

Επιπλέον ένα ακόμη μειονέκτημα είναι η μη δυνατότητα κλιμάκωσης στον έλεγχο που γίνεται σε αυτό το επίπεδο. Η αδυναμία αποκλεισμού υπηρεσίας ή θύρας επικοινωνίας έχει σαν αποτέλεσμα να προκύπτουν θέματα υπερβολικού ελέγχου. Για παράδειγμα αν αποτραπεί η πρόσβαση σε έναν εξυπηρετητή που φιλοξένει μια ιστοσελίδα με ακατάλληλο περιεχόμενο, θα είναι αδύνατο να υπάρξει οποιαδήποτε μορφή άλλης διαδικτυακής επικοινωνίας όπως ηλεκτρονικό ταχυδρομείο ή chat, μέσω αυτού του εξυπηρετητή [93].

3.3.2 Επίπεδο 4

Το επίπεδο 4 (Επίπεδο Μεταφοράς) του μοντέλου OSI είναι υπεύθυνο για την μορφοποίηση και διαχείριση της μεταφοράς των δεδομένων με ένα διαφανή τρόπο. Παρέχει αξιόπιστη και ακριβή παράδοση των δεδομένων στο επόμενο επίπεδο και χρησιμοποίει πρωτόκολλα όπως TCP, UDP και ICMP. Στο επίπεδο 4 χρησιμοποιείται όλη η πληροφορία από το επίπεδο 3 αλλά επιπλέον ελέγχεται και το περιεχόμενο της κεφαλίδας του IP πακέτου με κύρια πληροφορία τον αριθμό θύρας επικοινωνίας. Τα TCP και UDP πρωτόκολλα συμπεριλαμβάνουν πληροφορίες, (πχ αριθμό θύρας) σχετικές με το τύπο της υπηρεσίας του πακέτου. Οι διάφοροι αριθμοί θύρας επιτρέπουν στους εξυπηρετητές του διαδικτύου να φιλοξενούν πολλές υπηρεσίες σε μια IP διεύθυνση. Σε κάθε μία από τις γνωστές υπηρεσίες του διαδικτύου έχει εκχωρηθεί συγκεκριμένος αριθμός θύρας, όπως για τη μεταφορά αρχείων ο 21 (FTP), για την αποστολή ηλεκτρονικού

ταχυδρομείου ο 25 (SMTP), ο 80 για τον παγκόσμιο ιστό (HTTP), ο 110 για την ανάγνωση ηλεκτρονικού ταχυδρομείου. Η πρόσβαση στο Web εκτός από την θύρα 80 χρησιμοποιεί και άλλες, όπως η 443 για ασφαλείς συνδέσεις (HTTPS), ενώ πολλές φορές το λογισμικό πολλών Web εξυπηρετητών λειτουργεί στις θύρες 8000 και 8080 [21].

Αυτή η πληροφορία που αφορά την εφαρμογή μαζί με τη διεύθυνση του αποστολέα και του παραλήπτη του πακέτου, παρέχουν έναν αποτελεσματικότερο τρόπο διαχωρισμού και διάκρισης της κίνησης του δικτύου, συγκρινόμενο με το επίπεδο 3.

Βασίζοντας τον έλεγχο όχι μόνο στην IP διεύθυνση του προορισμού αλλά και στον αριθμό θύρας της, είναι δυνατό να έχουμε έλεγχο σε επίπεδο υπηρεσίας. Αυτό σημαίνει ότι αν αποκλειστεί η Web πρόσβαση από συγκεκριμένο εξυπηρετητή, αυτός μπορεί να παρέχει άλλες υπηρεσίες όπως ηλεκτρονικό ταχυδρομείο.

Παρόλο την μεγαλύτερη ευελιξία που προσφέρει ό έλεγχος στο επίπεδο αυτό και εδώ μπορεί να παρατηρηθούν φαινόμενα αποκλεισμού περιεχομένου που θα έπρεπε να είναι προσβάσιμο. Για παράδειγμα στο πρωτόκολλο HTTP ένας εξυπηρετητής με μία μοναδική IP διεύθυνση, μπορεί να φιλοξενεί αρκετούς (εκατοντάδες ή και χιλιάδες) ιστότοπους (εικονική φιλοξενία- virtual hosting). Αν αποκλειστεί ο εξυπηρετητής αυτός επειδή φιλοξενεί έναν ακατάλληλο ιστότοπο θα αποκλειστούν και όλοι οι άλλοι ιστότοποι [93].

3.3.3 Επίπεδο 7

Το επίπεδο 7 του μοντέλου αναφοράς OSI είναι υπεύθυνο για την ανάλυση των δεδομένων προτού αυτά αποσταλούν σε μια συγκεκριμένη εφαρμογή. Σε αυτό το επίπεδο τα πακέτα ανασυντίθενται και είναι δυνατό να ελεγχθούν σε βάθος. Αυτό έχει σαν αποτέλεσμα να μπορεί να αναλυθεί και να επιθεωρηθεί το φορτίο ή το περιεχόμενο ενός πακέτου, πριν αποτραπεί η πρόσβαση σε αυτό [28]. Με αυτόν τον τρόπο επιτρέπεται στο φίλτρο να εφαρμόζεται περισσότερο στο πρωτόκολλο παρά στο δίκτυο, δίνοντας τη δυνατότητα λεπτομερέστερης και ουσιαστικότερης ανάλυσης [21].

Επιπλέον, και σε αντιδιαστολή με το φιλτράρισμα σε επίπεδο δικτύου, σε αυτό το επίπεδο μπορεί να παρέχεται και πληροφόρηση στο χρήστη για το είδος του ελέγχου που εφαρμόζεται. Εδώ τα δεδομένα πρέπει να ελεγχτούν, να αναλυθούν, πιθανότατα να ανασυσταθούν ή ακόμη και να εκτελεστούν, για αυτό και είναι δύσκολος ο έλεγχος σε πραγματικό χρόνο, ιδιαίτερα σε

ευρυζωνικά περιβάλλοντα όπου απαιτείται μεγάλο πλήθος ακριβού εξοπλισμού, προκειμένου το φιλτράρισμα να θεωρείται εφαρμόσιμο. Επιπλέον εάν χρησιμοποιηθεί ένα κρυπτογραφημένο πρωτόκολλο όπως το Secure Socket Layer (SSL) ή Secure Shell (SSH) το φιλτράρισμα σε επίπεδο εφαρμογών γίνεται πολύ δύσκολο, μια που η κρυπτογραφημένη πληροφορία που μεταφέρεται στο δίκτυο δύσκολα μπορεί να επιθεωρηθεί [93].

3.4 Διάταξη του Ελέγχου στην Διαδικασία Αίτησης και Μεταφοράς της Πληροφορίας

Ο Παγκόσμιος Ιστός, όπως και οι περισσότερες υπηρεσίες του Διαδικτύου, στηρίζεται στο μοντέλο πελάτη-εξυπηρετητή. Το μοντέλο πελάτη-εξυπηρετητή αποτελεί σήμερα τον κύριο τρόπο ανάπτυξης λογισμικού για εφαρμογές δικτύου. Σύμφωνα με το μοντέλο αυτό, αναπτύσσουμε ένα πρόγραμμα το οποίο οργανώνει και διαχειρίζεται αυτόνομα το αρχείο δεδομένων, το πρόγραμμα αυτό αποτελεί τον εξυπηρετητή. Το πρόγραμμα του εξυπηρετητή μπορεί να δέχεται ερωτήσεις ή αιτήματα πάνω στη διαχείριση των δεδομένων και να ενεργεί εκτελώντας ή δίνοντας απαντήσεις σχετικά με πληροφορίες του αρχείου. Οι ερωτήσεις-αιτήματα διατυπώνονται από τον πελάτη τηρώντας κάποιους κανόνες. Η διαδικασία που συμπεριλαμβάνει αιτήματα και απαντήσεις ακολουθείται παρόλα αυτά και σε επιλογές άλλων μοντέλων δικτύωσης, όπως για παράδειγμα τα ομότιμα. Ο έλεγχος του περιεχομένου και η αποτροπή πρόσβασης σε αυτό μπορεί να γίνει σε αυτή την επικοινωνία αιτημάτων και απαντήσεων σε διαφορετικά χρονικά και διαδικαστικά σταδία.

Σχήμα 3.4: 1. Έλεγχος αιτήματος 2. Έλεγχος απάντησης.

3.4.1 Έλεγχος Αιτήματος

Ο έλεγχος αιτήματος πραγματοποιείται όταν επιθεωρούνται τα αιτήματα που προέρχονται από έναν πελάτη και κρίνεται μέσω αυτών αν πρέπει ή όχι να επιτραπεί η προσπέλαση στο αιτηθέν περιεχόμενο.

Λίγα αιτήματα μόνο μπορούν να προκαλέσουν πολύ μεγάλο όγκο δεδομένων και για αυτό το λόγο είναι πολύ λιγότερα τα πακέτα των αιτημάτων που πρέπει να ελεγχτούν από τα πακέτα των απαντήσεων, με αποτέλεσμα τη σημαντική εξοικονόμηση υπολογιστικής ισχύος. Οι αιτήσεις είναι πάντα διατυπωμένες με σαφώς καθορισμένα πρωτόκολλα γεγονός που τις καθιστά κατάλληλες για αυτοματοποιημένο έλεγχο, με συνέπεια αυτή η επιλογή να αποτελεί μια καλή βάση για πολλά «έξυπνα» φίλτρα.

Ένα μειονέκτημα του ελέγχου αιτήματος έγκειται στο ότι βασίζεται στην παραδοχή ότι μια συγκεκριμένη αίτηση θα έχει πάντοτε ως αποτέλεσμα την ίδια απόκριση. Αυτό όμως που μπορεί να συμβαίνει είναι ότι ένα προηγουμένως «αθώο» αίτημα να λαμβάνει ανεπιθύμητο υλικό σε απάντηση σε μια επόμενη αποστολή του ή μπορεί επίσης να συμβεί μια απάντηση σε ένα ερώτημα που παλαιοτέρα θεωρήθηκε μη αποδεκτή να έχει αλλάξει και να μη πρέπει να απορριφτεί [87].

3.4.2 Έλεγχος Απάντησης

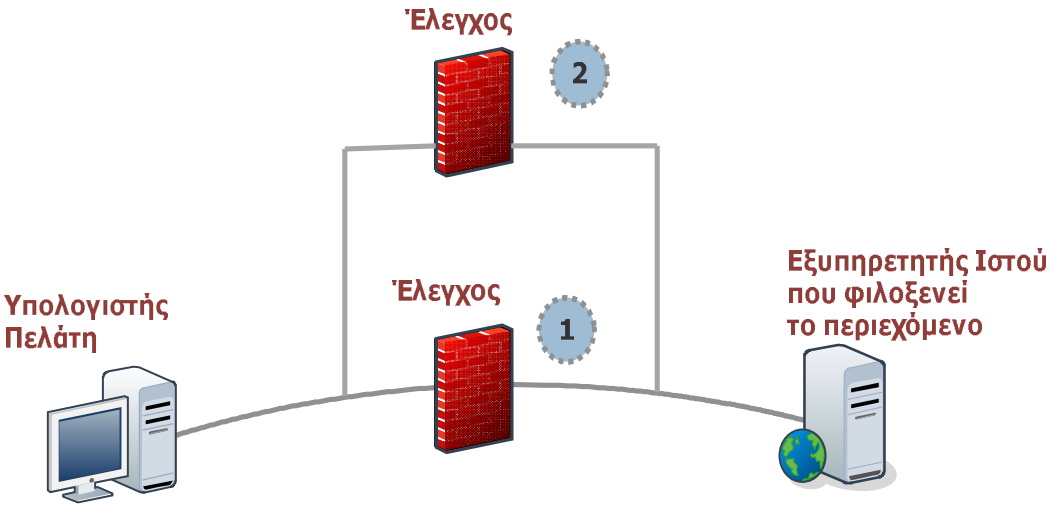
Ο έλεγχος απάντησης συμβαίνει όταν φιλτράρεται η πληροφορία που αποστέλλεται πίσω στον πελάτη. Όπως σημειώνεται παραπάνω, τα δεδομένα απόκρισης είναι γενικά πολύ μεγαλύτερα σε όγκο και εκεί είναι το κύριο μειονέκτημα, μια που επιφορτίζουν σημαντικά περισσότερο τους μηχανισμούς ελέγχου με την επιθεώρηση τους. Οι πληροφορίες στις απαντήσεις μπορούν να έχουν επίσης διάφορες μορφές όπως βίντεο, εικόνα, μουσική, ομιλία, κείμενο ή συνδυασμοί όλων αυτών, γεγονός που καθιστά πιο δύσκολη την αυτοματοποίηση του ελέγχου τους.

Το πλεονέκτημα του φιλτραρίσματος στην απάντηση είναι ότι το φίλτρο παραλαμβάνει το πραγματικό υλικό που αποστέλλεται στον πελάτη, ανεξάρτητα από το από που προέρχονται τα δεδομένα ή το είδος του αιτήματος. Αυτό το πλεονέκτημα υποβαθμίζεται σημαντικά από την σχετικά περιορισμένη δυνατότητα, με βάση την τρέχουσα τεχνολογία αυτοματοποιημένης επιθεώρησης των διαφόρων μορφών διακινούμενης πληροφορίας [87].

3.4.3 Έλεγχος σε Σειρά (Pass-Through)

Στον έλεγχο σε σειρά όλα τα δεδομένα κυκλοφορούν διαμέσου του φίλτρου (pass-through), που τοποθετείται σε σειρά μεταξύ του αιτούντος τη πληροφορία και αυτού που την παρέχει. Ο σχεδιασμός αυτής της τεχνικής είναι σχετικά απλός, μια που πρόκειται ουσιαστικά για μια διαμεσολάβηση, για αυτό και αναφέρεται συχνά ως proxying. Ανάλογα με την υλοποίηση η οποία ακολουθείται παρέχονται υψηλά επίπεδα ασφαλείας ενώ και οι διαχειριστικές δυνατότητες είναι αυξημένες.

Κρίσιμοι παράγοντες στην επιλογή αυτή αποτελούν η ταχύτητα και η κατανάλωση υπολογιστικής ισχύος, μια που κάθε μεμονωμένο πακέτο δεδομένων πρέπει να ελεγχτεί σε πραγματικό σχεδόν χρόνο προτού παραληφθεί. Στην περίπτωση που έχουμε κατάρρευση του σε σειρά μηχανισμού ελέγχου, ανάλογα με το σχεδιασμό του, μπορεί να έχουμε σημαντικές επιπτώσεις και στη κυκλοφορία συνολικά του δικτύου όπως συμφόρηση ή ακόμη και διακοπή [87].



Σχήμα 3.5: 1. Έλεγχος σε σειρά 2. Παράλληλος έλεγχος.

3.4.4 Παράλληλος Έλεγχος (Pass-By)

Στην επιλογή του παράλληλου ελέγχου το φίλτρο τοποθετείται δίπλα (pass-by), παράλληλα στη ροή των δεδομένων και παραλαμβάνει ένα αντίγραφο, (mirroring), κάποιων ή όλων των πακέτων δεδομένων που διέρχονται μέσω του δρομολογητή ή του μεταγωγέα, παρακολουθώντας, (monitoring) το περιεχόμενο τους. Στην περίπτωση που εντοπίσει ακατάλληλο υλικό το αποκλείει.

Όλη η διαδικασία και εδώ μπορεί να γίνεται σε πραγματικό χρόνο, σε αυτή την περίπτωση όμως υπάρχει το πλεονέκτημα ότι η προώθηση της διακίνησης των δεδομένων και ο έλεγχος τους διαχωρίζονται και κατανέμονται σε διαφορετικά, βελτιστοποιημένα για τη λειτουργία τους, τμήματα. Με τον τρόπο αυτό επιταχύνεται μείωση της χρονικής απόκρισης, αλλά ο σχεδιασμός του συστήματος γίνεται πιο σύνθετος [87].

Ανάλυση μετά τη Λήψη των Δεδομένων (After the Fact)

Μια άλλη επιλογή στον παράλληλο έλεγχο είναι δυνατό να επιτρέπει τα δεδομένα να περάσουν την πρώτη φορά αφιλτράριστα ουσιαστικά, αλλά και χωρίς καθόλου καθυστέρηση, ενώ ένα αντίγραφο τους οδηγείται στο φίλτρο. Εκεί ελέγχονται ασύγχρονα μετά τη λήψη τους από τον τελικό παραλήπτη [79].

Πλεονέκτημα αυτή της επιλογής είναι η έλλειψη καθυστέρησης και η δημιουργία ιστορικού εκμεταλλεύσιμου για μελλοντικές αιτήσεις του ίδιου περιεχομένου, για αυτό και η διαδικασία αυτή ακολουθείται συχνά κατά την ενημέρωση των μηχανισμών ελέγχου. Ένα μειονέκτημα εντοπίζεται στο ότι είναι δυνατό να διανεμηθεί ακατάλληλο περιεχόμενο για τουλάχιστον μια φορά που θα αιτηθεί κάποιος πρόσβαση σε αυτό [02].

Πιθανή αποτυχία του φίλτρου έχει περιορισμένες επιπτώσεις στη ροή της κυκλοφορίας στο δίκτυο, παρόλα αυτά όμως η πολυπλοκότητα της διάταξης αυξάνεται [87].

3.4.5 Υβριδικός Παράλληλος Έλεγχος (Hybrid Pass-By)

Στον υβριδικό παράλληλο έλεγχο ένα σύστημα πραγματοποιεί ένα γρήγορο, πρόχειρο και εύκολο έλεγχο των δεδομένων και είτε τα προωθεί είτε τα στέλνει σε ένα δεύτερο επίπεδο ελέγχου. Στο δεύτερο επίπεδο γίνεται ένας πιο εντατικός έλεγχος και τα δεδομένα αποκλείονται ή προωθούνται. Το πρώτο στάδιο μπορεί να είναι για παράδειγμα μια απλή επιθεώρηση των κεφαλίδων των πακέτων και αποκλεισμός κάποιων βασικών IP διευθύνσεων.

Το βασικό πλεονέκτημα της μεθόδου αυτής έγκειται στο γεγονός ότι συνήθως μόνο ένα μικρό ποσοστό της συνολικής κίνησης αξίζει αποκλεισμού και έτσι ένας μικρός όγκος δεδομένων περνάει στο δεύτερο πιο απαιτητικό στάδιο, στο οποίο δεν είναι απαραίτητη πάντα η λειτουργία σε πραγματικό χρόνο [87].

3.5 Τεχνικές Αναγνώρισης Περιεχομένου.

Τα προϊόντα φιλτραρίσματος επιτελούν δύο βασικές λειτουργίες με σκοπό να περιορίσουν την πρόσβαση των χρηστών σε περιεχόμενο:

- Πρώτα αναγνώριση του περιεχομένου που πρόκειται να αποκλειστεί ή να προωθηθεί.

- Στη συνέχεια αποκλεισμός (μπλοκάρισμα) ή προώθηση του περιεχόμενου, ανάλογα με το πώς έχει κριθεί.

Οι μέθοδοι αναγνώρισης είναι κοινές για πολλά προϊόντα που κυκλοφορούν και εξαρτώνται κυρίως από τις θέσεις που αυτά εφαρμόζονται, όπως αυτές περιγράφηκαν πιο πάνω [01].

Η αναγνώριση του περιεχομένου είναι η διαδικασία κατά την οποία χαρακτηρίζεται το προς διακίνηση στο δίκτυο περιεχόμενο κατάλληλο ή όχι. Για να κριθεί το περιεχόμενο ως ακατάλληλο (ή κατάλληλο αντίστοιχα) πρέπει να ικανοποιεί κάποια κριτήρια. Τα κριτήρια αυτά έχουν διαφορετική μορφή, ανιχνεύονται με διαφορετικές μεθόδους και η πολυπλοκότητα της δομής εντοπισμού που εφαρμόζουν, κλιμακώνεται από το επίπεδο μιας απλής σύγκρισης στατικών δεδομένων μέχρι το επίπεδο ενός αλγόριθμου εντοπισμού δυναμικών χαρακτηριστικών [04].

Οι τεχνικές αναγνώρισης περιεχομένου είναι δυνατό να χωριστούν σε τρεις κατηγορίες :

- Αναγνώριση βασισμένη σε ευρετήρια (listing-indexing).

- Δυναμική αναγνώριση βασισμένη σε ανάλυση (dynamic-intelligent-automated).

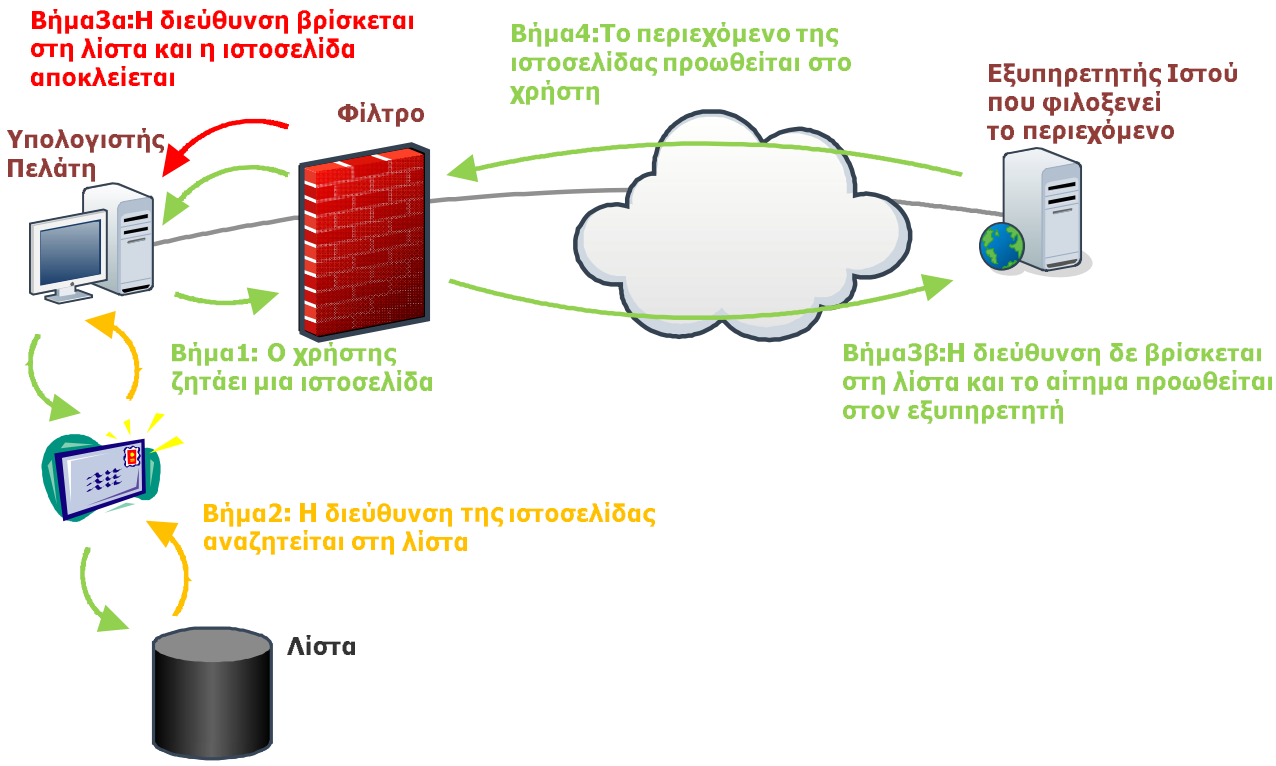
- Αναγνώριση με βάση τη διαβάθμιση περιεχομένου και αυτοκαθορισμό (rating-self regulation).

Σχήμα 3.6: Τεχνικές αναγνώρισης περιεχομένου.

3.5.1 Αναγνώριση Βασισμένη σε Ευρετήρια (Λίστες)

Η αναγνώριση βασισμένη σε ευρετήρια είναι η τεχνολογία που κρύβεται πίσω από τα περισσότερα web-προϊόντα φιλτραρίσματος. Οι λίστες περιλαμβάνουν λεπτομέρειες για τις διευθύνσεις URL (Uniform Resource Locators - άλφα-αριθμητικές διευθύνσεις ιστοσελίδων) ή τις διευθύνσεις IP (διευθύνσεις του πρωτοκόλλου IP - 32-bit αριθμούς αναγνώρισης στο διαδίκτυο) ή και τα δύο. Τα προϊόντα φιλτραρίσματος επιτρέπουν ή απαγορεύουν την πρόσβαση στο αιτούμενο περιεχόμενο συγκρίνοντας τη διεύθυνση URL ή τη διεύθυνση IP με τις λίστες που έχουν καταχωρημένες. Το ποιο είδος διεύθυνσης θα χρησιμοποιηθεί εξαρτάται από την επιλογή του μηχανισμού αποκλεισμού που θα ακολουθηθεί.

Η συγκεκριμένες τεχνικές εφαρμόζουν ουσιαστικά μια Επιφανειακή Επιθεώρηση των διακινούμενων Πακέτων (SPI-Shallow Packet Inspection), ελέγχοντας κυρίως το περιεχόμενο της κεφαλίδας τους, μια που αυτό είναι αρκετό για να τους δώσει την πληροφορία που απαιτείται για τη σύγκριση με τους καταλόγους [24].



Σχήμα 3.7: Αναγνώριση βασισμένη σε ευρετήρια.

Υπάρχουν δύο ειδών λίστες:

- Οι «άσπρες» λίστες. Στην περίπτωση αυτή επιτρέπεται η πρόσβαση μόνο στο περιεχόμενο που είναι καταχωρημένο στη λίστα. Είναι μια επιλογή που γίνεται σε εξειδικευμένες περιπτώσεις ελέγχου, όπως όταν είναι επιθυμητό να ρυθμιστεί η πρόσβαση των πολύ μικρών παιδιών για τα οποία είναι περισσότερα αυτά που πρέπει να αποκλειστούν από αυτά στα οποία επιτρέπεται η πρόσβαση.

- Οι «μαύρες» λίστες. Είναι η πιο συνηθισμένη επιλογή και εδώ επιτρέπεται η πρόσβαση σε όλο το περιεχόμενο εκτός από αυτό για το οποίο έχει γίνει αναφορά στη λίστα.

Κατηγορίες Ευρετηρίων

Οι περισσότεροι προμηθευτές προϊόντων ελέγχου πρόσβασης κατηγοριοποιούν τους καταλόγους τους σύμφωνα με μια ευρεία θεματολογία κατηγοριών που να ανταποκρίνεται στους τύπους του περιεχόμενου που επιθυμούν να αποκλείσουν αυτοί που επιβάλουν τον έλεγχο (γονείς, εργοδότες κ.α.), όπως βία, σεξ, τζόγος, κοινωνικά δίκτυα, ρατσισμός κ.α.. Στη βάση αυτών των κατηγοριοποιημένων καταλόγων, οι διαχειριστές του ελέγχου μπορούν να εφαρμόσουν αποκλεισμό με βάση το προφίλ του χρήστη, έτσι για παράδειγμα ένας χρήστης θα μπορούσε να έχει πρόσβαση σε ιστότοπους, στους οποίους δεν επιτρέπεται η πρόσβαση μέσω του ίδιου συστήματος φιλτραρίσματος σε άλλο χρήστη με διαφορετικά χαρακτηριστικά [79]. Επιπλέον κάποια προϊόντα επιτρέπουν τον αποκλεισμό κατηγοριών περιεχομένου με πρόσθετα κριτήρια όπως ώρα της ημέρας ή συνολικός χρόνος πλοήγησης [01].

Ανάλογα με τον προμηθευτή του προϊόντος, ο αριθμός των καταχωρήσεων στους καταλόγους που διαθέτει μπορεί να φτάνει τα εκατοντάδες εκατομμύρια, με μερικούς να ισχυρίζονται ότι ελέγχουν το 98% των συχνά επισκεπτόμενων ιστότοπων. Ο τρόπος με τον οποίο μπορεί να συμπληρωθεί και να ενημερωθεί μια τέτοια λίστα μπορεί να διαφέρει ανάλογα με το προϊόν που χρησιμοποιείται. Κάποιοι προμηθευτές επιλέγουν τη χρήση εξελιγμένου λογισμικού σάρωσης του παγκόσμιου ιστού προκειμένου να βρεθεί το ακατάλληλο υλικό, ενώ άλλοι βασίζονται στην αξιολόγηση από ανθρώπους. Σε κάθε περίπτωση πάντως, δεδομένου του δυναμικού χαρακτήρα του περιεχομένου του Διαδικτύου οι λίστες πρέπει να αναθεωρούνται και να ενημερώνονται συνεχώς. Αυτή είναι και η πιο απαιτητική από πλευράς χρόνου αλλά και πόρων λειτουργία τους. Για κάθε πάροχο υπηρεσιών ελέγχου ο τρόπος δημιουργίας της λίστας αποτελεί εμπιστευτική

πληροφορία και οι περισσότεροι συνδυάζουν τεχνολογίες τεχνητής νοημοσύνης με την απασχόληση ανθρώπινου προσωπικού [04].

Το βασικά πλεονεκτήματα της μεθόδου αυτής είναι η ταχύτητα και η αποδοτικότητα. Ένα τέτοιο σύστημα μπορεί να κάνει τον έλεγχο για τον αν μια αιτηθείσα ιστοσελίδα έχει URL που ανήκει στη λίστα, σε χρόνο πολλές φορές μικρότερο από αυτό που χρειάζεται για να αποκατασταθεί μια σύνδεση, μια που δεν είναι απαραίτητο να αναγνώσει το συνολικό περιεχόμενο της [29].

3.5.2 Αναγνώριση Βασισμένη σε Ανάλυση

Η αναγνώριση βασισμένη σε ανάλυση αναφέρεται στη δυναμική κατηγοριοποίηση του περιεχομένου με τη χρήση εξειδικευμένου λογισμικού και προέκυψε για να βοηθήσει να ξεπεραστεί η ανεπάρκεια της αναγνώρισης με τη χρήση ευρετηρίων, η οποία είναι δυνατό να εφαρμοστεί μόνο σε περιεχόμενο που έχει ήδη αξιολογηθεί. Η ανάλυση σε αυτή τη μέθοδο μπορεί να βασιστεί σε πολλών ειδών κριτήρια όπως για παράδειγμα λέξεις κλειδιά, προφίλ, ανάλυση εικόνας, τύπο αρχείου, ανάλυση συνδέσμων, έλεγχο φήμης, σε βάθος έλεγχος δέσμης δεδομένων κα . Η επιθεώρηση των δεδομένων σε αυτή την περίπτωση είναι πιο απαιτητική σε πόρους, ειδικά όταν εφαρμόζεται σε πραγματικό χρόνο ενώ είναι δυνατό να λειτουργήσει και ασύγχρονα [02].

Σχήμα 3.8: Αναγνώριση βασισμένη σε ανάλυση.

Η ευφυής ανάλυση περιεχομένου είναι μια προσπάθεια για την επίτευξη σημασιολογικής κατανόησης των περιεχόμενων του παγκόσμιου ιστού. Ειδικότερα, οι ευφυείς τεχνικές ταξινόμησης μπορούν να χρησιμοποιηθούν για κατηγοριοποίηση των ιστοσελίδων σε διαφορετικές ομάδες (π.χ. πορνογραφικές και μη πορνογραφικές) ακολουθώντας τη στατιστική εμφάνιση ενός συνόλου χαρακτηριστικών. Αυτή η κατηγοριοποίηση χρησιμοποιείται από το σύστημα για να επιλέξει εάν θα παραδοθεί το περιεχόμενο ή όχι σύμφωνα με την πολιτική ελέγχου που έχει αποφασιστεί.

Οι πιο σημαντικές τεχνολογίες στην ανάλυση περιεχομένου είναι η ταξινόμηση κειμένου, ο έλεγχος εικόνας και ο έλεγχος βίντεο ο οποίος παρουσιάζει ιδιαίτερες προκλήσεις Αυτές οι τεχνικές είναι συχνά εξαρτώμενες από την κατηγορία που εξετάζουν. Το γεγονός έχει σα συνέπεια, ένα εξειδικευμένο πρόγραμμα ταξινόμησης να πρέπει να δημιουργηθεί για κάθε κατηγορία. Συνήθως χρησιμοποιούνται προσεγγίσεις με μηχανές μάθησης (machine learning-ML) που μαθαίνουν τα πιο ενδιαφέροντα χαρακτηριστικά των ιστοσελίδων στη κατηγορία με διάφορες στατιστικές μεθόδους όπως Bayesian, k-Nearest Neighbors κ.α. [04]. Ωστόσο εξειδικευμένες τεχνικές που χρησιμοποιούνται στην ανίχνευση μιας κατηγορίας είναι δυνατό να είναι αναποτελεσματικές σε άλλους τύπους περιεχομένου. Για παράδειγμα ή αναγνώριση ανθρώπινου δέρματος στην επεξεργασία εικόνας που χρησιμοποιείται για την ανίχνευση πορνογραφικού υλικού, είναι ελάχιστα χρήσιμη στην ανίχνευση ναζιστικών συμβόλων [29].

Το πιο σημαντικό μειονέκτημα αυτών των τεχνικών, πέρα από την πολυπλοκότητα στην εγκατάσταση και συντήρηση τους, είναι η απόδοση τους. Αν και είναι δυνατή η κατασκευή αρκετά αποδοτικών συστημάτων, ο συνολικός χρόνος επεξεργασίας τις καθιστά ακατάλληλες για πιο απαιτητικές καταστάσεις. Ωστόσο, εάν το έξυπνο φίλτρο περιεχομένου καλείται μόνο όταν δεν είναι δυνατό να χρησιμοποιηθούν τεχνικές βασισμένες στη λίστα, με την έννοια ότι η URL ή η IP διεύθυνση δεν περιέχεται στη λίστα, το ποσοστό της χρήσης του μειώνεται σημαντικά, και αυξάνεται η αποδοτικότητα του. Τα αποτελέσματά μπορούν να χρησιμοποιηθούν για να ενημερωθούν οι λίστες [29]. Εξάλλου βασικό χαρακτηριστικό του δυναμικού τρόπου αναγνώρισης περιεχομένου είναι ότι το σύστημα φιλτραρίσματος αυτό-εκπαιδεύεται και βελτιώνεται συνεχώς με τη διαρκή χρήση του [04].

Σε Βάθος Επιθεώρηση των Πακέτων - DPI (Deep Packet Inspection)

Η αναφορά των δυναμικών μεθόδων αναγνώρισης περιεχομένου ως DPI (Deep Packet Inspection-σε βάθος επιθεώρηση των πακέτων), έχει την έννοια ότι στις περιπτώσεις αυτές ο

έλεγχος, πέρα από την κεφαλίδα, συμπεριλαμβάνει (πολλές φόρες εστιάζει σε αυτό) το ωφέλιμο φορτίο (payload), των πακέτων στα οποία έχει τεμαχιστεί η μεταδιδόμενη πληροφορία ανάλογα με το πρωτόκολλο που ακολουθείται. Πρόκειται για σχετικά νέες τεχνικές οι οποίες είναι δυνατό να εφαρμοστούν στον έλεγχο μεμονωμένων πακέτων σε πραγματικό χρόνο, είτε και να αναλύουν εκατοντάδες ή και χιλιάδες συγκεντρωμένα πακέτα, ασύγχρονα, πριν εντοπιστεί η ανεπιθύμητη πληροφορία [87].

Τα δεδομένα στο φορτίο του πακέτου συγκρίνονται με μια βάση με κωδικοποιημένες πληροφορίες επιβλαβούς περιεχομένου ή γίνεται χρήση στατιστικών αλγορίθμων με λειτουργία ιστορικού. Η πρώτη εφαρμογή του DPI ήταν για τον έλεγχο της κυκλοφορίας στο διαδίκτυο και την αποφυγή μετάδοσης επιβλαβούς κώδικα (ιών), ανεπιθύμητης αλληλογραφίας, και επιθέσεων άρνησης υπηρεσιών (DoS attacks). Σήμερα χρησιμοποιείται και για τον έλεγχο της πρόσβασης σε περιεχόμενο [86].

Λέξεις, Φράσεις Κλειδιά

Μια από τις πιο βασικές τεχνικές ανάλυσης και αναγνώρισης περιεχομένου είναι αυτή που χρησιμοποιεί λέξεις κλειδιά. Στη περίπτωση αυτή σαρώνεται η διακινούμενη στο δίκτυο πληροφορία και χαρακτηρίζεται ως ακατάλληλη όταν βρεθεί να περιέχει, σε ποσοστό που ξεπερνάει ένα όριο, μια σειρά από προσβλητικούς όρους ή φράσεις που έχουν ήδη καταχωρηθεί σε ένα λεξικό δημιουργημένο για το σκοπό αυτό.

Είναι μία μέθοδος αρκετά γρήγορη στην εφαρμογή της. Επιπλέον το λεξικό με τους ακατάλληλους όρους δεν απαιτεί ιδιαίτερα συχνή ενημέρωση, τουλάχιστον όχι τόσο συχνή όπως μια λίστα με απαγορευμένες διευθύνσεις, μια που η δυναμικότητα της μεταβολής της προς έλεγχο θεματολογίας είναι σαφώς μικρότερη από αυτή του Διαδικτύου [29].

Από τη άλλη πλευρά όμως παρουσιάζονται συχνά προβλήματα υπερβολικού φιλτραρίσματος δηλαδή χαρακτηρισμού ως ακατάλληλο περιεχόμενο το οποίο δεν είναι. Η ανίχνευση για παράδειγμα της λέξης «sex» σε έναν ιστότοπο που σχετίζεται με σεξουαλική αγωγή ή ιατρικά θέματα μπορεί να οδηγήσει στο χαρακτηρισμό του ως ακατάλληλο, χωρίς αυτός να περιέχει οτιδήποτε απρεπές. Το φαινόμενο αυτό το επιτείνει ο συντακτικός χαρακτήρας της επιλογής αυτής, που σημαίνει ότι θα μπλοκάρει λέξεις με προθέματα ή επιθέματα που συντακτικά μοιάζουν με τις απαγορευμένες, αγνοώντας τη σημασιολογία τους μέσα στο κείμενο [67]. Πιο

ακριβής και αποτελεσματικοί τρόποι φιλτραρίσματος κειμένου μπορούν να εφαρμοστούν αλλά αυτοί έχουν μεγαλύτερες απαιτήσεις από πλευράς χρόνου.

Σαν μειονέκτημα μπορεί ακόμη να παρατηρηθεί ή αδυναμία ελέγχου άλλων μορφών πληροφορίας όπως εικόνα ή βίντεο.

Αναγνώριση Κειμένου

Εξελίσσοντας την διαδικασία αναγνώρισης περιεχομένου βασιζόμενοι σε λέξεις κλειδιά οδηγούμαστε στην αναγνώριση με βάση ένα συνολικό κείμενο, τη μορφολογία του, το νόημα του, τη σύνταξη του. Είναι μια διαδικασία που άπτεται επιστημονικών πεδίων όπως αυτά της Εξόρυξης Δεδομένων, της Αναπαράστασης Γνώσης και της Στατιστικής Επεξεργασίας της Φυσικής Γλώσσας.

Συνηθέστερη επιλογή είναι η αυτόματη κατηγοριοποίηση κειμένου (TC text categorization). Ο σκοπός της μεθόδου αυτής είναι να παρέχει ενός είδους δομής σε μη δομημένα αποθηκευμένο κείμενο βοηθώντας στη εξερεύνηση και κατά συνέπεια στην αναγνώριση του. Το εξεταζόμενο κείμενο αντιστοιχίζεται σε ένα σύνολο προκαθορισμένων κατηγοριών (κλάσεις ή θέματα). Αν και η παραπάνω κατηγοριοποίηση μπορεί να γίνει από εμπειρογνώμονες, η πολυπλοκότητα του παγκόσμιου ιστού, επιβάλει την χρήση αυτοματοποιημένων μηχανισμών (ML machine learning).

Η διαδικασία χρησιμοποιεί εκπαιδευόμενους κατηγοριοποιητές (classifiers) κειμένου. Οι κατηγοριοποιητές έχουν σαν αναφορά ένα σύνολο από κείμενα που έχουν σημανθεί χειροκίνητα. Χρησιμοποιώντας μια ποικιλία από αλγόριθμους όπως Naïve Bayes, δέντρα απόφασης, K-κοντινότερων γειτόνων, νευρωνικά δίκτυα και μηχανές υποστήριξης διανυσμάτων, κατατάσσει δυναμικά το προς εξέταση κείμενο σε μια από τις προκαθορισμένες κατηγορίες [29].

Για παράδειγμα, κάποιες λέξεις ή φράσεις έχουν αυξημένες πιθανότητες εμφάνισης σε ορισμένους ιστότοπους. Οι περισσότεροι χρήστες όταν πλοηγούνται στο Web θα συναντήσουν συχνά το «λέξη» XXX σε μια ιστοσελίδα πορνογραφικού περιεχομένου, αλλά σπάνια σε άλλου τύπου ιστοσελίδες. Το φίλτρο δεν μπορεί να υπολογίσει εκ των προτέρων τις πιθανότητες συνδυασμού περιεχομένου με την εμφάνιση μιας λέξης, αλλά πρέπει πρώτα να εκπαιδευτεί. Για να συμβεί αυτό, ένας εξωτερικός χρήστης πρέπει να αναφέρει κατά πόσο η συγκεκριμένη σελίδα είναι πορνογραφικού περιεχομένου ή όχι. Για όλες τις λέξεις σε κάθε σελίδα το φίλτρο θα αναπροσαρμόζει συνεχώς τις πιθανότητες να εμφανιστούν σε μια ακατάλληλη σελίδα σε σχέση

με μια που δεν είναι. Έτσι ένα Bayesian φίλτρο περιεχομένου θα μάθει ότι ο συνδυασμός των λέξεων Paris Hilton είναι πιθανό να περιέχεται σε ιστοσελίδα με τολμηρές εικόνες, ενώ η μεμονωμένη εμφάνιση των λέξεων Paris και Hilton, όχι [76].

Το φιλτράρισμα του περιεχομένου του διαδικτύου μπορεί να αντιμετωπιστεί σαν ένα πρόβλημα συγκριτικής κατάταξης κειμένου, μια που μεγάλο κομμάτι της διακινουμένης πληροφορίας είναι κείμενο. Ένα κρίσιμο σημείο είναι οι πολλές κατηγορίες του προς αποκλεισμό κειμένου (πορνογραφία, τζόγος, ρατσισμός, μίσος κ.α.), ο εντοπισμός των οποίων είναι απαραίτητος από τον κατηγοριοποιητή, προκειμένου να δοθεί η δυνατότητα διαχείρισης του ελέγχου. Η πιο συνηθισμένη αντιμετώπιση είναι να δημιουργηθεί ξεχωριστός κατηγοριοποιητής για κάθε κατηγορία [29].

Τα σημαντικότερα πλεονεκτήματα τη επιλογής αυτής είναι :

- Ο υψηλός βαθμός αυτοματοποίησης, μια που οι μηχανικοί αναπτύσσουν ουσιαστικά αυτοματοποιημένους κατηγοριοποιητές.

- Επαναχρησιμοποίηση, μια που οι ίδιοι κατηγοριοποιητές είναι δυνατό να χρησιμοποιηθούν σε διαφορετικές κατηγόριες αλλάζοντας απλά το σύνολο εκπαίδευσης τους.

- Υψηλή διαθεσιμότητα (σήμερα και μελλοντικά) των επαγωγικών αλγορίθμων.

- Ακρίβεια και αποτελεσματικότητα κατάταξης η οποία προσεγγίζει αυτή που γίνεται από ομάδες ανθρώπων.

Αναγνώριση Εικόνων

Πολλές από τις υπάρχουσες τεχνικές ελέγχου κατατάσσουν το περιεχόμενο ενός ιστότοπου ως πορνογραφικό ή ασφαλές χρησιμοποιώντας το κείμενο που αυτός περιέχει. Ωστόσο, τέτοιες τεχνικές παρουσιάζουν κάποιους περιορισμούς που σχετίζονται με την επιλογή της γλώσσας ή την ασάφεια του κειμένου. Επιπλέον αρκετές ιστοσελίδες με περιεχόμενο για ενήλικες περιέχουν πολλές ή και μόνο εικόνες προκειμένου να είναι πιο ελκυστικές με αποτέλεσμα, η εμπλοκή των εικόνων στη διαδικασία φιλτραρίσματος να αποτελεί μονόδρομο.

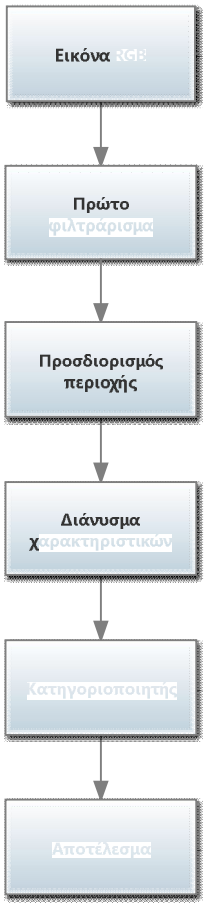
Η επεξεργασία εικόνας είναι ένας από τους πιο αναπτυσσόμενους τομείς και με δεδομένη τη πολύ μεγάλη και συνεχώς αυξανόμενη χρήση εικόνων στην επικοινωνία στο διαδίκτυο η εφαρμογή της στον έλεγχο περιεχομένου είναι σημαντική. Η κατηγορία περιεχομένου στην οποία εφαρμόζεται συνηθέστερα η αναγνώριση εικόνων με σκοπό τον αποκλεισμό τους είναι η πορνογραφία και το γυμνό ανθρώπινο σώμα, χωρίς να αποκλείονται άλλοι τομείς.

Μία πιο τις πρώτες, αλλά και πιο δημοφιλής μεθόδους φιλτραρίσματος περιεχομένου εικόνας είναι η ανίχνευση δέρματος. Σε αυτή τη προσέγγιση αναζητούνται περιοχές της εικόνας που προβάλουν ανθρώπινη επιδερμίδα και από αυτές εξάγονται κάποια ομαδοποιημένα χαρακτηριστικά. Αυτά τα χαρακτηριστικά τροφοδοτούν ένα γεωμετρικό φίλτρο με βάση τη σκελετική δομή για τον εντοπισμό ανθρώπινης παρουσίας [29].

Αρχικά αναγνωρίζεται το ανθρώπινο δέρμα και κατά συνέπεια το γυμνό σώμα μέσω των χρωματικών ιστογραμμάτων της εικόνας. Το χρώμα του ανθρώπινου δέρματος σε μια φωτογραφία είναι συνδυασμός τριών παραγόντων : αίμα, μελανίνη και συνθήκες φωτός. Τα δύο πρώτα στοιχεία περιέχουν τα χρώματα κόκκινο, κίτρινο και καφέ, για αυτό και τα χρώματα του δέρματος βρίσκονται μεταξύ αυτών των αποχρώσεων. Οι συνθήκες φωτός δεν είναι δυνατό να ελεγχθούν, αλλά μπορούν να εξαχθούν χαρακτηριστικά που δεν εξαρτώνται από αυτή την παράμετρο [76].

Εικόνα 3.1: Φωτογραφία με γυμνό σώμα πριν και μετά την ανίχνευση δέρματος [67].

Για τον εντοπισμό των περιοχών του ανθρώπινου δέρματος απαιτούνται 8bit RGB εικόνες. Μια που οι περισσότερος εικόνες ακολουθούν το πρότυπο jpeg, το πρώτο βήμα είναι να μειωθεί ο αριθμός των χρωμάτων για να μετατραπούν σε πρότυπο RGB. Κάποια φίλτρα μείωσης κλιμάκωσης ή θορύβου μπορούν επίσης να εφαρμοστούν σε αυτό το βήμα. Ακολούθως, επιλέγονται τα εικονοστοιχεία των οποίων το χρώμα είναι πολύ κοντά σε αυτό του δέρματος και μετά αυτά που έχουν παραπλήσιο χρώμα και υφή. Στη συνέχεια οι περιοχές pixel που προβάλουν δέρμα ομαδοποιούνται εφόσον παρουσιάζουν ομοιότητες στα χαρακτηριστικά τους πάνω από κάποιο όριο πχ 50% με 60%. Από τα χαρακτηριστικά αυτών των περιοχών δημιουργούνται διανύσματα, ψηφιακές υπογραφές, που είναι δυνατό να χρησιμοποιηθούν για την κατηγοριοποίηση της υπόλοιπης εικόνας αλλά και για τη τροφοδότηση γεωμετρικών φίλτρων για την σκελετική ανίχνευση ανθρώπινης παρουσίας [29].



Σχήμα 3.9: Βασικά στάδια στην επεξεργασία και κατηγοριοποίηση εικόνας [29].

Η παραπάνω διαδικασία αν και αποτελεσματική απαιτεί συνήθως μεγάλο χρονικό διάστημα προκειμένου να εφαρμοστεί για αυτό και έχουν προταθεί και άλλες μέθοδοι με κυριότερη αυτή που χρησιμοποιεί αναγνώριση βασισμένη σε κυματομορφές. Στην περίπτωση αυτή γίνεται

εφαρμογή ενός συνδυασμού από διάφορα φίλτρα όπως φίλτρο εικόνας, φωτοανιχνευτές, φίλτρο χρωματικού ιστογράμματος, φίλτρο υφής και ενός αλγόριθμου ανίχνευσης σχήματος βασισμένου σε κυματομορφές. Ο αλγόριθμος συγκρίνει το σημασιολογικό περιεχόμενο των εικόνων που περιέχουν ανθρώπινα σώματα. Χρησιμοποιώντας στιγμιαία ανάλυση υφής, ιστογραμμάτων και στατιστική ο αλγόριθμος παράγει διανύσματα χαρακτηριστικών που παρέχουν υψηλής ακρίβειας αναγνώριση του γυμνού ανθρώπινου σώματος σε μια φωτογραφία [29].

Παρόλο που οι τεχνικές ανίχνευσης εικόνας μπορούν να φτάσουν σε πολύ υψηλά ποσοστά επιτυχίας στην προσδιορισμό ανεπιθύμητου περιεχομένου, ακόμη και κοντά στο 90%, υπάρχουν μια σειρά από παράγοντες που αυξάνουν το βαθμό δυσκολίας της εφαρμογής τους [29] :

- Οι περισσότερες εικόνες που περιέχουν ανομοιόμορφο φόντο.
- Η εικόνα μπορεί να περιέχει κείμενο, όπως αριθμούς τηλεφώνου, διευθύνσεις URL, το οποίο λειτουργεί ως θόρυβος.
- Υπάρχει μεγάλη διακύμανση στο χρώμα, από ασπρόμαυρο έως 24 bit χρώμα.
- Κάποιες εικόνες έχουν πολύ χαμηλή ανάλυση.
- Υπάρχει μεγάλη διαφοροποίηση στην γωνία λήψης μια όψης.
- Σε μια εικόνα περιέχονται πλήθος ανθρώπων.
- Είναι δυνατό να περιέχονται άνθρωποι και ζώα.
- Μπορεί να υπάρχουν άνθρωποι μερικώς ντυμένοι.
- Είναι δυνατό να προβάλλονται μόνο τμήματα του ανθρώπινου σώματος.

Τύπος Αρχείου

Η ανάλυση του τύπου των αρχείων χρησιμοποιείται κυρίως για να εμποδιστεί η πρόσβαση σε συγκεκριμένα είδη αρχείων, συνήθως πολυμέσων, για παράδειγμα αρχεία MP3 ή video streams.

Το προϊόν που χρησιμοποιείται θα σαρώσει όλα τα διακινούμενα αρχεία, για να ανιχνεύσει επεκτάσεις αρχείων που δείχνουν συγκεκριμένο αρχείο ή τύπους μέσων (π.χ. το music.mp3 αρχείο είναι πιθανώς ένα αρχείο MP3, δεδομένου ότι έχει την επέκταση .mp3 και ως εκ τούτου θα πρέπει να αποκλειστεί από ένα προϊόν που έχει ρυθμιστεί για να μπλοκάρει MP3 αρχεία).

Ορισμένα προϊόντα αναλύουν φαινομενικά αθώα αρχεία για να ελέγξουν αν όντως είναι του τύπου που υποδηλώνει το όνομα τους ή αν τα στοιχεία τους δείχνουν ότι είναι κάποιου τύπου που συνήθως μπλοκάρεται. Για παράδειγμα είναι δυνατό να εντοπίσουν την υπογραφή των δεδομένων ενός αρχείου MP3 τύπου, ακόμη και αν η επέκταση του έχει αλλάξει από .mp3 σε κάτι άλλο. Πέρα από αυτό στη συγκεκριμένη τεχνική, το περιεχόμενο των αρχείων δεν αναλύεται βαθύτερα [79].

Η τεχνική αυτή επιλέγεται συχνά από οργανισμούς που ενδιαφέρονται να ελέγξουν το ηλεκτρονικό ταχυδρομείο τους για επιβλαβή επισυναπτόμενα ή να περιορίσουν την κατασπατάληση του εύρους ζώνης τους από το διαμοιρασμό συνήθως αρχείων πολυμέσων (μουσική, ταινίες κτλ) [01].

Σύνδεσμοι

Η ανάλυση των συνδέσμων είναι μια απλή μέθοδος προσδιορισμού της φύσης μιας σελίδας. Είναι αρκετά πιθανό μια ιστοσελίδα να έχει περιεχόμενο παρόμοιο με τις σελίδες στις οποίες αυτή συνδέεται [79].

Προφίλ

Η χρήση τεχνητής νοημοσύνης έχει σαν αποτέλεσμα ένα νέο τύπο προϊόντων ελέγχου περιεχομένου που βασίζονται σε συμβάντα του παρελθόντος, με σκοπό τη συνεχή εκπαίδευση τους αλλά και την αποσύνδεση του περιεχομένου από την πηγή του [67]. Στην περίπτωση αυτή γίνεται μια προσπάθεια να κατηγοριοποιηθεί το αιτούμενο περιεχόμενο συγκρίνοντας χαρακτηριστικά του όπως μορφή, χρήση λέξεων, λειτουργίες, με άλλο γνωστό και ήδη χαρακτηρισμένο ως προβληματικό. Είναι δυνατό να αναλυθεί μια ιστοσελίδα προκειμένου να εκτιμηθεί, αν για παράδειγμα είναι πορνογραφικού εμπορικού περιεχομένου, από τη κάλυψη της σε μεγάλο ποσοστό από φωτογραφίες, ανάμεσα και σε συνδυασμό με άλλα χαρακτηριστικά [01].

Η διαδικασία αυτή είναι συχνά αρκετά απαιτητική υπολογιστικά για αυτό και εφαρμόζεται συνήθως ασύγχρονα σε σχέση με τη μετάδοση της πληροφορίας, περισσότερο για να καλύψει την απαίτηση συμπλήρωσης μιας λίστας παρά να φιλτράρει σε πραγματικό χρόνο τα αιτήματα για πρόσβαση σε περιεχόμενο [01].

Φήμη (Reputation)

Στην επιλογή αυτή αξιολογούνται οι πηγές της επικοινωνίας στην βάση ιστορικών αλλά και τρεχουσών πληροφοριών για κακόβουλες συμπεριφορές και πιθανολογείται ότι και μελλοντικό περιεχόμενο με την ίδια προέλευση θα είναι επιβλαβές και ακατάλληλο.

Η μέθοδος αυτή χρησιμοποιείται κυρίως για τον έλεγχο της ανεπιθύμητης αλληλογραφίας αν και τελευταία εφαρμόζεται όλο και πιο συχνά για έλεγχο περιεχομένου στον παγκόσμιο ιστό και για αντιμετώπιση θεμάτων ασφαλείας και απάτης στο διαδίκτυο [01].

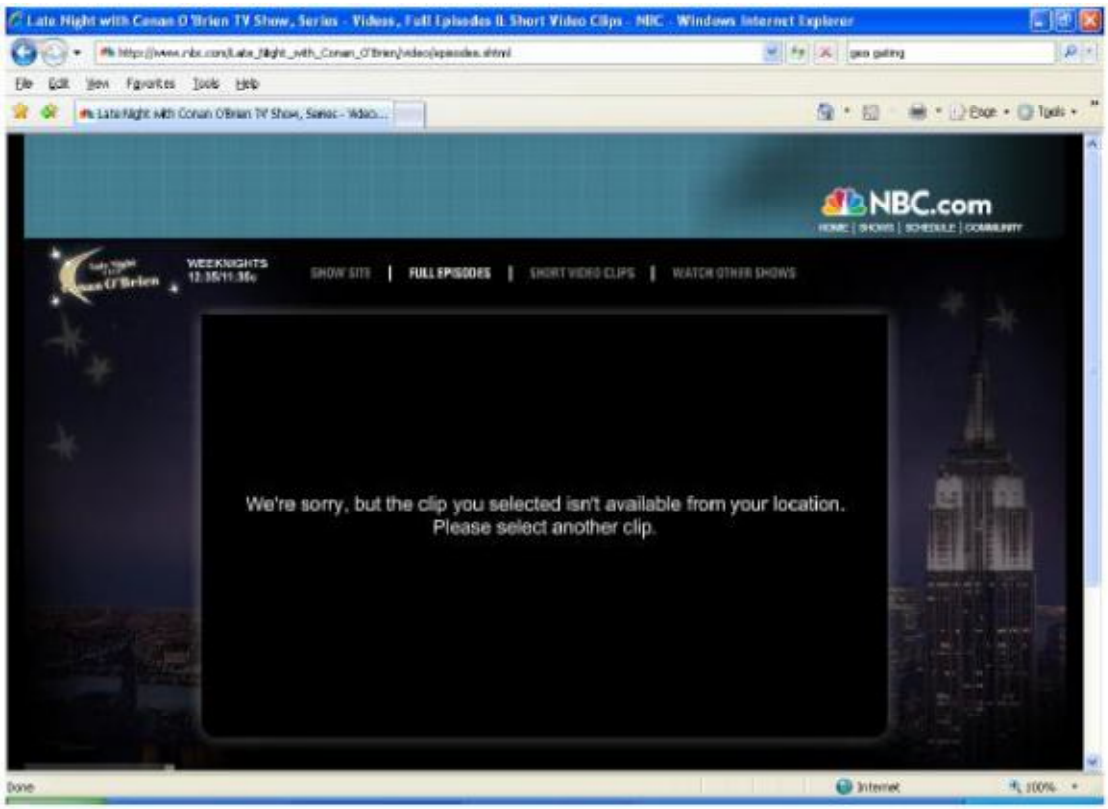
Περιοχή (Location)

Μια άλλη μέθοδος περιορισμού της πρόσβασης στο περιεχόμενο είναι αυτό που συχνά αναφέρεται ως «geo-gating». Ο όρος αυτός είναι ένας από τους πολλούς που χρησιμοποιούνται για να προσδιορίσουν μια τεχνολογική προσέγγιση που εφαρμόζεται κυρίως από αυτούς που είναι υπεύθυνοι για τη φιλοξενία περιεχομένου, και όχι από τους παρόχους διαδικτύου ή τις εθνικές κυβερνήσεις.

Είναι γενικά δυνατό να προσδιοριστεί η γεωγραφική θέση ενός χρήστη ή ενός παρόχου περιεχομένου, εξετάζοντας τη IP διεύθυνση του υπολογιστή που ζητά ή παρέχει το περιεχόμενο. Στο μητρώο με τα στοιχεία της IANA (Internet Assigned Numbers Authority - Αρχή για τη Διευθυνσιοδότηση στο Διαδίκτυο) είναι καταχωρημένη η τοποθεσία κάθε παρόχου στον οποίο έχουν αποδοθεί ένα σύνολο από IP διευθύνσεις. Για να υπάρχει μεγαλύτερη ακρίβεια στην πληροφορία οι πάροχοι υπηρεσιών έχουν εμπλουτίσει τα δεδομένα σχετικά με τη θέση των διευθύνσεων IP, τουλάχιστον μέχρι επίπεδο πόλης. Αυτή η δυνατότητα του εντοπισμού τη θέσης ενός υπολογιστή με βάση τη διεύθυνση IP, είναι κοινώς γνωστή ως «geo-location».

Στο geo-gating χρησιμοποιείται η δυνατότητα να αναγνωρίζονται οι χρήστες από το geo-location. Οι δικαιοδόχοι των πνευματικών δικαιωμάτων του περιεχομένου που προστατεύεται, όπως τηλεοπτικές εκπομπές, κινηματογραφικές ταινίες ή μουσική, περιορίζουν την πρόσβαση

στο περιεχόμενο για τους χρήστες που βρίσκονται στην περιοχή για την οποία ισχύουν τα πνευματικά δικαιώματα βασισμένοι στις IP διευθύνσεις τους. Για παράδειγμα μια τηλεοπτική σειρά μπορεί να είναι διαθέσιμη στις Η.Π.Α. δωρεάν μέσω του ιστότοπου του καναλιού που την προβάλει, την επόμενη περίοδο από αυτή της τηλεοπτικής μετάδοσης. Για τους χρήστες με IP διευθύνσεις από την Ευρώπη είναι δυνατό να μην επιτραπεί η θέαση της σειράς μέσω του ιστότοπου του καναλιού, με δεδομένο ότι για τη γεωγραφική αυτή περιοχή αυτή θα είναι η πρώτη περίοδος τηλεοπτικής μετάδοσης και συνεπώς διαφημιστικής εκμετάλλευσης της [86].



Εικόνα 3.2: Άρνηση προβολής περιεχόμενου με βάση την σε περιοχή από την οποία ζητείται [86].

Αποτύπωμα-Ψηφιακή Υπογραφή

Το περιεχόμενο μπορεί να ταυτοποιηθεί χρησιμοποιώντας ψηφιακές υπογραφές-αποτυπώματα τα οποία επιτρέπουν την κατηγοριοποίηση πληροφορίας που έχει χαρακτηριστεί ανεπιθύμητη σε προηγούμενους ελέγχους. Στην περίπτωση αυτή δημιουργείται μια μοναδική τιμή με τη βοήθεια αλγόριθμων κατακερματισμού (όπως SHA1, SHA256 ή MD5), η οποία συνδέεται αποκλειστικά με το περιεχόμενο ενός αρχείου.

Για παράδειγμα μια φωτογραφία παιδικής πορνογραφίας (με όνομα αρχείου «preteen.jpg») έχει υπολογιστεί ότι έχει μια μοναδική παγκοσμίως τιμή κατακερματισμού «87e1a46d2529fe4f42a75789f0bae7a1», (MD5). Η ψηφιακή αυτή υπογραφή είναι μια σύντομη αναπαράσταση του περιεχομένου του αρχείου, από την οποία το αρχείο δεν μπορεί να αναπαραχθεί, αλλά μπορεί να χρησιμοποιηθεί για να ταυτοποιηθεί. Αν ανακαλυφθεί μια εικόνα (με όνομα αρχείου «unknown.jpg») σε μια διαφορετική περιοχή και η τιμή κατακερματισμού που έχει υπολογιστεί είναι ίδια με αυτή που υπολογίστηκε για την εικόνα preteen.jpg, αυτό είναι μια απόδειξη ότι και τα δύο αρχεία περιέχουν ακριβώς την ίδια πληροφορία. Με αυτό τον τρόπο αποδεικνύεται ότι η δεύτερη εικόνα δεν είναι αθώα και αποκλείεται η πρόσβαση σε αυτήν [13].

Στην περίπτωση ηχητικών αρχείων οι ψηφιακές υπογραφές μπορούν να είναι αποτέλεσμα εφαρμογής αλγορίθμων που μετατρέπουν τα ψυχο-αντιληπτικά ακουστικά χαρακτηριστικά ενός αρχείου ήχου, όπως αυτό ακούγεται, σε ένα είδος ψηφιακού αποτυπώματος. Στη συνέχεια η σύγκριση του αποτυπώματος με μια βιβλιοθήκη μπορεί να οδηγήσει στην ταυτοποίηση του αρχείου και το πιθανό αποκλεισμό του [86].

Αναγνώριση στα Κοινωνικά Δίκτυα

Τα τελευταία χρόνια τα Κοινωνικά Δίκτυα που είναι σε Απευθείας σύνδεση (On Line Social Networks – OSNs) και οι υπηρεσίες μικρό-ιστολογίων (micro blogs) έχουν γίνει ένα ιδιαίτερα δημοφιλές μέσο επικοινωνίας, διαμοιρασμού και διάδοσης μεγάλης ποσότητας πληροφορίας που αφορά την ανθρώπινη ζωή και όχι μόνο. Καθημερινά διακινείται μεγάλη ποσότητα περιεχομένου διαφορετικής μορφής όπως σύντομο κείμενο, φωτογραφίες, βίντεο κ.α. [89].

Η αναγνώριση του περιεχομένου στην περίπτωση των Κοινωνικών Δικτύων παρουσιάζει ιδιαιτερότητες, λόγω κάποιων βασικών χαρακτηριστικών που έχει η επικοινωνία με τον τρόπο αυτό [16] :

- Η πληροφορία έχει ιδιαίτερα δυναμικό χαρακτήρα.
- Η επικοινωνία γίνεται σε πραγματικό χρόνο στις περισσότερες περιπτώσεις.
- Η ποσότητα του διακινούμενου περιεχομένου είναι πολύ μεγάλη.

- Οι συνθήκες και οι σχέσεις που αποκαθίστανται μεταξύ των χρηστών έχουν ιδιαίτερα μεταβαλλόμενο χαρακτήρα.

- Το κείμενο είναι συνήθως ιδιαίτερα σύντομο μη δίνοντας τη δυνατότατα για κατάλληλο δείγμα στους συνήθεις κατηγοριοποιητές (classifiers) κειμένου.

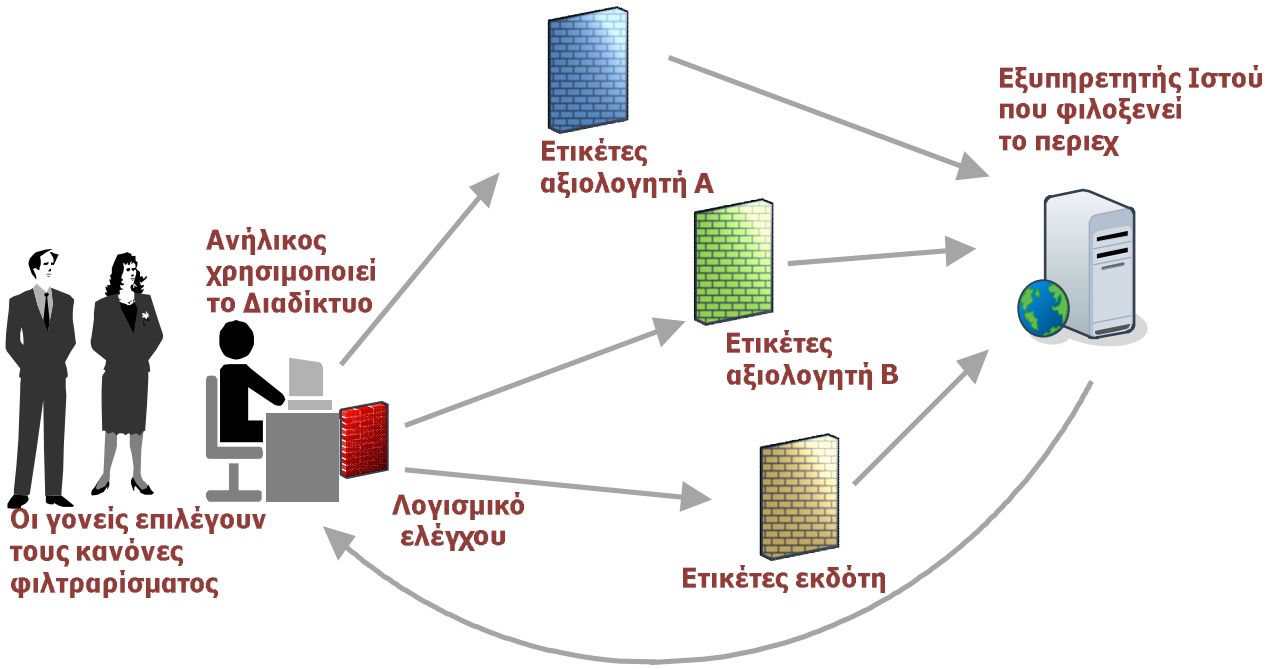
- Η γλώσσα είναι συνήθως άτυπη δημιουργώντας διαφορετικές σημασιολογικές ερμηνείες, ανάλογα τις συνθήκες. Το λεξιλόγιο μεταβάλλεται και ή χρήση διαφορετικών γλωσσών στην ίδια αναφορά δεν είναι κάτι σπάνιο.

Η ταυτοποίηση του περιεχομένου στις περιπτώσεις αυτές γίνεται με συστήματα τα οποία συνδυάζουν σχεδόν όλες τις προηγούμενες τεχνικές αναγνώρισης λαμβάνοντας υπόψη τις κατά περίπτωση ιδιαιτερότητες. Έτσι οι κατηγοριοποιητές είναι εξειδικευμένοι, για σύντομο κείμενο (short text classifiers), η ανάλυση εικόνας επιβάλλεται να είναι σε πραγματικό χρόνο κα.

Η πιο σημαντική όμως παράμετρος που διαφοροποιεί τις μεθόδους ελέγχου του περιεχομένου στην συγκεκριμένη περιοχή είναι η σχέση του καταναλωτή της πληροφορίας με την πηγή προέλευσης της. Ο βαθμός της σχέσης μπορεί να είναι άμεσα καθορισμένος από το χρήστη, είναι όμως δυνατό να προσδιορίζεται και έμμεσα μέσω των σχέσεων του με τρίτους ως προς την αναφορά του περιεχομένου. Στην περίπτωση αυτή λαμβάνεται υπόψη το πολύ-επίπεδο της εμπιστοσύνης που δημιουργείται εξορισμού σε ένα Κοινωνικό Δίκτυο [89].

3.5.3 Αναγνώριση με Βάση τη Διαβάθμιση και Σήμανση Περιεχομένου

Μια άλλη λύση για την εφαρμογή της λογοκρισίας είναι η βαθμονόμηση και η σήμανση του περιεχομένου, σε συνδυασμό με την οριοθέτηση του, συνήθως από τον καταναλωτή του. Ως βαθμονόμηση ή διαβάθμιση ή αξιολόγηση του περιεχομένου, θεωρείται η κατηγοριοποίηση και ετικετοδότηση του σύμφωνα με κάποια κριτήρια φιλτραρίσματος.



Σχήμα 3.10: Βαθμονόμηση περιεχομένου με ετικετοδότηση.

Η ιδέα της σήμανσης δεν είναι κάτι νέο. Για κάποια μέσα, όπως οι ταινίες στον κινηματογράφο, έχει εφαρμοστεί εδώ και πολλά χρόνια. Επιπλέον, σε πολλές χώρες τα τηλεοπτικά προγράμματα βαθμονομούνται και χαρακτηρίζονται με τη βοήθεια σημάτων. Στο περιεχόμενο στον παγκόσμιο ιστό μπορεί να ακολουθηθεί η προσέγγιση της αυτό-διαβάθμισης, με την έννοια ότι η αξιολόγηση γίνεται από τον δημιουργό μιας ιστοσελίδας. Εναλλακτικά, τρίτα μέρη, εξωτερικοί ουσιαστικά οργανισμοί είναι δυνατό να χρησιμοποιηθούν. Συνήθως η διαδικασία αυτή δεν πραγματοποιείται ταυτόχρονα με την αίτηση για πρόσβαση στο περιεχόμενο, μια που αυτό θα προκαλούσε σημαντικές καθυστερήσεις [27]. Σύμφωνα με τη στρατηγική που ακολουθείται για τη σήμανση, επισυνάπτεται στους ιστότοπους, μια ετικέτα η οποία αποτελείται από μετα-δεδομένα που περιγράφουν το περιεχόμενο τους.

Στρατηγική Βαθμονομημένης Σήμανσης – PICS

Η πιο γνωστή προσέγγιση βαθμονόμησης περιεχομένου είναι το PICS (Platform for Internet Content Selection - Πλατφόρμα για τη Διαλογή του Περιεχομένου στο Διαδίκτυο) [60], ένα πρότυπο του W3C (World Wide Web Consortium – Κοινοπραξία για τον Παγκόσμιο Ιστό) [61].

Το PICS είναι ένα γενικού σκοπού σύστημα για την τοποθέτηση ετικετών στα έγγραφα που παρουσιάζονται στον παγκόσμιο ιστό. Οι ετικέτες του PICS περιέχουν μια ή περισσότερες

αξιολογήσεις που εκδίδονται από την υπηρεσία βαθμονομήσεων. Το PICS συγκροτεί την πλατφόρμα πάνω στην οποία μπορούν να χτιστούν οι υπηρεσίες βαθμονόμησης.

Το λογισμικό που υλοποιεί το PICS έχει σημαντικά τεχνολογικά πλεονεκτήματα συγκρινόμενο με απλά προϊόντα ελέγχου πρόσβασης :

- Επιτρέπει τον αποκλεισμό ανά έγγραφο.
- Δίνει τη δυνατότητα λήψης αξιολογήσεων από περισσότερες από μια πηγές.
- Μια που το PICS αποτελεί ένα γενικότερο πλαίσιο για την αξιολόγηση της πληροφορίας, διαφορετικοί χρήστες ορίζουν διαφορετικούς κανόνες πρόσβασης.

Το PICS μπορεί να συσχετιστεί με πολλών ειδών ετικέτες οι οποίες είναι δυνατό να [25]:

- Καθορίσουν το τύπο ή τη ποσότητα σεξουαλικού ή βλάσφημου περιεχομένου σε ένα κείμενο
- Αξιολογήσουν πότε μια φωτογραφία είναι υπερεκτεθειμένη
- Καθορίσουν πότε ένα κείμενο περιέχει λόγους μίσους
- Προσδιορίσουν τις πολιτικές τάσεις ενός κειμένου
- Μπορούν να αναφέρουν εάν ένα chat room εποπτεύεται
- Μπορούν να υποδείξουν πότε ένα κείμενο έχει δημιουργηθεί, βοηθώντας στον καθορισμό των πνευματικών δικαιωμάτων.

Οι επικριτές της πλατφόρμας αυτής συνήθως της καταλογίζουν [25] ότι είναι δυνατό να οδηγήσει πολλές φορές στην αποτροπή πρόσβασης σε περιεχόμενο ακόμη και με υποψία μη αποδεκτού υλικού ή και στον αποκλεισμό συνολικά της πρόσβασης στο Διαδίκτυο.

Πολλοί από τους προμηθευτές υπηρεσιών στο δίκτυο υποστηρίζουν το PICS και προωθούν στους συνδρομητές λογισμικό που είναι συμβατό. Μια πολύ σημαντική υπηρεσία-σχήμα αξιολόγησης είναι το RSACi (Recreational Software Advisory Council - Γνωμοδοτικό Συμβούλιο

για Ψυχαγωγικό Λογισμικό) [27], ένας μη κερδοσκοπικός ανεξάρτητος οργανισμός. Το σύστημα RSACi παρέχει στους καταναλωτές πληροφορίες σχετικά με το επίπεδο παρουσίας, σε μια κλίμακα μεταξύ του 0 και του 4, περιεχομένου σχετιζόμενου με βία, σεξ, γυμνό και προσβλητική γλώσσα, σε παιχνίδια και ιστοσελίδες. Οι κλίμακες αυτές συνοψίζονται στον παρακάτω πίνακα [27] :

Επίπεδο	**Περιγραφή Βαθμονόμησης Βίας**	**Περιγραφή Βαθμονόμησης Γυμνού**	**Περιγραφή Βαθμονόμησης Σεξ**	**Περιγραφή Βαθμονόμησης Γλώσσας**
4	βιασμός, έντονη βία	εμπρόσθιο γυμνό, χαρακτηρισμένο ως προκλητική περιβολή	σαφείς σεξουαλικές πράξεις ή σεξουαλικά εγκλήματα	ωμή, χυδαία γλώσσα, ακραίος λόγος μίσους
3	επιθετική βία, δολοφονία	εμπρόσθιο γυμνό	μη Σαφείς σεξουαλικές πράξεις	υβριστική γλώσσα, λόγος μίσους
2	καταστροφή αντικειμένων	μερικό γυμνό	σεξουαλικό άγγιγμα πάνω από τα ρούχα	μέτρια βλασφημία, αισχρολογία
1	τραυματισμός ανθρώπων	αποκαλυπτική περιβολή	φλογερό φιλί	ήπια βλασφημία
0	κανένα από τα παραπάνω ή σχετιζόμενα με το αθλητισμό	κανένα από τα παραπάνω	κανένα από τα παραπάνω, αθώο φιλί, ειδύλλιο	κανένα από τα παραπάνω

Πίνακας 3.1: Τα επίπεδα RSACi για τη βία, το γυμνό, το σεξ και τη γλώσσα.

Το RSACi είναι το προηγηθέν σχήμα του ICRA (Internet Content Rating Association – Ένωση για την Αξιολόγηση του Περιεχομένου στο Διαδίκτυο) [27] και δεν είναι σήμερα ευρέως διαθέσιμο.

Γενικά, το PICS μπορεί να χρησιμοποιηθεί για τον χαρακτηρισμό του περιεχόμενου όχι μόνο από τους αυτόνομους ιδιοκτήτες ή εκδότες του στο διαδίκτυο, αλλά και από τρίτα μέρη, όπως ένα εξειδικευμένο γραφείο αξιολόγησης, έτσι :

- Αυτός που έχει τα δικαιώματα κάποιου περιεχομένου ή αυτός που το δημοσιεύει στο δίκτυο, αν θέλει να το χαρακτηρίσει θα πρέπει πρώτα να επιλέξει το λεξιλόγιο αξιολόγησης που θα χρησιμοποιήσει.

- Εκτός από την περίπτωση του αυτο-χαρακτηρισμού, σαν μια ενέργεια ανεξάρτητης αξιολόγησης, δεν είναι απαραίτητη η συνεργασία με τον κάτοχο ή τον εκδότη του περιεχομένου που το χαρακτηρίζει. Οποιοσδήποτε προβαίνει σε χαρακτηρισμό, αντί να επισυνάπτει απλά ετικέτες στα έγγραφα, μπορεί να τις διανέμει μέσω ξεχωριστών εξυπηρετητών (label bureau).

Οι προδιαγραφές των υπηρεσιών αξιολόγησης του PICS έχουν σχεδιαστεί για να διευκολύνουν πολλά διαφορετικά είδη βαθμονόμησης στο διαδίκτυο. Η υπηρεσία αξιολόγησης μπορεί να είναι κάποιο πρόσωπο, οργανισμός ή οποιαδήποτε οντότητα εκδίδει βαθμονόμηση. Η αξιολόγηση μπορεί να διατίθεται είτε άμεσα μαζί με το αξιολογούμενο περιεχόμενο, είτε από ιστοσελίδα τρίτου οργανισμού, ή ακόμη και με κάποιο άλλο ηλεκτρονικό μέσο.

Οι προδιαγραφές του PICS καθορίζουν τη σύνταξη για τα αρχεία κειμένου, που περιγράφουν τους διαφορετικούς τύπους βαθμονόμησης που μια υπηρεσία αυτού του είδους μπορεί να εκδώσει. Αυτό επιτρέπει στα προγράμματα να αναλύσουν τη σύνταξη και συνάγουν τα είδη των αξιολογήσεων που μια υπηρεσία παρέχει.

Ένα δείγμα υπηρεσίας αξιολόγησης βασισμένο στο σχέδιο του συστήματος βαθμονόμησης της MPAA (Motion Picture Association of America – Αμερικάνικη Ένωση Κινηματογραφικών Ταινιών) είναι αυτό που ακολουθεί [27] :

((PICS-version 1.0)
(rating-system http://moviescale.org/Ratings/Description/)
(rating service "http://moviescale.org/v1.0")
(icon "icons/moviescale.gif")
(name "The Movies Rating Service")
(description "A rating service based on the MPAA's movie rating scale")
(category
(transmit-as "r")
(name "Rating")
(label (name "G") (value 0) (icon "icons/G.gif"))
(label (name "PG") (value 1) (icon "icons/PG.gif"))
(label (name "PG-13") (value 2) (icon "icons/PG-13.gif"))
(label (name "R") (value 3) (icon "icons/R.gif"))

(label (name "NC-17") (value 4) (icon "icons/NC-17.gif"))))

Η περιγραφή της αξιολόγησης υποδεικνύει τη θέση Διαδίκτυο, όπου είναι δυνατό να βρεθεί η πληροφορία για το σύστημα και την υπηρεσία βαθμονόμησης, δίνει ένα όνομα και δημιουργεί μια μοναδική κατηγορία αξιολόγησης με την επωνυμία «Rating». Τα αντικείμενα τα οποία αξιολογούνται χαρακτηρίζονται από το μοντέλο με μια από τις πέντε τιμές : G, PG, PG-13 ή NC-17 και σχετίζονται με μια περιγραφή.

Η αξιολόγηση από το σύστημα PICS περιγράφεται σε ένα αρχείο τύπου MIME (Multipurpose Internet Mail Extensions) Στην εφαρμογή της πλατφόρμας γίνεται εκτεταμένη χρήση του συνδυασμού όνομα./τιμή, με την έννοια «το όνομα έχει την τιμή».

Οι προδιαγραφές των ετικετών του PICS καθορίζουν τη σύνταξη αυτών που θα χρησιμοποιηθούν σε κάθε έγγραφο. Οι ετικέτες είναι δυνατό να ανακτηθούν είτε από τον παγκόσμιο ιστό μέσω μηχανών αναζήτησης ή να είναι ενσωματωμένες αυτόματα στην κεφαλίδα του εγγράφου.

Για παράδειγμα [05] ακολουθεί μια ετικέτα που κατατάσσει μια διεύθυνση URL με την προαναφερθείσα υπηρεσία :

(PICS-1.1 “http://moviescale.org/v1.0”
Labels
on “2002.6.01T00:01-0500”
until “2003.12.31T23:59-0500”
for “http://www.missionimpossible.com/”

by “J.B.” ratings (r 0))

Η ετικέτα περιγράφει την ιστοσελίδα της ταινίας Mission Impossible (Επικίνδυνη Αποστολή) χρησιμοποιώντας την εικονική υπηρεσία χαρακτηρισμού που περιγράφηκε. Η ετικέτα έχει αξιολόγηση (r, 0), δημιουργήθηκε τον Ιούνιο του 1997 από τον J.B., ήταν έγκυρη μέχρι το τέλος της χρονιάς εκείνης και αφορά την πληροφορία που είναι αποθηκευμένη στη διεύθυνση http://www.missionimpossible.com/. Ακόμη και αν η ταινία Mission Impossible έχει βαθμολογηθεί με R, η σελίδα βαθμολογήθηκε με G. Η τιμή G μεταδίδεται με το 0, χρησιμοποιώντας την υπηρεσία βαθμονόμησης http://moviewscale.org/v1.0.

Η βαθμολόγηση μπορεί να περιλαμβάνει περισσότερες από μια τιμές, για παράδειγμα αν έχει δύο κλίμακες θα μπορούσε να είναι (r 3 n 4).

Οι ετικέτες είναι δυνατό να συμπιεστούν αφαιρώντας όλη την πληροφορία που περιέχουν εκτός από το χαρακτηρισμό. Έτσι ή προηγούμενη ετικέτα θα μπορούσε να μεταδοθεί ως :

(PICS-1.1 "http://moviescale.org/v1.0" r 0)

Επιπλέον, οι ετικέτες προαιρετικά συμπεριλαμβάνουν ένα δείκτη κατακερματισμού, που προκύπτει εφαρμόζοντας μια συνάρτηση κατακερματισμού στο μήνυμα. Αυτό επιτρέπει στο λογισμικό να εξακριβώσει την ακεραιότητα του περιεχομένου μετά τη δημιουργία της ετικέτας. Επίσης μπορούν να ενσωματωθούν ψηφιακές υπογραφές βοηθώντας την πιστοποίηση της ακεραιότητας και της ταυτότητας της πληροφορίας. Αυτό το γεγονός εξασφαλίζει τη διανομή από μια ιστοσελίδα, ετικετών που έχουν δημιουργηθεί από τρίτους, χωρίς να υπάρχουν ανησυχίες για την παραποίηση τους.

Σήμερα υπάρχουν υπηρεσίες αξιολόγησης συμβατές με το PICS, επιτρέποντας τους δημιουργούς αλλά και παρόχους περιεχομένου να αυτό-χαρακτηρίζονται (RSACi). Μερικές εταιρίες παροχής λογισμικού ελέγχου, χρησιμοποιούν ετικέτες που εκδίδονται από τρίτους οργανισμούς, βασιζόμενοι στα δικά τους συστήματα αξιολόγησης, που είναι συμβατές με το PICS. Παρόλα αυτά και παρά την υποστήριξη που παρέχουν στο PICS και τις σχετικές υπηρεσίες, δημοφιλείς προγράμματα πλοήγησης όπως το Microsoft Internet Explorer, η ανάπτυξη και η χρήση του είναι σχετικά περιορισμένη.

Συγκρινόμενα με άλλα μοντέλα αξιολόγησης, αυτά που είναι βασισμένα στο PICS, παρουσιάζουν ευρύτερη σημασιολογική κάλυψη, καθιστώντας την επιλογή του για φιλτράρισμα ίσως την πιο αποτελεσματική [1]. Για παράδειγμα, το πιο γνωστό συμβατό με το PICS σύστημα αξιολόγησης, το ICRA [1], διαθέτει 45 κριτήρια ομαδοποιημένα σε μεγάλες κατηγορίες, όπως chat, γλώσσα, γυμνό, σεξ, βία, ναρκωτικά, όπλα, αλκοόλ, τσιγάρα κα.

Ωστόσο και στην επιλογή αυτή, παρουσιάζονται μια σειρά από μειονεκτήματα [23]. Η περιγραφή του περιεχομένου δε γίνεται με οντολογίες οι οποίες θα επέτρεπαν μια ακριβέστερη προσέγγιση. Επιπλέον, λειτουργεί σύμφωνα με το Δυτικό σύστημα ηθικής και αξιών. Το PICS δεν είναι τόσο διαδεδομένο κυρίως γιατί απαιτεί οι ιστότοποι να συνδυάζονται με ετικέτες, αλλά μόνο ένα μικρό ποσοστό αυτών έχει βαθμολογηθεί.

Το RDF (Resource Description Framework – Πλαίσιο για την Περιγραφή Πόρων) [62, 63], είναι ένα γνωστό σύνολο από προδιαγραφές του W3C, το οποίο αρχικά σχεδιάστηκε σαν ένα μοντέλο

μετα-δεδομένων. Τελικά το RDF κατέληξε να χρησιμοποιείται σαν μια γενική μέθοδος μοντελοποίησης πληροφοριών διαμέσου διαφόρων συντακτικών προτύπων. Το μοντέλο μετα-δεδομένων RDF βασίζεται στη τριάδα : υποκείμενο, κατηγόρημα, αντικείμενο. Η διατύπωση προτάσεων για οποιαδήποτε θέμα, θα πρέπει να συντάσσεται σύμφωνα με αυτή τη τριάδα. Για παράδειγμα στην άποψη «Ο ουρανός στο Αιγαίο έχει το χρώμα βαθύ μπλε», έχουμε υποκείμενο το «Ο ουρανός στο Αιγαίο», κατηγόρημα το «έχει το χρώμα» και αντικείμενο «βαθύ μπλε»[27].

Οι RDF ετικέτες μπορούν να εκφράσουν ότι αναφέρθηκε για τις ετικέτες PICS, αλλά επιπλέον επιτρέπουν τιμές σειρών χαρακτήρων δομημένες τιμές και άλλες λειτουργίες. Το 2000 το W3C πρότεινε μια υλοποίηση του PICS, η οποία παρέχει μια εκφραστικότερη περιγραφή των περιεχομένων των ιστότοπων, επιτρέποντας αποτελεσματικότερο έλεγχο.

EUFORBIA, Μια Προσέγγιση Πολλαπλής Στρατηγικής

Ένα σχετικά νέο σύστημα φιλτραρίσματος περιεχομένου που αναπτύχθηκε στα πλαίσια της Ευρωπαϊκής ένωσης με την εργασία EUFORBIA, αντιμετωπίζει αρκετά βασικά μειονεκτήματα των υπαρχόντων συστημάτων, υποστηρίζοντας έλεγχο βασισμένο τόσο σε λίστες όσο και σε μετα-δεδομένα. Επιπλέον επιτρέπει την εφαρμογή πολιτικών με προδιαγραφές που λαμβάνουν υπόψη τους χρήστες αλλά και τις πηγές της πληροφορίας. Τα βασικά χαρακτηριστικά του πλαισίου αυτού είναι η δια-θεματική οντολογία, που επιτρέπει μια ακριβέστερη περιγραφή των πηγών στον παγκόσμιο ιστό, ένα νέο πρότυπο για ετικέτες το οποίο περιγράφει περιεχόμενο και δομή ιστοσελίδων και δύο ολοκληρωμένα συστήματα, ειδικά σχεδιασμένα να ικανοποιούν τις ανάγκες του οικιακού χρήστη αλλά και ολόκληρων οργανισμών [06].

Για να καταστεί δυνατή η υλοποίηση της μεθόδου είναι απαραίτητο να υπάρχουν τα κατάλληλα εργαλεία για τη περιγραφή της προέλευσης των δεδομένων από διαφορετικές σκοπιές. Αυτό γίνεται εν μέρει, με τη χρήση λεξιλογίου εξαρτώμενου από πολλαπλών τομέων μετα-δεδομένα, εστιάζοντας στην κατά περίπτωση χρήση των πηγών του Διαδικτύου. Δημιουργείται έτσι, μια δια-θεματική οντολογία, δομημένη με ιεραρχικό τρόπο, η οποία έχει την ευελιξία να είναι ανοικτή σε νέες θεματικές περιοχές [06].

Το γενικού σκοπού σύστημα αξιολόγησης που αναπτύσσεται επιτρέπει στους διαφόρων ειδών χρήστες του να περιγράφουν ακριβέστερα το περιεχόμενο και τη δομή των ιστοσελίδων, παρέχοντας τους ευελιξία και ταυτόχρονα αποτελεσματική προστασία, ανάλογα με τις επιλογές

που έχουν κάνει. Η προσέγγιση αυτή στοχεύει στη βελτίωση των υπαρχόντων τεχνικών προωθώντας δύο βασικές αρχές [27] :

- Θα πρέπει να παρέχεται υποστήριξη σε διαφορετικά συστήματα αξιολόγησης και φιλτραρίσματος με προοπτική να χρησιμοποιηθούν αυτόνομα ή σε συνδυασμό, σύμφωνα με τις ανάγκες του χρήστη.

- Τα χαρακτηριστικά του χρήστη θα πρέπει να περιγράφονται με ακρίβεια ώστε να είναι πιο αποτελεσματικός και ευέλικτος ο έλεγχος.

Οι ετικέτες που προτείνονται από τη μέθοδο είναι συγκρίσιμες με το σχήμα μετα-δεδομένων των ψηφιακών προτύπων MPEG-21 [27], αν και αυτό εστιάζει περισσότερο στο πρόβλημα της δομής και των δικαιωμάτων πρόσβασης του ψηφιακού μέσου.

Επιπλέον η δυνατότητα που δίνεται στους τελικούς χρήστες να καθορίζουν ελεύθερα το περιεχόμενο στο οποίο μπορούν να έχουν πρόσβαση, όχι μόνο δίνει λύση σε ηθικά ζητήματα που αφορούν τον έλεγχο, αλλά μειώνει και την πιθανότητα επιθυμίας παράκαμψης του [31].

3.6 Τεχνικές Αποκλεισμού Περιεχομένου

Μετά την αναγνώριση του περιεχομένου το οποίο πρέπει να αποκλειστεί από κάποιους χρήστες, ο μηχανισμός ελέγχου πρέπει να αποτρέψει και την πρόσβαση στο περιεχόμενο αυτό. Η τεχνική αποκλεισμού που θα επιλεγεί εξαρτάται σε σημαντικό βαθμό από τη τεχνική αναγνώρισης που έχει ακολουθηθεί. Για παράδειγμα, όταν χρησιμοποιούνται για την αναγνώριση του περιεχομένου, τεχνικές λίστας και μάλιστα σε επίπεδο πακέτου, οι αιτήσεις δεν φθάνουν ποτέ στον εξυπηρετητή που το φιλοξένει. Όταν επιλέγονται μέθοδοι ανάλυσης το περιεχόμενο πρέπει να παραληφθεί προκειμένου να ελεγχτεί και στη συνέχεια να απορριφθεί ή όχι [01].

3.6.1 Αποκλεισμός Πρόσβασης σε Επίπεδο Μεταγωγής Πακέτου

Ο αποκλεισμός της πρόσβασης σε επίπεδο πακέτου είναι μια τεχνική ή οποία εφαρμόζεται ουσιαστικά σε επίπεδο δικτύου και κατά τη λειτουργία της ένας δρομολογητής ή κάποια άλλη δικτυακή συσκευή επιτρέπουν ή όχι τη διέλευση της αίτησης για περιεχόμενο. Συνδυάζεται συνήθως με αναγνώριση περιεχομένου με την βοήθεια λίστας.

Το Διαδίκτυο είναι ένα δίκτυο μεταγωγής πακέτων. Αυτό σημαίνει ότι τα δεδομένα που μεταφέρονται είναι τεμαχισμένα σε μικρότερα τμήματα, τα «πακέτα», έτσι ώστε οι δίαυλοι μεταφοράς να μπορούν να διαμοιραστούν σε πολλούς χρήστες. Το μέγεθος των πακέτων ποικίλει και εξαρτάται από τη συμφόρηση του δικτύου. Κάθε συσκευή που λειτουργεί στο διαδίκτυο έχει ένα μοναδικό αριθμητικό αναγνωριστικό την IP (Internet Protocol) διεύθυνση. Όλα τα πακέτα πρέπει να περιέχουν ορισμένα στοιχεία που δείχνουν πού πηγαίνουν (IP προορισμού), από πού προήλθαν (IP προέλευσης), πώς αναμένεται να παραληφθούν (πρωτόκολλο), καθώς και τη σειρά με την οποία τα πακέτα θα πρέπει να ανασυντεθούν μόλις φθάσουν στον προορισμό τους. Η πληροφορία αυτή περιέχεται στην αρχή κάθε πακέτου, σε ένα τμήμα που ονομάζεται κεφαλίδα. Οι συσκευές του δικτύου έχουν σχεδιαστεί για να ελέγχουν τις πληροφορίες στις κεφαλίδες πακέτων, προκειμένου να καθορίσουν τον τρόπο που το πακέτο θα πρέπει να αντιμετωπίζεται [86].

Κεφαλίδα Πακέτου Δεδομένων και Φιλτράρισμα Περιεχόμενου

Η δέσμευση περιεχομένου στο επίπεδο μεταγωγής πακέτου, απαιτεί δρομολογητές φιλτραρίσματος (screening routers), οι οποίοι εξετάζουν την IP διεύθυνση της προέλευσης του εισερχόμενου πακέτου, τη συγκρίνουν με μια μαύρη λίστα (black list) και είτε προωθούν το πακέτο αν η IP διεύθυνση δεν ανήκει στη μαύρη λίστα, είτε το απορρίπτουν αν ανήκει [27].

Πιο συγκεκριμένα, η δέσμευση πραγματοποιείται με χρήση της Λίστας Ελέγχου Πρόσβασης (ACL, Access Control List) και με κριτήρια που καθορίζονται από την πληροφορία στο επίπεδο 3 (επίπεδο δικτύου του μοντέλου OSI) που υπάρχει στο πακέτο, όπως είναι οι διευθύνσεις προέλευσης και προορισμού ή ακόμα και θύρες που προσδιορίζουν εφαρμογές και υπηρεσίες. Για να γίνει αυτό απαιτείται η δημιουργία μιας λίστας με IP διευθύνσεις. Στη συνέχεια, κάθε πακέτο που φτάνει στο δρομολογητή του δικτύου, συγκρίνεται με τα περιεχόμενα της λίστας γραμμή προς γραμμή και ανάλογα με το αποτέλεσμα της σύγκρισης, ο δρομολογητής μπορεί να απαγορεύσει την πρόσβαση με βάση την IP διεύθυνση του αποστολέα ή του παραλήπτη, το πρωτόκολλο επικοινωνίας (TCP, UDP), το δίκτυο αποστολής ή λήψης και τέλος την θύρα εφαρμογής.

Η λογική μιας ACL μπορεί να είναι:

- Επιτρέπονται όλες οι IP διευθύνσεις, εκτός από αυτές που αναφέρονται στη λίστα (default permit, black list)

- Επιτρέπονται μόνο οι διευθύνσεις, που αναφέρονται στη λίστα και όλες οι άλλες απορρίπτονται (default deny, white list)

Οι Λίστες Ελέγχου Πρόσβασης, εφαρμόζονται στους δρομολογητές που ελέγχουν την εισερχόμενη και εξερχόμενη κίνηση του δικτύου. Επομένως η δέσμευση των IP διευθύνσεων μπορεί να πραγματοποιηθεί :

- Από οποιονδήποτε Πάροχο Υπηρεσιών Διαδικτύου (ISP, Internet Service Provider)

- Από τους Παρόχους Υπηρεσιών Κορμού (BSP, Backbone Service Providers). Λαμβάνοντας υπόψη, ότι οι BSP είναι πιο ψηλά στην ιεραρχία της αρχιτεκτονικής του Διαδικτύου η εφαρμογή των ACL στους BSP είναι πιο αποδοτική. Επίσης, για τη βελτίωση των προβλημάτων απόδοσης, μπορούν να χρησιμοποιηθούν και οι συναρτήσεις σύνοψης (hash functions).

- Από το δρομολογητή μιας επιχείρησης ή οργανισμού, που διαθέτει μόνιμη σύνδεση με το Διαδίκτυο. Αν η επιχείρηση ή ο οργανισμός διαθέτει συσκευή Firewall (Αναχώματα ασφαλείας), οι λίστες θα μπορούσαν να εφαρμοστούν σε αυτή.

Προκλήσεις, Προβλήματα και Περιορισμοί του Ελέγχου σε Επίπεδο Πακέτου

Σε κάθε περίπτωση, η αποτελεσματικότητα της δέσμευσης IP διευθύνσεων είναι ζήτημα αμφιλεγόμενο. Οι υποστηρικτές της τεχνολογίας αυτής ισχυρίζονται ότι πράγματι είναι ένας εφικτός τρόπος για αποτελεσματική δέσμευση παράνομου ή προσβλητικού περιεχομένου στον Παγκόσμιο Ιστό και γενικότερα στο Διαδίκτυο.

Αντίθετα, οι πολέμιοι της τεχνολογίας αυτής, αναφέρονται σε μια σειρά τεχνικά ή μη ζητήματα τα οποία σωρευτικά μπορούν να περιορίσουν την αποτελεσματικότητά της. Η δέσμευση μπορεί να είναι μεγαλύτερης έκτασης από την επιθυμητή. Η δέσμευση των IP διευθύνσεων δεν κάνει διακρίσεις, με την έννοια ότι η απόφαση να δεσμευτεί ένας δικτυακός τόπος ή μια ιστοσελίδα πρακτικά σημαίνει, ότι ολόκληρη η ιστοθέση θα δεσμευτεί και δε θα είναι προσπελάσιμη από τους χρήστες του Διαδικτύου, δηλαδή τους συνδρομητές των ISP's. Κατά συνέπεια, αν ένας δικτυακός τόπος φιλοξενείται από μια μεγάλη εταιρεία, όπως έναν ISP ή BSP, τότε οι υπόλοιπες ιστοσελίδες που φιλοξενούνται από αυτή την εταιρεία, επίσης θα δεσμευτούν και θα γίνουν μη προσπελάσιμες στους χρήστες του Διαδικτύου, και συνδρομητές των ISP's. Το γεγονός αυτό

μπορεί να προκαλέσει πολλαπλά πρακτικά και νομικά προβλήματα στις εταιρείες που φιλοξενούν πολλές ιστοσελίδες.

Ένα άλλο μειονέκτημα είναι ότι περιορίζονται και άλλες υπηρεσίες που πιθανόν να υποστηρίζονται από διακομιστή με την IP διεύθυνση που απορρίπτεται. Η δέσμευση IP διευθύνσεων μπορεί να επηρεάσει και άλλες υπηρεσίες TCP/IP, εκτός από το HTTP. Η απόφαση να δεσμευτούν συγκεκριμένες ιστοσελίδες εξαιτίας παράνομου ή προσβλητικού περιεχομένου, ουσιαστικά σημαίνει ότι όλες οι άλλες υπηρεσίες, όπως FTP, SMTP, επίσης θα δεσμευτούν. Αυτό θα συμβεί, επειδή οι αποφάσεις δέσμευσης IP διευθύνσεων βασίζονται κυρίως στις ίδιες τις IP διευθύνσεις. Οι παραπάνω κανόνες μπορούν να συμπεριλάβουν αριθμούς θύρας που προσδιορίζουν συγκεκριμένες υπηρεσίες, αλλά αυτό αποφεύγεται γιατί επιβαρύνει σημαντικά την απόδοση του δρομολογητή. Άλλωστε και αν γινόταν, οι αριθμοί θυρών μπορούν να αλλάξουν πολύ εύκολα, επομένως να παρακαμφθεί ο έλεγχος με βάση την ACL.

Η επιλογή του περιορισμού της κυκλοφορίας χρησιμοποιώντας ένα συγκεκριμένο πρωτόκολλο θα μπορούσε να οδηγήσει σε μπλοκάρισμα νόμιμη κίνηση η οποία χρησιμοποιεί αυτό το πρωτόκολλο. Για παράδειγμα, αποτρέποντας το HTTPS (κρυπτογραφημένο HTTP χρησιμοποιώντας δημόσιο κλειδί κρυπτογράφησης) θα έχει σαν αποτέλεσμα την αδυναμία πραγματοποίησης δραστηριοτήτων ηλεκτρονικού εμπορίου, τραπεζικών υπηρεσιών μέσω Διαδικτύου, και πολλών Web-based εφαρμογών ηλεκτρονικού ταχυδρομείου. Απαγόρευση των P2P πρωτόκολλων, θα παρεμπόδιζε τη με peer to peer νόμιμη μεταφορά αρχείων από οργανισμούς όπως το νορβηγικό Broadcasting Corporation, το οποίο χρησιμοποιεί Bit Torrent για την παροχή περιεχομένου στο κοινό του, ανεξάρτητους καλλιτέχνες να επικοινωνήσουν με το κοινό τους, καθώς και λειτουργία εφαρμογών διαδικτυακής τηλεφωνίας, όπως το Skype, που βασανίζονται σε τέτοια πρωτόκολλα [86].

Η αποτροπή πρόσβασης σε αυτό το επίπεδο δεν παρέχει καμία πληροφορία για τα μέτρα περιορισμού, στο χρήστη που ζητάει πρόσβαση σε απαγορευμένο περιεχόμενο. Ακόμη πιο σημαντικό είναι το γεγονός της αδυναμίας πληροφόρησης και στην περίπτωση που δεν επιτευχτεί η πρόσβαση σε υπηρεσία, όχι λόγω της ακαταλληλότητας της, αλλά εξαιτίας άλλων γεγονότων.

Η δέσμευση των IP διευθύνσεων απαιτεί κάποια υπολογιστική ισχύ από τις συσκευές δρομολόγησης και φιλτραρίσματος. Κατά συνέπεια, οι BSP δρομολογητές, μπορεί να χρειαστεί να αναβαθμιστούν για να κατορθώσουν να υλοποιήσουν δέσμευση των IP διευθύνσεων. Ας

σημειωθεί ότι ένας κατάλληλα ρυθμισμένος αξιόλογος εμπορικός δρομολογητής, μπορεί να πραγματοποιήσει τη δέσμευση στο επίπεδο μεταγωγής πακέτου, σχεδόν σε ταχύτητα γραμμής, ενώ άλλοι φθηνότεροι θα πρέπει να αντικατασταθούν ή τουλάχιστον να αναβαθμιστούν, ώστε να μπορέσουν να ανταποκριθούν στις απαιτήσεις για ικανοποιητική απόδοση των σημερινών εργασιών στο Διαδίκτυο.

3.6.2 Αποκλεισμός με τη Χρήση Διακομιστή Μεσολάβησης (Proxy)

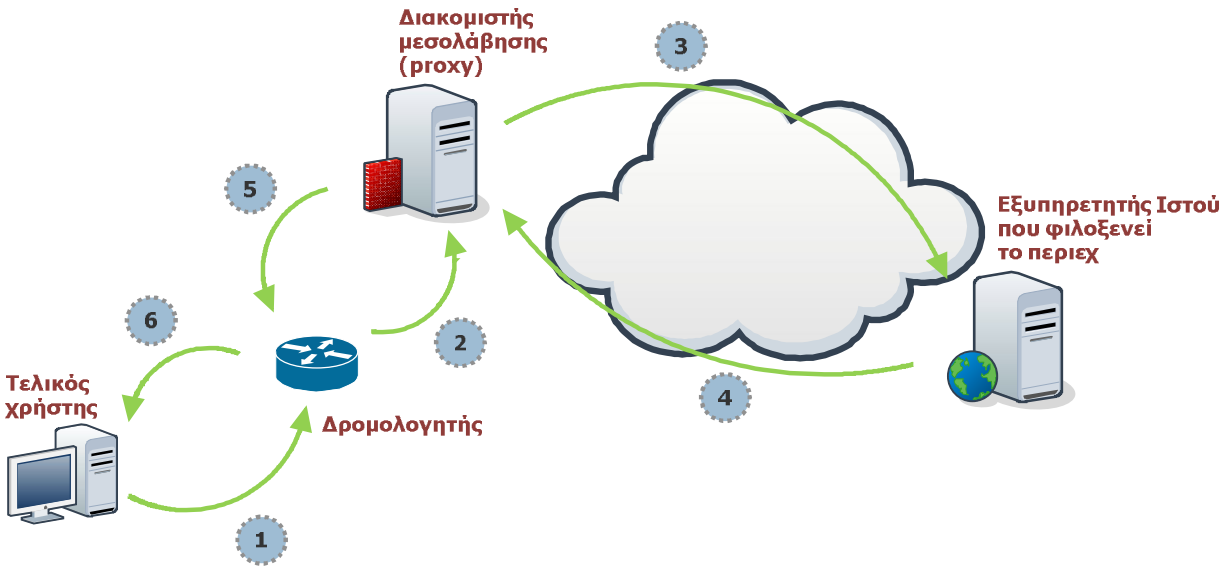
Ο έλεγχος σε επίπεδο εφαρμογής απαιτεί συχνά την ύπαρξη διακομιστή διαμεσολάβησης (proxy server) και εφαρμογών πυλών δικτύου (application gateway) που ελέγχουν το περιεχόμενο ή πληροφορίες για την προέλευση του, προκειμένου να το προωθήσουν ή όχι. Οι πάροχοι προστατεύουν ή ελέγχουν τους πελάτες τους αναγκάζοντας τους να έχουν πρόσβαση στο διαδίκτυο μέσω proxy servers. Οι διακομιστές διαμεσολάβησης είναι συστήματα τα οποία παρεμβάλλονται μεταξύ πελάτη και εξυπηρετητή, δεχόμενοι αυτοί τα αιτήματα για περιεχόμενο. Οι proxy servers λειτουργώντας ως ενδιάμεσοι, συνδέονται στους εξυπηρετητές εκ μέρους του πελάτη, αποθηκεύουν το αιτούμενο περιεχόμενο και διαχειρίζονται το φιλτράρισμα του. Ο έλεγχος μπορεί να γίνει είτε με μεθόδους λίστας, συγκρίνοντας το αίτημα του πελάτη με μια «μαύρη λίστα» που περιέχει για παράδειγμα ιστοσελίδες στην περίπτωση του HTTP πρωτοκόλλου ή ακόμη και με πιο δυναμικές μεθόδους αναλύοντας το αιτηθέν περιεχόμενο[27] .

Οι διακομιστές μεσολάβησης μπορούν να [21]:

- Λειτουργήσουν σε εθελοντική βάση, (voluntary proxy), με την έννοια ότι ο χρήστης επιλέγει αν θέλει να έχει πρόσβαση μέσω αυτών ή όχι.

- Είναι (enforced proxy) υποχρεωτικό να ελέγχουν όλη τη κίνηση στο δίκτυο.

- Παρακολουθούν απλά, παράλληλα και με διαφανή τρόπο (interception ή transparency proxy) την κίνηση στο δίκτυο.



Σχήμα 3.11: Διακομιστής μεσολάβησης (proxy server).

Τα βήματα που ακολουθούνται στη διαδικασία φιλτραρίσματος είναι τα εξής [32] :

1. Η εφαρμογή πλοήγησης του χρήστη ρυθμίζεται στον επιθυμητό διακομιστή μεσολάβησης. Εναλλακτικά όλη η κίνηση του δικτύου δρομολογείται μέσω του proxy.

2. Ο χρήστης προσπαθεί να «ανοίξει» μια ιστοσελίδα.

3. Όλες οι συνδέσεις ανακατευθύνονται προς τον proxy server, ο οποίος μπορεί να απαιτήσει ταυτοποίηση πριν επιτρέψει την πρόσβαση.

4. Ο διακομιστής μεσολάβησης εξετάζει τις προσπάθειες για σύνδεση κάνοντας σύγκριση με μια λίστα προκαθορισμένων πολιτικών πρόσβασης.

5. Αν η σύνδεση δεν επιτρέπεται, δείχνεται συνήθως στον χρήστη μια σελίδα που τον ενημερώνει για την πολιτική πρόσβασης.

6. Αν η σύνδεση επιτρέπεται, ο proxy server κάνει τις απαραίτητες συνδέσεις για να κατεβάσει το περιεχόμενο το οποίο αποθηκεύει και το προωθεί στον χρήστη.

Ο διακομιστής μεσολάβησης αποθηκεύει περιεχόμενο που ζητείται συχνά, βοηθώντας έτσι στη βελτιστοποίηση της διαχείρισης του εύρους ζώνης και αυξάνοντας την ταχύτητα πρόσβασης

[21]. Περιεχόμενο όμως που δεν είναι αποθηκευμένο στο διαμεσολαβητή θα επιβαρυνθεί με πρόσθετη καθυστέρηση στην παράδοση του λόγω της επεξεργασίας που θα υποστεί.

Οι proxy server με τη λειτουργία τους επιτρέπουν τον έλεγχο και την κατάταξη της κίνησης στο δίκτυο σε επιτρεπόμενη και μη ή διαφορετικά σε κατάλληλη και ακατάλληλη. Ένας διαμεσολαβητής υλοποιείται συνηθέστερα με λογισμικό παρά με υλικό, παρόλα αυτά οι απαιτήσεις σε ευελιξία που πρέπει να διαθέτουν αυξάνουν τις απαιτήσεις σε εξοπλισμό, κυρίως επεξεργαστική ισχύ και μνήμη, συνεπώς και σε χρήματα. Προκειμένου να είναι πιο αποτελεσματικοί διαχειρίζονται συνήθως ένα ή δυο πρωτόκολλα και μόνο στο επίπεδο 7 (εφαρμογής) του μοντέλου OSI [87]. Οι πιο δημοφιλείς είναι οι διαμεσολαβητές ιστού (web proxy ή http proxy).

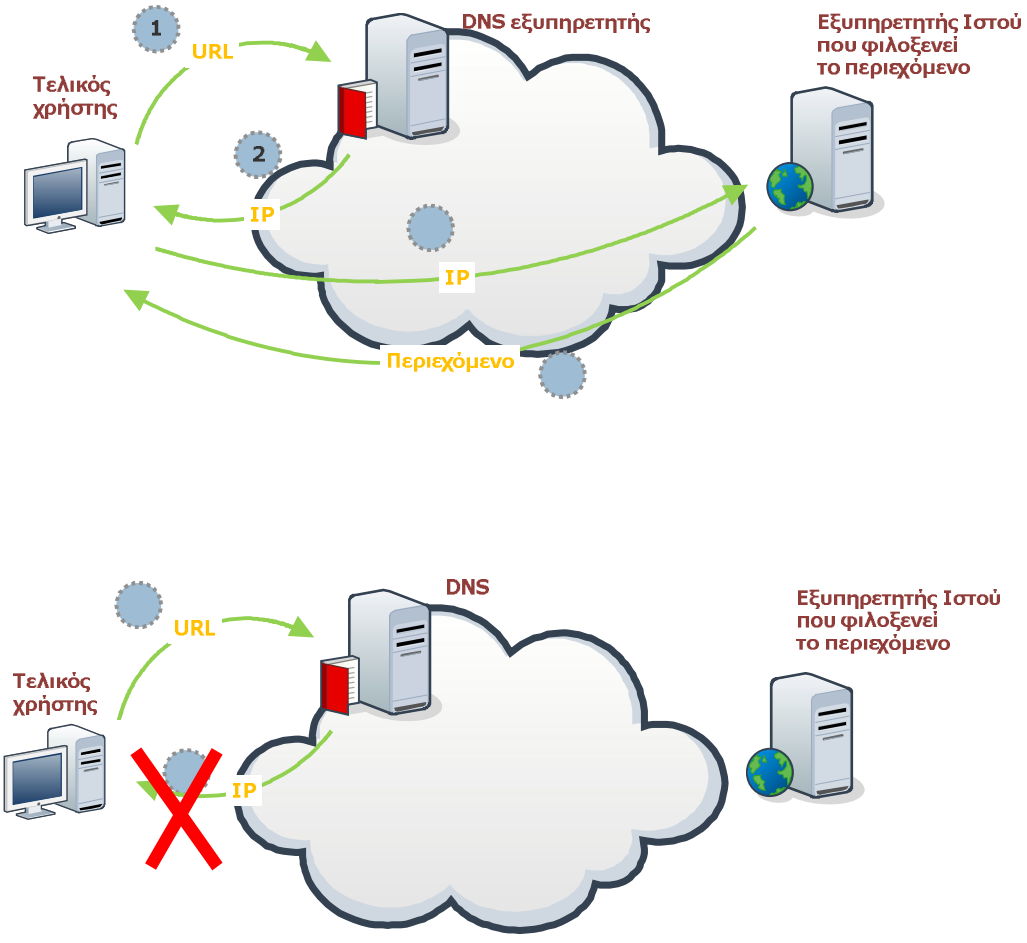
Μια επιλογή που μπορεί να γίνει για να μειωθεί η καθυστέρηση αλλά και η απαιτουμένη υπολογιστική ισχύ και μνήμη είναι να χρησιμοποιηθούν τροποποιημένοι διαμεσολαβητές (modified proxies). Στην περίπτωση αυτή διαχωρίζονται τα καθήκοντα του ελέγχου και του αποκλεισμού και κατανέμονται σε δυο διαφορετικές συσκευές, έναν εξυπηρετητή που περιέχει μόνο τις πολιτικές πρόσβασης και μια συσκευή που προωθεί ή αποκλείει απλά το περιεχόμενο ανάλογα με τις εντολές που θα δεχθεί. Όταν ο χρήστης αιτηθεί κάποιο περιεχόμενο αυτή η αίτηση προωθείται από την συσκευή προώθησης, τόσο στον εξυπηρετητή που περιέχει τις πολιτικές πρόσβασης όσο και σε αυτόν που περιέχει το περιεχόμενο. Μέχρι να «φορτωθεί» το περιεχόμενο από τον εξυπηρετητή περιεχόμενου αυτός που περιέχει τις πολιτικές πρόσβασης έχει ελέγξει το αρχικό αίτημα και δίνει εντολή στη συσκευή προώθησης να προωθήσει ή όχι το περιεχόμενο στον τελικό χρήστη [32].

3.6.3 DNS Αλλοίωση (Tampering)

Το Domain Name System ή DNS (Σύστημα Ονομάτων Τομέων ή Χώρων ή Περιοχών) είναι ένα ιεραρχικό σύστημα ονοματοθεσίας για δίκτυα υπολογιστών που χρησιμοποιούν το πρωτόκολλο IP. Το σύστημα DNS μπορεί και αντιστοιχίζει ονόματα με διευθύνσεις IP ή άλλα ονόματα στο Διαδίκτυο ή κάποιο άλλο δίκτυο. Όλες οι συσκευές του δικτύου με IP διεύθυνση δεν αντιστοιχίζονται στο DNS. Επιπλέον δεν υπάρχει μια σχέση ένα προς ένα μεταξύ IP διευθύνσεων και DNS ονομάτων. Οι μεγάλοι ιστότοποι, πολλές φορές, δομούνται σε συστάδες, όπου πολλοί υπολογιστές ο καθένας με διαφορετική IP διεύθυνση, απαντούν στο ίδιο αίτημα για DNS όνομα.

Όταν ένας χρήστης πληκτρολογεί μια διεύθυνση στο πρόγραμμα πλοήγησης ο DNS εξυπηρετητής που του αντιστοιχεί, (συνήθως αυτός του παρόχου του), αναζητεί στις καταγεγραμμένες IP διευθύνσεις την αντιστοίχιση και αν δεν βρεθεί μεταβιβάζει το αίτημα σε επόμενο εξυπηρετητή μέχρι να ικανοποιηθεί. Το περιεχόμενο τελικά αποστέλλεται στον χρήστη και παράλληλα αποθηκεύεται στο DNS εξυπηρετητή για γρηγορότερη απάντηση σε ισοδύναμες μελλοντικές αιτήσεις [86].

Η DNS αλλοίωση, (tampering ή spoofing ή poisoning ή manipulation, όπως αναφέρεται στη βιβλιογραφία), είναι η στρατηγική αποκλεισμού περιεχομένου κατά την οποία, παρεμβαίνοντας στη παραπάνω διαδικασία, επιστρέφεται λάθος ή και καθόλου περιεχόμενο στον χρήστη που ζητά πρόσβαση σε DNS όνομα που αντιστοιχεί σε διεύθυνση η οποία περιέχεται σε μια μαύρη λίστα στο DNS εξυπηρετητή [17].



Σχήμα 3.12: DNS tampering

Προκειμένου να περιοριστεί η πρόσβαση με αυτή τη τεχνική, αναγνωρίζονται έξι πιθανές επιλογές [21, 93]:

- Άρνηση : Ο ευκολότερος τρόπος να εμποδιστεί ο χρήστης από τη σύνδεση του σε συγκεκριμένο εξυπηρετητή που φιλοξενεί ιστοσελίδες, είναι απλά να μην του επιτραπεί η DNS ανάλυση. Στην περίπτωση αυτή εμφανίζεται το μήνυμα «REFUSED» το οποίο σημαίνει ότι ο DNS εξυπηρετητής αρνείται να εκτελέσει τη συγκεκριμένη λειτουργία. Σαν αποτέλεσμα προβάλλεται κάποιο μήνυμα της μορφής «host not found» ή «connection refused».

- Nxdomain: Ένας χειρισμός κατά τον οποίο ο DNS εξυπηρετητής του παρόχου αρνείται την ύπαρξη του συγκεκριμένου τομέα (Nxdomain – non existing domain). Κάποιο μήνυμα «host not found» είναι συνηθισμένο και σε αυτή την περίπτωση.

- DNS πειρατεία (hijacking): Στην περίπτωση αυτή μετά την ανάλυση της διεύθυνσης επιστρέφεται διαφορετικό περιεχόμενο από αυτό που έχει ζητηθεί. Επιστρέφεται δηλαδή διαφορετική ιστοσελίδα.

- Ακύρωση (invalidation ή astrayment) ονόματος : Είναι μια επιλογή η οποία μοιάζει με το DNS hijacking μόνο που σε αυτή την περίπτωση επιστρέφεται άκυρο περιεχόμενο και όχι απλά διαφορετικό. Κάποιο μήνυμα «could not connect» είναι συνηθισμένο σε αυτή την περίπτωση.

- Σιγή : Ένας άλλος τρόπος άρνησης της εξυπηρέτησης είναι να μη δοθεί καμία απάντηση. Αυτό θα προκαλέσει μια καθυστέρηση ή και υπέρβαση του χρόνου, με συνέπεια ένα μήνυμα της μορφής «host not found».

- Πρόκληση σφάλματος εξυπηρετητή : Σε αυτού του είδους την αλλοίωση δημιουργείται ένα μήνυμα λάθους από τον εξυπηρετητή και στέλνεται στον πελάτη που προσπαθεί να έχει πρόσβαση στο συγκεκριμένο τομέα. Κάποιο μήνυμα «could not connect» είναι συνηθισμένο και σε αυτή την περίπτωση.

Όπως και στην περίπτωση του ελέγχου σε επίπεδο πακέτου (IP διεύθυνσης ουσιαστικά) και σε αυτή τη μέθοδο παρουσιάζεται συχνά το πρόβλημα του φιλτραρίσματος περιεχομένου το οποίο δεν είναι ακατάλληλο. Αυτό συμβαίνει γιατί πολλές φορές αποκλείεται ένα συνολικός τομέας

περιεχομένου στον οποίο όμως υπάρχουν και υποτομείς με υλικό μη χαρακτηρισμένο ως ακατάλληλο.

3.6.4 Αποκλεισμός Θυρών (Port Blocking)

Κάποια φίλτρα αποκλείουν συγκεκριμένες θύρες μεταφοράς δεδομένων. Σε έναν διασυνδεδεμένο υπολογιστή διαφορετικές κατηγορίες προγραμμάτων ή υπηρεσιών χρησιμοποιούν διαφορετικές θύρες προκειμένου να στείλουν ή να λάβουν δεδομένα [01], η σχέση δε μεταξύ τους, είναι καθορισμένη από τον IANNA, χωρίς όμως να είναι δεσμευτική. Αυτές οι συσχετίσεις επιτρέπουν στους δρομολογητές να «υποθέσουν» για το σε ποια υπηρεσία ζητείται πρόσβαση. Έτσι προκειμένου να αποκλειστεί η κίνηση στον παγκόσμιο ιστό είναι δυνατό να αποκλειστεί η θύρα 80, ενώ για την ηλεκτρονική αλληλογραφία ή θύρα 110 [33].

Η πρόσβαση στις θύρες μπορεί να ελεγχθεί από το διαχειριστή του δικτύου, το τελικό χρήστη ή τον πάροχο και ο αποκλεισμός τους γίνεται συχνά και για λόγους πέρα από τη συνηθισμένη λογοκρισία. Για παράδειγμα κάποιες θύρες αποκλείονται για να αποθαρρυνθούν χρήσεις του δικτύου όπως διαμοιρασμός αρχείων.

Με τον αποκλεισμό των θυρών όλη η κίνηση μέσω αυτών σταματά. Συχνά αυτοί που επιβάλουν τον έλεγχο περιεχομένου αποκλείουν τις θύρες 1080, 3128 και 8080, γιατί χρησιμοποιούνται συχνά για παράκαμψη του ελέγχου μέσω διαμεσολάβησης [33].

3.6.5 Αποκλεισμός με τη Βοήθεια Μηχανών Αναζήτησης (Search Engine Indexing)

Υπάρχουν αρκετές μηχανές αναζήτησης που χρησιμοποιούνται προκειμένου να εντοπιστεί το περιεχόμενο για το οποίο κάποιος ενδιαφέρεται. Η κάθε μηχανή έχει τη δική της μεθοδολογία για την κατάταξη του παγκόσμιου ιστού αλλά και για την αντιστοίχιση των αναζητούμενων όρων σε αυτή τη κατάταξη. Ενώ η ακριβής μέθοδος είναι εμπορικά εμπιστευτική, οι μηχανές αναζητήσεις τείνουν να χρησιμοποιούν προγράμματα που ονομάζονται ανιχνευτές (crawlers) Web. Σαρώνουν τις ιστοσελίδες και αποθηκεύουν τμήμα ή όλο από το περιεχόμενο στους καταλόγους τους. Όταν ένας χρήστης εισάγει έναν όρο αναζήτησης, η μηχανή εξετάζει το κατάλογο της για να εντοπίσει μια λίστα με σελίδες που ταιριάζουν με το ερώτημα και να παρέχει συνδέσμους προς αυτές. Μια σειρά από διάφορα άλλα κριτήρια, όπως γεωγραφικά για παράδειγμα, καθορίζουν τη προτεραιότητα με την οποία εμφανίζονται τα αποτελέσματα.

Η αφαίρεση ή η αλλοίωση των αποτελεσμάτων της αναζήτησης δεν είναι ακριβώς μέθοδος περιορισμού πρόσβασης, με την τυπική έννοια των όρων, μια που δεν αποκλείει πρόσβαση σε περιεχόμενο. Ωστόσο, έχει τη δυνατότητα να μειώσει την πρόσβαση, εμποδίζοντας την ενημέρωση των χρηστών σχετικά με την ύπαρξη ορισμένου περιεχόμενου. Αν ο χρήστης δεν γνωρίζει ότι το περιεχόμενο υπάρχει, θα μπορούσε να θεωρηθεί αποκλεισμένο. Σε πολλές περιπτώσεις, ο χρήστης έχει τη δυνατότητα αλλάζοντας τους όρους αναζήτησης να επιτύχει την προβολή διαφορετικών αποτελεσμάτων, αποκλεισμένων υπό άλλες συνθήκες και να παρακάμψει ουσιαστικά τον υποτιθέμενο έλεγχο.

Έχουν γίνει γνωστές, κατά καιρούς, συμφωνίες της Google αλλά και άλλων παρόχων μηχανών αναζήτησης για αφαίρεση αποτελεσμάτων αναζήτησης για ευαίσθητα θέματα, σύμφωνα με τις απαιτήσεις κυβερνήσεων. Μια από τις πιο γνωστές συμφωνίες είναι αυτή της κυβέρνησης της Κίνας με την Google σύμφωνα με την οποία μια λίστα περιορισμών έχει επιβληθεί στους χρήστες του Google.cn (ή τοπική έκδοση του Google για την Κίνα) η οποία πάντως δε κατάφερε να αποτρέψει την κατά καιρούς διακοπή της υπηρεσίας στη χώρα αυτή.

Η επιλογή αυτή απαιτεί σε κάθε περίπτωση τη συνεργασία με τον πάροχο της μηχανής αναζήτησης. Μια τέτοια συμφωνία έχει επιπτώσεις τόσο σε οικονομικό όσο και σε επίπεδο αξιοπιστίας για τον πάροχο, οι οποίες εξαρτώνται ανάλογα με το μέγεθος της αλλοίωσης που έχει συμφωνηθεί. Για να είναι αποτελεσματική μια τέτοια στρατηγική θα πρέπει να συμπεριλαμβάνει όλες τις μηχανές αναζήτησης που λειτουργούν σε μια περιοχή, γεγονός αρκετά δύσκολο, δεδομένου του πλήθους τους [86].

3.6.6 Περιορισμός Εύρους Ζώνης

Ο περιορισμός του εύρους ζώνης αναφέρεται απλά στη τεχνητή μείωση της δυνατότητας, της ταχύτητας ουσιαστικά, κυκλοφορίας της πληροφορίας στο Διαδίκτυο. Σαν επιπλέον πλεονέκτημα της τακτικής αυτής παρατηρείται και η διευκόλυνση όλων των άλλων μεθόδων λόγω του μειωμένου όγκου πληροφορίας που διάκεινται και συνεπώς υπόκειται σε έλεγχο [24].

3.6.7 Διαμόρφωση της Κυκλοφορίας στο Δίκτυο

Η διαμόρφωση της κυκλοφορίας είναι μια τεχνική που χρησιμοποιούν οι διαχειριστές των δικτύων προκειμένου να επιτύχουν την ομαλότερη λειτουργία τους. Προωθούν γρηγορότερα

κάποια διακινούμενα πακέτα, καθυστερώντας κάποια άλλα σύμφωνα με συγκεκριμένα κριτήρια.

Η τακτική αυτή μοιάζει με την ρύθμιση της κυκλοφορίας των οχημάτων στους δρόμους. Πινακίδες, φωτεινοί σηματοδότες και ο κώδικας οδικής κυκλοφορίας καθορίζουν την προτεραιότητα των οχημάτων στους δρόμους και τις διασταυρώσεις με γνώμονα την αποφυγή της συμφόρησης και την ασφάλεια. Επιπλέον κάποια οχήματα ειδικών υπηρεσιών (ασθενοφόρα πυροσβεστικά), είναι ανάγκη να φτάσουν γρηγορότερα στον προορισμό τους για αυτό τους δίνεται προτεραιότητα καθυστερώντας τα υπόλοιπα. Κάτι ανάλογο συμβαίνει στο διαδίκτυο με πακέτα που επιδέχονται μικρή καθυστέρηση και για αυτό δίνεται προτεραιότητα (όπως VoIP - τηλεφωνίας μέσω του πρωτοκόλλου IP).

Η διαμόρφωση της κυκλοφορίας μπορεί να χρησιμοποιηθεί από αυτούς που ασκούν τη λογοκρισία για να καθυστερήσει πακέτα με συγκεκριμένη πληροφορία. Αν κάποιος θέλει να περιστείλει την πρόσβαση σε συγκεκριμένες υπηρεσίες, μπορεί να αναγνωρίσει τα πακέτα που συσχετίζονται με αυτές και να αυξήσει την καθυστέρηση, θέτοντας χαμηλή προτεραιότητα. Αυτό θα μπορούσε να δώσει στους χρήστες την παραπλανητική εντύπωση ότι μια ιστοσελίδα είναι εγγενώς αργή ή αναξιόπιστη και έτσι να την καταστήσει δύσχρηστη σε σχέση με άλλους δικτυακούς τόπους. Η τεχνική αυτή χρησιμοποιείται συχνά από τους παρόχους για να περιορίσουν, το συνήθως ανεπιθύμητο, διαμοιρασμό αρχείων μέσω ομότιμων δικτύων όπως τα Bit Torrent [33]

3.6.8 Άρνηση Υπηρεσιών

Όταν ο οργανισμός που εφαρμόζει τον έλεγχο δεν έχει δικαιοδοσία (ή πρόσβαση στις δικτυακές υποδομές) να κάνει χρήση συμβατικών μηχανισμών αποκλεισμού, οι ιστότοποι μπορούν να γίνουν μη προσβάσιμοι υπερφορτώνοντας τον εξυπηρετητή που τους φιλοξενεί ή τη διασύνδεση του. Η τεχνική αυτή είναι γνωστή σαν Επίθεση Άρνησης Υπηρεσιών (Denial of Service - DDos attack) και είναι δυνατό να πραγματοποιηθεί από ένα υπολογιστή με πολύ γρήγορη διασύνδεση αν και πιο συχνά χρησιμοποιείται μεγάλος αριθμός υπολογιστών [17].

3.6.9 Αποταξινόμηση Τομέα

Όπως περιγράφηκε πιο πάνω, στη τεχνική του DNS tampering, το πρώτο στάδιο ενός αιτήματος για τον παγκόσμιο ιστό, είναι η επικοινωνία με τον τοπικό DNS εξυπηρετητή, προκειμένου να προσδιοριστεί η IP διεύθυνση του επιθυμητού προορισμού. Η αποθήκευση όλων των διευθύνσεων τοπικά θα ήταν αδύνατη, για αυτό χρησιμοποιείται η αποκαλούμενη αναδρομική αναζήτηση σε άλλους DNS εξυπηρετητές που είναι πιθανότερο να γνωρίζουν την απάντηση. Αυτοί οι εξυπηρετητές θα επιχειρήσουν αναδρομική αναζήτηση σε άλλους μέχρι να βρεθεί αυτός που είναι υπεύθυνος και να επιστρέψει την σωστή διεύθυνση.

Το DNS είναι οργανωμένο ιεραρχικά, με τους τομείς ανά χώρα όπως για παράδειγμα .gr για την Ελλάδα, και .de για την Γερμανία, στη κορυφή μαζί με μη γεωγραφικούς τομείς όπως .org και .com. Οι εξυπηρετητές που είναι υπεύθυνοι για αυτούς τους τομείς μεταφέρουν αρμοδιότητες στους πιο κάτω ιεραρχικά τομείς σε άλλους DNS εξυπηρετητές, οδηγώντας τα αιτήματα σε αυτούς. Κατά συνέπεια αν ένας εξυπηρετητής που βρίσκεται στην κορυφή, αποταξινομίσει, ουσιαστικά διαγράψει, ένα Domain όνομα, η αναδρομική αυτή ανάλυση θα είναι αδύνατο να επιτρέψει τον προσδιορισμό της αντίστοιχης IP διεύθυνσης καθιστώντας τον ιστότοπο μη προσβάσιμο.

Οι εξειδικευμένοι σε επίπεδο χώρας τομείς συνήθως εποπτεύονται από τις κυβερνήσεις της χώρας ή κρατικούς οργανισμούς. Έτσι αν ένας ιστότοπος είναι καταχωρημένος σε επίπεδο τομέα μια χώρας η οποία εφαρμόζει έλεγχο περιεχομένου, έχει τη πιθανότητα αποκλεισμού με τη μέθοδο που περιγράφηκε [17].

3.6.10 «Βίαιες Τεχνικές» (Server Shutdown)

Οι εξυπηρετητές οι οποίοι φιλοξενούν τους ιστότοπους και οι διαχειριστές τους, έχουν σε μια τοποθεσία μια φυσική παρουσία. Αν οι τοποθεσίες αυτές βρίσκονται κάτω από το νόμιμο ή παράνομο έλεγχο κάποιου που αντίκεινται στο φιλοξενούμενο περιεχόμενο, ο εξυπηρετητής μπορεί να αποσυνδεθεί ή ο διαχειριστής μπορεί να τον απενεργοποιήσει. Πρόκειται ουσιαστικά για το σταμάτημα της λειτουργίας ή και την φυσική καταστροφή του εξοπλισμού ο οποίος φιλοξένει το προς αποκλεισμό περιεχόμενο [17].

3.6.11 Επιτήρηση

Όλες οι παραπάνω τεχνικές έχουν σα σκοπό τον αποκλεισμό της πρόσβασης σε περιεχόμενο, είναι όμως δυνατό να παρουσιάζουν καθυστέρηση στην εφαρμογή τους ή και να παρακαμφθούν. Μια τακτική η οποία μπορεί να εφαρμοστεί παράλληλα με το φιλτράρισμα είναι η παρακολούθηση των ιστοσελίδων τις οποίες επισκέπτεται κάποιος. Νόμιμες ή παράνομες ποινές είναι δυνατό να επιβληθούν, αν πραγματοποιείται πρόσβαση (ή προσπάθεια για πρόσβαση) σε ανεπιθύμητο περιεχόμενο.

Αν το παραπάνω γεγονός γίνει ευρύτερα γνωστό, αποθαρρύνονται άλλοι χρήστες να αιτηθούν το ανάλογο περιεχόμενο, ακόμη και αν τεχνικά αυτό δεν έχει αποκλειστεί αποτελεσματικά. Αυτού του τύπου η δημοσιοποίηση έχει παρατηρηθεί στην Κίνα, με τους Jingjing και Chacha, δύο αστυνομικούς, ήρωες κινουμένων σχεδίων, οι οποίοι πληροφορούν του χρήστες του Διαδικτύου ότι παρακολουθούνται και τους ενθαρρύνουν να αναφέρουν πιθανούς παραβάτες [17].

3.6.12 Κοινωνικές Τεχνικές

Συχνά εφαρμόζονται κοινωνικοί μηχανισμοί για να αποτρέψουν του χρηστές από το να έχουν πρόσβαση σε ακατάλληλο περιεχόμενο. Για παράδειγμα οι οικογένειες μπορούν να τοποθετήσουν τον υπολογιστή στο καθιστικό σε σημείο όπου η οθόνη μπορεί να παρακολουθηθεί από όλους, παρά σε ένα πιο ιδιωτικό χώρο, όπως ένα υπνοδωμάτιο, αποτρέποντας τα παιδία να παρακολουθούν ακατάλληλες ιστοσελίδες. Σε μια βιβλιοθήκη οι υπολογιστές είναι δυνατό να χωροθετηθούν κατάλληλα ώστε οι οθόνες τους να είναι ορατές από το γραφείο του υπεύθυνου. Ένα Internet cafe μπορεί να έχει κλειστό κύκλωμα τηλεόρασης για να παρακολουθεί τους πελάτες του. Είναι δυνατό να υπάρξουν νόμοι που να επιβάλλουν τη χρήση των καμερών ή ακόμη και η πρόσβαση στο Διαδίκτυο να γίνεται μετά από καταγραφή μέσω της φωτογραφίας της ταυτότητας του χρήστη. Υπάρχει γενικά, ένα ευρύ φάσμα από διαθέσιμους λογικούς ή εξεζητημένους ελέγχους [17].

3.7 Αξιολόγηση των Τεχνικών του Ελέγχου Προσπέλασης- Αποτελεσματικότητα και Επιπτώσεις

Η χρήση των μηχανισμών για έλεγχο και αποτροπή της πρόσβασης σε συγκεκριμένο περιεχόμενο, δηλαδή τα φίλτρα, είναι μια τεχνολογία που επιδέχεται σημαντική κριτική.

Πρόκειται για μια τεχνολογία η οποία παρουσιάζει εγγενείς ατέλειες και περιορισμούς οι οποίοι έχουν σχέση με [01] :

- Επιπτώσεις στην απόδοση του δικτύου ή του υπολογιστή.
- Αποτελεσματικότητα ελέγχου και αξιοπιστία.
- Απαιτούμενη δαπάνη για την εφαρμογή της.
- Δυνατότητα παράκαμψης της.

3.7.1 Επιπτώσεις στο Δίκτυο

Ένας πολύ σημαντικός παράγοντας στη λειτουργία, κάποιες φορές και στην αποτελεσματικότητα, των επιλογών ελέγχου είναι οι επιπτώσεις που επιφέρουν στο σύστημα στο οποίο εφαρμόζονται. Οι επιπτώσεις αυτές είναι άμεσα συνδεδεμένες με τη θέση στη τοπολογία του δικτύου που είναι εγκατεστημένος ο μηχανισμός ελέγχου, όπως προσωπικός υπολογιστής, ISP, ασύρματο δίκτυο ή κάποιος τρίτος οργανισμός, αλλά και από τις επιλογές στη ρύθμιση που έχουν γίνει για να αντιμετωπίζει συγκεκριμένες κατηγορίες περιεχομένου, όπως παράνομο περιεχόμενο ή κατηγορίες που έχουν επιλεγεί από το τελικό χρήστη.

Όλες οι επιλογές φιλτραρίσματος καταναλώνουν επεξεργαστικούς πόρους στον υπολογιστή ή σε οποιαδήποτε άλλη συσκευή είναι εγκατεστημένες. Όταν οι διεργασίες ελέγχου και αποκλεισμού έχουν παρόμοιο μέγεθος και λειτουργικότητα με αυτές για τις όποιες μια συσκευή έχει σχεδιαστεί οι πρόσθετοι υπολογιστικοί πόροι που απαιτούνται, μπορεί να έχουν αμελητέα επίδραση στο υλικό του δικτύου. Για παράδειγμα στο δρομολογητή, που σχεδιάστηκε για να δρομολογεί πακέτα προς διαφορετικές κατευθύνσεις η πρόσθετη λειτουργία φιλτραρίσματος που περιλαμβάνει αναδρομολόγηση ή απόρριψη πακέτων δε θα επιφέρει σημαντικό επιπρόσθετο φόρτο.

Γενικότερα επιλογές μεθόδων που χρησιμοποιούν λίστες με απαγορευμένες διευθύνσεις προκαλούν μικρή η καθόλου μείωση στην απόδοση του δικτύου. Αυτό συμβαίνει γιατί το μέγεθος της διεργασίας (ο αποκλεισμός συνήθως σχετίζεται με μερικές χιλιάδες διευθύνσεις) δεν αυξάνει σημαντικά την απαίτηση σε επεξεργαστική ισχύ της συσκευής στην οποία είναι εγκατεστημένο.

Λύσεις ελέγχου που απαιτούν διαχείριση μεγαλύτερων καταλόγων ή σύνθετη ανάλυση του περιεχομένου ή και τα δύο, εκ των πραγμάτων απαιτούν μεγαλύτερη άντληση επεξεργαστικών πόρων που συνεπάγεται μείωση της απόδοσης της υλικοτεχνικής υποδομής του συγκεκριμένου δικτύου.

Οι επιδράσεις στην απόδοση είναι ωστόσο, σχετικά μικρές όταν ο έλεγχος εφαρμόζεται σε προσωπικούς υπολογιστές, μια που ο πρόσθετος επεξεργαστικός φόρτος είναι συγκρίσιμος με τις υπόλοιπες διεργασίες που εκτελεί ο υπολογιστής και σχετικά μικρός συγκρινόμενος με την επεξεργαστική ισχύ του.

Για τους Παρόχους Υπηρεσιών Διαδικτύου το μέγεθος του πρόσθετου φόρτου που προκύπτει από την εφαρμογή φιλτραρίσματος, εξαρτάται από το πλήθος των συνδρομητών στους οποίους εφαρμόζεται. Χωρίς ουσιαστική αύξηση των επεξεργαστικών δυνατοτήτων, μια υπολογίσιμη μείωση της απόδοσης του δικτύου είναι αναπόφευκτη.

Η μείωση της απόδοσης είναι δυνατό να περιοριστεί με επενδύσεις σε υλικοτεχνική υποδομή, οι οποίες όμως μπορεί να έχουν σημαντικό κόστος αναλογικά και σε επίπεδο τελικού χρήστη αλλά και σε επίπεδο παρόχου [01].

3.7.2 Υπερβολικός και Ελλιπής Αποκλεισμός (Under blocking, Over blocking)

Όλες οι τεχνικές αποκλεισμού του περιεχομένου πάσχουν από πιθανότητα λάθους το οποίο μπορεί να είναι δύο ειδών :

- Ψευδώς θετικά αποτελέσματα (false positive), όπου ένας ιστότοπος που δεν προορίζονταν να αποκλειστεί, καθίσταται μη προσβάσιμος

- Ψευδώς αρνητικά αποτελέσματα (false negative), όπου ιστότοποι είναι προσβάσιμοι, παρά την πρόθεση να αποκλειστούν.

Τα δύο αυτά είδη σφαλμάτων αναφέρονται ως over blocking (υπερβολικός αποκλεισμός) και under blocking (ελλιπείς αποκλεισμός) και είναι συνήθως ανταγωνιστικά μεταξύ τους. Η εξισορρόπηση μεταξύ των ψευδώς θετικών και των ψευδώς αρνητικών αποτελεσμάτων είναι κυρίαρχο ζητούμενο για τους μηχανικούς ασφαλείας, βρίσκοντας εφαρμογή σε διαφόρους τομείς, από την ταυτοποίηση με βάση βιομετρικά χαρακτηριστικά ως τον ηλεκτρονικό πόλεμο. Η

καμπύλη που αναπαριστά την εξισορρόπηση μεταξύ των δύο καταστάσεων ονομάζεται ROC (Receive Operating Characteristic – Χαρακτηριστικό Λειτουργίας του Δέκτη). Τροποποιώντας μια παράμετρο μετακινείται το σημείο λειτουργίας του συστήματος, κατά μήκος της καμπύλης. Για παράδειγμα αν κάποιος απαιτήσει χαμηλότερο επίπεδο ελλιπούς αποκλεισμού, θα υποστεί το κόστος των περισσότερων ψευδώς θετικών αναφορών. Γενικά για να επιτευχτεί η καλύτερη ισορροπία μεταξύ των δύο καταστάσεων πρέπει να καθοριστούν ακριβέστεροι τρόποι διαχωρισμού μεταξύ του επιθυμητού και του ανεπιθύμητου αποτελέσματος. Αυτό θα έχει σα συνέπεια τη μετατόπιση της καμπύλης ROC έτσι ώστε να μειωθούν ταυτόχρονα και τα δύο είδη λάθους [17].

Το φιλανδικό σύστημα φιλτραρίσματος απέκλεισε λανθασμένα το 2008 τον ιστότοπο του W3C, ενός από τους βασικούς παγκόσμιους οργανισμούς που καθορίζουν σημαντικά πρότυπα για το Διαδίκτυο, όπως HTML και XML. Ο αποκλεισμός αυτός μπορεί να οφείλεται είτε σε παντελή έλλειψη σωστής αξιολόγησης από τους αρμόδιους που καθορίζουν την ακαταλληλότητα του περιεχομένου, είτε από αστοχία του αυτοματοποιημένου λογισμικού που ενημερώνει την μαύρη λίστα της εφαρμογής. Δεδομένου ότι είναι απίθανο να αποκλείστηκε σκόπιμα ό ιστότοπος του W3C και μια που το URL του W3C ενσωματώνει με διαφανή τρόπο τον πηγαίο κώδικα για το ορθό γράψιμο ιστοσελίδων, η δεύτερη αιτιολόγηση είναι πιθανότερη [26].

Το φιλτράρισμα που βασίζεται στην κεφαλίδα του TCP/IP πακέτου είναι σχετικά χονδροειδές μια που αποκλείει ολόκληρη την IP διεύθυνση ή περιοχή διευθύνσεων, οι οποίες μπορεί να φιλοξενούν περισσότερους του ενός ιστότοπους ή και άλλες υπηρεσίες. Συμπεριλαμβάνοντας στο φιλτράρισμα τον αριθμό θύρας, γίνεται λιγότερο επιρρεπές στα λάθη, κινούμενο πλέον σε επίπεδο υπηρεσίας, ενώ με το ολοκληρωτικό κλείσιμο του εξυπηρετητή χάνεται η πρόσβαση σε κάθε είδους κατάλληλη υπηρεσία ή πληροφορία.

Η κατάσταση βελτιώνεται με το DNS tampering όπου ο αποκλεισμός περιορίζεται σε επίπεδο ιστότοπου, αλλά όλες οι υπηρεσίες του τομέα, εκτός από το ηλεκτρονικό ταχυδρομείο που αντιμετωπίζεται διαφορετικά, χάνουν την προσβασιμότητα τους.

Στην περίπτωση του ελέγχου στο περιεχόμενο του TCP/IP πακέτου είναι δυνατός ο αποκλεισμός σε επίπεδο ιστοσελίδας. Εδώ υπάρχει πάντα ο κίνδυνος στην αναζήτηση λέξεων κλειδιών, να μη εντοπιστούν λόγω της διάσπασης τους σε πολλαπλά πακέτα, γεγονός σχετικά σπάνιο, με τα συνηθισμένα προγράμματα πλοήγησης.

Τη μεγαλύτερη ευελιξία προσφέρουν μέθοδοι βασιζόμενες σε διαμεσολάβηση (proxying) επιτρέποντας αποκλεισμό από μια ιστοσελίδα ως ένα ολόκληρο ιστότοπο ή και εξυπηρετητή. Ενώ η πιο «χοντροκομμένη» επιλογή είναι αυτή του DDoS όπου στη προσπάθεια να τεθεί κάποιο περιεχόμενο σε αποκλεισμό, με τον καταιγισμό στις υποδομές του δικτύου, και όχι στον μεμονωμένο εξυπηρετητή, αποκλείονται πλήθος από εξυπηρετητές ή και ολόκληρο το δίκτυο του παρόχου που το φιλοξενεί.

Η επιτήρηση και η απειλή κυρώσεων μπορεί να είναι αρκετά αποτελεσματική μια που η ανθρώπινη παρέμβαση βελτιώνει σημαντικά την ποιότητα της διάκρισης. Ακόμη και αν δεν έχει χαρακτηριστεί κάποιο περιεχόμενο ως ανεπιθύμητο, η αυτολογοκρισία αποθαρρύνει τους χρήστες από το να το προσπελάσουν. Πάντως τέτοια μέτρα συχνά προκαλούν και υπερβολικό έλεγχο με τη δημιουργία κλίματος φόβου [17].

3.7.3 Κόστος Εφαρμογής

Το κόστος εφαρμογής των μηχανισμών ελέγχου εξαρτάται από την πολυπλοκότητα του υλικού που απαιτείται προκειμένου να λειτουργήσει. Επίσης εξαιτίας της σχετικά περιορισμένης αγοράς, ο ειδικός διαδικτυακός εξοπλισμός φιλτραρίσματος είναι συγκριτικά ακριβός. Το κόστος αυτό συχνά μεταβιβάζεται στον τελικό καταναλωτή αυξάνοντας το μέσο κόστος διασύνδεσης στο διαδίκτυο [26]. Αν χρησιμοποιηθεί γενικής χρήσης εξοπλισμός για τον έλεγχο είναι δυνατό να περιοριστεί η δαπάνη εφαρμογής του [17].

Οι παραπάνω παράγοντες έχουν σαν αποτέλεσμα ο έλεγχος των κεφαλίδων των διακινούμενων πακέτων να είναι η φθηνότερη επιλογή. Οι δρομολογητές που είναι ήδη εγκατεστημένοι για να ανακατευθύνουν πακέτα μπορούν εύκολα, με προσθήκη εντολών αποκλεισμού για τους ιστότοπους που είναι απαγορευμένοι, να απορρίψουν τα πακέτα που προορίζονται για αυτούς. Ωστόσο και οι δρομολογητές έχουν ένα όριο στη διαχείριση πλήθους κανόνων, το οποίο όταν προσεγγιστεί είναι δυνατό να δημιουργηθούν προβλήματα. Η προσθήκη του αριθμού θύρας στους κανόνες δρομολόγησης, απαιτεί προσθετό εξοπλισμό στους δρομολογητές και μια που μόνο η κεφαλίδα του πακέτου χρειάζεται να ελεγχτεί, η επιβάρυνση στην ταχύτητα είναι μικρή.

Ο έλεγχος του φορτίου των πακέτων TCP/IP είναι μια εργασία που δε γίνεται συνήθως από τους δρομολογητές. Απαιτείται επιπρόσθετος εξοπλισμός, ο όποιος για δεδομένα με υψηλούς ρυθμούς διακίνησης στο Διαδίκτυο, είναι αρκετά ακριβός. Μια φτηνότερη επιλογή, είναι το φίλτρο να εξετάζει το περιεχόμενο των πακέτων καθώς διέρχονται και να μη τα σταματά κατά τη διάρκεια

του ελέγχου, παρουσιάζει όμως μειωμένη αξιοπιστία που μπορεί να οδηγήσει τελικά σε αύξηση του κόστους. Στην περίπτωση αυτή ο εξοπλισμός ελέγχου μπορεί να προκαλέσει συμφόρηση καθυστέρηση καθώς και απώλεια ορισμένων πακέτων. Όταν διαπιστώνεται η παραβίαση μιας πολιτικής ελέγχου, ο σχετικός εξοπλισμός μπορεί να στείλει ένα μήνυμα και στις δύο πλευρές της σύνδεσης, ζητώντας το τερματισμό της.

Το DNS tampering είναι επίσης μια σχετικά φθηνή επιλογή, μια που η απόκριση της αναδρομικής ανάλυσης, δεν απαιτείται να είναι ιδιαίτερα γρήγορη και μπορεί να χρησιμοποιηθεί ο υπάρχον εξοπλισμός των DNS εξυπηρετητών.

Η δημιουργία συνδέσεων με την επανασύνδεση των συστατικών πακέτων που απαιτείται από τους HTTP διακομιστές καθιστά την επιλογή αυτή ακριβή. Οι υβριδικού HTTP διακομιστές είναι πιο πολύπλοκοι στο να ρυθμιστούν, αλλά αν συμβεί αυτό μια φορά, είναι μόνο λίγο ακριβότεροι από το IP φιλτράρισμα έχοντας όμως μεγαλύτερη ευελιξία. Αυτό συμβαίνει γιατί το ακριβό κομμάτι της διάταξης (HTTP proxy) δέχεται μόνο ένα μικρό ποσοστό της κίνησης και έτσι δεν απαιτείται να είναι ιδιαίτερα ισχυρό.

Το κόστος μιας επίθεσης Άρνησης Υπηρεσίας είναι δύσκολο να εκτιμηθεί, μια που εξαρτάται από τις δυνατότητες του εξυπηρετητή στόχου και τη ταχύτητα διασύνδεσης του Διαδικτύου. Τέτοιου είδους επιθέσεις αγγίζουν τα όρια της νομιμότητας, ειδικότερα όταν κατευθύνονται προς άλλες χώρες. Θέματα νομιμότητας τίθενται και για τις περιπτώσεις των κοινωνικών τεχνικών, της επιτήρησης αλλά και της απενεργοποίησης των εξυπηρετητών [17].

Η Αυστραλιανή κυβέρνηση ξόδεψε περίπου 128 εκατομμύρια δολάρια το 2008 για την εγκατάσταση ενός συστήματος ελέγχου. Στο ποσό αυτό δεν συμπεριλαμβάνονται έμμεσα κόστη, όπως η πρόσληψη από τους παρόχους επιπλέον προσωπικού για να αντεπεξέλθουν στις αυξημένες απαιτήσεις των τμημάτων εξυπηρέτησης πελατών, λόγω του αυξημένου πλήθους κλήσεων από πελάτες που δέχονταν τις επιπτώσεις της εφαρμογής. Σε ακόμη μεγαλύτερης κλίμακας εφαρμογές, όπως αυτή που συμβαίνει στην Κίνα τα ποσά είναι σημαντικά μεγαλύτερα.

Εκτός από την άμεση χρηματική δαπάνη, ένα από τα σημαντικότερα κόστη για τα φίλτρα περιεχομένου είναι η μειωμένη απόδοση του δικτύου. Στα δοκιμαστικά που διεξήχθησαν για το προτεινόμενο σύστημα φιλτραρίσματος στην κυβέρνηση της Αυστραλίας, ορισμένα στοιχεία έδειξαν ότι η περιήγηση στο Διαδίκτυο θα μπορούσε να επιβραδυνθεί έως 87% από

συγκεκριμένα προγράμματα. Παρά το γεγονός ότι άλλες λύσεις δεν είναι τόσο επιζήμιες για την λειτουργία του δικτύου, η βελτίωση της απόδοσης έχει το αντίστοιχο τίμημα.

Ένα πρόσθετο σημαντικό κόστος που προκύπτει κατά την εφαρμογή του φιλτραρίσματος περιεχομένου, είναι αυτό που συνδέεται με την πιθανότητα για ψευδώς θετικά ή ψευδώς αρνητικά αποτελέσματα. Ακόμη και το καλύτερο από τα συστήματα ελέγχου περιεχομένου που εξετάστηκαν στα δοκιμαστικά στην Αυστραλία είχε ένα 1% ποσοστό ψευδώς θετικών. Η πιθανή οικονομική ζημία προκαλείται από τον αποκλεισμό, αυθαίρετα, ιστοσελίδων νόμιμων επιχειρήσεων [26].

3.7.4 Ανιχνευσιμότητα

Έχοντας πρόσβαση στους υπολογιστές οι οποίοι έχουν αποκλειστεί από περιεχόμενο, δεν είναι πάντα δυνατό να ανιχνευτούν αξιόπιστα οι περισσότεροι μηχανισμοί οι οποίοι έχουν αναφερθεί.

Στη μεριά του εξυπηρετητή ανάλογος προσδιορισμός είναι δύσκολο να πραγματοποιηθεί. Για παράδειγμα αν και ένας εξυπηρετητής, ο οποίος έχει αποκλειστεί μπορεί να αναγνωρίσει μια επίθεσης Άρνησης Υπηρεσίας, είναι σχετικά δύσκολο να τη διαχωρίσει από «νόμιμη» υπερβολικά αυξημένη κίνηση. Ανάλογα ένας εξυπηρετητής ο οποίος έχει απενεργοποιηθεί ή έχει διαγράφει το Domain όνομα του για λόγους αποκλεισμού, εμφανίζεται με την ίδια λειτουργικότητα με έναν που έχει τεχνικά προβλήματα ή προβλήματα ρύθμισης του DNS.

Η επόπτευση είναι πολύ δύσκολο να εντοπιστεί τεχνικά, εφόσον έχει εγκατασταθεί πλήρως. Άλλωστε τα αποτελέσματα μιας επιτήρησης γίνονται γνωστά με σκοπό αποτρεπτικό, χωρίς συνήθως να αποκαλύπτονται οι πηγές πληροφόρησης που χρησιμοποιήθηκαν [17].

3.7.5 Αξιοπιστία

Ακόμη και οι χρήστες που δεν προσπαθούν να παρακάμψουν τα συστήματα, μπορούν πολλές φορές να έχουν πρόσβαση στο απαγορευμένο περιεχόμενο. Με δεδομένο ότι έχουν εγκατασταθεί σωστά και δεν υπάρχουν τεχνικά προβλήματα, όλες οι τεχνικές, εκτός της Άρνησης Υπηρεσιών και των κοινωνικών τεχνικών, θα αποκλείσουν την πρόσβαση σχετικά αξιόπιστα. Στην περίπτωση της Άρνησης Υπηρεσιών, αυτό που συμβαίνει είναι ότι το σύστημα όταν υπερφορτώνεται απορρίπτει κάποια αιτήματα με αποτέλεσμα περιεχόμενο που επρόκειτο

να αποκλειστεί να προβάλλεται. Ενώ στην περίπτωση των κοινωνικών τεχνικών απλά η αγνόηση τους θα είχε το ίδιο αποτέλεσμα.

Οι οργανισμοί που λειτουργούν τους μηχανισμούς ελέγχου πρόσβασης πρέπει να δημιουργούν και να συντηρούν λίστες με ιστότοπους και ιστοσελίδες προς αποκλεισμό. Αυτό είναι μία αρκετά υπολογίσιμη εργασία αν το περιεχόμενο που πρόκειται να αποκλειστεί είναι μια ολόκληρη θεματολογία, όπως η πορνογραφία, και όχι ένας συγκεκριμένος ιστότοπος. Υπάρχουν προϊόντα στην αγορά τα οποία ενημερώνουν τακτικά τις λίστες τους, αλλά ακόμη και αυτές έχουν αναπόφευκτα σημαντικές ελλείψεις. Ο έλεγχος που βασίζεται σε λέξεις κλειδιά (σε επίπεδο πακέτου ή με τη βοήθεια HTTP proxy) αντιμετωπίζει εν μέρει αυτή την αδυναμία, μια που στις λίστες χρειάζεται να εμπεριέχοντα μόνο οι απαγορευμένες λέξεις και όχι χιλιάδες ιστότοποι. Ωστόσο και στην περίπτωση αυτή ιστοσελίδες που θέλουν να αντιμετωπίσουν αυτή τη τεχνική, κάνουν χρήση ισοδύναμων όρων και όχι των απαγορευμένων [17].

3.8 Παράκαμψη των Τεχνικών Ελέγχου

Τα εργαλεία παράκαμψης επιτρέπουν στους λογοκρινόμενους να ξεπεράσουν τους μηχανισμούς ελέγχου πρόσβασης στο περιεχόμενο, που επιβάλλονται από κυβερνήσεις, εργοδότες, οργανισμούς ή ακόμη και τους ίδιους τους εαυτούς τους. Υπάρχουν διαφορετικοί τύποι τέτοιων ανθεκτικών στον έλεγχο μηχανισμών, από απλούς διακομιστές μεσολάβησης έως κρυπτογραφημένα εικονικά δίκτυα, σχεδόν όλοι όμως παρέχουν την ίδια λειτουργικότητα, διαμεσολάβηση στο χρήστη προκειμένου να υπάρχει πρόσβαση σε διαφορετικά αποκλεισμένο περιεχόμενο [81].

Η ευκολία με την οποία οι μηχανισμοί αποκλεισμού περιεχομένου είναι δυνατό να παρακαμφθούν εξαρτάται από τις τεχνικές γνώσεις του χρήστη, ενώ η μέθοδος παράκαμψης εξαρτάται από τη τοποθεσία στην οποία εφαρμόζεται ο μηχανισμός. Για παράδειγμα, μέθοδοι παράκαμψης που χρησιμοποιούνται για λογισμικό γονικού ελέγχου είναι εγκατεστημένες στον οικιακό υπολογιστή και είναι συνήθως διαφορετικές από αυτές που προορίζονται να λειτουργήσουν σε εξυπηρετητές του παρόχου. Η επιλογή της τεχνικής παράκαμψης είναι πάντα συνάρτηση της τεχνικής αποκλεισμού και του τρόπου λειτουργίας της [01].

3.8.1 Αλλαγή Θέσης και IP Διεύθυνσης

Οι πάροχοι του περιεχομένου μπορούν να ξεπεράσουν το IP φιλτράρισμα αλλάζοντας την IP διεύθυνση του εξυπηρετητή που τους φιλοξενεί ή ακόμη και τον εξυπηρετητή τον ίδιο. Αυτό θεωρητικά μπορεί να είναι αδιάφορο για το χρήστη, μια που το DNS αυτόματα θα επιτρέψει στο πρόγραμμα πλοήγησης του να επικοινωνήσει με τη νέα διεύθυνση.

Στην πράξη η συχνή αλλαγή IP διεύθυνσης (αρκετές φορές στην ίδια μέρα) απαιτεί ιδιαίτερα πολύπλοκες τεχνικές δυνατότητες. Στην βιβλιογραφία αναφέρεται συχνά η περίπτωση του παρόχου xs4all στην Ολλανδία που το 1997 άλλαζε σε ωριαία βάση IP διευθύνσεις προκειμένου να παρακάμψει προσπάθειες ελέγχου [21].

3.8.2 Αλλαγή Θύρας Επικοινωνίας

Η αλλαγή αριθμού θύρας που χρησιμοποιείται για μια υπηρεσία, μπορεί να αποτελέσει μια απλή μέθοδο παράκαμψης φιλτραρίσματος στο επίπεδο 4 και πιθανόν ελέγχου με τη βοήθεια HTTP διαμεσολαβητών. Αυτό μπορεί να γίνει με μια απλή ρύθμιση στο λογισμικό του Web εξυπηρετητή. Ο χρήστης πρέπει να ενημερωθεί για να αλλάξει ρυθμίσεις τοπικά ή να χρησιμοποιεί διαφορετική URL διεύθυνση για να έχει πρόσβαση στο αποκλεισμένο περιεχόμενο [21].

3.8.3 Χρήση Εναλλακτικών Domain Ονομάτων ή URL

Ένας από τους πιο συνηθισμένους τρόπους για να αποκλειστεί ένας ιστότοπος είναι μέσω του Domain ονόματος του ή της URL διεύθυνσης του. Συχνά οι ιστότοποι είναι προσβάσιμοι με διαφορετικά ονόματα, για παράδειγμα το «news.bbc.co.uk» με το όνομα «newsrss.bbc.co.uk».

Αν το ένα όνομα είναι αποκλεισμένο μπορεί κάποιος να ζητήσει πρόσβαση με κάποιο άλλο. Τα πρόσθετα ονόματα, συνήθως δεν είναι προφανή στου χρήστες, οι οποίοι θα πρέπει να τα αναζητήσουν προκειμένου να έχουν πρόσβαση στο αποκλεισμένο περιεχόμενο.

Μια άλλη προσέγγιση είναι να επιχειρηθεί η ο πρόσβαση μέσω ειδικής έκδοσης των ιστοσελίδων προορισμένων για έξυπνα τηλέφωνα (smart phones) η οποία συνήθως προκύπτει με την προσθήκη του m στο URL του ιστότοπου, πχ. «http://m.facebook.com» ή «http://touch.facebook.com» [33].

Η τεχνική αυτή, φυσικά είναι ανεφάρμοστη στην περίπτωση του βασισμένου σε IP διευθύνσεις, αποκλεισμού [01], ενώ είναι αποτελεσματική στην περίπτωση των διακομιστών μεσολάβησης και του DNS tampering [21].

3.8.4 Εναλλακτικοί DNS εξυπηρετητές

Λαμβάνοντας υπόψη μια κατάσταση κατά την οποία ο διακομιστής DNS του χρήστη υπόκειται σε παρέμβαση, ο ευκολότερος τρόπος για να ξεπεραστούν αυτοί οι χειρισμοί είναι να χρησιμοποιείται συνεχώς ένας δημόσια προσβάσιμος, ελεύθερος DNS εξυπηρετητής που δεν έχει αλλοιωθεί. Συνεπώς ο χρήστης δεν θα πρέπει να χρησιμοποιεί τους διακομιστές DNS που του εκχωρούνται αυτόματα από τον πάροχο του, αλλά να τροποποιήσει τις ρυθμίσεις του δικτύου του, ώστε να χρησιμοποιούνται ρητά μόνον εξωτερικοί εξυπηρετητές, οι οποίοι δεν υπόκεινται σε παραβιάσεις.

Μια λίστα από τέτοιους εναλλακτικούς εξυπηρετητές, μπορεί να αναζητηθεί από το Διαδίκτυο. Θα πρέπει να παρατηρηθεί ότι σε κάθε περίπτωση, για λόγους ασφαλείας, αυτοί οι εξυπηρετητές μπορεί να αρνηθούν να απαντήσουν σε ερωτήματα από αυθαίρετους μη εξουσιοδοτημένους πελάτες [93].

3.8.5 Χρήση Ιστοθέσεων και Υπηρεσιών Τρίτων Μερών

Υπάρχουν διάφοροι τρόποι για να προσεγγίσει κάποιος το περιεχόμενο μιας ιστοσελίδας πηγαίνοντας μέσω ιστότοπων τρίτων ή άλλων υπηρεσιών, παρά μέσω του ιστότοπου προέλευσης των δεδομένων [33].

Αποθηκευμένες Ιστοσελίδες

Πολλές μηχανές αναζήτησης διατηρούν αντίγραφα των ιστοσελίδων που κατά καιρούς έχουν αναζητηθεί (cached pages). Οι ιστοσελίδες αυτές εμφανίζονται στα αποτελέσματα αναζήτησης με ένα πρόσθετο σύνδεσμο που παρέχει πρόσβαση στο προσωρινά αποθηκευμένο περιεχόμενο τους. Η επιλογή αυτού του συνδέσμου επιτρέπει τη λήψη των απαγορευμένων δεδομένων, μια που αυτά δεν προέρχονται από τον αποκλεισμένο ιστότοπο [33].

Μεταφραστές Ιστοσελίδων

Υπάρχουν πολλές υπηρεσίες μετάφρασης ιστοσελίδων, συνήθως παρεχόμενες από μηχανές αναζήτησης. Αν ένας χρήστης προβάλει μια ιστοσελίδα μέσω ενός μεταφραστή, ο μεταφραστής ζητά και αποκτά πρόσβαση στην ιστοσελίδα και όχι ο χρήστης. Η διαδικασία αυτή επιτρέπει την ανάγνωση αποκλεισμένου περιεχομένου μεταφρασμένου σε ένα πλήθος από γλώσσες.

Η χρήση του μεταφραστή μπορεί να γίνει για να παρακαμφθεί ο αποκλεισμός, ακόμη και αν δεν είναι απαραίτητη η μετάφραση του κειμένου. Ο χρήστης επιλέγει την μετάφραση από μια γλώσσα που δεν εμφανίζεται στην αρχική σελίδα, στη γλωσσά της αρχικής σελίδας. Για παράδειγμα για την προβολή ενός ελληνικού ιστότοπου, είναι δυνατό να επιλεγεί η μετάφραση από τα κινέζικα στα ελληνικά. Η υπηρεσία μετάφρασης μεταφράζει μόνο τα τμήματα που είναι στα κινέζικα (τα οποία δεν υπάρχουν) και αφήνει και προβάλει το τμήμα στην ελληνική γλώσσα (δηλαδή ολόκληρο τον ιστότοπο), αμετάφραστο [33].

RSS

Το RSS (Really Simple Syndication) αποτελεί ένα πρότυπο βασισμένο σε XML για διανομή περιεχομένου. Οι Συλλέκτες (Aggregator) RSS είναι ιστότοποι που επιτρέπουν, μετά από συνδρομή, την ανάγνωση τροφοδοσίας RSS η οποία συνεχώς παρέχει ειδήσεις ή άλλες πληροφορίες, που προέρχονται από επιλεγμένους ιστότοπους. Οι συλλέκτες συνδέονται αυτοί, με τους αποκλεισμένους ιστότοπους κατεβάζουν περιεχόμενο από τις επιλεγμένες πηγές και το προβάλουν. Η εφαρμογή αυτή φυσικά, μπορεί να λειτουργήσει μόνο σε ιστότοπους που υποστηρίζουν RSS τροφοδοσία [33].

Είδωλα Ιστότοπων

Τα είδωλα των ιστότοπων, (Mirrors) είναι αντίγραφα τους, δημιουργημένα κυρίως για την μείωση του φόρτου της κίνησης και την εξοικονόμηση πόρων στους εξυπηρετητές που τους φιλοξενούν. Το είδωλο ανακτά συνεχώς, πολλές φορές και με αυτοματοποιημένο τρόπο, το περιεχόμενο από τον αρχικό ιστότοπο και το δημοσιεύει.

Ένας χρήστης, ο οποίος επιδιώκει πρόσβαση σε απαγορευμένο περιεχόμενο, μπορεί να προσεγγίσει το είδωλο του αποκλεισμένου ιστότοπου, το ποιο πιθανόν να μην είναι καταχωρημένο στην λίστα αποκλεισμού [01]. Η επιλογή αυτής της μεθόδου μπορεί να γίνει για

την παράκαμψη IP φιλτραρίσματος, DNS tampering και ελέγχου μέσω διαμεσολαβητών. Η εκμετάλλευση των ειδώλων για το σκοπό αυτό δεν είναι προφανής στους χρήστες, οι οποίοι θα πρέπει να ενημερωθούν σχετικά με την ύπαρξη τους αλλά και τις διευθύνσεις τους προκείμενου να τα προσεγγίσουν [21].

Σε κάθε περίπτωση το mirroring είναι ευρέως χρησιμοποιούμενο σε παλιού τύπου, στατικούς ιστότοπους με περιορισμένο διαδραστικό περιεχόμενο. Στο σύγχρονο Web με τα έντονα δυναμικά χαρακτηριστικά είναι δύσκολο να εφαρμοστεί [21].

Φίλτρα Χαμηλού Εύρους Ζώνης

Τα Φίλτρα Χαμηλού Εύρους Ζώνης είναι υπηρεσίες σχεδιασμένες για την διευκόλυνση της πλοήγησης στον παγκόσμιο ιστό, σε περιοχές όπου η ταχύτητα διασύνδεσης είναι μικρή. Αφαιρούν εικόνες και διαφημίσεις και γενικά συμπιέζουν το περιεχόμενο του ιστότοπου ώστε να απαιτείται η μικρότερη μετάδοση δεδομένων και κατά συνέπεια η ταχύτερη προβολή τους.

Τα φίλτρα αυτά είναι δυνατό να χρησιμοποιηθούν, όπως οι μεταφραστές και οι Συλλέκτες RSS, προκειμένου να παρακαμφθεί ο αποκλεισμός ιστότοπων, μια που οι εξυπηρετητές των φίλτρων αιτούνται πλέον την πρόσβαση και όχι ο χρήστης. Παράδειγμα τέτοια υπηρεσίας είναι η http://loband.org [33].

Αρχεία του Παγκόσμιου Ιστού

Το archive.org, (η μηχανή Wayback – http://www.archive.org/web/web.php) αποθηκεύει και επιτρέπει στους χρήστες να δουν αρχειοθετημένες εκδόσεις ιστοσελίδων του παρελθόντος. Εκατομμύρια ιστότοποι και τα συσχετιζόμενα με αυτούς δεδομένα, (εικόνες, πηγαίος κώδικας, έγγραφα κ.α.), αποθηκεύονται σε γιγαντιαίες βάσεις δεδομένων.

Σε κάθε περίπτωση δεν είναι διαθέσιμος όλος ο Παγκόσμιος Ιστός, μια που πολλοί ιδιοκτήτες ιστότοπων επιλέγουν να μη αρχειοθετηθούν. Επιπλέον η ενημέρωση των εκδόσεων απαιτεί αρκετό χρόνο [33].

Χρήση του Ηλεκτρονικού Ταχυδρομείου

Οι υπηρεσίες ηλεκτρονικού ταχυδρομείου και ιδιαίτερα αυτές που λειτουργούν μέσω του Παγκόσμιου Ιστού (Web mail), μπορεί να χρησιμοποιηθούν μεταξύ χρηστών για την ανταλλαγή εγγράφων, ακόμη και για την πλοήγηση σε ιστοθέσεις.

Ανάλογα με τα φίλτρα χαμηλού εύρους ζώνης, η υπηρεσία πρόσβασης σε ιστοσελίδες μέσω ηλεκτρονικού ταχυδρομείου, στοχεύει στην εξυπηρέτηση ανθρώπων με αργές ή αναξιόπιστες διασυνδέσεις στο Διαδίκτυο, στους οποίους επιτρέπει την αίτηση ιστοσελίδων μέσω ηλεκτρονικών μηνυμάτων. Η υπηρεσία αποστέλλει ηλεκτρονικό μήνυμα με επισυναπτόμενα τα περιεχόμενα της ιστοσελίδας. Η υπηρεσία αυτή μπορεί να είναι ιδιαίτερα αποτελεσματική μια που συχνά στο ηλεκτρονικό ταχυδρομείο χρησιμοποιείται κρυπτογράφηση.

Μια τακτική που είναι δυνατό να χρησιμοποιηθεί για το διαμοιρασμό εγγράφων μέσω ηλεκτρονικού ταχυδρομείου είναι η κοινοποίηση των στοιχείων του λογαριασμού. Μια που η δημιουργία λογαριασμού σε υπηρεσίες Web mail είναι ιδιαίτερα εύκολη και ανέξοδη, η κοινοποίηση των στοιχείων εισόδου σε χρήστες θα επιτρέψει την πρόσβαση σε περιεχόμενα που είναι αποθηκευμένα στους λογαριασμούς [33].

Εναλλακτική Χρήση Διαφόρων άλλων Υπηρεσιών

Διάφορες άλλες υπηρεσίες του web2 είναι δυνατό να χρησιμοποιηθούν εναλλακτικά, για να μεταδοθεί αποκλεισμένο περιεχόμενο. Για παράδειγμα on line υπηρεσίες δημιουργίας αντιγράφων ασφαλείας και αποθήκευσης δεδομένων όπως το Dropbox , Google Drive, Idrive κ.α., επιτρέπουν το διαμοιρασμό εγγράφων αλλά και κάθε τύπου δεδομένων μεταξύ χρηστών.

3.8.6 Εναλλακτικοί Διακομιστές Μεσολάβησης

Η χρησιμοποίηση ενός εναλλακτικού διακομιστή μεσολάβησης είναι ίσως ο πιο εύκολος τρόπος παράκαμψης της λογοκρισίας. Επιτρέπεται με τον τρόπο αυτό ακόμη και σε μη πεπειραμένους χρήστες να έχουν πρόσβαση σε αποκλεισμένη πληροφορία [93].

Web Http Proxies

Πρόκειται για εφαρμογές που λειτουργούν στην πλευρά του διακομιστή και η προσπέλαση τους γίνεται μέσω φορμών που έχουν την μορφή ιστοσελίδας. Ο χρήστης απλά επισκέπτεται την ιστοσελίδα του διαμεσολαβητή η οποία συμπεριλαμβάνει μια φόρμα με ένα πλαίσιο εισαγωγής URL διεύθυνσης. Σε αυτό το πλαίσιο εισάγει τη διεύθυνση του ιστότοπου στον οποίο επιθυμεί να έχει πρόσβαση και όχι στη γραμμή διευθύνσεων του προγράμματος πλοήγησης που χρησιμοποιεί. Με την υποβολή αυτής της ιστοσελίδας-φόρμας, ο χρήστης στέλνει το URL αίτημα στο διακομιστή μεσολάβησης ο οποίος ζητά αυτός τώρα το περιεχόμενο και τελικά το προβάλει στον τελικό χρήστη [81].

Οι απλοί web proxies δεν απαιτούν από το χρήστη να εγκαταστήσει τοπικά κάποια εφαρμογή. Μοναδική απαίτηση είναι η επίσκεψη στην ιστοσελίδα που φιλοξένει την εφαρμογή διαμεσολάβησης. Κάποιες φορές υπάρχει ο περιορισμός της χρήσης της διεπαφής όχι του προγράμματος πλοήγησης, αλλά της εφαρμογής [81] αν και κάποιοι διαμεσολαβητές επιτρέπουν την πλοήγηση μέσω του τοπικού περιηγητή χωρίς διακοπή της διαμεσολάβησης. Αυτό συμβαίνει γιατί ο διαμεσολαβητής έχει ξαναγράψει όλους τους συνδέσμους της σελίδας και επιτρέπει στο πρόγραμμα περιήγησης να αιτείται το περιεχόμενο μόνο μέσω του proxy. Με δεδομένη την πολυπλοκότητα των σημερινών ιστότοπων η παραπάνω διαδικασία είναι συχνά δύσκολη παρουσιάζοντας μερικές φορές διακοπή της διαμεσολάβησης [33].

Μερικοί γνωστές εφαρμογές web proxy είναι τα CGIProxy, PHProxy, Zelune, Glype, Psiphon και Picade. Όπως προαναφέρθηκε όλες αυτές οι εφαρμογές εγκαθίστανται μόνο στον υπολογιστή που θα κάνει τη διαμεσολάβηση και ενώ βασικά επιτελούν την ίδια λειτουργία παρουσιάζουν διαφορετικά πλεονεκτήματα και μειονεκτήματα σχετικά με τον τρόπο παρουσίασης του περιεχόμενου που τους ζητείται.

Μερικοί διακομιστές είναι ιδιωτικοί. Αυτοί είναι συνήθως προσβάσιμοι μόνο σε μικρές ομάδες χρηστών, γνωστών σε αυτόν που εγκαθιστά το πρόγραμμα ή πελατών που πληρώνουν για την υπηρεσία. Βασικό πλεονεκτήματα τους είναι ότι επειδή είναι λιγότερο γνωστοί είναι σπανιότερα προσπελάσιμοι, δεν παρουσιάζουν συμφόρηση και μειωμένη ταχύτητα, ενώ συνήθως είναι πιο αξιόπιστοι δεδομένης της εμπιστοσύνης που υπάρχει σε αυτούς που τους λειτουργούν. Η πρόσβαση περιορίζεται απαιτώντας τη σύνδεση μέσω ονόματος χρήστη και κωδικού, ή παρεμποδίζοντας το URL του διακομιστή από το να εμφανίζεται σε δημόσιους καταλόγους [33].

Open Proxies

Το πολυπληθέστερο εργαλείο παράκαμψης μηχανισμών ελέγχου είναι οι HTTP και SOCKS ανοικτοί διακομιστές μεσολάβησης [81]. Οι HTTP proxies προφανώς προορίζονται για την κίνηση στον Παγκόσμιο Ιστό. Το SOCKS είναι ένα πρωτόκολλο του Διαδικτύου που χρησιμοποιεί συνήθως την θύρα 1080, χωρίς να αποκλείεται και η χρήση άλλων θυρών. Η πρακτική διάφορα των SOCKS διακομιστών από αυτούς του HTTP είναι ότι πέρα από την πλοήγηση στο ιστό βρίσκουν εφαρμογή και σε άλλες περιπτώσεις όπως μεταφορά αρχείων, παιχνίδια, άμεσα μηνύματα κ.α., έχουν δηλαδή τη δυνατότητα να διαμεσολαβήσουν και σε αλλά προγράμματα εκτός από αυτά της πλοήγησης στο Web , όπως προγράμματα ηλεκτρονικού ταχυδρομείου, και instant messaging [33].

Το πρόγραμμα πλοήγησης και ο υπολογιστής γενικότερα, είναι ρυθμισμένα να εξυπηρετούν τα αιτήματα για περιεχόμενο μέσω συγκεκριμένων IP διευθύνσεων και θυρών επικοινωνίας. Στην περίπτωση αυτή πραγματοποιείται χειροκίνητη αλλαγή στις ρυθμίσεις αυτές για την επιλογή συγκεκριμένου διακομιστή (open proxy), για την εξυπηρέτηση των αιτημάτων.

Όταν ο υπολογιστής ρυθμιστεί να χρησιμοποιεί έναν ανοικτό διαμεσολαβητή, απλά στέλνει όλα τα αιτήματα του για Web και όχι μόνο, περιεχόμενο στο διακομιστή αντί να αναλύει τη URL διεύθυνση σε IP προκείμενου να επικοινωνήσει άμεσα με τον τελικό ιστότοπο. Ο διαμεσολαβητής τότε πραγματοποιεί την DNS ανάλυση του ονόματος, συνδέεται στον τελικό ιστότοπο και στέλνει τα περιεχόμενα του στο πρόγραμμα πλοήγησης [76]. Δεν είναι απαραίτητη η χρήση εξειδικευμένων εφαρμογών στην πλευρά του τελικού χρήστη και αυτός μπορεί να χρησιμοποιήσει την διεπαφή των ήδη εγκατεστημένων προγραμμάτων στον υπολογιστή του.

Αυτή η διαμεσολάβηση έχει γενικά ανοικτό χαρακτήρα, δεν απαιτεί πληρωμή ή εγγραφή και οι ιδιοκτήτες των διακομιστών είναι ανώνυμοι. Ο χρήστης πρέπει να αναζητήσει τέτοιου είδους διακομιστές μέσα από μια πολύ μεγάλη λίστα η οποία συνεχώς ανανεώνεται, μια που πολλοί κλείνουν ενώ κάποιοι άλλοι νέοι εμφανίζονται [81].

Client Based Proxies

Είναι εφαρμογές που καλείται να λειτουργήσει ο χρήστης τοπικά στον υπολογιστή του. Πολλά από αυτά τα προγράμματα δεν απαιτούν εγκατάσταση, μπορούν δηλαδή να είναι «φορητά» και

να εφαρμοστούν με τη βοήθεια ενός φορητού μέσου αποθήκευσης (usb drive) από χρήστες με περιορισμένα δικαιώματα.

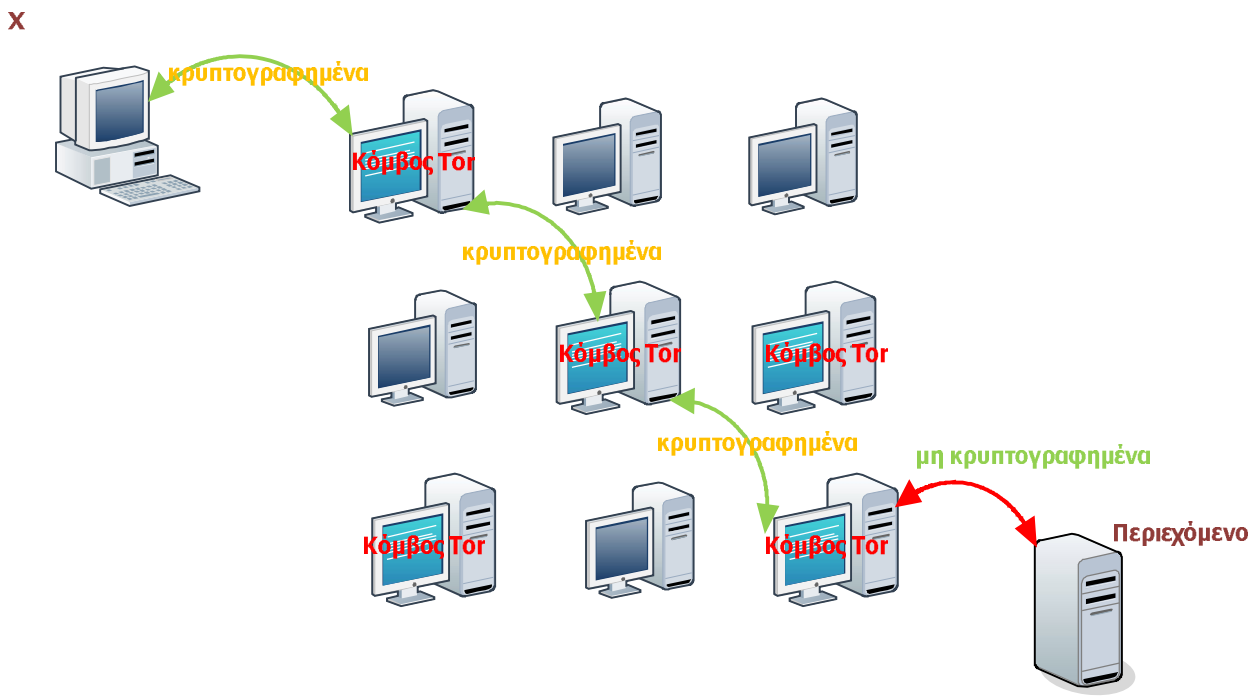
Οι εφαρμογές αυτές δημιουργούν ένα τοπικό διακομιστή μεσολάβησης χρησιμοποιώντας μια μη προκαθορισμένη θύρα επικοινωνίας. Στη συνέχεια ρυθμίζουν το πρόγραμμα πλοήγησης να χρησιμοποιεί τον τοπικό διακομιστή, ώστε όλες οι αιτήσεις του για περιεχόμενο να διέρχονται μέσα από αυτόν, ακολουθώντας συγκεκριμένο, συνήθως κρυπτογραφημένο πρωτόκολλο. Το σύστημα φιλτραρίσματος δεν μπορεί να ανιχνεύσει την κίνηση μεταξύ του προγράμματος πλοήγησης και του τοπικού διακομιστή, παρά μόνο τα αιτήματα του χρήστη που είναι διαμορφωμένα με βάση το πρωτόκολλο [76].

Tor

Μια ιδιαίτερα ενδιαφέρουσα περίπτωση διακομιστή βασισμένου στον πελάτη είναι το Tor. Το Tor (συντομογραφία του The onion router) είναι ένα σύστημα που δίνει στους χρήστες του τη δυνατότητα ανωνυμίας στο διαδίκτυο. Το λογισμικό πελάτη Tor δρομολογεί τη διαδικτυακή κίνηση μέσω ενός παγκόσμιου εθελοντικού δικτύου διακομιστών με σκοπό να αποκρύψει την τοποθεσία ενός χρήστη ή τη χρήση της κίνησης, από οποιονδήποτε διεξάγει διαδικτυακή παρακολούθηση ή ανάλυση της διαδικτυακής κίνησης.

Η χρήση Tor κάνει δύσκολη την ανίχνευση διαδικτυακής δραστηριότητας του χρήστη, συμπεριλαμβανομένου επισκέψεων σε κάποια ιστοσελίδα, διαδικτυακές αναρτήσεις, προγράμματα άμεσων μηνυμάτων και άλλων μέσων διαδικτυακής επικοινωνίας κι έχει σκοπό να προστατεύσει την ατομική ελευθερία, την ιδιωτικότητα και τη δυνατότητα του χρήστη να διεξάγει εμπιστευτικές εργασίες χωρίς να καταγράφονται οι διαδικτυακές δραστηριότητές του.

Το «Onion routing» αναφέρεται στη στρωματοποιημένη φύση της υπηρεσίας κρυπτογράφησης. Τα αρχικά δεδομένα κρυπτογραφούνται και επανακρυπτογραφούνται πολλές φορές, έπειτα στέλνονται μέσω διαδοχικών κόμβων του Tor, ο καθένας από τους οποίους αποκρυπτογραφεί ένα «στρώμα» κρυπτογράφησης προτού μεταφέρει τα δεδομένα στον επόμενο κόμβο και τελικά στον προορισμό τους. Αυτό μειώνει την πιθανότητα τα αρχικά δεδομένα να αποκρυπτογραφηθούν ή να γίνουν κατανοητά κατά τη μεταφορά τους. Το Tor είναι ελεύθερο λογισμικό πελάτη και η χρήση του είναι δωρεάν [19].



Σχήμα 3.13: Λειτουργία Tor

3.8.7 VPN

Το VPN (Virtual Private Network – Εικονικό Ιδιωτικό Δίκτυο) χρησιμοποιείται για να κρυπτογραφήσει και να καθοδηγήσει μέσα από «σήραγγα» διακομιστών, όλη την κίνηση στο Διαδίκτυο. Η τεχνολογία VPN παραδοσιακά χρησιμοποιήθηκε για να επιτρέψει την πρόσβαση σε εσωτερικά δίκτυα οργανισμών και επιχειρήσεων, από εξωτερικές δημόσιες θέσεις διασύνδεσης, με ασφαλή τρόπο, αλλά τα τελευταία χρόνια παρουσιάζουν ιδιαίτερη ανάπτυξη οι σε προσωπικό επίπεδο VPN υπηρεσίες. Ανάμεσα στις άλλες χρήσεις, αυτές οι προσωπικές VPN υπηρεσίες, βρίσκουν εφαρμογή στα εργαλεία παράκαμψης του ελέγχου περιεχομένου, με την προϋπόθεση φυσικά ότι οι διακομιστές που χρησιμοποιούνται βρίσκονται εκτός της λογοκρινόμενης περιοχής [81]. Είναι σημαντικό να τονιστεί ότι τα δεδομένα είναι κρυπτογραφημένα μόνο όσο κινούνται σε αυτή την εικονική σήραγγα [33].

Οι υπηρεσίες αυτές μπορεί να απαιτούν ή όχι, εγκατάσταση λογισμικού από την πλευρά του πελάτη, (πολλές στηρίζονται στις VPN δυνατότητες των λειτουργικών συστημάτων) και επιτρέπουν στο χρήστη να έχει πρόσβαση στο Web μέσω του οικείου περιβάλλοντος των προγραμμάτων του υπολογιστή του. Επειδή οι VPN υπηρεσίες μεταφέρουν όλων των ειδών την κίνηση, μπορούν να χρησιμοποιηθούν για ηλεκτρονικό ταχυδρομείο, chat και πολλές άλλες υπηρεσίες του Διαδικτύου επιπρόσθετα της πλοήγησης στον Ιστό [81].

Τα περισσότερα εργαλεία που κάνουν χρήση της τεχνολογίας αυτής, λειτουργούν με χρηματική συνδρομή, εκτός από κάποια που συλλέγουν έσοδα μέσω διαφημίσεων. Οι υπηρεσίες VPN μπορούν να εξουδετερωθούν είτε αποκλείοντας τις IP διευθύνσεις που χρησιμοποιούν, είτε αποκλείοντας τα πρωτόκολλά που χρησιμοποιούν για να αποκαταστήσουν τις συνδέσεις τους. Ωστόσο, δεδομένου ότι τα VPN χρησιμοποιούνται συχνά από τους επαγγελματίες χρήστες για να έχουν πρόσβαση στο εταιρικό intranet, πολλές κυβερνήσεις είναι απρόθυμες να αποκλείσουν την λειτουργία τους [81].

3.8.8 Tunneling

Η διαδικασία με την οποία εφαρμόζονται τα VPN λέγεται tunneling. Το tunneling αναφέρεται στη μέθοδο της ενθυλάκωσης ενός πρωτοκόλλου ή ενός πλήθους πρωτοκόλλων μέσα σε ένα άλλο (συχνά αναφέρεται ως πρωτόκολλο μεταφοράς). Ανάλογα με τη φύση του πρωτοκόλλου μεταφοράς η ενθυλάκωση μπορεί να είναι ή να μην είναι διαφανής για τον τελικό χρήστη και συνεπώς να απαιτούνται αλλαγές στο σύστημα ή στις ρυθμίσεις της εφαρμογής. Επί πλέον αν το πρωτόκολλο μεταφοράς χρησιμοποιεί κρυπτογράφηση, τότε η σήραγγα της επικοινωνίας είναι επίσης εμπιστευτική μέχρι το τελικό σημείο της. Ωστόσο, πολλά πρωτόκολλα ενθυλάκωσης δεν υποστηρίζουν κρυπτογράφηση και ως εκ τούτου, μεταφέρουν τα δεδομένα στη σήραγγα σε ελεύθερο κείμενο, εκτός εάν το ίδιο το πρωτόκολλο είναι κρυπτογραφημένο σε επίπεδο εφαρμογής [93].

Συνήθως το tunneling χρησιμοποιείται σε περιπτώσεις κατά τις οποίες ένας πεπειραμένος σε θέματα τεχνολογίας χρήστης αντιμετωπίζει σοβαρούς περιορισμούς για το τύπο ή τον αριθμό των πρωτοκόλλων που μπορεί να χρησιμοποιήσει για να συνδεθεί με ένα συγκεκριμένο απομακρυσμένο υπολογιστή ή το Διαδίκτυο. Αν για παράδειγμα σε ένα δίκτυο φιλτράρονται οι TCP και UDP συνδέσεις είναι δυνατό να χρησιμοποιηθεί το ICMP πρωτόκολλο σαν μέσο μεταφοράς στο τούνελ. Στη διαδικασία αυτή το απομακρυσμένο σύστημα δεν μπορεί να είναι αντικείμενο φιλτραρίσματος, προκειμένου να μπορεί να εγκατασταθούν πρόσθετα τμήματα δικτυακού λογισμικού [93].

ICMP Tunneling

Το πρωτόκολλο ICMP (Internet Control Message Protocol) χρησιμοποιείται για να παρέχει πληροφορίες σχετικά με αποτυχίες δρομολόγησης, σφάλματα λήψης, καθυστερήσεις και άλλες

συνθήκες του δικτύου. Για το λόγο αυτό είναι σπανιότερα στόχος λογοκρισίας και συνεπώς ιδιαίτερα κατάλληλο για μηχανισμούς που έχουν σκοπό να παρακάμψουν τον έλεγχο σε πιο ελκυστικά για αυτόν πρωτόκολλα, όπως το TCP και το UDP.

Για την εφαρμογή του είναι απαραίτητο ο απομακρυσμένος φιλοξενητής να μην υπόκεινται σε έλεγχο περιεχομένου. Επιπρόσθετα χρησιμοποιείται ειδικό λογισμικό όπως το puntel (το οποίο ενθυλακώνει το πρωτόκολλο TCP) ή το ICMPTX (που ενθυλακώνει όλη την IP σύνδεση) τα οποία είναι δωρεάν διαθέσιμα [93].

SSH Tunneling

Το SSH (Secure Shell) είναι ένα πρωτόκολλο επιπέδου εφαρμογής, βασισμένο σε ένα δημόσιο κλειδί κρυπτογράφησης. Συνοπτικά παρέχει μια ισχυρή και εύκολη προσέγγιση για την προστασία των επικοινωνιών σε ένα δίκτυο υπολογιστών. Μέσω τεχνολογιών ταυτοποίησης και κρυπτογράφησης, το SSH υποστηρίζει ασφαλείς απομακρυσμένες συνδέσεις, ασφαλή απομακρυσμένη εκτέλεση εντολών, ασφαλή μεταφορά αρχείων, έλεγχο πρόσβασης, προώθηση TCP/IP θυρών, καθώς και άλλα σημαντικά χαρακτηριστικά. Αυτά τα προηγμένα χαρακτηριστικά του SSH, όπως η προώθηση θυρών, επιτρέπουν την ασφαλή και αξιόπιστη παράκαμψη οποιουδήποτε φιλτραρίσματος. Η προώθηση θύρας (port forwarding) αναφέρεται σε μια διαφανή τεχνική κατά την οποία μη ασφαλή πρωτόκολλα που λειτουργούν σε TCP μπορούν να γίνουν ασφαλή με τη διαβίβαση των συνδέσεων μέσω SSH.

Ωστόσο, όπως σχεδόν όλοι οι μηχανισμοί tunneling, το SSH tunneling απαιτεί από το χρήστη να έχει πρόσβαση στο απομακρυσμένο υπολογιστικό σύστημα το οποίο θα πρέπει να είναι ανεπηρέαστο από οποιοδήποτε είδος φιλτραρίσματος για να μπορεί να χρησιμοποιηθεί ως το τελικό σημείο της σήραγγας. Στη συνέχεια, προκειμένου να παρακαμφθεί η λογοκρισία, κάποιος μπορεί να δημιουργήσει ένας κρυπτογραφημένο ασφαλές τούνελ σε ένα απομακρυσμένο σύστημα μέσω SSH και να προωθήσει μια τοπική θύρα σε ένα HTTP διακομιστή μεσολάβησης που βρίσκεται στον ίδιο ή και σε απομακρυσμένο φιλοξενητή.

Επιπλέον αλλάζοντας τις ρυθμίσεις στο πρόγραμμα πλοήγησης ώστε να στέλνει όλα τα δεδομένα μέσω του SSH τούνελ του τοπικού συστήματος, κάθε αίτημα θα μεταφέρεται κρυπτογραφημένα στον διακομιστή και η απάντηση θα φτάνει ανεπηρέαστη πίσω. Έτσι αποφεύγεται το DNS tampering μια που τώρα η DNS ανάλυση γίνεται μόνο στο απομακρυσμένο σύστημα [93].

Αυτοί που λογοκρίνουν αποφεύγουν να αποκλείσουν το SSH τελείως γιατί χρησιμοποιείται και για άλλους σκοπούς, όπως για την διαχείριση συστημάτων ασφαλείας.

Η χρήση του SSH απαιτεί ένα λογαριασμό σε έναν αξιόπιστο εξυπηρετητή, συνήθως Linux ή Unix με απεριόριστη πρόσβαση στο διαδίκτυο. Μερικές εταιρίες πωλούν τους λογαριασμούς πρόσβασης στους εξυπηρετητές τους [33].

SSL Tunneling

Το πρωτόκολλο SSL (Secure Socket Layer) αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα ηλεκτρονικών υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του Διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP και το telnet [34].

Κατά συνέπεια το SSL μπορεί να χρησιμοποιηθεί για την δημιουργία ενός τούνελ για άλλα πρωτόκολλα, ακόμη και για την αποκατάσταση ενός VPN. Και στην περίπτωση αυτή για να χρησιμοποιηθεί το πρωτόκολλο για παράκαμψη του αποκλεισμού πρόσβασης σε περιεχόμενο, απαραίτητος είναι ο έλεγχος του απομακρυσμένου και ελεύθερου από λογοκρισία φιλοξενητή. Επιπλέον είναι απαραίτητο να εγκατασταθεί λογισμικό όπως το OpenVPN και στις δύο πλευρές μεταξύ των οποίων αποκαθίσταται η σύνδεση. Το λογισμικό αυτό είναι δωρεάν και παρέχει ένα εύρος δυνατοτήτων, μεταξύ των οποίων η εξ' αποστάσεως πρόσβαση, δημιουργία VPN, Wi-Fi ασφάλεια, λύσεις εξ' αποστάσεως πρόσβασης σε επίπεδο επιχείρησης με μεγάλη μεταβολή στο διακινούμενο φορτίο και υψηλής ακρίβειας έλεγχο πρόσβασης [93].

Άλλοι Μέθοδοι Tunneling

Σχεδόν κάθε πρωτόκολλο δικτύου ή εφαρμογής μπορεί να χρησιμοποιηθεί προκειμένου να μεταφέρει ένα άλλο δημιουργώντας μια σήραγγα. Ωστόσο, στην πραγματικότητα η επιλογή του πρωτοκόλλου που θα χρησιμοποιηθεί, εξαρτάται σε μεγάλο βαθμό από συνθήκες που είναι

συχνά πέρα από τον έλεγχο του χρήστη (π.χ. εγκατάσταση δικτύου ή firewall). Έτσι, προκειμένου να παρακαμφθεί με επιτυχία ένας μηχανισμός φιλτραρίσματος όπως ένα firewall ή μια προσπάθεια λογοκρισίας σε εθνικό επίπεδο, πρέπει κανείς να επιλέξει ένα κατάλληλο και μερικές φορές ακόμη και εξεζητημένο τρόπο για να δημιουργήσει τούνελ μεταξύ των δύο πλευρών του δικτύου.

Εκτός από τα πρωτόκολλα που προαναφέρθηκαν, είναι δυνατό να εφαρμοστεί DNS tunneling με εργαλεία όπως το NSTX ή το OzymanDNS που παρέχουν μονόδρομη διέλευση ολόκληρης της IP κίνησης μέσω ενός δικτύου στο οποίο επιτρέπονται μόνο DNS ερωτήματα και απαντήσεις (π.χ. δημόσια hotspots Wi-Fi). Επιπλέον, αν μια σύνδεση στο Διαδίκτυο περιορίζεται από ένας διακομιστή μεσολάβησης, κάποιος μπορεί να χρησιμοποιήσει λογισμικό, όπως το httptunnel για να στείλει αιτήσεις HTTP, να παρακάμψει το φιλτράρισμα και να συνδεθεί σε έναν υπολογιστή εκτός του τοπικού δικτύου [93].

3.9 Συμπεράσματα

Οι τεχνολογίες ελέγχου προσπέλασης με βάση το περιεχόμενο επιτελούν δύο βασικές λειτουργίες, την αναγνώριση του ακατάλληλου περιεχομένου και στη συνέχεια τον αποκλεισμό του. Η εφαρμογή τους μπορεί να γίνει σε διαφορετικά επίπεδα της τοπολογίας των δικτύων, από το κορμό ενός εθνικού δικτύου ως τον προσωπικό υπολογιστή ενός ανήλικου, ανάλογα την κλίμακα του αποκλεισμού που είναι επιθυμητή αλλά και τις τεχνικές δυνατότητες που είναι διαθέσιμες.

Η αναγνώριση του περιεχομένου, η διαδικασία δηλαδή κατά την οποία «αποφασίζεται» αν μια πληροφορία είναι επιθυμητό να μεταδοθεί ή όχι, έχει σχέση με το είδος των κριτηρίων που θα χρησιμοποιηθούν προκειμένου να γίνει αυτή η κατάταξη. Η πιο συμβατική μέθοδος, που μπορεί να λειτουργήσει σε διαφορετικά επίπεδα της διαδικασίας διασύνδεσης στο δίκτυο, είναι η χρήση «μαύρων» και «άσπρων» λιστών με ακατάλληλο ή όχι υλικό. Είναι μια μέθοδος που εφαρμόζεται εύκολα στις υπάρχουσες υποδομές δικτύων, χωρίς ιδιαίτερες επιπτώσεις στην ροή της πληροφορίας, παρουσιάζει όμως σημαντικά μειονεκτήματα λόγω της μειωμένης ευελιξίας της. Κυριότερη αδυναμία της είναι το υπερβολικό ή ελλιπές φιλτράρισμα, δηλαδή η κατάταξη σαν ακατάλληλη πληροφορία η οποία είναι κατάλληλη και το αντίθετο.

Η εξέλιξη του υλικού και του λογισμικού των υποδομών που διατίθενται επέτρεψε τα τελευταία χρόνια να μετατοπιστεί το κέντρο βάρους όλης τη διαδικασίας στο πεδίο της εφαρμογής. Η τεχνητή νοημοσύνη η ανάπτυξη ταχύτερων υπολογιστικών συστημάτων, η επεξεργασία εικόνας και βίντεο επιτρέπουν την εφαρμογή της σε βάθος επιθεώρησης της πληροφορίας και την δημιουργία «έξυπνων», δυναμικών και ευέλικτων τρόπων αναγνώρισης του περιεχομένου. Σε κάθε περίπτωση πάντως, σημαντικός είναι και ο ρόλος του τελικού χρήστη, μια που η επιλογή του αυτοελέγχου μπορεί να αυξήσει σημαντικά την αποτελεσματικότητα των μηχανισμών, δυναμικών και μη.

Ο αποκλεισμός, το μπλοκάρισμα ουσιαστικά της πληροφορίας, μπορεί να γίνει με διαφορετικές τεχνικές που εξαρτώνται από την πρόσβασή που έχει στο δίκτυο αυτός που ασκεί τον έλεγχο, αλλά και την κλίμακα εφαρμογής που είναι επιθυμητή. Η διαφάνεια των τεχνικών αυτών, είναι διαφορετική μια που μπορούν να φτάσουν μέχρι το επίπεδο κοινωνικών επιλογών.

Στην επιλογή μιας μεθόδου ελέγχου του περιεχομένου πρέπει να συνεκτιμώνται διάφοροι παράγοντες που έχουν σχέση με την αποτελεσματικότητα της. Οι επιπτώσεις στο δίκτυο και την ταχύτητα μεταφοράς δεδομένων, ο υπερβολικός ή ελλιπείς έλεγχος, το οικονομικό κόστος, η ανιχνευσιμότητα και η αξιοπιστία είναι παράμετροι που συνεκτιμώνται στην επιλογή αλλά και την αξιολόγηση τέτοιων συστημάτων.

Σε κάθε περίπτωση πάντως καμία τεχνική ή μέθοδος αποκλεισμού δεν μπορεί να είναι πλήρως αποτελεσματική, μια που παράλληλα με την εξέλιξη τους εξελίσσονται και οι τρόποι παράκαμψης τους, Αυτοί μπορεί να είναι αρκετά απλοϊκοί, από την αλλαγή βασικών στοιχείων επικοινωνίας προκειμένου να «ξεγελάσουν» τον έλεγχο, μέχρι πιο εξεζητημένοι. Η λογική που ακλουθείτε συνηθέστερα στις περιπτώσεις αυτές είναι η παράκαμψη μέσω διαμεσολάβησης. Όταν δηλαδή ένα τρίτο μέρος, διαδρομή υπολογιστής ή πρωτόκολλο, αναλαβαίνει να μεταφέρει την απαγορευμένη πληροφορία.

Κεφάλαιο 4

Έλεγχος Προσπέλασης με Βάση το Περιεχόμενο, Πολιτική, Νομική, Κοινωνική Διάσταση

Οι κυρίαρχες φιλελεύθερες δημοκρατίες, όπως αυτές της Ευρωπαϊκής Ένωσης, των Η.Π.Α., του Καναδά και της Αυστραλίας, προωθούν την ελευθερία στο Διαδίκτυο παράλληλα με τον έλεγχο σε αυτό, ένας έλεγχος που σχετίζεται τόσο με τη λογοκρισία του περιεχομένου που άπτεται δικαιωμάτων ελευθερίας έκφρασης, όσο και με την επιτήρηση του περιεχομένου που αφορά το δικαίωμα στην προστασία της ιδιωτικής ζωής. Ο διττός αυτός χαρακτήρας καθιστά τα σύγχρονα κοινωνικά δίκτυα όχι απλά μέσα ελεύθερης έκφρασης αλλά και χώρους ελέγχου, αποκλεισμού και δημοσιοποίησης προσωπικών πληροφοριών.

Επιπρόσθετα στον έλεγχο του Διαδικτύου μπορούν να προσδιοριστούν δύο διαστάσεις η τεχνολογική, η οποία και αναλύθηκε εκτενώς στο προηγούμενο κεφάλαιο, αλλά και η κοινωνικοπολιτική. Κάποιες φορές είναι δυσδιάκριτα τα όρια μεταξύ των δύο αυτών επιλογών. Για παράδειγμα η επιβολή ελέγχου σε περιεχόμενο τους πριν δημοσιευτεί σε πλατφόρμες ιστολογίων, όπως το WorldPress και το LiveJournal παρότι μπορεί να θεωρηθεί σαν κοινωνικοπολιτική μέθοδος, απαιτεί τη χρήση τεχνολογικών εφαρμογών [73].

Αν και οι περισσότερες αναφορές σχετίζονται με τις τεχνολογικές μεθόδους ελέγχου του περιεχομένου, η αποτελεσματικότητα τους σε σχέση με τις κοινωνικοπολιτικές είναι συζητήσιμη. Η αποκεντρωμένη δομή του Διαδικτύου καθιστά πολύ δύσκολη την ύπαρξη ενός φίλτρου απόλυτα αποτελεσματικού, εκτός ίσως από τις περιπτώσεις που αφορούν κλειστά εθνικά δίκτυα με συγκεκριμένους κεντρικά ελεγχόμενους εξυπηρετητές (Intranet). Σε κάθε άλλη περίπτωση έχει αποδειχθεί ότι με την διαμεσολάβηση υπολογιστών τρίτων μερών είναι δυνατό να παρακαμφθεί τεχνικά ο έλεγχος και εκεί συνήθως αναλαμβάνουν ρόλο οι κοινωνικοπολιτικές ενέργειες. Πολλές φορές είναι δυσκολότερο για μια κυβερνητική αρχή να λογοκρίνει το περιεχόμενο ενός ιστολογίου από το να φυλακίσει τον συντάκτη του.

Φαίνεται ίσως ότι η κυρίαρχη παράμετρος στην προσπάθεια για αποφυγή του ελέγχου είναι τεχνολογική. Κάποιοι οικονομικοί πόροι και μερικές έξυπνες ιδέες μπορούν θεωρητικά να δώσουν αποτελεσματικές λύσεις σε θέματα λογοκρισίας [70]. Κλασικό παράδειγμα ο Shiyu Zhou, ιδρυτής της ομάδας Falun Gong που σχεδιάζει και διανέμει λογισμικό που βοηθάει στην πρόσβαση σε απαγορευμένους από την κινεζική κυβέρνηση ιστότοπους, ο οποίος αναφέρει ότι η διαμάχη για την πρόσβαση σε περιεχόμενο στο διαδίκτυο καταλήγει να είναι διαμάχη πόρων. Ακόμη όμως και σε αυτές τις περιπτώσεις η πολιτική διάσταση είναι αναπόφευκτη. Το κοινωνικοπολιτικό περιβάλλον πάντοτε θα επιδρά και στη στόχευση αλλά και την αποτελεσματικότητα των τεχνολογικών μεθόδων παράκαμψης του ελέγχου. Ένα εργαλείο που βοηθά αντιφρονούντες σε αυταρχικά κράτη να έχουν πρόσβαση σε πληροφορία που είναι αποκλεισμένη, είναι δυνατό να διευκολύνει τρομοκράτες ή παιδόφιλους να παρακάμψουν ελεγκτικούς μηχανισμούς που λειτουργούν δημοκρατικές κυβερνήσεις προκειμένου να προστατέψουν τους πολίτες τους.

Πολλές είναι οι περιπτώσεις που καταδεικνύουν τη πολιτική διάσταση των μηχανισμών αυτών. Ένα από τα βασικά πρόσωπα στη λειτουργία του δικτύου Tor, το οποίο κατά κάποιο τρόπο χρηματοδοτείται από την κυβέρνηση των Η.Π.Α., εμπλέκεται με την υπόθεση των WikiLeaks [28]. Δεν είναι σίγουρη άλλωστε η αντίδραση των διαφόρων κυβερνήσεων σε μια περίπτωση

βελτίωσης του δικτύου Tor σε θέματα ταχύτητας και λειτουργικότητας που θα το καθιστούσαν πιο φιλικό στον μέσο χρήστη [82]. Ενώ αντίθετα είναι γνωστή η κυβερνητική πίεση που ασκείται σε εταιρίες παροχής υπηρεσιών, όπως Skype ή Google προκειμένου να επιτρέψουν μέσω εσκεμμένων «κερκόπορτων» τον έλεγχο περιεχομένου από νομικές ή ακόμη και μυστικές υπηρεσίες.

Μια επιλογή που συνήθως προτείνεται είναι η εφαρμογή εξειδικευμένων λύσεων για περιπτώσεις χωρών με αποδεδειγμένα ανελεύθερες πολιτικές σε θέματα ελευθερίας λόγου. Τέτοιο παράδειγμα είναι το εργαλείο παράκαμψης ελέγχου Haystack που δημιουργήθηκε από αμερικανούς ακτιβιστές προκειμένου να βοηθήσουν Ιρανούς αντιφρονούντες. Παρόλα αυτά, αυτή η εξειδικευμένη εφαρμογή και η αποφυγή γενίκευσης της χρήσης των εργαλείων είναι δύσκολη [73].

4.1 Η Κοινωνικοπολιτική Διάσταση

Το φιλτράρισμα του Διαδικτύου είναι μια επιλογή πού έχουν οι κυβερνήσεις προκειμένου να ασκήσουν έλεγχο, η οποία πολλές φορές είναι ανιχνεύσιμη. Εξαιτίας αυτής της σχετικής διαφάνειας και της επιθυμίας των περισσότερων κρατών να μην συνδεθούν με διαδικασίες λογοκρισίας, πολλές κυβερνήσεις επιλέγουν εναλλακτικούς και πιο αποτελεσματικούς τρόπους ελέγχου.

4.1.1 Συντονισμένες Επιθέσεις Άρνησης Παροχής Υπηρεσιών (DDos Attacks)

Αν και δεν μπορούν να υπάρχουν συγκεκριμένα στατιστικά στοιχεία, οι επιθέσεις τύπου DDoS με πολιτικά κίνητρα φαίνεται να παρουσιάζουν αύξηση [75]. Σε αυτές τις επιθέσεις οι φιλοξενητές του προς αποκλεισμό περιεχομένου κατακλύζονται με εξοντωτικού όγκου τεχνητή κίνηση με αποτέλεσμα την κατάρρευση τους.

Οι συνέπειες αυτών των επιθέσεων είναι όχι μόνο ο αποκλεισμός του περιεχομένου, αλλά και η συνολική διακοπή παροχής υπηρεσιών από τον φορέα που το φιλοξένει, με αποτέλεσμα πολλές φορές την διαταραχή των σχέσεων του με τον εκδότη του περιεχομένου. Επιπλέον με τον τρόπο αυτό καθίσταται το περιεχόμενο μη διαθέσιμο όχι μόνο στην περιοχή όπου είναι επιθυμητό να εφαρμοστεί το σύστημα φιλτραρίσματος, αλλά παντού.

Οι επιθέσεις αυτού του τύπου είναι πολλές φορές δύσκολο να ταυτοποιηθούν μια που κατάρρευση εξυπηρετητών μπορεί να προκληθεί από μια σειρά από άλλα συμβάντα, όπως διακοπή ρεύματος, παροδικές πραγματικές αυξήσεις της ροής της κίνησης κ.α. [73]. Παρόλα αυτά η δυναμική τους είναι εμφανής και από την αγορά που έχει δημιουργηθεί γύρω τους, όπου με οικονομικά ανταλλάγματα μπορεί κάποιος να αγοράσει τέτοιου είδους επιθέσεις [36].

4.1.2 Σκόπιμη Διάβρωση του Κοινωνικού Κεφαλαίου

Μια ακόμη εναλλακτική κοινωνικοπολιτική επιλογή στην προσπάθεια για τον έλεγχο του περιεχομένου είναι όχι απλά ο αποκλεισμός του αλλά η διάβρωση του. Όταν οι τεχνολογίες της λογοκρισίας παρακάμπτονται τεχνικά, επιλογές όπως η στρατολόγηση προσωπικού προκειμένου να αλλοιώσει εσκεμμένα την ποιότητα της ελεγχόμενης πληροφορίας με «αθώες» τεχνικές, μπορούν να φανούν αποτελεσματικότερες. Είναι γνωστοί οι «fifty centers» της Κινεζικής κυβέρνησης που πληρώνονται για να υποβάλουν σχόλια σε πίνακες ανακοινώσεων και φόρουμ υποστηρίζοντας κυβερνητικές επιλογές. Αλλά και στη Ρωσία υπάρχουν φιλικά προσκείμενα προς το Κρεμλίνο κινήματα νέων που υπερασπίζονται στο Διαδίκτυο τις πολιτικές της παράταξης που κυβερνά [73].

4.1.3 Η «Εθνικοποίηση» του Κυβερνοχώρου

Μετά από την ομιλία της αμερικανίδας υπουργού εξωτερικών Χίλαρι Κλίντον για την ελευθερία στο Διαδίκτυο [15], πολλές κυβερνήσεις φαίνεται να έχουν συνειδητοποιήσει το ενδεχόμενο ότι οι Ηνωμένες Πολιτείες μπορεί να έχουν πρόθεση να εκμεταλλευτούν την υπάρχουσα δεσπόζουσα θέση τους στον κυβερνοχώρο, προκειμένου να προωθήσουν μια συγκεκριμένη πολιτική ατζέντα. Άσχετα με το αν οι ανησυχίες αυτές είναι δικαιολογημένες, είναι πλέον κοινή αντίληψη σε κυβερνήσεις πολλών χωρών, ότι οι πολίτες τους εξαρτώνται σε μεγάλο βαθμό από υπηρεσίες που παρέχονται από εταιρίες με έδρα στις Η.Π.Α.. Καταλήγοντας να μιλάμε για μια πληροφοριακή επικυριαρχία, οι σύγχρονες ψηφιακές οικονομίες δεν είναι δυνατό να λειτουργήσουν ανεξάρτητα από ξένους παρόχους υπηρεσιών.

Η παραπάνω κατάσταση, είχε ως συνέπεια οι κυβερνήσεις να ενισχύουν τις εγχώριες επιχειρήσεις Διαδικτύου σε βάρος των ξένων ανταγωνιστών. Η Τουρκία έκανε την πρώτη κίνηση σε αυτό το χώρο όταν το 2009 ξεκίνησε το έργο Anabena , το οποίο έχει ως στόχο τη δημιουργία μιας εθνικής μηχανής αναζήτησης που εξυπηρετεί καλύτερα τις «τουρκικές ευαισθησίες», με ένα

εθνικό σύστημα e-mail να έπεται. Το Ιράν ακολούθησε γρήγορα το παράδειγμά της, με την απαγόρευση του Gmail το Φεβρουάριο του 2010 και ανακοινώνοντας ένα εθνικό σύστημα ηλεκτρονικού ταχυδρομείου. Αργότερα την ίδια χρονιά, η Ρωσία προώθησε σχέδιά παρόμοια με της Τουρκίας, συμπεριλαμβανομένης της δημιουργίας μια εθνικής υπηρεσίας ηλεκτρονικού ταχυδρομείου και την δαπάνη 100 εκατομμυρίων δολαρίων για τη διερεύνηση της σκοπιμότητας μιας εθνικής μηχανής αναζήτησης.

Δεν θα ήταν έκπληξη να δούμε την Κινεζική, τη Ρωσική, άλλα και άλλες κυβερνήσεις να δηλώνουν ότι το Διαδίκτυο και η αναζήτηση πληροφοριών είναι μια στρατηγική βιομηχανία όπως η ενέργεια και οι μεταφορές και να αποκλειστούν ξένες εταιρείες από τον τομέα αυτό. Με δεδομένο ότι η εντύπωση ότι το Twitter και το Facebook μπορούν να διευκολύνουν πολιτικές επαναστάσεις συνεχώς κερδίζει έδαφος, τα κοινωνικά δίκτυα και τα μικρο-ιστολόγια μπορούν να θεωρηθούν στρατηγικά από εθνική άποψη [73].

4.1.4 Η ανάθεση του Ελέγχου του Διαδικτύου σε Τρίτους

Ένας τρόπος για να αποφύγουν οι διάφορες κυβερνήσεις την κριτική για το φιλτράρισμα του περιεχομένου στο Διαδίκτυο είναι να το αναθέσουν σε ενδιάμεσους. Αυτό γίνεται θεωρώντας τις εταιρίες που παρέχουν πρόσβαση στο Διαδίκτυο, τις πλατφόρμες κοινωνικών δικτύων ή ιστολογίων και τις μηχανές αναζήτησης, συνυπεύθυνες για το περιεχόμενο που δημοσιεύουν ή αναζητούν οι χρήστες τους. Αναγκάζοντας τις εταιρίες να ασκήσουν πολιτικές ελέγχου που έχουν επιλεγεί κεντρικά μετατοπίζεται το δύσκολο έργο σε αυτές παράλληλα με την όποια δυσαρέσκεια από τους καταναλωτές. Οι εταιρίες άλλωστε είναι πιο εύκολο να ελέγξουν το ακατέργαστο περιεχόμενο, μια που λειτουργούν πιο αποκεντρωμένα και γνωρίζουν καλύτερα το σύστημα επικοινωνιών από τους κρατικούς λογοκριτές.

Δεν είναι μόνο αυταρχικές κυβερνήσεις αυτές που εφαρμόζουν τέτοιες πολιτικές. Η Ιταλική κυβέρνηση θεωρεί υπόλογο το You Tube για τα βίντεο που δημοσιεύει, δίνοντας έτσι επιχειρήματα σε πιο αυταρχικές κυβερνήσεις προκειμένου να ασκήσουν πιο ακραίες πολιτικές ελέγχου.

Στη Ταϋλάνδη όπου υπάρχει απαγόρευση για οποιαδήποτε δημοσίευση με προσβλητικό περιεχόμενο για τη βασιλική οικογένεια της χώρας, όταν ή διάδοση των ιστολογίων έφτασε σε σημείο που ήταν αδύνατη η κεντρική παρακολούθηση τους, δημιουργήθηκε ένας ιστότοπος με το όνομα ProtectTheKing.net (προστατέψτε το βασιλιά), όπου ο καθένας θα μπορούσε να

υποβάλει συνδέσμους ιστότοπων προσβλητικών για την μοναρχία. Σύμφωνα με το BBC τις πρώτες εικοσιτέσσερις ώρες αποκλείστηκαν πέντε χιλιάδες υποβληθέντες σύνδεσμοι [37].

Ανάλογα στη Σαουδική Αραβία υπάρχει η δυνατότατα σους πολίτες να αναφέρουν κάποιο σύνδεσμο τον οποίο θεωρούν επιβλαβή στην Επιτροπή Τεχνολογίας Επικοινωνιών και Πληροφορικής. Ένας ρυθμός περίπου 1200 αναφορών την ημέρα επιτρέπει στην Σαουδαραβική κυβέρνηση να ασκεί αποτελεσματική λογοκρισία απασχολώντας μόνο 25 άτομα [12]. Στην ίδια χώρα μια καλά οργανωμένη ομάδα, αυτοαποκαλούμενη ως «Saudi Flager», από διακόσιους εθελοντές, με συντηρητικό πολιτισμικό υπόβαθρο, παρακολουθεί όλα τα σχετικά με την χώρα βίντεο στο You Tube και υποβάλει μαζικά κριτική και σχόλια στους διαχειριστές του ιστότοπου, αν εντοπίσει κάποιο που ασκεί κριτική στο Ισλάμ ή στην κατάσταση στη χώρα, θεωρώντας ότι επιτελεί το θρησκευτικό και πατριωτικό της καθήκον [07].

4.1.5 Καινοτομίες του Ιδιωτικού Τομέα

Μεγάλη ώθηση στον έλεγχο του περιεχομένου στο διαδίκτυο δίνεται από τις τεχνολογικές καινοτομίες στην ανάλυση δεδομένων, που μέσω του παγκόσμιου ιστού είναι πιο εύκολα προσβάσιμες. Δεν είναι μόνο η οργάνωση της κίνησης των μηνυμάτων κειμένου που είναι πλέον ευκολότερη, αλλά και η συστηματική παρακολούθηση και κατάταξη πλάνων βίντεο. Χαρακτηριστικό είναι ότι η Κινέζικη κυβέρνηση εκμεταλλευόμενη αυτές τις δυνατότητες εγκατέστησε μέσα στο 2010 πάνω από 47000 κάμερες παρακολούθησης στο κέντρο την πόλης Urumqi [92].

Αυτή η εξέλιξη στη επιτήρηση μέσω βίντεο θα ήταν αδύνατη χωρίς τη συνεισφορά Δυτικών επιστημόνων. Η Κινεζική κυβέρνηση χρηματοδότησε ερευνητές στο UCLA, προκειμένου να αναπτύξουν λογισμικό, το οποίο θα επιτρέπει τον αυτόματο σχολιασμό πλάνων βίντεο και την παραγωγή κειμένων τα οποία αργότερα θα μπορούν να διαβαστούν από ανθρώπους, οι οποίοι διαφορετικά θα έπρεπε να παρακολουθήσουν πολλές ώρες βίντεο προκειμένου να εξάγουν ανάλογη πληροφορία [85]. Η τεχνική αυτή επιτρέπει την σε μεγάλο όγκο επόπτευση διακινούμενων βίντεο στο διαδίκτυο και όχι μόνο.

Μια πολύ σημαντική τεχνολογία η οποία διευκολύνει την επόπτευση του διακινούμενου περιεχομένου είναι αυτή της αναγνώρισης προσώπων. Το 2009 η σχετικά μικρή εταιρία Face.com εισήγαγε μια εφαρμογή στο Facebook που επέτρεπε στους χρήστες να αναγνωρίσουν κάποιο φίλο τους σε μια φωτογραφία και στη συνέχεια σάρωνε ολόκληρο το κοινωνικό δίκτυο

αναζητώντας άλλες φωτογραφίες με αυτόν. Ανάλογες εφαρμογές εντάσσουν στις υπηρεσίες του και άλλες εταιρίες κολοσσοί, όπως η Google. Η κοινωνικοπολιτική διάσταση της χρήσης τέτοιων τεχνικών είναι προφανής, ιδιαίτερα στην περίπτωση αυταρχικών καθεστώτων. Η αναγνώριση προσώπων θα επέτρεπε την εύρεση και ταυτοποίηση αντιφρονούντων σε διαδηλώσεις ή άλλου είδους κοινωνικές ή διαδικτυακές εκδηλώσεις [73].

Μηχανές αναζήτησης που να μπορούν να βρουν φωτογραφίες που περιέχουν ένα συγκεκριμένο πρόσωπο οπουδήποτε στο διαδίκτυο δεν είναι κάτι πολύ μακρινό. Για παράδειγμα το SAPIR, ένα φιλόδοξο πρόγραμμα που χρηματοδοτείται από την Ευρωπαϊκή Ένωση και επιδιώκει να δημιουργήσει μια οπτικοακουστική μηχανή αναζήτησης η οποία θα αναλύει αυτόματα μια φωτογραφία, ένα βίντεο, ή έναν ήχο εξάγοντας ορισμένα χαρακτηριστικά και μοναδικά αναγνωριστικά για να τα χρησιμοποιήσει για να αναζητήσει και να εντοπίσει παρόμοιο περιεχόμενο στον Παγκόσμιο Ιστό. Με ανάλογο τρόπο μια εφαρμογή για κινητά τηλέφωνα, το Reognizr, που αναπτύχθηκε από δύο Σουηδικές εταιρίες επιτρέπει στο χρήστη του κινητού τηλεφώνου να φωτογραφίσει κάποιον και σχεδόν άμεσα να αναζητήσει για αυτόν πληροφορίες στο Διαδίκτυο [78].

4.1.6 Η Αυξητική Τάση της Έκθεσης Προσωπικών Δεδομένων στον Παγκόσμιο Ιστό

Μια πολύ σημαντική καινοτομία που εισήγαγε το Διαδίκτυο την τελευταία δεκαετία, είναι ότι επιτρέπεται η κοινή χρήση προσωπικών πληροφοριών. Όλο και περισσότερο η δραστηριότητα μας στο διαδίκτυο είναι προσαρμοσμένη. Η Google οργανώνει τα αποτελέσματα της αναζήτησης μας, εν μέρει με βάση το τι έχουμε ψάξει στο παρελθόν, ενώ η ταυτότητα μας στο Facebook μπορεί τώρα να «ταξιδεύει» μαζί μας κατά την πλοήγηση σε διάφορους ιστοχώρους. Υπάρχουν σημαντικά πλεονεκτήματα από την διαχείριση όλων αυτών των στοιχείων, όπως την αναγνώριση τοποθεσίας που βρίσκεται κάποιος ή την αγαπημένη του μουσική, υπάρχουν όμως και οι περιπτώσεις που όλη αυτή η δημοσιοποίηση μπορεί να γυρίσει εις βάρος του χρήστη.

Μια που η Amazon έχει τη δυνατότητα να συνιστά βιβλία με βάση τα βιβλία που έχει κάποιος ήδη αποκτήσει, δεν είναι δύσκολο να διαμορφωθεί ένα σύστημα λογοκρισίας που λαμβάνει αποφάσεις με βάση τις ιστοσελίδες που έχουμε επισκεφτεί και τα είδη των ανθρώπων οι οποίοι είναι φίλοι μας στους ιστοχώρους κοινωνικής δικτύωσης. Μιας τέτοιας μορφής έλεγχος περιεχομένου, θα επέτρεπε σε ένα χρήστη με «ασφαλές» για το κοινωνικό και πολιτικό

κατεστημένο, προφίλ να πλοηγείται οπουδήποτε το επιθυμεί, ενώ θα επέβαλε περιορισμούς σε κάποιον με πιο ανατρεπτικές ή έστω πιο ενεργές πολιτικά διαδικτυακές αναζητήσεις και δραστηριότητες. Με παρόμοιο τρόπο με τον οποίο η Google και το Facebook εφαρμόζουν τις στοχευόμενες διαφημίσεις ανάλογα με τις διαδικτυακές συνήθειες, μπορεί να εφαρμοστεί στοχευόμενος έλεγχος στην πρόσβαση σε περιεχόμενο.

Η βαρύτητα των τεχνικών λογοκρισίας κρίνεται σκόπιμο, να μετατοπιστεί από τις παραδοσιακές λίστες με αποκλεισμένο περιεχόμενο σε πιο δυναμικές και ευέλικτες κοινωνικά τεχνικές. Το ερώτημα που τίθεται πλέον δεν περιορίζεται στο αν πρέπει ή όχι κάτι να αποκλειστεί, αλλά και σε ποιον αφορά αυτή η λογοκρισία, όχι με την έννοια της κοινωνικής ομάδας στην οποία ανήκει, αλλά της μέχρι τώρα συμπεριφοράς του στον κυβερνοχώρο. Ένα σύστημα λογοκρισίας που καταφέρνει να παντρέψει την τεχνητή νοημοσύνη και την ανάλυση της βασικής κοινωνικής δικτύωσης όχι μόνο θα είναι εξαιρετικά ισχυρό, αλλά θα βοηθήσει στο να περιοριστεί η απειλή ότι η λογοκρισία θέτει εμπόδια επί του παρόντος στην οικονομική ανάπτυξη, ώστε να αρθεί ένας από τα σημαντικότερους λόγους που ωθεί σήμερα τις κυβερνήσεις να την αποφεύγουν.

4.2 Αποκλεισμός Περιεχομένου στο Διαδίκτυο και Νόμος

Η προσπάθεια αποκλεισμού συγκεκριμένου παράνομου υλικού δε συνεπάγεται και την οριστική αποτροπή της πρόσβασης σε αυτό. Οι αναπόφευκτες δυνατότητες καταστρατήγησης του ελέγχου, ο υπερβολικός ή ο ελλιπής αποκλεισμός (over–under blocking), η μη ορθή εφαρμογή των τεχνικών φιλτραρίσματος, οι νομικές ασυμβατότητες και κυρίως το πρόβλημα ότι ο αποκλεισμός αφήνει το απαγορευμένο υλικό διαθέσιμο στο δίκτυο, οδηγούν στο συμπέρασμα ότι το διακύβευμα δεν συνοψίζεται στην πρόταση «να αποκλειστεί ή να μην αποκλειστεί», αλλά στο να επιλεγεί συνολικά ένα πλαίσιο ελέγχου συμβατό με τις σύγχρονες δημοκρατικές κοινωνίες. Είναι πολύ σημαντικό λοιπόν να εξετάζονται πάντα οι νομικές, κοινωνικές και πολιτικές προκλήσεις που εγείρονται με την επιβολή του αποκλεισμού περιεχομένου.

Μια ολοκληρωμένη θεώρηση του αποκλεισμού του Διαδικτύου σε σχέση με τη νομική του διάσταση απαιτεί αναφορά στο νομικό και δικαιϊκό σύστημα το οποίο επηρεάζει. Οι σύγχρονες δημοκρατίες παίζουν σημαντικό ρόλο με τον ενεργό σεβασμό των θεμελιωδών ελευθεριών και των πολιτικών δικαιωμάτων. Τόσο η εθνική όσο και η διεθνείς κατάσταση πρέπει να ληφθούν υπόψη για να καθοριστεί ποια είναι τα θεμελιώδη δικαιώματα που αντίκεινται στον αποκλεισμό του Διαδικτύου και ποια τα θεμελιώδη δικαιώματα προστατεύονται από αυτόν. Ο ρόλος των

παρόχων υπηρεσιών Διαδικτύου είναι βασικός για τον έλεγχο του περιεχομένου σε αυτό, μια που είναι αναγκασμένοι να λειτουργήσουν σε ένα ανταγωνιστικό, μπερδεμένο και πολλές φορές αντιφατικό νομικό περιβάλλον [13].

Οι νόμοι που σχετίζονται με τον έλεγχο του περιεχομένου στο διαδίκτυο καλούνται να καθορίσουν ποιος έχει δικαίωμα να εφαρμόσει τον αποκλεισμό, ποιος έχει το δικαίωμα να καθορίσει το απαγορευμένο περιεχόμενο, με ποιες τεχνολογίες και αποσκοπώντας να προστατέψει ποιες κοινωνικές ομάδες, λαμβάνοντας πάντα υπόψη ότι μπορεί να επηρεάσει και άλλες. Κατά συνέπεια ο έλεγχος περιεχομένου που εφαρμόζεται για την προστασία συγκεκριμένων δικαιωμάτων ή ελευθεριών έχει άμεσες επιπτώσεις σε άλλα δικαιώματα και ελευθερίες. Οι ελευθερίες και τα δικαιώματα καθορίζονται από νόμους, η σύγκρουση με τους οποίους καθορίζει το μέτρο της νομιμότητας της εφαρμογής των ελεγκτικών μηχανισμών.

Ο αποκλεισμός του περιεχομένου στο διαδίκτυο είναι ένα μέτρο το οποίο συζητείται διεθνώς, για αυτό και η νομική θεώρηση του θα πρέπει να γίνεται σε ευρωπαϊκό και γενικότερα διεθνές επίπεδο. Σε αυτό το νομικό σύστημα διακρίνονται δύο περιοχές, αυτή των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών και αυτή που σχετίζεται με τις ηλεκτρονικές επικοινωνίες. Η πρόκληση που προκύπτει είναι να καθοριστεί σε πιο βαθμό μπορεί να περιοριστεί μια ελευθερία προκειμένου να προστατευθεί μια άλλη. Κάθε τέτοια ελευθερία πρέπει να θεωρηθεί και να αναλυθεί προκειμένου να αποφασιστεί κάτω από ποιες συνθήκες ο έλεγχος είναι νομικά αποδεκτός. Πολλά εθνικά, αλλά και διεθνή νομικά συστήματα ιεραρχούν πολύ υψηλά ανθρωπινά δικαιώματα και θεμελιώδης ελευθερίες, που σχετίζονται με τον έλεγχο περιεχομένου είτε επειδή προστατεύονται από αυτόν είτε επειδή καταστρατηγούνται.

Συχνά ανθρώπινα δικαιώματα που θεωρούνται θεμελιώδη για τις σύγχρονες δημοκρατίες, όπως το δικαίωμα στην ιδιωτική ζωή ή το δικαίωμα στην ελευθερία της έκφρασης, έρχονται σε σύγκρουση με τους μηχανισμούς ελέγχου. Υπάρχουν τρεις περιοχές όπου μπορούν να παρατηρηθούν οι σχέσεις ελέγχου πρόσβασης σε περιεχόμενο και δημοκρατίας [13]:

- Εκλογές – Η αρχή της καθολικής συμμετοχής στην δημόσια ζωή.

- Διαχωρισμός των εξουσιών – Οι συνταγματικά καθορισμένες δομές για τον διαχωρισμό των εξουσιών.

- Θεμελιώδη δικαιώματα – Η κρατική προθυμία και δέσμευση για σεβασμό των ελευθεριών.

Η διαφορά μεταξύ ανθρωπίνων δικαιωμάτων, θεμελιωδών ελευθεριών και πολιτικών ελευθεριών εξαρτάται από το σε ποιον απευθύνονται και από το νομικό κείμενο που καθορίζει το πλαίσιο τους. Ένα συγκεκριμένο δικαίωμα μπορεί να εμπίπτει και στις τρεις περιπτώσεις, όπως για παράδειγμα το δικαίωμα στην ιδιωτικότητα. Οι πολιτικές ελευθερίες αφορούν τους περιορισμούς της κρατικής εξουσίας προς του πολίτες.

Στις έννοιες των ανθρωπίνων δικαιωμάτων και των πολιτικών ελευθεριών, έχουν προστεθεί οι έννοιες των θεμελιωδών δικαιωμάτων και των θεμελιωδών ελευθεριών που συνοψίζονται στη προστασία από την εκτελεστική και νομοθετική εξουσία με βάση το σύνταγμα, αλλά και τις διεθνείς συνθήκες και με την εφαρμογή τους μέσω ανώτατων, συνταγματικών και διεθνών δικαστηρίων.

Τα πρώτα κείμενα που αφορούσαν ανθρώπινα δικαιώματα ήταν εθνικά, με τις πρώτες σχετικές διεθνείς συνθήκες να παρουσιάζονται μετά το δεύτερο παγκόσμιο πόλεμο διαμορφώνοντας ένα διεθνές νομικό σύστημα από το οποίο προκύπτουν οι αλληλεπιδράσεις με τον έλεγχο της ροής της πληροφορίας στο Διαδίκτυο. Τα βασικότερα από αυτά τα κείμενα που έχουν υιοθετηθεί από τον Ο.Η.Ε. και το Συμβούλιο της Ευρώπης είναι τα εξής [35] :

- Χάρτης των Ηνωμένων Εθνών

- Οικουμενική Διακήρυξη των Ηνωμένων Εθνών για Δικαιώματα του Ανθρώπου (UDHR), Άρθρο 19 «Ο καθένας έχει το δικαίωμα στην ελευθερία της γνώμης και της έκφρασης, συμπεριλαμβανομένου του δικαιώματος του καθενός να διατηρεί ανενόχλητος τις απόψεις του καθώς επίσης του δικαιώματος να αναζητά και να μεταδίδει πληροφορίες και ιδέες με οποιοδήποτε μέσο σε όλο το κόσμο.»

- Διεθνές Σύμφωνο των Ηνωμένων Εθνών για τα Ατομικά και Πολιτικά Δικαιώματα (ICCPR), Άρθρο 19, παρ 1,2 «Ο κάθε άνθρωπος έχει το δικαίωμα να έχει την άποψη του χωρίς καμία παρέμβαση. Ο κάθε άνθρωπος πρέπει να έχει το δικαίωμα ελευθερίας της έκφρασης. Το δικαίωμα αυτό περιλαμβάνει και το δικαίωμα του καθενός να αναζητά, να λαμβάνει και να μεταδίδει οποιεσδήποτε πληροφορίες και ιδέες ανεξαρτήτως συνόρων,

είτε προφορικά, είτε γραπτά ή εκτυπωμένα, σε μορφή τέχνης, ή με οποιοδήποτε άλλο μέσο της επιλογής του».

- Σύμβαση των Ηνωμένων Εθνών για τα Δικαιώματα του Παιδιού

- Σύμβαση των Ηνωμένων Εθνών για τα Δικαιώματα των Ατόμων με Αναπηρία

- Σύμβαση των Ηνωμένων Εθνών για την εξάλειψη όλων των μορφών φυλετικών διακρίσεων

- Ευρωπαϊκή Σύμβαση του Συμβουλίου της Ευρώπης για τα Δικαιώματα του Ανθρώπου (ECHR), Άρθρο 10, «Ο κάθε άνθρωπος έχει το δικαίωμα ελευθερίας της έκφρασης. Το δικαίωμα αυτό περιλαμβάνει την ελευθερία διατήρησης της άποψης του καθώς επίσης και του δικαιώματος να αναζητά και να μεταδίδει πληροφορίες και ιδέες χωρίς τη παρέμβαση οποιασδήποτε κρατικής αρχής σε όλο το κόσμο.»

- Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο.

Στην Ελλάδα, με την συνταγματική αναθεώρηση του 2001 ολοκληρώθηκε η θεσμοθέτηση του πληροφοριακού συντάγματος, ενός υποσυστήματος συνταγματικών κανόνων που τυγχάνουν σε εσωτερική και λογική αλληλουχία με σημείο σύνδεσης την αναφορά στο αγαθό της πληροφορίας. Το πληροφοριακό σύνταγμα αποτελεί κατ' ουσία το συνταγματικό δίκαιο της Κοινωνίας της Πληροφορίας (ΚτΠ), ενώ τελεί σε διαλεκτική σχέση με τις σχετικές διατάξεις των διεθνών συμβάσεων προστασίας των ανθρωπίνων δικαιωμάτων, δημιουργώντας τελικά ένα ενοποιημένο σύνολο κανόνων δικαίου υπέρτερης ισχύος που εγγυάται την εξέλιξη της κοινωνίας της πληροφορίας μέσα σε συνθήκες ελευθερίας και κοινωνικής δικαιοσύνης [49].

Η διείσδυση του δικαίου στο νέο περιβάλλον έχει δισυπόστατο χαρακτήρα. Αφενός ρυθμίζει τις έννομες σχέσεις του ατόμου ως μέλους της ΚτΠ, καθιερώνοντας συνταγματικά δικαιώματα και ελευθερίες και θέτοντας αντιστοίχως τα όρια αυτών. Τα βασικότερα από αυτά είναι η ελευθερία της πληροφόρησης και το δικαίωμα συμμετοχής στην ΚτΠ. Αφετέρου το δίκαιο διασφαλίζει και καθιστά διακριτή μία σφαίρα οικειότητας του ατόμου από τους κινδύνους της σύγχρονης τεχνολογίας, ως απαραίτητο υπόβαθρο για την ουσιαστική συμμετοχή στον νεοπαγή δημόσιο χώρο επικοινωνίας. Η σφαίρα της οικειότητας στην ΚτΠ διασφαλίζεται συνταγματικά κυρίως με

το δικαίωμα του πληροφοριακού αυτοκαθορισμού και με την προστασία του απορρήτου της ελεύθερης ανταπόκρισης ή επικοινωνίας [49].

4.2.1 Θεμελιώδεις Ελευθερίες σε Αντίθεση με τον Αποκλεισμό Περιεχομένου

Ο αποκλεισμός περιεχομένου στο διαδίκτυο μπορεί να έχει επιπτώσεις σε ορισμένα ανθρώπινα δικαιώματα [13].

- Το δικαίωμα στην ιδιωτική ζωή παρεμποδίζεται από την πολλές φορές αναγκαία για τον έλεγχο περιεχομένου διατήρηση και επιθεώρηση εμπιστευτικού και προσωπικού περιεχομένου πληροφοριών. Επιπλέον προς τον περιορισμό της ιδιωτικότητας συμβάλει και η παρεμπόδιση δημιουργίας κοινωνικών διασυνδέσεων μέσω των δικτύων βασιζόμενων σε συγκεκριμένες επιλογές.

- Οι προσπάθειες αποκλεισμού του Διαδικτύου επηρεάζουν την ελευθερία της έκφρασης περιορίζοντας την πρόσβαση σε πληροφορίες ή μην επιτρέποντας την δημοσιοποίηση τους.

- Ο έλεγχος περιορίζει κάποια δικαιώματα από ορισμένες κατηγορίες ανθρώπων, όπως άτομα με κινητικά προβλήματα.

- Ο περιορισμός των δικαιωμάτων των ανηλίκων που προκαλείται από την προσπάθεια προστασίας τους από ακατάλληλο για αυτούς υλικό.

Η ελευθερία της πληροφόρησης περιλαμβάνει την ελευθερία λήψης και την ελευθερία μετάδοσης πληροφοριών, δηλαδή τόσο την παθητική όσο και την ενεργητική της όψη. Θεμελιώνεται στην ελευθερία ανάπτυξης της προσωπικότητας και την ελεύθερη συμμετοχή του ατόμου στην κοινωνική, οικονομική και πολιτική ζωή της χώρας, στην ελευθερία της έρευνας και στην ελευθερία της έκφρασης. Περαιτέρω, θεμελιώνεται και ως ανθρώπινο δικαίωμα στις διεθνείς συμβάσεις της ECHR (άρθρο 10) και του ICCPR, (άρθρο 19§2) καθώς και στον Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ (άρθρο 11). Διαμορφώνεται ως κλασικό ατομικό δικαίωμα, με βάση το οποίο γεννάται η αξίωση του καθενός απέναντι σε ένα κράτος που απέχει από κάθε ενέργεια που παραβλάπτει την ελευθερία λήψης (όπως και μη λήψης) και παραγωγής/διάδοσης πληροφοριών. Ακόμη τελεί υπό την γενική επιφύλαξη υπέρ του νόμου, ενώ οριοθετείται ρητώς από περιορισμούς, που θεσπίζονται νομικά, είναι απολύτως αναγκαίοι και δικαιολογούνται για

λόγους εθνικής ασφάλειας, καταπολέμησης του εγκλήματος ή προστασίας δικαιωμάτων και συμφερόντων τρίτων. Η προστασία δικαιωμάτων και συμφερόντων τρίτων ως επιτρεπτός περιορισμός της ελευθερίας πληροφόρησης αναφέρεται κυρίως στην προστασία της προσωπικότητας, της πνευματικής ιδιοκτησίας και της ιδιωτικότητας.

Η συνταγματική ρύθμιση των διατομικών σχέσεων, που δομούν τη δημόσια σφαίρα της ΚτΠ, ολοκληρώνεται με ένα πλέγμα γενικότερων συνταγματικών δικαιωμάτων και συγκεκριμένα με την ελευθερία ανάπτυξης της προσωπικότητας και την ελεύθερη συμμετοχή του ατόμου στην κοινωνική, οικονομική και πολιτική ζωή της χώρας, το δικαίωμα πληροφόρησης ,το δικαίωμα του συνέρχεσθαι, την ελευθερία της έκφρασης του τύπου, τις θεσμικές εγγυήσεις για τα ΜΜΕ, την ελευθερία της τέχνης, της επιστήμης, της έρευνας και της διδασκαλίας, ερμηνευμένων με τέτοιο τρόπο ώστε να ανταποκρίνονται στις κοινωνικό – τεχνολογικές εξελίξεις εντός της ΚτΠ [13].

Το Δικαίωμα στην Ιδιωτική Ζωή

Πέρα από τη σφαίρα των διατομικών σχέσεων το δίκαιο επεμβαίνει στην κοινωνία της πληροφορίας για τη διασφάλιση της σφαίρας της οικειότητας του ατόμου από τις διακινδυνεύσεις της σύγχρονης τεχνολογίας. Η σφαίρα της οικειότητας θα πρέπει να οριστεί ως εκείνη η σφαίρα δραστηριότητας την οποία το άτομο καθορίζει ως οικεία και επιθυμεί να την διατηρεί ως τέτοια, αποτρέποντας ανεπιθύμητες διεισδύσεις της δημόσιας σφαίρας επί αυτής. Υπό αυτή την έννοια της ιδιωτικότητας, το άτομο είναι αυτόνομο ως προς το να οριοθετεί το ίδιο την ιδιωτική του σφαίρα έναντι της δημόσιας και να ελέγχει ανενόχλητα κάθε φορά το περιεχόμενό της [49].

Οι διεθνείς συμβάσεις και διακηρύξεις προστατεύουν τα άτομα από αυθαίρετες επεμβάσεις στην ιδιωτική τους ζωή, την οικογένειά τους, το σπίτι ή την αλληλογραφία και από επιθέσεις κατά της τιμής και της υπόληψής τους. Στη UDHR διακηρύσσεται ότι «Ο καθένας έχει το δικαίωμα στην προστασία του νόμου έναντι τέτοιων επεμβάσεων ή προσβολών», ενώ στη ECHR αναφέρεται ότι κάποιες παρεμβολές επιτρέπονται, σε συνθήκες που περιγράφονται στο πλαίσιο της λεγόμενης «ρήτρας δημόσιας τάξης» συμπεριλαμβανομένης της αρχής της νομιμότητας.

Η αρχή του απορρήτου της αλληλογραφίας, η οποία από το Ευρωπαϊκό Δικαστήριο των Ανθρωπίνων Δικαιωμάτων ερμηνεύεται ως «η προστασία του απορρήτου της ιδιωτικής

επικοινωνίας», είναι μια από τις θεμελιώδεις ελευθερίες, που θα μπορούσε να υπονομευτεί άμεσα από τη διαδικτυακή λογοκρισία.

Ανάλογα με το στόχο του αποκλεισμού, (τύπος περιεχομένου, πρωτόκολλα επικοινωνίας), τα μέσα που χρησιμοποιούνται για να επιτευχθεί και τους πρόσθετους κανόνες που ενδεχομένως θα τεθούν σε εφαρμογή για τη λειτουργία ολόκληρου του μηχανισμού, προκαλείται συχνά η διατήρηση προσωπικών πληροφοριών χωρίς τη συναίνεση του σχετιζόμενου προσώπου. Ακόμη και αν οι επικοινωνία ενός άτομου δεν κατηγοριοποιείται ως αλληλογραφία, παρόλα αυτά προστατεύεται από το δικαίωμα της ιδιωτικής ζωής. Με βάση την αρχή αυτή, ένα μέτρο αποκλεισμού που θα οδηγήσει σε παρακολούθηση ή διατήρηση των δεδομένων σχετικά με την περιεχόμενο που λαμβάνει, στέλνει ή απλά παρατηρεί ένα άτομο, ακόμη και αν πρόκειται μόνο για την επίσκεψη του σε μια ιστοσελίδα ιδιαίτερου χαρακτήρα, θα ήταν προσβολή του δικαιώματος της ιδιωτικής ζωής. Θα ήταν επίσης, παραβίαση του δικαιώματος προστασίας των προσωπικών δεδομένων.

Η αρχή της προστασίας των προσωπικών δεδομένων συνεπάγεται την εμπιστευτικότητα των δεδομένων, όταν αυτά δίνουν τη δυνατότητα αναγνώρισης, άμεσα ή έμμεσα, ενός φυσικού προσώπου. Σε ένα δημοκρατικό κράτος, κάθε κομμάτι των δεδομένων που επιτρέπει την παρακολούθηση των ανθρώπων θεωρείται επικίνδυνο, ακόμα και αν αυτό δεν χρησιμοποιείται για το σκοπό αυτό.

Η ελευθερία της ιδιωτικής ζωής μπορεί να θεωρηθεί και ως η ελευθερία δημιουργίας και διατήρησης σχέσεων και μέσω των ηλεκτρονικών επικοινωνιών. Στην ίδια κατηγορία εντάσσονται και οι διαδικτυακές πολιτιστικές, ψυχαγωγικές ή καταναλωτικές συνήθειες, ή και η ελεύθερη πλοήγηση στο διαδίκτυο απλά και μόνο για πρόσβαση σε πληροφορίες.

Η ελευθερία της επιλογής των προσώπων και των συνθηκών αλληλογραφίας, προστατεύεται από το δικαίωμα του απορρήτου της αλληλογραφίας. Μια επιλογή λογοκρισίας που θα είχε οιαδήποτε αρνητική επίδραση σε αυτό το δικαίωμα, αντίκεινται με διατάξεις της ECHR [13].

Ελευθερία της Έκφρασης

Η ελευθερία της έκφρασης όπως προσδιορίζεται αλλά και προστατεύεται από εθνικές ευρωπαϊκές και διεθνείς συνθήκες αφορά τη δυνατότατα κάθε ανθρώπου να εκφράζει τη γνώμη του, να λαμβάνει αλλά και να παρέχει πληροφορίες, και ιδέες, χωρίς περιορισμούς συνόρων και

παρεμβολή δημοσίων αρχών. Η διασπορά αυτή μπορεί να γίνεται με τη βοήθεια οπουδήποτε μέσου, προφορικά γραπτά, έντυπα ή και μέσω καλλιτεχνικών εκφράσεων. Σε κάθε περίπτωση όμως είναι συνυφασμένη και με ευθύνες και καθήκοντα και πολλές φορές αποτελεί αντικείμενο συγκεκριμένων περιορισμών.

Η ελευθερία της έκφρασης συμπεριλαμβάνει και τη κυκλοφορία της πληροφορίας μέσω Διαδικτύου, με συνέπεια οποιοσδήποτε περιορισμός της κυκλοφορίας αυτής να έχει επιπτώσεις και στις δυνατότητες ελεύθερης έκφρασης. Στο πλαίσιο της μεταρρύθμισης της νομοθεσίας που σχετίζεται με τις τηλεπικοινωνίες, το Ευρωπαϊκό Κοινοβούλιο επαναδιατυπώνει στις 6 Μαΐου του 2009 ότι «δεν μπορεί να επιβάλλεται περιορισμός επί των θεμελιωδών δικαιωμάτων και ελευθεριών των τελικών χρηστών, χωρίς προηγουμένως να υπάρχει απόφαση των δικαστικών αρχών (…) εκτός και εάν απειλείται η δημόσια ασφάλεια». Πολλοί ερευνητές και μέλη του Ευρωπαϊκού Κοινοβουλίου πιστεύουν ότι αυτό ήταν η αναγνώριση της πρόσβασης στο Διαδίκτυο ως θεμελιώδες δικαίωμα.

Ανεξάρτητα από το αν η πρόσβαση στο Διαδίκτυο είναι ένα ανεξάρτητο θεμελιώδες δικαίωμα ή όχι, τουλάχιστον προστατεύεται ως μέσο για την άσκηση της ελευθερίας της έκφρασης και κάθε προσπάθεια ελέγχου που επιχειρεί να αποτρέψει τους ανθρώπους από την πρόσβαση σε πληροφορίες έρχεται σε σύγκρουση με αυτήν την ελευθερία. Κάθε μέτρο αποκλεισμού περιορίζει το δικαίωμα στην ελευθερία της έκφρασης, σε μεγαλύτερο ή μικρότερο βαθμό, ανάλογα με τα χαρακτηριστικά του και το βαθμό υπερβολικού φιλτραρίσματος που προκαλεί [13].

Δικαιώματα του Παιδιού

Κάθε προσπάθεια λογοκρισίας που αποτρέπει τα παιδιά από το να έχουν πρόσβαση σε πληροφορίες που θα είναι χρήσιμες για την ανάπτυξη, την εκπαίδευση τους και την προετοιμασία τους για μια υπεύθυνη ζωή, θα ήταν σε σύγκρουση με τη Σύμβαση για τα Δικαιώματα του Παιδιού και βεβαίως με το δικαίωμα της ελευθερίας της έκφρασης, ειδικά αν δεν είναι υπό την επίβλεψη των γονέων τους [13].

Δικαιώματα των Ατόμων με Αναπηρία

Τα άτομα με αναπηρία έχουν το πρόσθετο πρόβλημα ότι η αναπηρία τους θα μπορούσε να τα περιορίσει μερικές φορές από την πλήρη άσκηση των δικαιωμάτων τους. Μπορούν παρόλα

αυτά να βοηθηθούν με τη χρήση των ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών του Διαδικτύου. Κατά συνέπεια επιλογές ελέγχου του περιεχομένου που δε θα επιτρέψουν σε αυτούς του ανθρώπους να έχουν πρόσβαση σε ηλεκτρονικές επικοινωνίες μπορεί να περιορίσουν την δυνατότητα τους για άσκηση ορισμένων θεμελιωδών δικαιωμάτων που εύκολα κάποιοι χωρίς ειδικές ανάγκες μπορούν να ασκήσουν [13].

4.2.2 Δικαιώματα και Ελευθερίες που Υποστηρίζονται από τον Αποκλεισμό Περιεχομένου στο Διαδίκτυο

Η προστασία κάποιων δικαιωμάτων και ελευθεριών μπορεί να ενισχύεται από τον έλεγχο του περιεχομένου στο διαδίκτυο. Κάποια από αυτά τα δικαιώματα είναι :

- Το δικαίωμα των παιδιών για προστασία από τη βία.
- Το δικαίωμα των ανθρώπων να μην υφίστανται διακρίσεις.
- Δικαιώματα πνευματικής ιδιοκτησίας.

Είναι ιδιαίτερα σημαντική η προστασία των παιδιών από τη βία. Υπάρχουν δύο πτυχές της κοινωνικής προστασίας του παιδιού που παρουσιάζουν ιδιαίτερο ενδιαφέρον.

- Ο μεγάλος αριθμός των κειμένων που τονίζουν την απαγόρευση της ψυχικής και σωματικής βίας εις βάρος παιδιών, ιδιαίτερα της σεξουαλικής φύσεως.
- Η απαγόρευση της προβολής εγκλήματος σεξουαλικής φύσης που διαπράττονται εις βάρος ενός παιδιού, μέσα από την απαγόρευση της παιδικής πορνογραφίας.

Η σημασία της καταπολέμησης της παιδικής πορνογραφίας, καθώς και η σημασία της προστασίας των παιδιών από τη βία και οτιδήποτε μπορεί να διαταράξει την ανάπτυξη της προσωπικότητας τους, είναι πολύ συχνά το βασικό επιχείρημα για να δικαιολογηθεί η εφαρμογή μέτρων λογοκρισίας στο Διαδίκτυο. Είναι κάποιες φορές η μόνη δικαιολογία από κυβερνήσεις ή ιδιωτικούς φορείς που υποστηρίζουν την εφαρμογή του αποκλεισμού στο Διαδίκτυο.

Εάν γίνει αποδεκτό το παραπάνω επιχείρημα για την εφαρμογή του ελέγχου στο περιεχόμενο είναι νομικά δύσκολο να κατανοηθεί γιατί το μέτρο πρέπει να περιοριστεί σε θέματα παιδικής

πορνογραφίας και μόνο. Με δεδομένο ότι ο νόμος προστατεύει επίσης άλλες κατηγορίες ατόμων από απειλές, κυρίως από απειλές που δημιουργούνται από τις διακρίσεις, η εφαρμογή της λογοκρισίας μπορεί να διευρυνθεί.

Τα ανθρώπινα δικαιώματα και οι θεμελιώδεις ελευθερίες αντιστοιχούν σε κάθε άτομο, χωρίς διάκριση. Ωστόσο, οι διακρίσεις υπήρχαν και εξακολουθούν να υφίστανται σε ορισμένες χώρες. Περιεχόμενο στο Διαδίκτυο που αποτελεί μια εξίσου έγκυρη αιτιολόγηση για την εφαρμογή λογοκρισίας με την παιδική πορνογραφία, είναι κείμενα για την ενθάρρυνση των διακρίσεων, αλλά και εικόνες από βασανιστήρια ή φόνους που διαπράττονται για λόγους φυλετικού μίσους [13].

Δικαιώματα Πνευματικής Ιδιοκτησίας

Τα δικαιώματα πνευματικής ιδιοκτησίας προστατεύονται από διάφορες συνθήκες σε διεθνές επίπεδο. Η αναφορά στα πνευματικά δικαιώματα συμπεριλαμβάνει την προστασία των δικαιωμάτων των δημιουργών, των ερμηνευτών, των παραγωγών και των διανομέων και συμβάλει στην πολιτιστική και οικονομική ανάπτυξη των εθνών. Το δικαίωμα στην προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας ως εκ τούτου θεωρείται ως ένα ανθρώπινο δικαίωμα και εκ των θεμελιωδών ελευθεριών και θα μπορούσε επίσης να είναι μια πολιτική ελευθερία σε ορισμένες χώρες. Το δικαίωμα αυτό μπορεί να αποτελεί βασικό επιχείρημα δημιουργίας μηχανισμών ελέγχου με βάση το περιεχόμενο στο Διαδίκτυο.

Ιστορικά, δύο σχολές έχουν αναπτυχθεί αναφορικά με την φιλοσοφική δικαιολόγηση του θεσμού της πνευματικής ιδιοκτησίας. Σύμφωνα με την προσέγγιση του Ηπειρωτικού Ευρωπαϊκού Δικαίου το ατομικό δικαίωμα του δημιουργού στο πνευματικό του έργο ως ηθικοπολιτική επιταγή προκύπτει από το ότι κάθε άνθρωπος έχει φυσικό δικαίωμα στο αποτέλεσμα της εργασίας του. Κατά την προσέγγιση της σχολής του Κοινοδίκαιου (common law) η απονομή από την πολιτεία εν είδει προνομίου αποκλειστικών δικαιωμάτων των δημιουργών στα πνευματικά τους έργα λειτουργεί ως οικονομικό κίνητρο για την ανάπτυξη της ανθρώπινης δημιουργικότητας και τελικά την πολιτισμική άνθηση [13].

4.2.3 Λογοκρισία και Ειδικές Διατάξεις που Αφορούν τις Ηλεκτρονικές Επικοινωνίες

Οποιαδήποτε εφαρμογή περιοριστικών μέτρων στην επικοινωνία στο διαδίκτυο πρέπει να είναι σύμφωνη με την ευρωπαϊκή νομοθεσία που αφορά τις ηλεκτρονικές επικοινωνίες.

Αυτή η νομοθεσία συμπεριλαμβάνει την υποχρέωση των παρόχων υπηρεσιών διαδικτύου (ISP) για ουδετερότητα, ποιότητα και παγκόσμια καθολικότητα των υπηρεσιών τους. Παράλληλα αποτελεί βάση για την επιχειρηματολογία των παρόχων στην προσπάθεια τους να αποφύγουν πιέσεις για λογοκρισία έξω από το νομικό πλαίσιο.

Υπηρεσίες που περιλαμβάνονται στο πεδίο εφαρμογής της καθολικής παγκόσμιας υπηρεσίας είναι βασικές υπηρεσίες επικοινωνίας, συμπεριλαμβανομένων των επικοινωνιών φωνής και διασύνδεσης στο Διαδίκτυο. Κάθε μηχανισμός ελέγχου που θα αποτρέψει ένα χρήστη του Διαδικτύου από την πρόσβαση στο δημόσιο τηλεφωνικό δίκτυο, έρχεται σε σύγκρουση με την υποχρέωση παροχής καθολικής υπηρεσίας. Επιτρέποντας στους πολίτες να έχουν πρόσβαση στο Διαδίκτυο ικανοποιούνται βασικά δικαιώματα και ελευθερίες σε σχέση με το γενικό συμφέρον του κοινού.

Με δεδομένο ότι οι ευριζωνικές συνδέσεις αποτελούν βασικό στοιχειό της καθολικότητας και της ποιότητας των υπηρεσιών, ένα κράτος δε νομιμοποιείται να επιβάλει μέτρα αποκλεισμού σε οπουδήποτε χρήστη, χωρίς αυτά να συμφωνούν με την Ευρωπαϊκή διακήρυξη ανθρωπίνων δικαιωμάτων, ιδίως όσον αφορά την ανάγκη να τηρηθεί η ρήτρα δημόσιας τάξης.

Οι πάροχοι ακόμη θα πρέπει να εξασφαλίζουν ένα επίπεδο ποιότητας της υπηρεσίας πρόσβασης που παρέχουν. Είναι υπεύθυνοι για την ορθή λειτουργία μιας δημόσιας υπηρεσίας μεταφοράς πληροφορίας, ενός δημόσιου δηλαδή αγαθού, την απρόσκοπτη παροχή του οποίου πρέπει να διασφαλίζουν σε κάθε περίπτωση.

Τα δημόσια δίκτυα υπολογιστών είναι τεχνικά αρκετά πολύπλοκα και η εφαρμογή των μηχανισμών λογοκρισίας αυξάνει σημαντικά την ευαισθησία τους σε βλάβες καθώς και σε καθυστερήσεις. Ως εκ τούτου, η λειτουργία ενός δικτύου ηλεκτρονικών επικοινωνιών και ο έλεγχος περιεχομένου είναι φιλοσοφικά αλλά και τεχνολογικά δυο αντιφατικές έννοιες, που πρέπει να συγκεραστούν όταν ο αποκλεισμός είναι επιβεβλημένος.

Οι πάροχοι υπηρεσιών Διαδικτύου, ακόμη έχουν την υποχρέωση να παραμένουν ουδέτεροι ως προς το περιεχόμενο και την σημασία της πληροφορίας την οποία μεταφέρουν ακολουθώντας το παράδειγμα παραδοσιακών παρόχων άλλων υπηρεσιών όπως τηλεφωνία και ταχυδρομείο. Σαν αποτέλεσμα αυτής της αρχής, ένας πάροχος δεν έχει το δικαίωμα να επιλέξει αν θα μεταδώσει ή όχι ένα μήνυμα με βάση το περιεχόμενο του, εκτός αν αυτό αποτελεί επιλογή του χρήστη που το δημιούργησε ή αν υπάρχει νομικό κώλυμα..

Ακόμη η παρακολούθηση και επιθεώρηση του περιεχομένου από τον πάροχο της υπηρεσίας διασύνδεσης είναι επιτρεπτή μόνο όταν το επιβάλει ο νόμος. Οποιοδήποτε μέτρο αποκλεισμού που απαιτεί έλεγχο του περιεχομένου που μεταφέρεται στο δίκτυο προκειμένου να διαπιστωθεί η ακαταλληλότητα του, επιτρέπεται μόνο στην περίπτωση που είναι σύμφωνο με νόμους συμβατούς με την ευρωπαϊκή οδηγία για την δημόσια τάξη [13].

4.3 Από το Take Down Notice στην ACTA

Το 1995 είναι μια χρόνια-ορόσημο, μια που έκτοτε πλήθος νομικών στο Κοινοβούλιο της Μεγάλης Βρετανίας, της Ευρωπαϊκής Ένωσης αλλά και το Αμερικανικό Κογκρέσο εστίασαν στο πώς θα γίνει πιο άμεσο και ευκολότερο το «κατέβασμα» ενοχλητικού υλικού από το Διαδίκτυο: από δυσφημιστικά κείμενα έως υλικό που καταπατάει νόμους περί πνευματικής ιδιοκτησίας και από βίντεο παιδικής πορνογραφίας έως δημοσιεύματα αντιτιθέμενα σε αντιτρομοκρατικούς νόμους [41].

Αποτέλεσμα όλης αυτής της προσπάθειας ήταν το Digital Millennium Copyright Act του 1998 στις ΗΠΑ [40], όπως επίσης και το European Union Copyright Directive που ψηφίστηκε το 2001 και εφαρμόζεται σε κάθε μέλος της Ε.Ε. Ο νόμος επιτρέπει στον καθένα να «κατεβάσει» υλικό από το Διαδίκτυο, απλά και μόνο κάνοντας μια καταγγελία στην υπηρεσία που το φιλοξενεί (hosting services) και ενημερώνοντας την πως γίνεται καταπάτηση πνευματικών δικαιωμάτων.

Αν και με μια πρώτη ματιά ο νόμος φαίνεται σωστός, στην πραγματικότητα μειώνει κατά πολύ το πλήθος των αποδείξεων που χρειάζεται για να αφαιρεθεί κάτι από το Διαδίκτυο δημιουργώντας έτσι μια επικίνδυνη νομοθεσία που επιτρέπει την κατάχρηση της δυνατότητας αυτής δίνοντας την ευκαιρία σε εταιρίες, οργανισμούς και ιδιώτες, με μια απλή καταγγελία, να επιτύχουν την απομάκρυνση οποιουδήποτε δημοσιεύματος τους ενοχλεί. Με λίγα λόγια, δεν χρειάζονται ούτε αποδείξεις ούτε ντοκουμέντα για την καταγγελία, μια και πρώτα «κατεβαίνει»

το ύποπτο υλικό από το Internet και εκ των υστέρων έρχεται η υπόθεση ενώπιον της δικαιοσύνης.

Σύντομα, όμως, η χαώδης φύση του Internet έκανε ξεκάθαρο πως ακόμα και μια τόσο άμεση νομοθεσία δεν μπορεί να δώσει ουσιαστικές λύσεις. Χαρακτηριστικό παράδειγμα αποτελεί η εταιρία Viacom, η οποία έστειλε το Φεβρουάριο του 2008 100.000 αιτήσεις για «κατέβασμα» από τη You Tube βίντεο που καταπατούσαν πνευματικά δικαιώματα, όμως δευτερόλεπτα αργότερα νέοι χρήστες ανέβασαν ξανά τα περισσότερα από αυτά. Επιπρόσθετα, ανάμεσα στα βίντεο που διαγράφηκαν υπήρχαν και μερικά καθ' όλα νόμιμα που λανθασμένα αποκλειστήκαν. «Όταν προσπαθείς να καθαρίσεις το Internet, θα πιάσεις αναγκαστικά και κάποια δελφίνια», δήλωσε χαρακτηριστικά ο εκπρόσωπος της Motion Picture Association of America, Dan Glickman [39].

4.3.1 Το Πέρασμα στα Αυτόματα Συστήματα Λογοκρισίας

Η αποτυχία της παραπάνω νομοθεσίας, οδήγησε στο επόμενο στάδιο του διαδικτυακού περιορισμού, στην ανάπτυξη, δηλαδή, συστημάτων αυτόματης διαδικτυακής λογοκρισίας, σε επίπεδο κρατών, ως τη μόνη λύση στο πρόβλημα των «ενοχλητικών δημοσιεύσεων». Πρωτοπόρος στην εν λόγω μέθοδο λογοκρισίας θεωρείται δικαιολογημένα η Κίνα, η οποία διαθέτει ένα σύστημα firewall που απορρίπτει αιτήματα σύνδεσης, το επονομαζόμενο ανεπίσημα «Μεγάλο Σινικό Τείχος». Στη Σαουδική Αραβία, από την άλλη, χρησιμοποιείται ένα σύστημα web proxy που μπλοκάρει την πρόσβαση σε ιστοσελίδες, οι οποίες περιλαμβάνονται στη «μαύρη λίστα» που συντάσσεται από αναφορές πολιτών.

Ερχόμενη στην Ευρώπη, η νορβηγική εταιρία τηλεφωνίας Telenor, σε συνεργασία με την υπηρεσία KRIPOS (Νορβηγική Εθνική Υπηρεσία Έρευνας Εγκλημάτων), ανέπτυξαν ένα σύστημα διαδικτυακής λογοκρισίας που εστιάζει στην παιδική πορνογραφία, το οποίο και έθεσαν σε εφαρμογή τον Οκτώβριο του 2004. Όταν ένας χρήστης προσπαθεί να επισκεφθεί μια απαγορευμένη ιστοσελίδα, το σύστημα τον στέλνει σε μια σελίδα με πληροφορίες για το σύστημα λογοκρισίας και έναν σύνδεσμο για την υπηρεσία KRIPOS. Παρόμοιο σύστημα εφαρμόστηκε από την Telenor και στη Σουηδία (2005) [38], ενώ σήμερα πλέον αντίστοιχα συστήματα εφαρμόζονται σε πλήθος ευρωπαϊκών χωρών (Δανία, Φινλανδία, Ολλανδία, Ελβετία, Ιταλία κ.ά.).

Στην Ευρώπη, πρωτοπόρος θεωρείται η Μεγάλη Βρετανία και το σύστημα λογοκρισίας CleanFeed [68], που τέθηκε σε λειτουργία τον Ιούνιο του 2004, με συνεργασία της εταιρίας τηλεφωνίας BT και της Βρετανικής κυβέρνησης. Μάλιστα, η Βρετανική κυβέρνηση, έως το τέλος του 2008, ανάγκασε όλες τις εταιρίες παροχής Internet της χώρας να απαγορεύσουν την πρόσβαση σε μια σειρά ιστοσελίδων οι οποίες περιλαμβάνονται στη «μαύρη λίστα» των απαγορευμένων ιστοσελίδων που εκδίδει η υπηρεσία Internet Watch Foundation. Στην περίπτωση του CleanFeed, όταν ένας χρήστης προσπαθεί να επισκεφθεί έναν απαγορευμένο ιστότοπο, δεν δέχεται κάποιο μήνυμα ενημέρωσης για το σύστημα, ούτε του προσφέρεται κάποιος τρόπος επικοινωνίας με τους υπευθύνους, παρά ένα αόριστο μήνυμα λάθους που εμφανίζεται σε πλήθος άλλων περιπτώσεων (πρόβλημα σύνδεσης, πρόβλημα στον server κ.λπ.). Με λίγα λόγια, ο χρήστης δεν καταλαβαίνει ότι πέφτει θύμα διαδικτυακού περιορισμού.

Στηριζόμενες στο σύστημα της Μεγάλης Βρετανίας, οι μεγαλύτερες εταιρίες παροχής Internet της Αυστραλίας ανακοίνωσαν το 2006, την ανάπτυξη λογισμικού διαδικτυακής λογοκρισίας που θα εστιάζει σε ιστοσελίδες παιδικής πορνογραφίας. Ένα χρόνο αργότερα, ο Υπουργός Τηλεπικοινωνιών, S. Conroy, δήλωσε πως το εν λόγω σύστημα θα εφαρμόζεται υποχρεωτικά σε όλους και πως πέραν της παιδικής πορνογραφίας, θα εστιάζει και σε «ακατάλληλο περιεχόμενο», αφήνοντας το τελευταίο αόριστο και αρκετά ανοικτό.

4.3.2 Οι Πρώτες Αντιδράσεις

Όπως ήταν φυσικό, από τα πρώτα ακόμα, περιστατικά διαδικτυακής λογοκρισίας που είδαν το φως της δημοσιότητας, άρχισαν να δραστηριοποιούνται διαδικτυακές οργανώσεις ενάντια στο φαινόμενο, όπως το Βρετανικό Index of Censorship, το αμερικανικό Electronic Frontier Foundation, το ιρανικό iraniazad.com, το διεθνές Freedom Against Censorship Thailand (FACT) κ.ά. Επιπλέον, γνωστές οργανώσεις ανθρώπινων δικαιωμάτων άρχισαν να εστιάζουν στο εν λόγω φαινόμενο μέσω των υπαρχόντων ιστοσελίδων τους, ή ακόμα και ξεκινώντας καμπάνιες και ιστοσελίδες αποκλειστικά κατά της διαδικτυακής λογοκρισίας (π.χ. το irrepressible.info της Διεθνούς Αμνηστίας). Άξιο αναφοράς είναι πως πολλές προσπάθειες εξ αυτών προστέθηκαν σύντομα στις «μαύρες λίστες» συστημάτων αρκετών κρατών [17].

Αυτό όμως που πραγματικά αξίζει εκτενούς αναφοράς είναι η έντονη κινητοποίηση μεγάλης μερίδας της παγκόσμιας ακαδημαϊκής κοινότητας ενάντια στο φαινόμενο, μιας και όπως πιστεύουν πολλοί πανεπιστημιακοί, είμαστε πολύ κοντά σε νομοθετικές αλλαγές που θα αλλάξουν μια για πάντα, προς το χειρότερο, τη λειτουργία του Internet. Ανάμεσα σε αυτές τις

προσπάθειες είναι και το OpenNet Initiatiave (ONI), μια διεθνής ακαδημαϊκή συνεργασία του Citizen Lab του Munk Center for International Studies (Πανεπιστήμιο του Toronto), του Berkman Center for Internet and Society (Πανεπιστήμιο του Harvard) και του SecDev Group, που σε σταθερή βάση παράγει και δημοσιεύει αναφορές για το επίπεδο διαδικτυακής λογοκρισίας σε διάφορα κράτη [17]. Πρόσφατα, μάλιστα, έπεσε και αυτό θύμα λογοκρισίας.

4.3.3 Προστασία ή Λογοκρισία, Βασικά Διλλήματα

«Σε όσους πιστεύουν πως η ελευθερία του λόγου σημαίνει να βλέπουν παιδική πορνογραφία, η ομοσπονδιακή κυβέρνηση απαντάει όχι», ανέφερε στις 31 Δεκεμβρίου του 2007 ο Stephen Conroy, Υπουργός Τηλεπικοινωνιών της αυστραλιανής κυβέρνησης, κατά την ανακοίνωση της επιβολής συστήματος διαδικτυακού ελέγχου στη χώρα. Την ίδια ακριβώς πρόφαση έχουν χρησιμοποιήσει μέχρι σήμερα όλες οι φιλελεύθερες χώρες που θέλησαν να εφαρμόσουν αντίστοιχα συστήματα διαδικτυακού ελέγχου, όπως για παράδειγμα η Μεγάλη Βρετανία.

Αν και όλες οι φιλελεύθερες χώρες πρόβαλλαν ως αιτία εφαρμογής συστημάτων διαδικτυακής λογοκρισίας, την αντιμετώπιση της παιδοφιλίας, εντούτοις οι «μαύρες λίστες» ορισμένων χωρών που διέρρευσαν στον Τύπο (χάρη στο WikiLeaks) περιέχουν και ιστοσελίδες άλλου είδους, όπως πολιτικού περιεχομένου. Χαρακτηριστικό παράδειγμα αποτελεί η «μαύρη λίστα» της Αυστραλίας (η οποία βασίστηκε στη λίστα που χρησιμοποιεί το CleanFeed στη Μεγάλη Βρετανία), που περιέχει ιστοσελίδες ενάντια στην άμβλωση, καθώς και σελίδες αιρέσεων, ομοφυλοφιλικών κοινοτήτων, ισλαμιστών, κοινοτήτων υπέρ της ευθανασίας κ.ά. Η αποκάλυψη μέρους της λίστας ανάγκασε τον Υπουργό Τηλεπικοινωνιών να παραδεχθεί πως οι μισές ιστοσελίδες της «μαύρης λίστας» δεν έχουν να κάνουν με παιδική πορνογραφία. Καθώς όλο και περισσότερες εφημερίδες και έντυπα «μεταναστεύουν» αποκλειστικά στο Διαδίκτυο, συστήματα ελέγχου και λογοκρισίας τέτοιου είδους δίνουν τεράστια δύναμη στα χέρια λίγων. Τα αθόρυβα (διότι παραμένουν εσκεμμένα άγνωστα στο ευρύ κοινό) κρατικά συστήματα λογοκρισίας είναι επικίνδυνα και πληθαίνουν μέρα με τη μέρα. Μπορεί οι κυβερνήσεις κρατών ανά τον κόσμο (δυστυχώς, όλο και περισσότερες δημοκρατικές χώρες) να βλέπουν προς την επέκταση των συστημάτων τους, όμως όλο και περισσότερος κόσμος γνωρίζει πλέον τέτοιου είδους κινήσεις.

Κατά τη διάρκεια του 4ου Φόρουμ για τη Διαδικτυακή Διακυβέρνηση στο Sharm El Sheikh της Αιγύπτου (15-18 Νοεμβρίου 2009), το ακαδημαϊκό βιβλίο Access Controlled του ONI [19], που καταπιάνεται με το διαρκώς αυξανόμενο φαινόμενο του φιλτραρίσματος των πληροφοριών που

δημοσιεύονται στο Διαδίκτυο και της on line παρακολούθησης χρηστών, έπεσε θύμα λογοκρισίας. Θύτης, όσο παράξενο και αν ακουστεί αρχικά, ήταν ο ίδιος ο διοργανωτής του ετήσιου συνεδρίου, τα Ηνωμένα Έθνη. Η πράξη της λογοκρισίας αφορούσε μία αφίσα προώθησης του βιβλίου, η οποία, ανάμεσα στα άλλα, περιείχε την εξής φράση: «Η πρώτη γενιά λογισμικών διαδικτυακού ελέγχου αποτελείται κυρίως από firewalls σε καίρια Internet gateways, όπως για παράδειγμα το περιώνυμο Μεγάλο (Σινικό) Τείχος της Κίνας, που ήταν ένα από τα πρώτα συστήματα περιορισμού του Διαδικτύου που εφαρμόστηκε σε εθνικό επίπεδο». Η αναφορά στην Κίνα, ισχυρότατο μέλος των Ηνωμένων Εθνών, δεν πέρασε απαρατήρητη. «Η εμφάνιση της εν λόγω πρότασης ήταν αρκετή, ώστε να τη χαρακτηρίσει απαγορευμένη από τους φύλακες ασφαλείας των Ηνωμένων Εθνών στο Internet Governance Forum, οι οποίοι και την απομάκρυναν, παρά τις διαμαρτυρίες των ακαδημαϊκών του ONI, Ronald Deibert and Ratal Rohozinski», ανέφερε ο δρ. Jonathan Zittrain, καθηγητής στο Πανεπιστήμιο του Harvard, σε άρθρο του με τίτλο «Η πρόταση που τα Ηνωμένα Έθνη δεν θέλουν να διαβάσεις».

Το 2007 στο Στρασβούργο παρουσιάστηκε ως πρόταση από το μέλος της Κομισιόν, Viviane Reding και εξαρχής προκάλεσε έντονες αντιδράσεις για αρκετά άρθρα και παραγράφους του που για πολλούς, βάζουν τέλος στην ανοικτή και ελεύθερη φύση του Διαδικτύου, ένα άγνωστο στο ευρύ κοινό νομικό πακέτο, με την ονομασία Telecoms Reform Package (TRP) [98]. Συμφωνά με το Blackout Europe (μια διεθνή συνεργασία οργανισμών ενάντια στον περιορισμό του Διαδικτύου), το TRP θα δίνει τη δυνατότητα στους παρόχους Internet να περιορίσουν νόμιμα τον αριθμό των ιστοσελίδων που μπορούν οι χρήστες να επισκεφθούν, αλλά και να καθορίσουν ποιες υπηρεσίες θα μπορούν να χρησιμοποιούν (You Tube, Skype κ.λπ.). Όπως χαρακτηριστικά αναφέρει: «(Ο περιορισμός) θα παρουσιαστεί υπό τη μορφή νέων καταναλωτικών επιλογών. Το Internet θα προσφέρεται όπως ακριβώς και τα πακέτα συνδρομητικών καναλιών, δηλαδή θα δίνεται στον χρήστη ένας περιορισμένος αριθμός επιλογών για πρόσβαση. Το Διαδίκτυο Θα χωριστεί σε πακέτα, με αποτέλεσμα η δυνατότητα για πρόσβαση και δημοσίευση περιεχομένου να περιοριστεί δραματικά. Θα δημιουργηθούν κουτιά διαδικτυακής πρόσβασης, κάτι που διαφέρει τελείως από τον τρόπο που το χρησιμοποιούμε σήμερα».

Οι εκάστοτε λοιπόν, πάροχοι Internet (με την επιτήρηση των επί μέρους κυβερνήσεων και τον κεντρικό έλεγχο της Ε.Ε.) θα προσφέρουν πρόσβαση μόνο σε ελεγμένες ιστοσελίδες στο Διαδίκτυο, κόβοντας το υπόλοιπο Internet. Με λίγα λόγια, λύνεται σε μεγάλο βαθμό το πρόβλημα των «ενοχλητικών δημοσιεύσεων», βάζοντας απλά σε τάξη το (διαδικτυακό) χάος.

Ανάμεσα στις αλλαγές που επιχείρησε να επιφέρει το νομικό αυτό πακέτο, βρίσκεται και μία ακόμα σημαντικότατη λεπτομέρεια: η άρση της διαδικτυακής ουδετερότητας. Μέχρι σήμερα, κάθε πληροφορία στο Διαδίκτυο, είτε προερχόταν από ένα blog είτε από το BBC News, αντιμετωπιζόταν με τον ίδιο ακριβώς τρόπο από τις εταιρίες παροχής Internet. Με τις τροποποιήσεις που προτείνονται, όλες οι πληροφορίες θα μπαίνουν σε σειρά προτεραιότητας και σημαντικότητας (με τις θέσεις αυτές να αγοράζονται νόμιμα με το κατάλληλο αντίτιμο), περιορίζοντας έτσι τις δυνατότητες νέων και χαμηλών οικονομικών δυνατοτήτων προσπαθειών για διάδοση. Στα παραπάνω αντέδρασε μέχρι και η Google, αναφέροντας χαρακτηριστικά πως «Θα μπορούσαμε εύκολα να πληρώσουμε για τα πακέτα premium, όμως δεν είναι εκεί το θέμα. Εδώ πρόκειται για θέμα αρχών. Ξεκινήσαμε ως μικρή επιχείρηση. Δεν θα μπορούσαμε να κάνουμε το ίδιο πράγμα στο μέλλον, εφόσον οι τροποποιήσεις αυτές περάσουν» [41].

4.3.4 PIPA – SOPA – ACTA

Το PIPA (Protect Intelectual Property Act – Πράξη για την Προστασία της Πνευματικής Ιδιοκτησίας) [43], είναι μια πρόταση νόμου στις Ηνωμένες Πολιτείες που υποβλήθηκε στις 12 Μαΐου του 2011. Είχε σαν σκοπό να δώσει στην κυβέρνηση και στους κατόχους πνευματικών δικαιωμάτων πρόσθετα εργαλεία για τον αποκλεισμό της πρόσβασης σε παράνομους ιστότοπους που περιέχουν αντίγραφα περιεχομένου που προστατεύεται από δικαιώματα πνευματικής ιδιοκτησίας, ιδιαίτερα εκτός της επικράτειας των Η.Π.Α.. Το SOPA (Stop Online Piracy Act - Πράξη για τη Διακοπή της Δικτυακής Πειρατείας) [44], γνωστό επίσης ως H.R. 3261, είναι νομοσχέδιο που είχε υποβληθεί στην Βουλή των Αντιπροσώπων των Ηνωμένων Πολιτειών στις 26 Οκτωβρίου 2011 με σκοπό την επέκταση των δυνατοτήτων των Σωμάτων Ασφαλείας των Ηνωμένων Πολιτειών και των κατεχόντων πνευματικών δικαιωμάτων για να αντιμετωπίσουν την διαδικτυακή πειρατεία πνευματικής ιδιοκτησίας και απομιμήσεων [48]. Μετά από διαμαρτυρίες πολιτών και οργανισμών στο Διαδίκτυο, τα νομοσχέδια αποσύρθηκαν στις 20 Ιανουαρίου 2012, ενώ η επιτροπή δεσμεύτηκε να βρει λύση στο πρόβλημα της διαδικτυακής πειρατείας, αναβάλλοντας την εκτίμηση νέας νομοθεσίας μέχρι να δημιουργηθεί ευρύτερη συμφωνία [42].

Η Εμπορική Συμφωνία Κατά της Παραποίησης γνωστή και ως ACTA (Anti-Counterfeiting Trademark Agreement) είναι μια ολιγομερής διεθνής συνθήκη με σκοπό την εγκαθίδρυση διεθνών προτύπων για την άσκηση των δικαιωμάτων πνευματικής ιδιοκτησίας [47]. Η συμφωνία επιδιώκει να εγκαθιδρύσει ένα διεθνές νομικό πλαίσιο για την στοχοποίηση της

απομίμησης των αγαθών, των γενόσημων φαρμάκων και της παραβίασης πνευματικών δικαιωμάτων στο Διαδίκτυο και να δημιουργήσει ένα νέο κυβερνητικό όργανο πέρα από τα ήδη υπάρχοντα fora, όπως είναι ο Παγκόσμιος Οργανισμός Εμπορίου και ο Παγκόσμιος Οργανισμός Διανοητικής Ιδιοκτησίας, ή τα Ηνωμένα Έθνη [22].

Η συμφωνία υπογράφτηκε στις 1 Οκτωβρίου του 2011 από την Αυστραλία, τον Καναδά, την Ιαπωνία, το Μαρόκο, τη Νέα Ζηλανδία, τη Σιγκαπούρη, τη Νότια Κορέα και τις Ηνωμένες Πολιτείες. Τον Ιανουάριο του 2012, η Ευρωπαϊκή Ένωση και 22 από τα κράτη μέλη της, μεταξύ των οποίων και η Ελλάδα, υπέγραψαν επίσης, ανεβάζοντας τον συνολικό αριθμό των υπογραφόντων σε 31. Μετά την επικύρωση από έξι 6 κράτη, η σύμβαση θα τεθεί σε ισχύ μόνον σε εκείνα τα κράτη που τη έχουν επικυρώσει [47].

Η συμφωνία επί της ουσίας, καθιστά τους παρόχους (ISP) αποκλειστικά υπεύθυνους για τις όποιες παραβάσεις πνευματικών δικαιωμάτων πραγματοποιούνται στο δίκτυό τους. Αυτό σημαίνει ότι προκειμένου να μην βρεθούν προ απροόπτου (ακόμα και κατηγορούμενοι) θα πρέπει να χρησιμοποιήσουν συστήματα παρακολούθησης κάθε διαδικτυακού βήματος των χρηστών τους. Οι πάροχοι μάλιστα θα έχουν την δυνατότητα να αποστέλλουν προειδοποιήσεις στον χρήστη που επιδεικνύει «παραβατική» συμπεριφορά και αν δεν συμμορφώνεται να τον αποκλείουν από το δίκτυό τους.

Οι υποστηρικτές της έχουν περιγράψει την συμφωνία ως αντίδραση στην «αύξηση των πειρατικών αγαθών σε παγκόσμιο επίπεδο και των πειρατικών αντιγράφων έργων πνευματικής ιδιοκτησίας», ενώ οι αντίπαλοί της την κατέκριναν για τα εν δυνάμει δυσμενή αποτελέσματα που θα έχει στα θεμελιώδη πολιτικά και ψηφιακά δικαιώματα, περιλαμβάνοντας το δικαίωμα της έκφρασης και του απορρήτου της επικοινωνίας [46]. Άλλοι, όπως το Electronic Frontier Foundation, έχουν καταγγείλει τον αποκλεισμό των οργανώσεων την πολιτικής κοινωνίας, των αναπτυσσομένων χωρών και του γενικού κοινού από την διαδικασία διαπραγμάτευσης της συμφωνίας.

Στις 4 Ιουλίου 2012, το Ευρωπαϊκό Κοινοβούλιο καταψήφισε με ευρεία πλειοψηφία τη Συμφωνία. Στην ψηφοφορία για την ACTA 478 ευρωβουλευτές ψήφισαν κατά της συμφωνίας έναντι 39 που ψήφισαν υπέρ, ενώ υπήρξαν και 165 αποχές [45]. Είναι η πρώτη φορά που το Ευρωπαϊκό Κοινοβούλιο χρησιμοποιεί τη δυνατότητα που του παρέχει η Συνθήκη της Λισαβόνας να απορρίψει διεθνή εμπορική συμφωνία. Η ACTA αποτέλεσε αντικείμενο διαπραγμάτευσης από την ΕΕ και τα κράτη μέλη της, με τις ΗΠΑ, την Αυστραλία, τον Καναδά,

την Ιαπωνία, το Μεξικό, το Μαρόκο, τη Νέα Ζηλανδία, τη Σιγκαπούρη, τη Νότια Κορέα και την Ελβετία με σκοπό τη βελτίωση της επιβολής του νόμου κατά της παραποίησης διεθνώς. Η ψηφοφορία της 4ης Ιουλίου 2012 σημαίνει ότι ούτε η ΕΕ ούτε τα επιμέρους κράτη μέλη της θα συμμετάσχουν στη συμφωνία[49].

4.4 Συμπεράσματα

Καθημερινά παρουσιάζονται καινούργια παραδείγματα όπου, παρά την προσπάθεια επιβολής περιορισμών, η σύγχρονη τεχνολογία επικοινωνιών συμβάλει σε σημαντικές κοινωνικές εξελίξεις. Καμιά άλλη τεχνολογία στην ιστορία της ανθρωπότητας δεν έχει εξαπλωθεί τόσο γρήγορα, γεωγραφικά και πληθυσμιακά και κανένας άλλος τρόπος επικοινωνίας δεν έχει διευκολύνει τόσο πολύ τον εκδημοκρατισμό της επικοινωνίας όσο το Διαδίκτυο [18].

Παρόλα αυτά δεν είναι λίγες οι φορές που οι ίδιες οι τεχνολογίες που χρησιμοποιούνται για ελεύθερη κοινωνικοποίηση και εκδημοκρατισμό, αποτελούν πεδίο ή και εργαλείο επιτήρησης ή και καταπίεσης. Τεχνολογίες που έχουν δημιουργηθεί για κάποιο σκοπό μπορούν να έχουν διαφορετικές χρήσεις ανάλογα με το κοινωνικοπολιτικό περιβάλλον στο οποίο εφαρμόζονται. Αμέτρητα απελευθερωτικά κινήματα και μηχανισμοί κοινωνικού ελέγχου συνυπάρχουν μέσα σε ένα κοινό, αλλά συνεχώς εξελισσόμενο χώρο επικοινωνιών.

Αυτή η κοινωνική πολυπλοκότητα είναι ένα καθολικό χαρακτηριστικό όλων των τεχνολογικών συστημάτων, αλλά είναι ιδιαίτερα έντονη στο χώρο των επικοινωνιών για διάφορους λόγους. Από τη μία πλευρά η διάσταση της παγκοσμιοποίησης, σαν αίτιο αλλά και αποτέλεσμα της επικοινωνίας αυτής, με δεδομένο ότι μια δημιουργία ενός χρήστη σε μια μεριά του πλανήτη μπορεί να επηρεάσει γεγονότα και καταστάσεις στην άλλη άκρη του. Από την άλλη το γεγονός ότι ο κυβερνοχώρος ελέγχεται εν πολλοίς από χιλιάδες ιδιωτικούς φορείς, κάποιες δραστηριότητες των οποίων, καθοδηγούμενες από εμπορικές σκοπιμότητες έχουν κοινωνικές επιπτώσεις που υπερβαίνουν τα εθνικά δικαστήρια. Ένας χρήστης μπορεί να χειρίζεται δεδομένα και υπηρεσίες που υπόκεινται σε νομοθεσία κρατών στα οποία δεν έχει πολιτικά δικαιώματα. Και εδώ εντοπίζεται ο ρόλος των εθνικών κυβερνήσεων που ασκούν έλεγχο μέσω της καθοριζόμενης από αυτές νομοθεσίας. Αποτέλεσμα αυτής της διαμάχης συμφερόντων και περιορισμών προερχόμενων από ανεξαρτήτους χρήστες, εμπορικές επιχειρήσεις και κυβερνήσεις είναι η δημιουργία μιας κατάστασης στον κυβερνοχώρο όπου μονοδιάστατες έννοιες όπως «έλεγχος» και «ελευθερία» αποκτούν νέα σημασία.

Παρότι συνηθέστερα ο κυβερνοχώρος και η κοινωνική κινητοποίηση που μπορεί αυτός να προκαλέσει συνδέεται με φιλελεύθερες δημοκρατικές αξίες, δεν πρέπει να παραβλεφθεί και η προς αντίθετους σκοπούς χρήση του. Επειδή μια τεχνολογία έχει εφευρεθεί για ένα σκοπό, δεν σημαίνει ότι δεν θα βρει άλλες χρήσεις απρόβλεπτες από τους δημιουργούς της. Αυτό ισχύει ιδιαίτερα στους τομείς της εγκληματικότητας, κατασκοπείας, και σε εμφύλιες συγκρούσεις, όπου δεν είναι υποχρεωμένη να ακολουθήσει κανόνες ή να σεβαστεί το κράτος δικαίου. Εγκληματικές ή παρασιτικές ενέργειες όπως η δημιουργία κακόβουλου λογισμικού (malware), δημιουργία σκοτεινών δικτύων για διάδοση μόνο πορνογραφικού ή εξτρεμιστικού περιεχομένου, αλλά και επιθέσεις πάσης φύσεως σε νόμιμες διαδικτυακές υπηρεσίες δεν είναι κάτι σπάνιο [18].

Η σύνδεση των νέων τεχνολογιών με κινήματα απελευθέρωσης εξετάζεται πάντα σε συνδυασμό με την ανάπτυξη πιο αποτελεσματικών μηχανισμών ελέγχου του κυβερνοχώρου. Οι σημερινές κυβερνήσεις διαθέτουν ένα πλήθος από τεχνικά ή μη τεχνικά μέσα για τον έλεγχο της ροής της πληροφορίας. Αν και τα πρώτα χρόνια της ραγδαίας ανάπτυξης του διαδικτύου τη δεκαετία του 1990, αυτό αντιμετωπίστηκε με ένα πιο ανοικτό φιλελεύθερο οικονομικό μοντέλο, σήμερα λόγω των συνεχώς αυξανόμενων κινδύνων που παρουσιάζονται σε αυτό, αναγνωρίζεται από κάποιους η ανάγκη ελέγχου και σε επίπεδο περιεχομένου. Όταν δικαιολογείται σε κάποιες βιομηχανικές φιλελεύθερες δημοκρατίες, όπως ο Καναδάς, η Γερμανία ή η Ιρλανδία, ο έλεγχος στο περιεχόμενο προκειμένου να υπάρχει συμμόρφωση με τους νόμους τους για θέματα όπως για παράδειγμα, αυτά της πνευματικής ιδιοκτησίας, είναι δύσκολο να αρνηθεί το ίδιο δικαίωμα κάποιος σε χώρες όπως η Λευκορωσία, η Τυνησία ή το Ουζμπεκιστάν, όταν θέτουν θέματα δημόσιας ασφάλειας και εθνικής κυριαρχίας [18].

Η προσπάθεια για έλεγχο του περιεχόμενου που διακινείται στο Διαδίκτυο συνδέεται άμεσα με θεμελιώδη δικαιώματα και βασικές ελευθερίες του ανθρώπου, όπως αυτά καθορίζονται από εθνικές νομοθεσίες αλλά και διεθνείς συμβάσεις και διακηρύξεις. Ο έλεγχος αυτός κάποιες φορές εφαρμόζεται με επιχείρημα και αποτέλεσμα, την προστασία αξιών όπως η πνευματική ιδιοκτησία ή η ευθύνη απέναντι στους ανήλικους. Κάποιες φορές όμως καταστρατηγεί άλλες αξίες όπως η ελευθερία της έκφρασης και το δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση των προσωπικών δεδομένων. Με δεδομένη την αποκεντρωμένη λογική της δομής του Διαδικτύου οποιαδήποτε προσπάθεια σε εθνικό η διεθνές επίπεδο για νομική κατοχύρωση του έλεγχου και του αποκλεισμού περιεχομένου, θα πρέπει να λαμβάνει υπόψη τις επιπτώσεις της και προς τι δυο διαφορετικές κατευθύνσεις. Σήμερα άλλωστε και λόγω της πολύ μεγάλης εξάπλωσης των διαδικτυακών υπηρεσιών ή ευαισθησία αλλά και η αποτελεσματικότητα αντίδρασης της παγκόσμιας κοινότητας είναι ιδιαίτερα αυξημένη. Είναι ευρύτερα αποδεκτή η

προστασία ηθικών και οικονομικών αξιών διεθνώς, αλλά χωρίς βασικούς περιορισμούς στη λειτουργία του μέσου που άλλαξε τον τρόπο με τον οποίο επικοινωνεί, επιχειρεί, δημιουργεί και συναλλάσετε, ο σύγχρονος άνθρωπος.

Κεφάλαιο 5

Διεθνής Εμπειρία - Γεωγραφία της Λογοκρισίας στο Διαδίκτυο

Υπάρχει μια πολύ ανομοιόμορφη κατανομή της τοπογραφίας της λογοκρισίας στο Διαδίκτυο παγκοσμίως, κάτι που αντανακλά τα διαφορετικά πολιτικά συστήματα, τα κυμαινόμενα ποσοστά διείσδυσης του, τις κοινωνικές, πολιτιστικές, και οικονομικές συνθήκες των διαφόρων κοινωνιών και το βαθμό της πολιτικής έντασης στις διάφορες γεωγραφικές περιοχές. Αυτή η πολυπλοκότητα σημαίνει ότι ο έλεγχος περιεχομένου στο Διαδίκτυο δεν προσφέρεται εύκολα για χαρακτηρισμούς βασισμένους σε συγκεκριμένα μοντέλα αλλά απαιτεί μια πιο λεπτομερή κατά περίπτωση ανάλυση. Το ανομοιογενές τοπίο της λογοκρισίας στο Διαδίκτυο αντανακλά την αλληλεπίδραση ανάμεσα στην ανάπτυξη του κυβερνοχώρου και τη μεγάλη ποικιλία από τις περιφερειακές, εθνικές και τοπικές πολιτικές και πολιτιστικές συνθήκες.

Οι αποφάσεις του κατά πόσον και πώς ρυθμίζεται η πρόσβαση στο Διαδίκτυο αντανακλά το συγκεντρωτισμό της πολιτικής εξουσίας, τη στάση των κοινωνιών απέναντι στη

διαφορετικότητα καθώς και τις όποιες γεωπολιτικές ανησυχίες, ιδιαίτερα για κράτη που επιδιώκουν να προσελκύσουν ξένες επενδύσεις. Για παράδειγμα χώρες που επιδιώκουν να προωθήσουν την ανάπτυξη του τομέα των σύγχρονων τεχνολογιών ή της παροχής διεθνών υπηρεσιών (π.χ. Μαλαισία), συμπεριλαμβανομένου και του τουρισμού, συχνά ανησυχούν ότι η λογοκρισία στο Διαδίκτυο μπορεί να αποτελέσει ανασταλτικό παράγοντα για αυτές τους τις προσπάθειες [90].

Η σύγκρουση αξιών έχει από καιρό αναγνωριστεί ως μείζον ζήτημα της πολιτικής ενημέρωσης. Η παγκοσμιοποιημένη φύση του Διαδικτύου και ο αποκεντρωμένος σχεδιασμός του ενισχύουν την πολυπλοκότητα της αντιπαράθεσης μετατοπίζοντας τη σε διεθνές πεδίο. Ο έλεγχος της πρόσβασης με βάση το περιεχόμενο που αφορά ουσιαστικά τη ρύθμιση της ροής των πληροφοριών σε ολόκληρο το Διαδίκτυο πρέπει να είναι συμβατός με τις κατά περίπτωση τοπικές προδιαγραφές και πρότυπα.

Το συμπέρασμα που προκύπτει από τις περισσότερες μελέτες είναι ότι το φιλτράρισμα του περιεχομένου αυξάνεται συνεχώς σε όλο τον κόσμο. Οι περισσότερες χώρες που εφαρμόζουν τέτοιες τεχνικές συνδέονται με λιγότερο ή περισσότερο αυταρχικά καθεστώτα, χωρίς όμως να αποκλείονται από αυτές τις επιλογές χώρες με ισχυρούς δημοκρατικούς θεσμούς.

Παραδοσιακά, τα κράτη υποστηρίζουν την κυριαρχία επί του εδάφους τους και του πληθυσμού τους. Πολλές φορές το Διαδίκτυο έρχεται να αμφισβητήσει αυτή την επικυριαρχία. Από την άλλη πλευρά, όταν μια χώρα φιλτράρει πακέτα πληροφοριών εντός των γεωγραφικών ορίων της, επηρεάζει τις επικοινωνίες των πολιτών όχι μόνο στο έδαφός της, αλλά δυνητικά σε όλο τον κόσμο [27].

5.1 Ευρώπη

Το Διαδίκτυο στην Ευρώπη ελέγχεται κατά κύριο λόγο μέσω ενός συνδυασμού ενεργειών των κυβερνήσεων και των εταιριών επικοινωνιών και πληροφορικής (ΤΠΕ - ICT). Οι διάφορες ευρωπαϊκές χώρες, ανεξάρτητα του αν είναι μέλη της Ευρωπαϊκής Ένωσης ή όχι, επεμβαίνουν σε μικρότερο ή μεγαλύτερο βαθμό στη λειτουργία του Διαδικτύου, αποκλείοντας δυσφημιστικά κείμενα ή υλικό που σχετίζεται με παραβίαση πνευματικών δικαιωμάτων. Εν τω μεταξύ, οι επιχειρήσεις ΤΠΕ έχουν αναλάβει οι ίδιες να λογοκρίνουν την παιδική πορνογραφία και τη ρητορική μίσους. Ωστόσο σε αντίθεση με άλλα μέρη του κόσμου, το Διαδίκτυο στην Ευρώπη

ρυθμίζεται σε ένα μεγάλο βαθμό μέσα από τη συντονισμένη δράση των κρατών, συνήθως μέσα από τις διαδικασίες της Ευρωπαϊκής Ένωσης (ΕΕ). Καθώς οι ευρωπαϊκές κυβερνήσεις επιθυμούν την εναρμόνιση των νόμων τους που σχετίζονται με το κυβερνοχώρο, στρέφονται όλο και περισσότερο προς την ΕΕ για να αποφασίσει τα κριτήρια και τη μέθοδο του ελέγχου στο Διαδίκτυο [19].

Αν και γενικά οι ευρωπαϊκές χώρες είναι σχετικά «ανοικτές» σε θέματα πρόσβασης στο Διαδίκτυο, υπάρχουν αρκετές κυβερνητικά καθοδηγούμενες προσπάθειες περιορισμού του κυβερνοχώρου. Συνήθως η λογοκρισία σε οικονομικά ανεπτυγμένα κράτη εστιάζει σε θέματα κοινωνικού ενδιαφέροντος, όπως η πορνογραφία, ή η πνευματική ιδιοκτησία παρά σε θέματα που άπτονται πολιτικών διαφορών. Πολλές προσπάθειες για λογοκρισία έχουν αποτύχει λόγω της αρνητικής στάσης πολλών παρόχων υπηρεσιών Διαδικτύου αλλά και εξαιτίας των παραβιάσεων που προκαλούν στην ιδιωτική ζωή. Άλλες καταστάσεις που περιορίζουν τις όποιες προθέσεις των κυβερνήσεων να επιβάλλουν ελέγχους, είναι φυσικά οι κοινωνικές αντιδράσεις και διαμαρτυρίες καθώς και η οικονομική διάσταση της διακίνησης των πληροφοριών στο Διαδίκτυο. Το Ευρωπαϊκό Κοινοβούλιο αναγνωρίζει από το 2008 την λογοκρισία ως εμπόδιο για τις ελεύθερες εμπορικές συναλλαγές [90].

Το πρόγραμμα Safer Internet (Ασφαλέστερο Διαδίκτυο), που είναι η διάδοχη κατάσταση των Action Plan for Safer Internet (1999-2004) και SaferInternet Plus (2005-2009), υιοθετήθηκε από την Ευρωπαϊκή Ένωση αποσκοπώντας στην προστασία μειονοτήτων και αφορά ιδιαίτερα υλικό σεξουαλικής κακοποίησης παιδιών και εκφοβισμού στον κυβερνοχώρο. Με κόστος από το 2009 έως σήμερα περίπου 55 εκατομμύρια ευρώ, ενεργοποιεί τεχνολογίες παρακολούθησης παιδικής πορνογραφίας βοηθώντας την ευρωπαϊκή αστυνομία [50].

Στα πλαίσια των παραπάνω προγραμμάτων γίνετε διάκριση μεταξύ παράνομου και βλαβερού περιεχομένου και οι δύο αυτοί τύποι περιεχομένου αντιμετωπίζονται διαφορετικά:

- το παράνομο περιεχόμενο πρέπει να αντιμετωπίζεται στην πηγή από τις αστυνομικές και δικαστικές αρχές, οι δραστηριότητες των οποίων καλύπτονται από τους κανόνες της εθνικής νομοθεσίας και τις συμφωνίες δικαστικής συνεργασίας. Η βιομηχανία πάντως μπορεί να προσφέρει σημαντική βοήθεια για τη μείωση της κυκλοφορίας παράνομου περιεχομένου (ιδιαίτερα περιεχομένου σχετικού με παιδική πορνογραφία, ρατσισμό και αντισημιτισμό) μέσω της θέσπισης αποτελεσματικών μηχανισμών αυτορρύθμισης (όπως οι κώδικες καλής συμπεριφοράς και η δημιουργία ανοικτών τηλεφωνικών

γραμμών), που θα διέπονται και θα υποστηρίζονται από νομικές διατάξεις και θα έχουν την υποστήριξη των καταναλωτών.

- το βλαβερό περιεχόμενο είναι το επιτρεπόμενο περιεχόμενο, αλλά του οποίου συγχρόνως η διάδοση είναι περιορισμένη (για παράδειγμα, απευθύνεται στους ενήλικους) και το οποίο μπορεί να θίξει ορισμένους χρήστες, ακόμη και αν η διάδοσή του δεν είναι περιορισμένη, βάσει της αρχής της ελευθερίας της έκφρασης. Για την αντιμετώπιση του βλαβερού περιεχομένου οι δράσεις προτεραιότητας θα πρέπει να είναι η παροχή στους χρήστες της δυνατότητας να αρνούνται το βλαβερό περιεχόμενο με την ανάπτυξη τεχνολογικών λύσεων (συστήματα φιλτραρίσματος και διαβάθμισης περιεχομένου), η αύξηση της ευαισθητοποίησης των γονέων και η ανάπτυξη της αυτορρύθμισης η οποία μπορεί να προσφέρει ένα επαρκές πλαίσιο, ιδιαίτερα για την προστασία των ανηλίκων.

Το μεγαλύτερο τμήμα της ισχύουσας νομοθεσία της ΕΕ σχετικά με το φιλτράρισμα επικαλύπτεται με τις υφιστάμενες πολιτικές των επιμέρους κρατών. Στα θέματα της παιδικής πορνογραφίας, της εμπορίας ανθρώπων, της τρομοκρατικής προπαγάνδας, και της απάτης, υπάρχει μια ευρεία συναίνεση για την παρακολούθηση και τον αποκλεισμό του σχετικού υλικού. Παραδόξως, δεν υπάρχει τέτοια συναίνεση για το ποιος θα πρέπει να θεωρηθεί υπεύθυνος για το εν λόγω υλικό. Οι περισσότερες χώρες έχουν συμφωνήσει για τη αντιμετώπιση των Παρόχων Υπηρεσιών Διαδικτύου ως απλών δίαυλων πληροφοριών, ωστόσο, κάποιες άλλες θεωρούν τους εν λόγω οργανισμούς υπεύθυνους για το παραβατικό υλικό [19].

Παρά την έλλειψη ισχυρών κανονισμών σε επίπεδο ΕΕ, πολλά κράτη μέλη έχουν λάβει μέτρα τοπικά για να φιλτράρουν το ανεπιθύμητο περιεχόμενο. Πολλές χώρες, όπως το Ηνωμένο Βασίλειο, οι Σκανδιναβικές χώρες, η Γερμανία και η Ιταλία αποκλείουν αυστηρά την παιδική πορνογραφία, ενώ ορισμένες κυβερνήσεις (π.χ., Ηνωμένο Βασίλειο, Γαλλία) πιέζουν τους παρόχους για την αποφυγή παραβιάσεων δικαιωμάτων πνευματικής ιδιοκτησίας μέσω του φιλτραρίσματος [19].

Οι χώρες της Νότιας Ευρώπης εμφανίζουν γενικά μικρότερη ανοχή στην ελευθερία στο Διαδίκτυο από ότι αυτές στα βόρεια. Στην Ιταλία, το Βατικανό ζήτησε περιορισμό του διαδικτυακού «ριζοσπαστικού φιλελευθερισμού» και η ιταλική κυβέρνηση έχει κλείσει ιστοσελίδες που ασκούσαν κριτική στον καθολικισμό. Η κυβέρνηση επίσης προσπάθησε να

αναγκάσει τους ISP να αποκλείσουν ιστοσελίδες που υπερασπίζονται ηθικούς αυτουργός εγκλημάτων ή προβάλουν θετικά τη μαφία [90].

Συμπερασματικά μπορεί να διατυπωθεί, ότι σήμερα το περιεχόμενο του Διαδικτύου στην Ευρώπη ελέγχεται από τρείς ομάδες παραγόντων, αυτές που κινούνται σε ευρύτερο ευρωπαϊκό επίπεδο (ΕΕ), τα ανεξάρτητα κράτη, και τις εταιρίες (πχ παρόχους και μηχανές αναζήτησης). Ενώ οι κυβερνήσεις είναι εξαιρετικά δραστήριες στην προώθηση τεχνολογιών φιλτραρίσματος κατά της παιδικής πορνογραφίας και της παραβίασης πνευματικών δικαιωμάτων, διαπιστώνουν όλο και περισσότερο ότι μπορούν να επιτύχουν τους στόχους τους με έμμεσο τρόπο. Προωθώντας ρητές διατάξεις, οι κυβερνήσεις πιέζουν τις επιχειρήσεις σε «οικειοθελή» αυτορρύθμιση του περιεχομένου, είτε πρόκειται για πορνογραφία ή ρητορική μίσους ή περιεχόμενο που παραβιάζει πνευματικά δικαιώματα.

Σε επίπεδο ΕΕ, τα κράτη εργάζονται προς την ομογενοποίηση των κανονισμών στο Διαδίκτυο, ειδικά όσο αφορά το πορνογραφικό και δυσφημιστικό περιεχόμενο. Δεδομένων των πολιτιστικών διαφορών μεταξύ των χωρών και των υπαρχόντων νομικών πλαισίων, η δημιουργία μια κοινής αναφοράς είναι μια πολύπλοκη διαδικασία [19].

5.1.1 Ηνωμένο Βασίλειο

Το Ηνωμένο Βασίλειο έχει μια αξιοσημείωτη φιλελεύθερη παράδοση που εκδηλώνεται μεταξύ άλλων, με εγγυήσεις για την ελευθερία της έκφρασης, την ελευθερία της πληροφόρησης και την προστασία της ιδιωτικής ζωής. Η ελευθερία της έκφρασης και η προστασία της ιδιωτικής ζωής στο Διαδίκτυο είναι εγγυημένη από το νόμο. Παρ 'όλα αυτά, τα τελευταία χρόνια έχει υπάρξει μια στροφή προς την αύξηση της επιτήρησης και των μέτρων αστυνόμευσης. Η καταπολέμηση της τρομοκρατίας και η πρόληψη της παιδικής κακοποίησης έχουν ευρέως χρησιμοποιηθεί ως αφορμή ή δικαιολογία από τους κρατικούς φορείς και τις ιδιωτικές εμπορικές εταιρίες Παροχής Υπηρεσιών Διαδικτύου για την εφαρμογή επόπτευσης και αποκλεισμού περιεχομένου. Παρ 'όλα αυτά, το 2010 η πρωτοβουλία OpenNet δεν βρήκε κανένα αποδεικτικό στοιχείο εφαρμογής φιλτραρίσματος σε επίπεδο πολιτικό, κοινωνικό ή δημόσιας ασφάλειας [19]. Ωστόσο, το Ηνωμένο Βασίλειο ανοιχτά αποκλείει ιστοσελίδες παιδικής πορνογραφίας, για την οποία το ONI δεν πραγματοποιεί ελέγχους [66].

Ένας βασικός πάροχος, η British Telecom εισήγαγε την υπηρεσία Cleanfeed η οποία σε αιτήματα ιστοσελίδων που σχετίζεται με εκμετάλλευση ανηλίκων επιστρέφει μήνυμα σφάλματος χωρίς να

προσδιορίζει την αιτία. Τον Ιούλιο και τον Οκτώβριο του 2011, το Ανώτατο Δικαστήριο της χώρας, έκρινε ότι η British Telecom πρέπει να μπλοκάρει την πρόσβαση σε συγκεκριμένη ιστοσελίδα (την newzbin.com), η οποία «παρέχει συνδέσεις για πρόσβαση σε πειρατικές ταινίες. Τον Σεπτέμβριο του 2011, οι πάροχοι με έκδοση δικαστικής απόφασης και με ενθάρρυνση από την κυβέρνηση, ανακοινώνουν ιδιωτικές συμφωνίες για περιορισμό πρόσβασης σε ιστοσελίδες, όταν αυτό υποστηρίζεται από δικαστικές αποφάσεις. Τον Μάιο του 2012, το Ανώτατο Δικαστήριο διέταξε Βρετανικούς ISP να μπλοκάρουν το Pirate Bay προκειμένου να εμποδίσουν περεταίρω παραβίαση δικαιωμάτων πνευματικής ιδιοκτησίας [66].

5.1.2 Γερμανία

Η πρώτη προσπάθεια διαδικτυακής λογοκρισίας στη Γερμανία έγινε το 1996. Επιβλήθηκε στους παρόχους υπηρεσιών να εμποδίσουν την πρόσβαση σε περιεχόμενο που είναι εκτός της δικαιοδοσίας του γερμανικού κράτους και περιέχει υλικό που κρίνεται παράνομο βάσει του γερμανικού δικαίου, όπως περιεχόμενο παιδικής πορνογραφίας, ρατσιστικού υλικού, αντισημιτικό περιεχόμενο κλπ. Η προσπάθεια αυτή δεν ήταν τόσο επιτυχής όσο η κυβέρνηση θα ήθελε, μια που αντιμετώπισε πολλές νομικές διαμάχες, επειδή οι περισσότεροι από τους παρόχους δεν ήταν στην Γερμανία και ως εκ τούτου δεν είχαν υποχρέωση να συμμορφωθούν με τη γερμανική νομοθεσία [77].

Ο έλεγχος περιεχομένου στη Γερμανία καθορίζεται από νομικά πλαίσια, μια που πολλές φορές η κυβέρνηση μπορεί να λογοκρίνει μόνο με δικαστική απόφαση. Θεματικές περιοχές οι οποίες συνήθως νόμιμα υπόκεινται σε φιλτράρισμα είναι εγκληματικές πράξεις, η άρνηση του ολοκαυτώματος, κλπ. Τον Ιούνιο του 2009 η Γερμανία εισήγαγε για πρώτη φορά νόμο που επιτρέπει τον αποκλεισμό ιστοσελίδων που διανέμουν παιδική πορνογραφία. Η κατάσταση αντιμετωπίστηκε με μεγάλη καθυστέρηση από το γερμανικό κοινοβούλιο, κυρίως λόγω των παραβιάσεων που μπορεί να προκύψουν σε θέματα ελευθερίας του λόγου. Τα μέτρα που ακολούθησαν ήταν αρκετά έντονα μια που ο νόμος επέτρεπε και πέτυχε τη διακοπή της λειτουργίας εξυπηρετητών με σχετικό υλικό [11].

5.1.3 Γαλλία

Η λογοκρισία στην Γαλλία παρουσιάζει ανάλογο προφίλ με αυτό της Γερμανίας μια που ο νόμος επιτρέπει τον αποκλεισμό περιεχομένου που σχετίζεται με παιδική πορνογραφία, άρνηση του

ολοκαυτώματος, τρομοκρατία κτλ. Τα τελευταία χρονιά ο έλεγχος επεκτείνεται και εντείνεται σε περιοχές που αφορούν κυρίως θέματα πνευματικής ιδιοκτησίας [77].

Στις 10 Φεβρουαρίου του 2011 δικαστήριο του Παρισιού (TGI) διέταξε τον αποκλεισμό του ιστότοπου Copwatch (copwatchnord-idf.eu.org) που δημοσιοποιούσε προσωπικά στοιχεία αστυνομικών θέτοντας τους σε κίνδυνο. Παρόλα αυτά το δικαστήριο αρνήθηκε το αίτημα του υπουργού Εσωτερικών για αποκλεισμό και των ιστότοπων που αναπαρήγαν το περιεχόμενο της συγκεκριμένης ιστοσελίδας [80].

5.1.4 Σκανδιναβικές Χώρες

Η Σουηδία, η Φιλανδία, η Δανία η Νορβηγία και η Ισλανδία, με δεδομένο ότι θεωρούνται πρωτοπόρες σε θέματα επικοινωνιών, πληροφορικής και γενικότερα σύγχρονων τεχνολογιών, είναι σημαντικοί παράγοντες και στη διαδικασία διαμόρφωσης ενός διεθνούς πλαισίου για τον έλεγχο στο Διαδίκτυο. Σε όλες τις χώρες εφαρμόζεται νομικά κατοχυρωμένος αποκλεισμός περιεχομένου που σχετίζεται με παιδική πορνογραφία, ενώ υπάρχει σημαντική παράδοση στην προστασία ατομικών ελευθεριών, όπως αυτό της ελεύθερης έκφρασης και πολιτικών δικαιωμάτων [77]. Παρόλα αυτά σε απόρρητες «μαύρες» λίστες αποκλεισμένων ιστοσελίδων με περιεχόμενο παιδικής πορνογραφίας που έχουν διαρρεύσει, έχουν εντοπιστεί και ιστοσελίδες με άσχετο με αυτήν περιεχόμενο. Για παράδειγμα παρατηρήθηκε ότι όταν ο hacker Matti Nikki's άσκησε κριτική στην Φιλανδική κυβέρνηση για θέματα πιθανής λογοκρισίας, ο ιστότοπος του συμπεριλήφθητε στην σχετική με πορνογραφικό περιεχόμενο λίστα χωρίς να περιέχει ανάλογο υλικό [90]. Η Σκανδιναβική χώρα που, κατά καιρούς, εφαρμόζει την πιο έντονη προσχηματική λογοκρισία με την χρήση λιστών είναι η Δανία [19].

Στις χώρες αυτές είναι ιδιαίτερα ανεπτυγμένη η επικοινωνία με διαμοιρασμό αρχείων μέσω ομότιμων δικτύων, όπως για παράδειγμα μέσω torrent. Η Σουηδία άλλωστε αποτελεί την πατρίδα του Pirate bay, γνωστού ιστότοπου, που συμβάλει στο διαμοιρασμό αρχείων με περιεχόμενο το οποίο συνδέεται με δικαιώματα πνευματικής ιδιοκτησίας. Η ευαισθησία σε θέματα προστασίας πνευματικών δικαιωμάτων είναι ιδιαίτερα ανεπτυγμένη και γίνεται συνεχώς μια συζήτηση και μια προσπάθεια για πληρέστερη νομική κατοχύρωση της. Η Δανία αποκλείει συστηματικά το Pirate bay. Από την άλλα πλευρά εγείρονται ιδιαίτερες διαμαρτυρίες, συνήθως από ακτιβιστές, που σχετίζονται με την ελευθερία της έκφρασης, οι οποίες έχουν οδηγήσει ακόμη και στη δημιουργία πολιτικών κομμάτων, όπως αυτό των «Πειρατών» στη Σουηδία [96].

5.1.5 Ρωσία – Ουκρανία – Λευκορωσία

Στις χώρες της πρώην Σοβιετικής Ένωσης, αντίθετα με τις Σκανδιναβικές, παρουσιάζονται συχνά φαινόμενα έλλειψης διαφάνειας, παραβίασης ανθρωπίνων δικαιωμάτων και χειραγώγησης των μέσων μαζικής ενημέρωσης. Τα τελευταία χρόνια με την παράλληλη βελτίωση των τεχνικών πρόσβασης στο διαδίκτυο και την αύξηση της διείσδυσης του πληθυσμού σε αυτό, παρατηρείται έντονη αύξηση των προσπαθειών ελέγχου του περιεχομένου του, αλλά και αντιδράσεων και διαμαρτυριών για αυτό τον έλεγχο [90].

Στη Ρωσία των κυβερνήσεων Πούτιν, ταυτόχρονα με τον έλεγχο των μέσων ενημέρωσης επιχειρείται η εγκαθίδρυση ενός μηχανισμού ελέγχου του Διαδικτύου, στα πρότυπα της Κίνας, με πρόσχημα πάντα την προστασία από τη διαφθορά. Ο νόμος για την επιτήρηση του Διαδικτύου στη Ρωσία επιτρέπει στις υπηρεσίες ασφαλείας να επεμβαίνουν στους παρόχους και να ζητούν από αυτούς αποκλεισμό υλικού ή στατιστικά στοιχεία για τη διασύνδεση των χρηστών. Στις λίστες του αποκλεισμένου περιεχόμενου συμπεριλαμβάνονται συχνά ιστολόγια και τόποι κοινωνικής δικτύωσης [66].

Στην Ουκρανία παρά τη σχετική ελευθερία πρόσβασης ο μεγαλύτερος πάροχος, η Ukrtelecom, ασκεί έλεγχο στο Διαδίκτυο έπειτα από κυβερνητικές πιέσεις και με πρόσχημα πάντα την εθνική ασφάλεια έναντι των τρομοκρατών [90].

Στη Λευκορωσία, τη κυβέρνηση της οποίας ο διεθνής οργανισμός «Δημοσιογράφοι χωρίς σύνορα», αποκαλεί έναν από τους μεγαλύτερους εχθρούς του Διαδικτύου, ο πρόεδρος Λουκοσένκο ισχυρίζεται ότι θα βάλει τέλος στην αναρχία που επικρατεί στο Διαδίκτυο αποτρέποντας τη μετατροπή του από σημαντικό τεχνολογικό επίτευγμα σε «υπόνομο» ειδήσεων [80]. Για όλους τους ISP της Λευκορωσίας απαιτείται να γίνεται σύνδεση μέσω της Belpak, μιας θυγατρικής του η υπό κρατικό έλεγχο παρόχου Beltelecom. Κατά τη διάρκεια των προεδρικών εκλογών του 2006 η κυβέρνηση επιχείρησε συντονισμένες κυβερνοεπιθέσεις εναντίον διαδικτυακών τόπων κομμάτων της αντιπολίτευσης, με αποτέλεσμα να υποφέρουν από συχνές μυστηριώδης αποσυνδέσεις.

5.1.6 Τουρκία

Παρά το γεγονός ότι υπάρχει αύξηση στην πρόσβαση στο Διαδίκτυο, ιδιαίτερα με ασύρματα μέσα, πολλές περιοχές της Τουρκίας εξακολουθούν να υπολείπονται σε υποδομές. Σε κάθε

περίπτωση πάντως υπάρχει εκτεταμένη εφαρμογή της λογοκρισίας. Ο έλεγχος του περιεχομένου στην Τουρκία αποσκοπεί στην προστασία παραδοσιακών αξιών, σύμφωνα με την στενή τοπική αντίληψη, όπως της οικογένειας, ιδίως όσον αφορά την προστασία έναντι στην πορνογραφία. Όπως και σε πολλές άλλες χώρες, το πραγματικό πεδίο εφαρμογής της λογοκρισίας είναι ευρύτερο με αποτέλεσμα να αποκλείονται διαφόρων τύπων πληροφορίες. Οι ιστοσελίδες με αρνητικές πληροφορίες σχετικά με τον Μουσταφά Κεμάλ Ατατούρκ είναι αποκλεισμένες.

Η Τουρκία χρησιμοποιεί ένα συγκεντρωτικό σύστημα φιλτραρίσματος με σαφή έλλειψη διαφάνειας όσον αφορά τις ιστοσελίδες που αποκλείονται. Αν και αρχικά δεν υπήρχε καμία επίσημη νομοθεσία σχετικά με τον έλεγχο και την επιτήρηση περιεχόμενου στον Παγκόσμιο Ιστό, υπάρχουν κινήσεις προς αυτή την κατεύθυνση. Κατά τη διάρκεια μεγάλης κλίμακας διαδηλώσεων κατά των εθνικής πολιτικής φιλτραρίσματος του Διαδικτύου ελήφθησαν μέτρα για να αποτραπούν επιθέσεις σε κυβερνητικές ιστοσελίδες.

Η αυξητική τάση στον έλεγχο στην πρόσβαση με βάση το περιεχόμενο φαίνεται και από την τακτική της κυβέρνησης ενάντια σε οργανώσεις και δράσεις που αντιτίθενται στον έλεγχο του κυβερνοχώρου. Σε κάθε περίπτωση και στα θετικά όσο αφορά τους ελεγχόμενους, είναι η ύπαρξη δυνατοτήτων παράκαμψης των ελεγκτικών μηχανισμών οι οποίοι συχνά χρησιμοποιούνται αποτελεσματικά [08].

5.1.7 Ελλάδα

Σε μια απόφαση σταθμό για την Ελλάδα, το Μονομελές Πρωτοδικείο Αθηνών διέταξε τη λήψη τεχνολογικών μέτρων για την παρεμπόδιση της πρόσβασης χρηστών σε ιστοσελίδες. Συγκεκριμένα για πρώτη φορά στη χώρα μας διατάχθηκε η λήψη τεχνολογικών μέτρων παρεμπόδισης της πρόσβασης χρηστών σε ιστοσελίδες μέσω των οποίων διακινούνται παράνομα ψηφιακά έργα προστατευόμενα με δικαίωμα πνευματικής ιδιοκτησίας.

Στις 16 Μαΐου 2012 δημοσιεύθηκε η απόφαση 4658/2012 του Μονομελούς Πρωτοδικείου Αθηνών, η οποία έκανε δεκτό αίτημα οργανισμών συλλογικής διαχείρισης δικαιωμάτων επί μουσικών και οπτικοακουστικών έργων, σύμφωνα με το οποίο οι ελληνικές εταιρίες παροχής υπηρεσιών σύνδεσης στο Διαδίκτυο (ISP) υποχρεώνονται εκτός άλλων να λάβουν τεχνολογικά μέτρα προκειμένου να καταστεί αδύνατη η πρόσβαση των συνδρομητών τους σε διαδικτυακές τοποθεσίες μέσω των οποίων πραγματοποιείται παράνομη παρουσίαση και ανταλλαγή έργων. Η απόφαση εφαρμόζει για πρώτη το άρθρο 64 Α του ν. 2121/1993 που ενσωματώνει πρόβλεψη

Οδηγίας της Ευρωπαϊκής Ένωσης για τη δυνατότητα λήψης ασφαλιστικών μέτρων κατά των διαμεσολαβητών (παρόχων υπηρεσιών διαδικτύου), οι υπηρεσίες των οποίων χρησιμοποιούνται από τρίτο για την προσβολή του δικαιώματος του δημιουργού ή συγγενικού δικαιώματος.

Παρόμοιες αποφάσεις έχουν ήδη εκδοθεί σε άλλα κράτη μέλη της Ευρωπαϊκής Ένωσης όπως για παράδειγμα στο Ηνωμένο Βασίλειο και την Ολλανδία. Η απόφαση αφορά τα site ellinadiko.com και music-Bazzar.com και θα γίνεται με δύο τρόπους:

1. Εφαρμογή κατάλληλων φίλτρων στους δρομολογητές (routers) των ISPs ώστε να αποκλειστεί οποιαδήποτε κίνηση καταλήγει σε συγκεκριμένη IP.

2. Εφαρμογή κατάλληλης ανακατεύθυνσης, μέσω τροποποίησης των DNS εγγραφών στους name servers του κάθε ISP ώστε τα αιτήματα προς συγκεκριμένα Domains να καταλήγουν σε διαφορετικούς ιστότοπους.

Ήδη πάντως, το Κόμμα Πειρατών Ελλάδας με δελτίο Τύπου, πέρα από την καταδίκη της απόφασης, τόνισε ότι είναι έτοιμο να εφαρμόσει κάθε νόμιμο τεχνολογικό μέτρο ώστε να διασφαλιστεί η ελευθερία της επικοινωνίας, του λόγου και της ανταλλαγής ιδεών στο Διαδίκτυο αλλά και στην κοινωνία. Στο ίδιο κείμενο αναφέρει επίσης ότι έχει θέση σε λειτουργία σύστημα ανακατεύθυνσης για την παράκαμψη του αποκλεισμού του Pirate Bay από τους Ολλανδικούς παρόχους (ISPs), σε συνεργασία με το κόμμα των Ολλανδών Πειρατών. Επισημαίνεται πάντως ότι η πιθανή εφαρμογή τεχνολογικών μέτρων από μέρους του Κόμματος Πειρατών δεν θα προσβάλλει τα συγκεκριμένα ασφαλιστικά μέτρα, τα οποία αφορούν την παρεμπόδιση πρόσβασης από μέρους των παρόχων (ISPs) και όχι απαγόρευση επίσκεψης στις συγκεκριμένες ιστοσελίδες. Το δελτίο Τύπου διευκρινίζει επίσης ότι το κόμμα δεν υποστηρίζει παράνομες ενέργειες, αλλά θεωρεί πιο σημαντικό το δικαίωμα πρόσβασης στην κοινωνία της πληροφορίας όπως αναφέρεται στο Σύνταγμα [52].

5.2 Βόρεια Αμερική

Το Διαδίκτυο στις Ηνωμένες Πολιτείες και τον Καναδά υπόκειται σε αυστηρές ρυθμίσεις, που υποστηρίζονται από ένα πολύπλοκο σύνολο νομικών δεσμεύσεων και ιδιωτικών μηχανισμών μεσολάβησης. Η τεχνική του φιλτραρίσματος παίζει μικρό ρόλο σε αυτήν την διαδικασία. Το

πρώτο κύμα των ρυθμιστικών δράσεων προέκυψε στη δεκαετία του 1990 στις Ηνωμένες Πολιτείες ως απάντηση στην εύκολη πρόσβαση των ανηλίκων, σε πληθώρα σκληρού σεξουαλικά υλικού. Από εκείνη τη στιγμή, αρκετές νομοθετικές προσπάθειες για τη δημιουργία ενός υποχρεωτικού συστήματος ελέγχου περιεχομένου στις Ηνωμένες Πολιτείες έχουν αποτύχει να καταλήξουν σε συνολική λύση για όσους πιέζουν για πιο αυστηρούς ελέγχους. Την ίδια στιγμή που γίνονται νομοθετικές προσπάθειες για τον έλεγχο της διανομής κοινωνικά απαράδεκτου υλικού, έχει δημιουργηθεί ένα ισχυρό σύστημα που περιορίζει την ευθύνη των μεσαζόντων του περιεχομένου στο Διαδίκτυο, όπως οι Πάροχοι Υπηρεσιών Διαδικτύου και εταιρείες που φιλοξενούν το περιεχόμενο. Οι υποστηρικτές της προστασίας της πνευματικής ιδιοκτησίας κατάφεραν να επιβάλλουν ένα σύστημα για την απομάκρυνση υλικού που τη παραβιάζει, αν και πολλοί ισχυρίζονται ότι αυτό περιορίζει την ελευθερία της έκφρασης [19].

Ο δημόσιος διάλογος, η νομοθετική συζήτηση και ο δικαστικός έλεγχος έχουν παράγει στρατηγικές φιλτραρίσματος στις Ηνωμένες Πολιτείες και στον Καναδά που είναι διαφορετικές από εκείνες που συνηθίζονται αλλού. Στις Ηνωμένες Πολιτείες, πολλές φορές η κυβέρνηση όταν επιχειρεί να ρυθμίσει το περιεχόμενο συναντά νομικές δυσκολίες για αυτό και επιλέγει πιο έμμεσες μεθόδους. Στον Καναδά έχει δοθεί βάρος σε μια υποβοηθούμενη από την κυβέρνηση αυτορρύθμιση της βιομηχανίας των επικοινωνιών. Με εξαίρεση τη παιδική πορνογραφία, στον Καναδά και τις ΗΠΑ οι περιορισμοί του περιεχομένου τείνουν να βασίζονται περισσότερο στην αφαίρεση του παρά στον αποκλεισμό του. Αρκετά συχνά οι έλεγχοι βασίζονται στη συμμετοχή ιδιωτών με κρατική ενθάρρυνση ή νομική απειλή. Σε αντίθεση με πολλά μέρη του κόσμου όπου ISP υπόκεινται σε κυβερνητικές μεθοδεύσεις, το μεγαλύτερο μέρος του ελέγχου του περιεχομένου σε αυτές τις χώρες συμβαίνει σε ιδιωτικό επίπεδο [19].

5.2.1 Ηνωμένες Πολιτείες Αμερικής

Παρά το γεγονός ότι οι Η.Π.Α. συχνά αυτοπροβάλλονται ως υπόδειγμα δημοκρατίας, και η λογοκρισία στη χώρα αυτή είναι ελάχιστη και εκεί η πολιτεία παρεμβαίνει κατά καιρούς προσπαθώντας να διαμορφώσει τη πρόσβαση στο Διαδίκτυο. Αν και οι πρώτες προσπάθειες για τη ρύθμιση του κυβερνοχώρου οδήγησαν σε μια πολιτισμική διαμάχη ανάμεσα σε φιλελεύθερους και συντηρητικούς, οι πιο πρόσφατες προσπάθειες ήταν σαφέστερα πιο γόνιμες.

Η πρώτη σημαντική περίπτωση αμερικανικής λογοκρισίας στο διαδίκτυο, η οποία σχετίζεται με το νόμο για την Ευπρέπεια στις Επικοινωνίες (CDA), ψηφίστηκε από το Κογκρέσο το 1996, σε μια προσπάθεια να περιορίσει την πρόσβαση των παιδιών στην πορνογραφία (με ευρεία έννοια

ορισμένη) στο Διαδίκτυο και ήταν καθοδηγούμενη από το σκεπτικό διαφόρων Χριστιανικών οργανώσεων. Η αντίσταση στο CDA ήταν έντονη, και συμπεριλάμβανε αγωγές από ένα συνασπισμού παρόχων, με αποτέλεσμα το 1997 το Ανώτατο Δικαστήριο να ανατρέψει το νόμο.

Στις πιο πρόσφατες προσπάθειες της κυβερνητικής λογοκρισίας του διαδικτύου στην Αμερική συμμετέχουν ιδιωτικοί φορείς μεσολάβησης. Έτσι, με οδηγίες του Κογκρέσου τα δημόσια σχολεία και οι βιβλιοθήκες εγκατέστησαν λογισμικό φιλτραρίσματος και οι ISP καθίστανται υπεύθυνοι για πιθανή πρόσβαση σε παιδική πορνογραφία. Σε αυτήν την περίπτωση, η λογοκρισία αντιμετωπίζεται σαν ένα μέσο ελέγχου αρνητικών εξωτερικών και ανεξέλεγκτων από τους κοινούς χρήστες, παραγόντων, όπως η διαδικτυακή εγκληματικότητα και η πορνογραφία. Το Κογκρέσο επίσης, παρέχει κίνητρα στους ISP προκειμένου να μπλοκάρουν την πρόσβαση σε ιστοσελίδες που παραβιάζουν δικαιώματα πνευματικής ιδιοκτησίας. Σύμφωνα με το νόμο Patriot, το Ομοσπονδιακό Γραφείο Ερευνών δημιουργεί το πρόγραμμα του «καλά συνεργαζόμενου πολίτη», το οποίο ενθαρρύνει τους ISP να λογοκρίνουν ιστοσελίδες που δεν συνάδουν με το δημόσιο συμφέρον και να παραδίδουν πληροφορίες σχετικά με τους χρήστες των οποίων η ηλεκτρονική αλληλογραφία μπορεί να χαρακτηριστεί ύποπτη. Η διακυβέρνηση του Τζορτζ Μπους θεσπίζει νομοθεσία ενθάρρυνσης των εταιρειών τηλεπικοινωνιών να συμμετάσχουν σε τεχνολογίες εξόρυξης δεδομένων για την καταπολέμηση της τρομοκρατίας. Οι Ηνωμένες Πολιτείες αν και υστερούν σε θέματα επιτήρησης του Διαδικτύου, είναι ένα από τα πιο επιθετικά κράτη του κόσμου όσον αφορά την παρακολούθηση των απευθείας συνομιλιών. Με εκκίνηση θέματα παραβίασης πνευματικών δικαιωμάτων ή παιδικής πορνογραφίας που αποτελούν άλλωστε θεμιτές ανησυχίες στο θέμα αυτό, εφαρμόζονται περιορισμοί και στην πολιτική πληροφόρηση.

Η περίπτωση των Wikileaks, όπου το 2010, 250.000 περίπου μυστικά διπλωματικά τηλεγραφήματα του υπουργείου Εξωτερικών των ΗΠΑ διέρρευσαν, με προοπτική να δημοσιοποιηθούν στο Διαδίκτυο, προσφέρει μια καλή ευκαιρία αξιολόγησης της πολιτικής στον κυβερνοχώρο. Η υπόθεση αναδεικνύει την γεωπολιτική διάσταση του Διαδικτύου καθώς και τα πλεονεκτήματα, τους περιορισμούς και τα μειονεκτήματα του κυβερνο-ακτιβισμού [90].

5.2.2 Καναδάς

Η καναδική νομοθεσία δεν αναγνωρίζει δικαιοδοσία αποκλεισμού περιεχομένου, ιδιαίτερα αν αυτό φιλοξενείται έξω από τα όρια της χώρας. Από το Νοέμβριο του 2006, οι κυριότεροι πάροχοι Διαδικτύου στον Καναδά αποφάσισαν τον περιορισμό της πρόσβασης σε εκατοντάδες

ιστοσελίδες παιδικής πορνογραφίας. Η λίστα των αποκλεισμένων ιστότοπων καταρτίζεται από εκθέσεις χρηστών του Internet και ερευνάται από τον ανεξάρτητο οργανισμό "cybertip.ca". Αν και αυτή ήταν μια εθελοντική ιδιωτική πρωτοβουλία, χωρίς συμμετοχή των αρχών, η καναδική κυβέρνηση είχε εκφράσει την έγκρισή της.

Τον Οκτώβριο του 2011, το Ανώτατο Δικαστήριο του Καναδά ομόφωνα έκρινε ότι οι πάροχοι δεν μπορούν να θεωρηθούν υπεύθυνοι για δυσφημιστικό υλικό, εφόσον δεν είναι αυτοί οι οποίοι το εκδίδουν [51].

5.3 Λατινική Αμερική

Η λογοκρισία στο Διαδίκτυο είναι πιο περιορισμένη, κατά μέσο όρο, στην Λατινική Αμερική από ότι σε άλλες αναπτυσσόμενες περιοχές του πλανήτη. Πολλές χώρες της περιοχής, χωρίς ιδιαίτερη παράδοση σε σεβασμό ανθρωπίνων δικαιωμάτων, όπως η Βραζιλία, παρουσιάζονται ανοικτές σε θέματα που αφορούν τον κυβερνοχώρο. Παρόλα αυτά βραζιλιάνικο δικαστήριο απαίτησε από τους παρόχους της χώρας να αποκλείσουν την πρόσβαση σε ιστολόγια και στο YouTube με την αιτιολογία ότι είναι φορείς δυσφημιστικού για το κράτος περιεχομένου. Το Σεπτέμβριο του 2010, ο σατιρικός ιστότοπος Falha de Sao Paulo αφαιρέθηκε από τον ιστό, έπειτα από λήψη ασφαλιστικών μέτρων. Σε μερικές περιπτώσεις αναγκάστηκαν περιοδικά στο Διαδίκτυο να αφαιρέσουν άρθρα, σε άλλες περιπτώσεις εμποδίστηκε η δημοσιοποίηση δημοσκοπήσεων και επιβλήθηκε η αφαίρεση δημοσιεύσεων από το Twitter. Στην Αργεντινή πέρασε ένα διάταγμα κατά της λογοκρισίας στο διαδίκτυο. Η Εθνική Επιτροπή Τηλεπικοινωνιών της Αργεντινής έχει αποκλείσει δύο ιστοσελίδες το leakymails.com και το leakymails.blogspot.com επειδή δημοσιοποίησαν κυβερνητική αλληλογραφία. Σε ορισμένες χώρες, συμπεριλαμβανομένης της Κόστα Ρίκα, η οποία είναι γνωστή για τη δημοκρατική της διακυβέρνηση, δημοσιογράφοι παρενοχλούνται από το κρατικές υπηρεσίες όταν κάνουν αναφορές στο Διαδίκτυο για τη διαφθορά.

Στη Χιλή η Βουλή των Αντιπροσώπων πέρασε ένα νομοσχέδιο που επιτρέπει στους δικαστές να τιμωρούν τους χρήστες του Διαδικτύου που είναι προσβλητικοί προς τα «χρηστά ήθη» και τη «δημόσια τάξη». Η διάταξη αυτή αφορά μόνο τις ιστοσελίδες που φιλοξενούνται μέσα στη Χιλή, δηλαδή, με κατάληξη «.cl» στην διεύθυνση τους και ήταν τελείως αναποτελεσματική σε οτιδήποτε βρίσκεται εκτός της χώρας. Σε αντίθεση με τη Χιλή, στο Περού η κυβέρνηση εισήγαγε τον νόμο για τη Διαφάνεια και την Πρόσβαση στη Δημόσια Πληροφορία με τον οποίο

δημιουργούνται δημόσια τερματικά πρόσβασης στο Διαδίκτυο και ιδρύεται το Ταμείο Επενδύσεων Τηλεπικοινωνιών, το οποίο είναι υπεύθυνο για την προώθηση της. Στο Μεξικό, η κυβέρνηση δεν προβαίνει σε λογοκρισία στο Διαδίκτυο, το κάνουν όμως τα καρτέλ των ναρκωτικών [90].

5.3.1 Κούβα

Η χώρα της Λατινικής Αμερικής, όπου με διαφορά εφαρμόζονται οι πιο περιοριστικές πολιτικές στην πρόσβαση σε διαδικτυακό περιεχόμενο είναι η Κούβα. Με την αρμοδιότητα για τον έλεγχο της πρόσβασης στο Διαδίκτυο να ανήκει στο Υπουργείο Πληροφορικής και Επικοινωνιών, η κουβανική κυβέρνηση ελέγχει πλήρως τη διαδικτυακή διασύνδεση της χώρας με το εξωτερικό καθώς και του τέσσερεις εθνικούς ISP. Αντιμέτωποι με τις υψηλές τιμές του εξοπλισμού πληροφορικής, εν μέρει λόγω του εμπορικού αποκλεισμού από τις ΗΠΑ, η Κούβα απέρριψε ένα μοντέλο ανάπτυξης του Διαδικτύου βασισμένο στην ελεύθερη αγορά, υπέρ ενός κεντρικού, καθοδηγούμενου από την κυβέρνηση, που το παρέχει κυρίως σε ιδρύματα και όχι σε ιδιώτες. Ως αποτέλεσμα, η ατομική πρόσβαση στην Διαδίκτυο έχει ουσιαστικά απαγορευτεί, με τους ISP να επιτρέπεται να παρέχουν ατομικούς λογαριασμούς μόνο σε άτομα που λαμβάνουν επιχορηγήσεις από κρατικούς φορείς. Μέχρι πρόσφατα, όλοι οι διαδικτυακοί λογαριασμοί έπρεπε να είναι καταχωρημένοι στο Εθνικό Κέντρο για την Αυτόματη Ανταλλαγή Δεδομένων με κόστος 260 δολάρια το μήνα (ο μέσος μισθός στην Κούβα είναι 240 δολάρια ανά έτος). Η χαλάρωση των περιοριστικών μέτρων το 2006, οδήγησε σε μια έκρηξη του ποσοστού διείσδυσης το οποίο έφτασε περίπου στο 14% του πληθυσμού [90].

Η κουβανική κυβέρνηση έχει δημιουργήσει ένα εσωτερικό δίκτυο, το επονομαζόμενο «Red Cubana», ουσιαστικά ένα intranet, το οποίο οι πολίτες μπορούν να χρησιμοποιήσουν μέσω πανεπιστήμιων, ταχυδρομείων ή οργανισμών πληροφορικής, χωρίς όμως να υπάρχει διασύνδεση του με το εξωτερικό. Διεθνείς διασυνδέσεις παρέχονται μέσω των internet καφέ, έχοντας όμως την υποχρέωση οι χρήστες να δηλώσουν τα στοιχεία τους κατά την είσοδο τους στους χώρους αυτούς. Παρόλα αυτά, η διαφορετική τιμολόγηση του εσωτερικού intranet σε σχέση με τις διεθνής διασυνδέσεις καταστούν τις δευτέρες απαγορευτικές. Για την πρόσβαση σε internet καφέ με διεθνείς συνδέσεις πρέπει η πληρωμή να γίνεται σε Αμερικάνικα δολάρια, κάτι συχνά απαγορευτικό για τους Κουβανούς [66].

5.3.2 Βενεζουέλα

Μετά την Κούβα, η Βενεζουέλα, είναι η δεύτερη χειρότερη στη Λατινική Αμερική, σε θέματα ελέγχου του περιεχομένου στο Διαδίκτυο. Ο Γενικός Εισαγγελέας της Βενεζουέλας Luisa Ortega, υποστήριξε ότι «το Διαδίκτυο δεν μπορεί να είναι ένας χώρος ελεύθερος από τον νόμο, όλες οι δραστηριότητες που λαμβάνουν χώρα σε αυτόν, σε εθνικό επίπεδο πρέπει να υπόκεινται σε νομική ρύθμιση». Τον Δεκέμβριο του 2010, η κυβέρνηση ανακοίνωσε ελέγχους στους ISP απαιτώντας από αυτούς να αναφέρουν οποιοδήποτε υλικό σχετικό με βία αναρτηθεί στην δικτυακούς τόπους που φιλοξενούν. Ο σημαντικότερος πάροχος της Βενεζουέλας, η CANTV, που ελέγχει το 90% της αγοράς του Διαδικτύου και το 100% των συνδέσεων υψηλής ταχύτητας στη χώρα, επανακρατικοποιήθηκε το 2007. Η κυβέρνηση της Βενεζουέλας έχει μπλοκάρει την πρόσβαση κατά καιρούς σε διαδικτυακούς τόπους όπως το Wordpress.com και το blogger.com και έχει επανειλημμένα αποκλείσει το Noticiero Digital, το οποίο υπήρξε ιδιαίτερα επικριτικό και συχνά προσβλητικό για τον Ούγκο Τσάβες. Ωστόσο αν και αρχικά ο Τσάβες επιτέθηκε στο Διαδίκτυο, κατηγορώντας το ως ένα «κίνημα συνωμοσίας» και τους χρήστες του Twitter ως τρομοκράτες και προδότες, το 2010 άρχισε να χρησιμοποιεί το Twitter, φτάνοντας να έχει στις αρχές του 2013 πάνω από 500.000 οπαδούς (followers) [65, 90].

5.4 Αυστραλία – Νέα Ζηλανδία

Η Αυστραλία εφαρμόζει μια από τις πιο περιοριστικές πολιτικές στο Διαδίκτυο σε σχέση με τις άλλες δυτικές χώρες και κατά τη διάρκεια των τελευταίων ετών έχει λάβει μέτρα προς την κατεύθυνση ενός εθνικού υποχρεωτικού συστήματος φιλτραρίσματος. Η Νέα Ζηλανδία, επεμβαίνει ρυθμιστικά στο περιεχόμενο του Διαδικτύου σημαντικά λιγότερο. Στο σύνταγμα της Αυστραλίας δεν αναφέρεται ρητά το δικαίωμα της ελευθερίας του λόγου και στην πραγματικότητα περιέχει μια ρήτρα η οποία δίνει στην αυστραλιανή κυβέρνηση εξουσίες επί των επικοινωνιών επιτρέποντας να ρυθμίζει τις ταχυδρομικές, τηλεγραφικές, τηλεφωνικές, και άλλες παρόμοιες υπηρεσίες, συμπεριλαμβανομένου του Διαδικτύου. Κάποιες από τις περιφερειακές κυβερνήσεις έχουν εισάγει νομοθεσία που καθορίζει ως ποινικό αδίκημα τη διανομή ακατάλληλου υλικού, καθώς το σύνταγμα δεν παρέχει αυτή την εξουσία στην εθνική κυβέρνηση.

Η αυστραλιανή κυβέρνηση έχει εδώ και αρκετό καιρό, μέσω της Αυστραλιανής Αρχής Επικοινωνιών και Μέσων (ACMA), προωθήσει και χρηματοδοτήσει ένα πρόγραμμα

προαιρετικού φιλτραρίσματος, στο οποίο οι χρήστες αποδέχονται οικειοθελώς λογισμικό ελέγχου που εμποδίζει την πρόσβαση σε απαγορευμένο περιεχόμενο που φιλοξενείται εκτός της χώρας. Το 2008, η κυβέρνηση ανακοίνωσε τα σχέδιά της για ένα πολυεπίπεδο σύστημα ελέγχου που συνδυάζει ένα υποχρεωτικό φίλτρο που αποκλείει πορνογραφικό και παράνομο περιεχόμενο, καθώς και ένα προαιρετικό φίλτρο που θα αποκλείει μεγαλύτερη θεματολογία περιεχόμενου. Το σύστημα αυτό αντιμετωπίστηκε δυναμικά από αυστραλιανές και διεθνείς κοινότητες που δραστηριοποιούνται σε θέματα ανθρωπίνων δικαιωμάτων.

Σε αντίθεση, η Νέα Ζηλανδία έχει λιγότερο αυστηρούς κανονισμούς Διαδικτύου. Η κυβέρνηση διατηρεί έναν πιο περιορισμένο ορισμό του προσβλητικού περιεχόμενου που μπορεί να καθοριστεί από κάποιον κυβερνητικό οργανισμό και σε αντίθεση με την Αυστραλία, ο ορισμός αυτός περιλαμβάνει και ομιλίες μίσους. Επιπλέον, η κυβέρνηση της Νέα Ζηλανδίας δεν έχει θεσπίσει νομοθεσία για να επιτρέψει τον αποκλεισμό του προσβλητικού περιεχόμενου, εκτός από την περίπτωση της παιδικής πορνογραφίας. Ακόμη παρουσιάζεται, σκοπίμως, πιο ευέλικτη σε θέματα περιεχομένου πνευματικής ιδιοκτησίας [19, 66, 80].

5.5 Ασία

Ο κυβερνοχώρος της Ασίας αποτελεί ένα μίγμα ελέγχου πληροφοριών και αντιδράσεων και αμφισβητήσεων έναντι αυτών των ελέγχων. Οι κυβερνήσεις της περιοχής αυτής προσπαθούν να εξισορροπήσουν μεταξύ της εκρηκτικής ανάπτυξης των τεχνολογιών της πληροφορικής και των επικοινωνιών (ΤΠΕ) και των ανησυχιών τους για κοινωνική σταθερότητα, εθνική ασφάλεια και διατήρηση των τοπικών πολιτιστικών αξιών. Αυτές οι εντάσεις εκδηλώνονται με διαφορετικό τρόπο ανάλογα με τις συνθήκες που επικρατούν σε κάθε κράτος. Η περιοχή συμπεριλαμβάνει μερικές από τις λιγότερο διασυνδεδεμένες χώρες, όπως η Βιρμανία, αλλά και αναδυόμενες αγορές στον τομέα της πληροφορικής και των επικοινωνιών, όπως η Κίνα και η Ινδία. Η κλιμάκωση του ελέγχου που εφαρμόζεται στη περιοχή, επί της διακινούμενης πληροφορίας, ποικίλλει καθώς εκεί υπάρχουν μερικά από τα καθεστώτα με τους πιο αυστηρούς ελέγχους στον κόσμο αλλά και περιβάλλοντα αδέσμευτης επικοινωνίας.

Η συνεχιζόμενη αύξηση του ποσοστού διείσδυσης του Διαδικτύου στην Ασία, ιδιαίτερα μέσω κινητής τηλεφωνίας, συμβαίνει παράλληλα με την αύξηση της ικανότητας των κρατών να παρακολουθούν και να ελέγχουν την ροή των πληροφοριών. Σε χώρες όπως το Μπαγκλαντές, η Ινδονησία και η Μαλαισία έχει αυξηθεί σημαντικά η συνδεσιμότητα ιδιαίτερα μέσω κινητού

τηλεφώνου. Ωστόσο, όπως η συνδεσιμότητα μεγαλώνει, το ίδιο κάνει και η νομική, κανονιστική και τεχνική ικανότητα των κρατών να παρακολουθούν και να ελέγχουν. Τόσο δημοκρατικές όσο και αυταρχικές κυβερνήσεις έχουν διευρύνει την έννοια του ακατάλληλου περιεχομένου καθώς και των μηχανισμών για την καταπολέμησή του. Αυτοί έχουν λάβει τη μορφή συγκεντρωτικών μηχανισμών φιλτραρίσματος, αυξάνοντας τις δυνατότητες των ρυθμιστικών αρχών να παρακολουθούν και να λογοκρίνουν το περιεχόμενο και να διώκουν τους παραβάτες.

Η έρευνα για τον έλεγχο του Διαδικτύου, της οργάνωσης OpenNet Initiative (ONI), που διεξήχθη το 2009 - 2010, στο Μπανγκλαντές, τη Βιρμανία, την Κίνα, την Ινδία, την Ινδονησία, τη Μαλαισία, το Πακιστάν, τις Φιλιππίνες, τη Σιγκαπούρη, τη Νότια Κορέα, την Ταϊλάνδη και το Βιετνάμ, έδειξε ότι το φιλτράρισμα των πληροφοριών εφαρμόζεται σε μεγάλη έκταση. Η Βιρμανία, η Κίνα και το Βιετνάμ είναι οι χώρες της περιοχής που ο έλεγχος είναι πιο εντατικοποιημένος, με στόχο κυρίως ανεξάρτητα μέσα μαζικής ενημέρωσης και περιεχόμενο που σχετίζονται με κοινωνικά θέματα, ανθρώπινα δικαιώματα, και πολιτικές μεταρρυθμίσεις. Στο άλλο άκρο του φάσματος, η Σιγκαπούρη συνεχίζει, συμβολικά, να αποκλείει έναν περιορισμένο αριθμό ιστοσελίδων πορνογραφικού υλικού.

Το φιλτράρισμα στη Νότια Κορέα και την Ινδία επικεντρώνεται κυρίως σε περιεχόμενο που σχετίζεται με θέματα εθνικής ασφάλειας, με τους παρόχους της Νότιας Κορέας να ελέγχουν εκτενώς περιεχόμενο που έχει σχέση με τη Βόρεια Κορέα και αυτούς στην Ινδία να αποκλείουν θεματολογία Hindu εξτρεμισμού. Και το Πακιστάν εστιάζει επίσης σε ζητήματα που θεωρούνται ευαίσθητα για την εθνική ασφάλεια, καθώς και βλάσφημου για θρησκευτικά θέματα περιεχομένου. Αν και σε προηγούμενες έρευνες της ONI δεν βρέθηκε κανένα αποδεικτικό στοιχείο για λογοκρισία στο Διαδίκτυο στην Ινδονησία, πιο πρόσφατες αποκάλυψαν ότι οι ISP ουσιαστικά αποκλείουν ότι έχει σχέση με πορνογραφία. Στην Ταϊλάνδη το φιλτράρισμα κατά κύριο λόγο επικεντρώνεται σε πολιτικό περιεχόμενο σε συνδυασμό με γεγονότα όπως η πολιτική αναταραχή του 2009. Η έρευνα του OpenNet δεν βρήκε κανένα αποδεικτικό στοιχείο για έλεγχο περιεχομένου στο Διαδίκτυο στο Μπαγκλαντές, τη Μαλαισία και τις Φιλιππίνες [20].

5.5.1 Κίνα

Σε μια χώρα με περισσότερους από 500 εκατομμύρια χρήστες του Διαδικτύου, η κρατική λογοκρισία σε αυτό, είναι αναμφισβήτητα η πιο εντατική παγκοσμίως. Το Κομμουνιστικό Κόμμα της Κίνας ασκεί πολύ αυστηρό κεντρικό έλεγχο επί της ροής της πληροφορίας εντός και εκτός συνόρων της χώρας, κυρίως μέσω του Υπουργείου Βιομηχανίας Πληροφοριών, αν και η

αστυνόμευση του Διαδικτύου γίνεται κατά κύριο λόγο μέσω του Υπουργείου Κρατικής Ασφάλειας. Το κράτος ενθαρρύνει τη χρήση του Διαδικτύου, αλλά μόνο μέσα σε ένα ελεγχόμενο περιβάλλον, αν και ο κυβερνοχώρος στην Κίνα παραμένει σχετικά ελεύθερος σε σύγκριση με τα παραδοσιακά μέσα ενημέρωσης. Στις πρώτες φάσης της ανάπτυξης του Διαδικτύου, το κράτος είχε μικρή παρέμβαση , αλλά όταν υπηρεσίες όπως το chat και τα blog (ιστολόγια) άρχισαν να διακινούν περιεχόμενο επικριτικό για την κυβέρνηση πάνω από το επιτρεπτό όριο, προκλήθηκε η δημιουργία ενός ασφυκτικού συστήματος ελέγχου. Το 2005, η OpenNet δήλωσε ότι «η Κίνα λειτουργεί το πιο εκτεταμένο και τεχνολογικά εξελιγμένο σύστημα φιλτραρίσματος του Διαδικτύου στον κόσμο». Η Κινεζική κυβέρνηση αιτιολογεί την ασκούμενη λογοκρισία, υποστηρίζοντας την ανάγκη να διατηρηθεί μια «αρμονική κοινωνία».

Η κυβέρνηση αναπτύσσει ένα ευρύ φάσμα μέτρων γνωστό και ως «Great Firewall», κατά το «Μεγάλο (Σινικό) Τείχος», το οποίο απασχολεί δημόσιους υπαλλήλους αλλά και εθελοντές ιδιώτες που παρακολουθούν τα ιστολόγια και τα μηνύματα ηλεκτρονικού ταχυδρομείου για πιθανές απειλές προς την υπάρχουσα πολιτική τάξη. Το Great Firewall είναι μια σύνθετη οντότητα, με την αποτελεσματικότητα των στοιχείων που το δομούν να ποικίλει. Οι διεθνείς συνδέσεις συμπιέζονται μέσα σε μια επιλεγμένη δέσμη, κρατικά ελεγχόμενων, δικτύων κορμού. Η δημόσια πρόσβαση σε πολλές συνηθισμένες υπηρεσίες του Παγκόσμιου Ιστού, όπως το Google και το Yahoo, είναι σε μεγάλο βαθμό περιορισμένη. Η εθνική κυβέρνηση προσλαμβάνει στρατιές χαμηλόμισθων σχολιαστών, γνωστοί με τον υποτιμητικό όρο «five-mao party» (ομάδα των 50 σεντς), με σκοπό την παρακολούθηση ιστολογίων και chat rooms και στη συνέχεια την συμμετοχή σε αυτά με σχολιασμούς ευνοϊκούς για το κινεζικό κράτος. Πολλές δημοτικές αρχές συμμετέχουν στη διαδικασία της λογοκρισίας, όπως για παράδειγμα στο Πεκίνο, όπου υπάρχουν 10.000 εθελοντές παρατηρητές του Διαδικτύου. Ωστόσο, ένα μεγάλο μέρος του ελέγχου πραγματοποιείται μέσω των παρόχων του Διαδικτύου οι οποίοι παρακολουθούν τα chat rooms, τα blog, τις μηχανές αναζήτησης, τις ιστοσελίδες με βίντεο, αναζητώντας πολιτικά ευαίσθητο υλικό, ώστε να συμμορφωθούν με τους περιορισμούς της κυβέρνησης.

Ιστοσελίδες που βοηθούν τους χρήστες να παρακάμψουν τη λογοκρισία όπως το anonymizer.com και το proxify.com απαγορεύονται. Οι χρήστες που προσπαθούν να έχουν πρόσβαση σε αποκλεισμένες ιστοσελίδες έρχονται αντιμέτωποι με τους Jingjing και Chacha, δύο αστυνομικούς, κινούμενα σχεδία, που τους ενημερώνουν ότι είναι υπό παρακολούθηση. Τα άμεσα μηνύματα και τα μηνύματα μέσω κινητού τηλεφώνου παρακολουθούνται μέσω ενός προγράμματος που ονομάζεται QQ, το οποίο εγκαθίσταται αυτόματα σε όλες τις συσκευές, για την παρακολούθηση των επικοινωνιών. Ιστολόγια τα οποία είναι επικριτικά για την κυβέρνηση

αποκλείονται αυτομάτως, αν και την διαχείριση των ιστολογίων η κυβέρνηση την έχει αναθέσει στις εταιρίες που τα φιλοξενούν. Το 2006, για παράδειγμα, το MSN Spaces, η ιστοσελίδα της Microsoft με ιστολόγια, συμφώνησε να εναρμονιστεί με τις κατευθυντήριες γραμμές της κυβέρνησης με αντάλλαγμα την ελευθερία από τη λογοκρισία σε επίπεδο παρόχου. Η δημοφιλής υπηρεσία Sina Weibo, με 300 εκατομμύρια μικροιστολόγια, χρησιμοποιεί ένα σύστημα βαθμών ποινής για την παρακολούθηση πολιτικά απαράδεκτων σχόλιων, ξεκινώντας από 80 βαθμούς, αφαιρούνται με κάθε παράβαση κάποιοι βαθμοί, ενώ όταν μηδενιστούν το ιστολόγιο τερματίζει την λειτουργία του.

Τον Ιούνιο του 2009, η κυβέρνηση επιχείρησε να απαιτήσει από τους κατασκευαστές υπολογιστικού εξοπλισμού, να εγκαταστήσουν ένα λογισμικό φιλτραρίσματος γνωστό ως «Green Dam Youth Escort» (πράσινο φράγμα συνοδός της νεολαίας), σε όλους τους νέους υπολογιστές, αλλά υποχώρησε απέναντι στη τεράστια λαϊκή κατακραυγή αλλά και εξαιτίας μιας μήνυσης από μια εταιρεία από τη Καλιφόρνια, τη CYBERsitter, που ισχυριζόταν ότι η Κίνα της έκλεψε το λογισμικό.

Το Great Firewall σύστημα ξεκίνησε το 2006 με μια πρωτοβουλία γνωστή ως η «Χρυσή Ασπίδα», ένα εθνικό δίκτυο παρακολούθησης που η Κίνα ανέπτυξε με την βοήθεια των αμερικανικών εταιρειών Nortel και Cisco Systems και επεκτάθηκε πέρα από το Διαδίκτυο για να συμπεριλάβει ψηφιακές ταυτότητες με μικροτσίπ οι οποίες περιέχουν προσωπικά δεδομένα, που επιτρέπουν στο κράτος να αναγνωρίζει πρόσωπα φωνές από τα δισεκατομμύρια πολίτες του. Η Χρυσή Ασπίδα έγινε περιζήτητη από πλήθος αυταρχικών κυβερνήσεων σε όλο τον κόσμο, με αποτέλεσμα να εξαχθεί στην Κούβα, το Ιράν και τη Λευκορωσία. Το κρατικό πρόγραμμα ανάπτυξης υπηρεσιών έλεγχου της Κίνας, αποτέλεσε πρότυπο για διάφορες απολυταρχικές κυβερνήσεις.

Η κινεζική κυβέρνηση έχει εφαρμόσει περιοδικά την εξαναγκασμένη διακοπή της λειτουργίας των κέντρων δεδομένων όπου στεγάζονται εξυπηρετητές ιστοσελίδων επηρεάζοντας εκατομμύρια χρήστες. Οι υπηρεσίες ηλεκτρονικού ταχυδρομείου όπως το Gmail και το Hotmail συχνά δεν λειτουργούν. Πριν από τους Ολυμπιακούς Αγώνες του 2008, επικριτικές σελίδες του Facebook είχαν μπλοκαριστεί. Το 2007, η κρατική υπηρεσία Ραδιοφωνίας Κινηματογράφου και Τηλεόρασης πήρε την απόφαση ότι όλοι οι ιστότοποι διανομής βίντεο πρέπει να είναι κρατικής ιδιοκτησίας. Η αστυνομία πραγματοποιεί περιπολίες σε Internet καφέ, όπου οι χρήστες πρέπει να παρέχουν προσωπικές πληροφορίες προκειμένου να συνδεθούν, ενώ οι διαχειριστές των ιστοσελίδων έχουν υποχρέωση από το νόμο να προσλαμβάνουν λογοκριτές.

Η κυβερνητική λογοκρισία μπορεί όμως να δημιουργήσει προβλήματα με τους ξένους επενδυτές. Η κινεζική κυβέρνηση εδώ και χρόνια μπλοκάρει την πρόσβαση στο The New York Times, ενώ άφηνε ελεύθερο το δικτυακό τόπο του USA Today, μέχρι που οι εκδότες του παραπονέθηκαν απευθείας στον Πρόεδρο Τζιάνγκ Ζεμίν. Η Google, ο μεγαλύτερος πάροχος στον κόσμο δωρεάν διαδικτυακών υπηρεσιών, δημιούργησε και λειτούργησε μια ξεχωριστή ιστοσελίδα, την Google.cn η οποία ήταν σύμφωνη με τα πολιτικά πρότυπα της κυβέρνησης της Κίνας, λογοκρίνοντας σύμφωνα με τις επιδιώξεις της. Η αμερικάνικη εταιρία αντέτεινε σε αυτούς που την κατηγορούσαν για αυτή της την επιλογή, ότι η λογοκριμένη υπηρεσία είναι καλύτερη από την παντελή έλλειψη της. Στις αρχές του 2010, υπό την πίεση της διεθνούς κριτικής, η Google ανακοίνωσε ότι δε θα συνεργάζεται πλέον με την κινεζικές αρχές και αποσύρθηκε από τη χώρα. Η κινεζική κυβέρνηση μπορεί πλέον ανενόχλητη να προωθεί εγχώριες και απόλυτα ελεγχόμενες μηχανές αναζήτησης όπως το Baidu, Sohu, και Sina.com.

Το κινεζικό κράτος έχει συλλάβει πολλούς χρήστες του Διαδικτύου που αποτόλμησαν να εκφραστούν σε πολιτικά ευαίσθητους τομείς. Λόγω της αδυναμίας παρακολούθησης όλων των ιστοσελίδων σε όλες τις χώρες, το κράτος εφαρμόζει συχνά για αποτρεπτικούς σκοπούς, στρατηγική εκφοβισμού. Τα μέτρα αυτά έχουν συμβάλει στον περιορισμό της χρήσης του Διαδικτύου από υπερασπιστές των ανθρωπίνων δικαιωμάτων, αυτονομιστές του Θιβέτ και θρησκευτικές ομάδες, όπως το Φάλουν Γκονγκ. Μπορούν επίσης να βοηθήσουν στον προληπτικό επηρεασμό της κοινής γνώμης υπέρ του κράτους. Ωστόσο, δεδομένης της πολυμορφικής φύσης του Διαδικτύου, τέτοιοι περιορισμοί, αργά ή γρήγορα τελικά αποτυγχάνουν. Με τη χρήση διακομιστών μεσολάβησης (proxies) και τη βοήθεια προγραμματιστών από τις ΗΠΑ, έχουν αναπτυχθεί μέθοδοι παράκαμψης της λογοκρισίας, όπως το λογισμικό Freegate από την ομάδα Φάλουν Γκονγκ. Παρόλα αυτά το κινεζικό σύστημα ελέγχου του περιεχομένου παραμένει αποτελεσματικό σε μεγάλο βαθμό κυρίως λόγω των πολλών διαστάσεων του, της ευελιξίας του και της συνεχούς εξέλιξης του [90] .

5.6 Μέση Ανατολή και Βόρεια Αφρική

Οι κυβερνήσεις στη Μέση Ανατολή και τη Βόρεια Αφρική επενδύουν σε υποδομές μέσων μαζικής ενημέρωσης και πληροφορικής και την ίδια στιγμή συνεχίζουν να επενδύουν σε τεχνολογίες λογοκρισίας, προκειμένου να εμποδίσουν τους πολίτες τους από το να έχουν πρόσβαση σε ένα ευρύ φάσμα περιεχόμενου. Ενώ κάποιες Δυτικές εταιρείες συμμετέχουν στην κατασκευή υποδομών ΤΠΕ που απαιτούνται για την ανάπτυξη της περιοχής, άλλες δυτικές εταιρείες

παρέχουν στις κυβερνήσεις τις τεχνολογίες και τα δεδομένα που απατούνται για το φιλτράρισμα του Διαδικτύου.

Η πρώτη και η δεύτερη γενιά ελέγχου πρόσβασης είναι εμφανής σε όλη τη Μέση Ανατολή και τη Βόρεια Αφρική. Οι κυβερνήσεις στην περιοχή προσπαθούν να ελέγξουν πολιτικό περιεχόμενο με τη χρήση τεχνικών φιλτραρίσματος, νομοθετικών και κανονιστικών διατάξεων, μηχανισμών επιτήρησης και παρακολούθησης, με φυσικούς περιορισμούς, άτυπη παρενόχληση και συλλήψεις. Είναι διαδεδομένος σε πολλές χώρες και συνεχώς αυξάνεται, ο αποκλεισμός περιεχομένου που θεωρείται προσβλητικό για τα θρησκευτικά και πολιτιστικά ήθη.

Αν και πολλές κυβερνήσεις δημοσιοποιούν την πρόθεση τους να ελέγξουν το περιεχόμενο, οι περισσότερες συνεχίζουν να αποκρύπτουν τις πρακτικές της πολιτικής φιλτραρίσματος, προσπαθώντας να προκαλέσουν σύγχυση στους χρήστες με διάφορα μηνύματα σφάλματος.

Η απουσία του ελέγχου μέσω τεχνολογικών λύσεων σε ορισμένες χώρες της περιοχής, σε καμία περίπτωση δεν υποδηλώνει ελεύθερο διαδικτυακό περιβάλλον στις χώρες αυτές. Πρακτικές επιτήρησης και παρακολούθησης και εκτός νόμου παρενόχληση από τις υπηρεσίες ασφαλείας δημιουργούν ένα κλίμα φόβου.

Πολλοί πάροχοι αποκλείουν δημοφιλής ουδέτερες υπηρεσίες όπως υπηρεσίες μετάφρασης και εργαλεία για την προστασία ιδιωτικών δεδομένων, για να αποφύγουν την περίπτωση της χρήσης τους για την παράκαμψη του κεντρικού ελέγχου. Οι λογοκριτές επίσης αποκλείουν χωρίς περιορισμό υπηρεσίες κοινωνικής δικτύωσης, διαμοιρασμού βίντεο και φωτογραφιών λόγω της αυξημένης πιθανότητας τους να περιέχουν ακατάλληλο υλικό [19]..

Τα τελευταία χρόνια όλο και περισσότερο χρησιμοποιείται το Διαδίκτυο στη Μέση Ανατολή και τη Βόρεια Αφρική για την εξυπηρέτηση κοινωνικού ακτιβισμού και πολιτικών εξεγέρσεων. Η νέα γενιά των Αράβων, σε αντίθεση με τις προηγούμενες, είναι τεχνολογικά άριστα καταρτισμένη, γεγονός που μπορεί να επιφέρει σημαντικές αλλαγές, όταν θα ανέλθει σε θέσεις επιρροής στον κρατικό και τον ιδιωτικό τομέα. Η χρήση του Facebook και του You Tube ήταν ευρέως εμφανής κατά τη διάρκεια της «Αραβικής Άνοιξης» του 2010, η οποία ανέτρεψε τις κυβερνήσεις της Τυνησίας, της Αιγύπτου και της Λιβύης, αν και είναι απλοϊκό να αποδίδονται αυτές οι εξεγέρσεις αποκλειστικά και μόνο για τη διάδοση των ψηφιακών τεχνολογιών [90].

5.6.1 Αίγυπτος

Παρά τις προθέσεις της κυβέρνησης για ενθάρρυνση της χρήσης του Διαδικτύου, οι αιγυπτιακές αρχές συνεχίζουν να θέτουν περιορισμούς σχετικά με το πώς οι Αιγύπτιοι πρέπει να χρησιμοποιούν το Διαδίκτυο. Τον Φεβρουάριο 2005, για παράδειγμα, το Υπουργείο Εσωτερικών της Αιγύπτου διέταξε τους ιδιοκτήτες και διαχειριστές των Internet καφέ, να καταγράφουν τα ονόματα των πελατών τους και τους αριθμούς ταυτότητας τους, απειλώντας τους με διακοπή της άδειας λειτουργίας των επιχειρήσεων τους εάν αρνηθούν να εφαρμόσουν την εντολή. Η ενέργεια αυτή παραβιάζει κατάφωρα το ανθρώπινο δικαίωμα της προστασίας της ιδιωτικής ζωής. Τον Αύγουστο του 2008, οι αιγυπτιακές αρχές επιβάλουν νέα μέτρα που αυξάνουν την έκταση της λογοκρισίας, με τους πελάτες των internet καφέ να υποχρεούνται να παρέχουν εκτός από τα ονόματά τους, διευθύνσεις ηλεκτρονικού ταχυδρομείου και αριθμούς τηλεφώνου. Μόλις οι πελάτες παράσχουν τα δεδομένα, λαμβάνουν ένα μήνυμα κειμένου στα κινητά τηλέφωνα τους με έναν προσωπικό αριθμό αναγνώρισης (PIN), τον οποίο θα μπορούν να χρησιμοποιήσουν για να έχουν πρόσβαση στο Διαδίκτυο. Το Αραβικό Δίκτυο για τα Ανθρώπινα Δικαιώματα στην Πληροφορία, μια ομάδα για τα ανθρώπινα δικαιώματα με έδρα το Κάιρο, θεωρεί τις απαιτήσεις αυτές σαν ακραία λογοκρισία.

Στην Αίγυπτο παρατηρήθηκε αύξηση στη χρήση του Facebook για κοινωνικό ακτιβισμό, η οποία προειδοποίησε την κυβέρνηση για την ενδεχόμενη δύναμη της κοινωνικής δικτύωσης. Ως αποτέλεσμα, υπήρχαν φήμες ότι θα μπορούσε να αποκλειστεί το κοινωνικό αυτό δίκτυο, ειδικά μετά από την ενέργεια μιας ομάδας ακτιβιστών που κατάφερε να στρατολογήσει υποστηρικτές για μια γενική απεργία που πραγματοποιήθηκε στις 6 Απριλίου του 2008, διαμαρτυρόμενοι για την αύξηση των τιμών των τροφίμων από τη κυβέρνηση του προέδρου Μουμπάρακ, χρησιμοποιώντας το Facebook. Μια άλλη τακτική προέβλεπε οι αρχές να επιτρέπουν την πρόσβαση στο Facebook, ώστε να μπορούν να εντοπίζουν ύποπτους από τις εκεί δραστηριότητες τους. Λόγω της αυξανόμενης χρήσης του Facebook για πολιτική δραστηριοποίηση, ακτιβιστές ανέφεραν ότι η κυβέρνηση παρακολουθεί το χώρο της κοινωνικής δικτύωσης για να προλάβει οργάνωση τυχόν ενεργειών, παρόμοιων με αυτών της έκτης Απριλίου, 2008 [19].

5.6.2 Σαουδική Αραβία

Στον αραβικό κόσμο η λογοκρισία είναι εντονότερη στη Σαουδική Αραβία. Η πρόσβαση του κοινού στο Internet έγινε δυνατή μόνο όταν η κατάσταση θεωρήθηκε ότι θα μπορούσε να

ελεγχτεί αποτελεσματικά. Ολόκληρο το δίκτυο κορμού του Διαδικτύου είναι κρατικής ιδιοκτησίας. Έτσι, ενώ η χώρα προσπάθησε να εκμεταλλευτεί τα οικονομικά οφέλη από το Διαδίκτυο, προσπάθησε επίσης έντονα να το αποτρέψει από το να αμφισβητήσει το άκρως συντηρητικό καθεστώς. Το σαουδαραβικό κράτος έχει εγκαταστήσει εκτεταμένα firewall για να ελέγχουν τη ροή των ψηφιακών πληροφοριών. Τα internet καφέ απαιτούν τη καταγραφή των ονομάτων των πελατών τους, καθώς και τους χρόνους άφιξης και αναχώρησης τους, πληροφορίες που παραδίδονται στην κρατική ασφάλεια. Σε άτομα κάτω των 18 ετών απαγορεύεται η πρόσβαση εκτός και αν συνοδεύονται από ενήλικα.

Με βασιλικό διάταγμα, η Πόλη του Βασιλιά Abdul Aziz για την Επιστήμη και την Τεχνολογία (KACST), ένα κρατικό ερευνητικό κέντρο, είναι η μόνη πύλη μέσα από την οποία οι ISP μπορούν να κάνουν διεθνείς συνδέσεις. Ο μηχανισμός αυτός λειτουργεί με τη χρήση του εμπορικού λογισμικού SmartFilter της Secure Computing, που παράγεται στις Ηνωμένες Πολιτείες και το οποίο πωλείται επίσης και στις κυβερνήσεις του Ιράν, της Υεμένης, της Τυνησίας, των ΗΑΕ και του Σουδάν. Κάθε αίτημα από τη σαουδαραβικό πάροχο για πρόσβαση στον έξω κόσμο πρέπει να περάσει μέσα από κρατικά ελεγχόμενους διακομιστές. Σύμφωνα με η οργάνωση OpenNet το 2004, περισσότερες από 400.000 ιστοσελίδες είχαν απαγορευτεί από το καθεστώς της Σαουδικής Αραβίας (περίπου 2,2% του συνόλου των ιστοσελίδων που ελέγχτηκαν), το μεγαλύτερο μέρος των οποίων αφορούσε υλικό για ενήλικες, ισότοπους παιχνιδιών, ιστοσελίδες αναψυχής και διαδικτυακών αγορών, το Yahoo, το America On Line ακόμη και ιατρικές ιστοσελίδες που χρησιμοποιούν λέξεις όπως «μαστός» έστω και σε ιατρικά πλαίσια [90].

Οι χρήστες που προσπαθούν να αποκτήσουν πρόσβαση σε μια απαγορευμένη ιστοσελίδα μεταφέρονται σε μια σελίδα που εμφανίζει το μήνυμα, «Η πρόσβαση στο ζητούμενο URL δεν επιτρέπεται!», καθιστώντας το σύστημα έλεγχου εν μέρη διαφανές. Σε κάθε περίπτωση δεν δημοσιοποιείται η λίστα των αποκλεισμένων ιστοσελίδων. Οι χρήστες ακόμη έχουν την δυνατότητα μέσα από μια ειδική για αυτόν το σκοπό ιστοσελίδα να υποβάλουν αιτήματα για αποκλεισμό ιστοχώρων ή και το αντίθετο. Μια ομάδα εργαζομένων καθορίζει αν το αίτημα είναι δικαιολογημένο. Ο υπεύθυνος δημοσίων σχέσεων της ελεγκτικής ομάδας είπε ότι η επιτροπή λαμβάνει περίπου 200 αιτήματα κάθε μέρα, αλλά δεν σχολίασε, το πόσο συχνά ξεμπλοκάρει μια τοποθεσία που έχει ήδη αποκλειστεί.

Η σαουδαραβική κυβέρνηση αυξάνει την ένταση του διαδικτυακού φιλτραρίσματος περιεχομένου, ιδιαίτερα από το 2011 και στις αρχές του 2012 μετά τις επαναστάσεις στην Τυνησία, την Αίγυπτο, τη Λιβύη, την Υεμένη και τη Συρία. Για το λόγο αυτό ιδιαίτερα ιστοσελίδες

κοινωνικής δικτύωσης όπως το You tube, το Facebook και το Twitter, αποκλειστήκαν όλο το 2011. Σελίδες που έχουν σχέση με πολιτικές, κοινωνικές ή οικονομικές μεταρρυθμίσεις ή τα βασικά ανθρώπινα δικαιώματα των πολιτών, με «αντι-ισλαμική» ρητορική, με κριτική κατά της χώρας ή της βασιλικής οικογένειας της, ναρκωτικά και τυχερά παιχνίδια έχουν επίσης αποκλειστεί [66].

5.6.3 Ιράν

Μία από τις πιο καταπιεστικές κυβερνήσεις του κόσμου σε όρους επεμβατικής ρύθμισης στο Διαδίκτυο, είναι αυτή του Ιράν. Η κυβέρνηση εφαρμόζει αυστηρό έλεγχο στο κυβερνοχώρο μέσω της υπό κρατικής ιδιοκτησίας, μονοπωλιακού χαρακτήρα, Εταιρείας Τηλεπικοινωνιών του Ιράν, η οποία λειτουργεί κάτω από την εποπτεία του Υπουργείου Τεχνολογιών Πληροφορικής και Επικοινωνιών. Σε αυτήν είναι συνδεδεμένοι όλοι οι πάροχοι διαδικτυακών υπηρεσιών του Ιράν. Όπως και σε πολλές άλλες χώρες, το Ιράν διαχειρίζεται τη λογοκρισία σε επίπεδο ISP, οι οποίοι πρέπει να συμφωνήσουν να απαγορεύσουν την πρόσβαση σε «μη – Ισλαμικές» ιστοσελίδες. Δεδομένου ότι το Διαδίκτυο έχει αναδειχθεί σε τομέα αιχμής στο πεδίο των πολιτικών διαφωνιών, οι κυβερνητικοί περιορισμοί έχουν αυξηθεί ανάλογα. Από το 2001, η κυβέρνηση ανέλαβε τον έλεγχο όλης της διακινούμενης πληροφορίας που εισέρχεται ή εξέρχεται από τη χώρα και ισχυρίζεται ότι έχει μπλοκάρει την πρόσβαση σε πέντε εκατομμύρια ιστοσελίδες. Υπάρχουν περίπου 20 επίσημες κατηγορίες απαγορευμένων ιστοσελίδων, συμπεριλαμβανομένων εκείνων που προσβάλλουν το Ισλάμ, την προώθηση της εθνικής διχόνοιας, την πορνογραφία, και την ανήθικη συμπεριφορά. Από το 2006, πρέπει όλες οι ιστοσελίδες και τα ιστολόγια να έχουν άδεια από το Υπουργείο Πολιτισμού και Ισλαμικής Καθοδήγησης, διαφορετικά διατρέχουν τον κίνδυνο να κηρυχθούν παράνομα. Επίσης το 2006, η κυβέρνηση έθεσε εκτός νόμου συνδέσεις στο Internet ταχύτερες από 128 kbps, αντιμετωπίζοντας πάντως, σθεναρή αντίσταση από τον επιχειρηματικό κόσμο.

Ο επιτήρηση της κυβέρνησης επί των διαφωνούντων βοηθήθηκε σημαντικά από την αγορά ευρωπαϊκής τεχνολογίας κατασκοπείας των εταιριών Nokia και Siemens, ιδιαίτερα με τη χρήση της τεχνικής DPI (Deep Packet Inspection – σε βάθος επιθεώρηση των πακέτων δεδομένων), η οποία επιτρέπει στις αρχές όχι μόνο να αποκλείσουν υπηρεσίες ηλεκτρονικής αλληλογραφίας και τηλεφωνίας μέσω Διαδικτύου, αλλά και να αναγνωρίσουν τα ονόματα των χρηστών. Οι εισαγόμενες αυτές τεχνολογίες, έχουν εξελιχτεί και προσαρμοστεί συμφωνά με τα δεδομένα της χώρας. Το 2009, εν όψει μιας μαζικής αντικυβερνητικής διαμαρτυρίας που οργανώθηκε μέσω

καναλιών κοινωνικής δικτύωσης, το ιρανικό καθεστώς επενέβει δυναμικά, φυλακίζοντας δεκάδες διαφωνούντες bloggers με την συνδρομή του Εισαγγελέα Τεχεράνης.

Παρόλα αυτά, στο Ιράν παρουσιάζονται δυσκολίες στη διαχείριση του ελέγχου του Διαδικτύου. Κατά τη διάρκεια της καταστολής του 2009 για παράδειγμα, ερασιτεχνικό βίντεο με τις επιθέσεις της κυβέρνησης στους διαδηλωτές κυκλοφόρησε ευρέως στον Παγκόσμιο Ιστό. Σε απάντηση, η κυβέρνηση μείωσε τις μέγιστες ταχύτητες μετάδοσης στο δίκτυο κορμού, καθιστώντας την μετάδοση του βίντεο απελπιστικά αργή. Χρησιμοποιώντας δωρεάν λογισμικό παράκαμψης των ελέγχων, όπως το Freegate και το Ultrasoft που αναπτύχτηκαν από κινέζικές αταβιστικές ομάδες, ιρανοί διαδηλωτές παρέκαμψαν επανειλημμένα τους ελέγχους στο κυβερνοχώρο κατά τη διάρκεια κρίσιμων πολιτικά στιγμών [91].

5.6.4 Τυνησία

Η πτώση του καθεστώτος Μπεν Άλι από την εξουσία είχε εγείρει ελπίδες ότι το «Ammar404», το σύστημα λογοκρισίας που έχει συσταθεί από αυτόν, θα διαλυόταν. Η αραβική άνοιξη, που ξεκίνησε στην Τυνησία, έφερε δραστικές αλλαγές σε όλη την περιοχή. Ωστόσο, πολλά μένουν να γίνουν προκειμένου να αποκατασταθεί ένα ικανοποιητικό επίπεδο ελευθερίας της έκφρασης και της πληροφόρησης μέσω του Παγκόσμιου Ιστού. Η αρμόδια υπηρεσία για το Διαδίκτυο στην χώρα, η ATI, αν και έχει κάνει σημαντικά βήματα προόδου σε θέματα ελευθερίας, έχει κατά καιρούς επιτρέψει την λογοκρισία στο Διαδίκτυο με τεχνολογικές αλλά και κοινωνικές μεθόδους [80].

5.7 Συμπεράσματα

Πολλές ομάδες πολιτών σε κλειστές κοινωνίες έχουν πρόσβαση σε ψηφιακές πληροφορίες μέσω του Διαδικτύου οι οποίες ήταν απαγορευμένες στα παραδοσιακά μέσα επικοινωνίας και πληροφόρησης. Ακριβώς επειδή ο κυβερνοχώρος διευκολύνει την απρόσκοπτη πρόσβαση σε πληροφορίες, έχει αντιμετωπιστεί με ανησυχία από πολυάριθμες κυβερνήσεις. Καθώς όλο και μεγαλύτερος αριθμός ανθρώπων έρχονται σε επαφή μεταξύ τους διαδικτυακά, ο κυβερνοχώρος μπορεί να αυξήσει τις ευκαιρίες για συμμετοχή σε πολιτική δραστηριότητα, η οποία μπορεί να αμφισβητήσει τα παραδοσιακά μοντέλα εξουσίας, υπονομεύοντας το μονοπώλιο της εγκατεστημένης εξουσίας πάνω στα μέσα επικοινωνίας.

Το διαδίκτυο έχει σχετικά χαμηλό κόστος και είναι εύκολο στη χρήση, έτσι παρακάμπτονται σημαντικά εμπόδια για την συμμετοχή σε δημόσια συζήτηση των οικονομικά και πολλές φορές μορφωτικά μειονεκτούντων. Επειδή επιτρέπει την πρόσβαση σε πολλαπλές πηγές πληροφόρησης, συμπεριλαμβανομένων της εικόνας και του βίντεο, το Διαδίκτυο έχει διευκολύνει μια γενικευμένη αύξηση της ευαισθητοποίησης για εισαγόμενες ιδέες, προϊόντα και πολιτικά πρότυπα. Πράγματι, με δεδομένο το πόσο έχουν διαδοθεί οι ψηφιακές επικοινωνίες ,το Διαδίκτυο και η κοινωνία όλο και περισσότερο συν-εξελίσσονται, ενεργοποιώντας και διαμορφώνοντας το ένα το άλλο στο χρόνο και στο χώρο.

Παρά την πολύ μεγάλη ικανότητα του Διαδικτύου να διαμορφώσει κοινωνικές εξελίξεις, η παγκόσμια διάδοση του έχει δημιουργήσει μια αυξανόμενη πρόκληση για πολλά αυταρχικά καθεστώτα, ενώ παράλληλα έχει αυξήσει σε μεγάλο βαθμό την αποτελεσματικότητα της παγκόσμιας κοινωνίας των πολιτών. Η αποστολή ηλεκτρονικών αναφορών, οι κυβερνοδιαμαρτυρίες, οι εκκλήσεις για δράση, η υπεράσπιση των διαφόρων περιθωριοποιημένων πολιτικά απόψεων και η μπλογκόσφαιρα έχουν γίνει αναπόσπαστο κομμάτι της πολιτικής δράσης, επιτρέποντας σε τοπικής εμβέλειας κοινωνικά κινήματα να επικοινωνήσουν με ένα εθνικό ή και παγκόσμιο κοινό. Σε απάντηση η κυβερνητική λογοκρισία, που κυμαίνεται από σχετικά ήπια μέτρα, όπως αυτά ενάντια στην πορνογραφία, έως την πιο δραστική σύλληψη των αντιστασιακών του Διαδικτύου, αποτελεί μια ουσιαστική διάσταση της γεωγραφίας του κυβερνοχώρου. Το ένα τέταρτο των πλοηγούμενων στο Διαδίκτυο, υφίσταται τις πιο σκληρές μορφές λογοκρισίας, και στις περισσότερες χώρες η αυτολογοκρισία καταφέρνει ότι δεν μπορούν να επιβάλουν με άμεσες τεχνικές ή κοινωνικές μεθόδους οι κυβερνήσεις.

Η επανάσταση της τεχνολογίας των πληροφοριών δημιουργεί προοπτικές οικονομικής ανάπτυξης και βελτίωσης της παραγωγικότητας. Πολλές κυβερνήσεις, ως εκ τούτου, έχουν να αντιμετωπίσουν ένα δίλλημα, από τη μια να ενθαρρύνουν την ανάπτυξη της τεχνολογίας των πληροφοριών, ενώ από την άλλη φοβούνται τις πολιτικές επιπτώσεις της. Οι κυβερνήσεις στη προσπάθεια τους να διαχειριστούν το περιεχόμενο στο Διαδίκτυο πρέπει να φροντίσουν να μην διαταράξουν τις επενδυτικές, τουριστικές, επιχειρηματικές και τεχνολογικές προοπτικές ανάπτυξης των χωρών τους. Οι περισσότερες κυβερνήσεις επιδιώκουν να επωφεληθούν από την ανάπτυξη της τεχνολογίας των πληροφοριών χωρίς να πληρώσουν το πολιτικό κόστος μιας ενισχυμένης δημοκρατίας. Οι στρατηγικές που χρησιμοποιούνται για τη διαχείριση αυτής της λεπτής ισορροπίας, εξαρτώνται και αντικατοπτρίζουν σε ένα μεγάλο βαθμό τις επικρατούσες πολιτικές, οικονομικές, και πολιτισμικές συνθήκες. Μη επιβεβαιώνοντας κάποιες ουτοπικές προβλέψεις, η διεύρυνση της παγκόσμιας κοινωνίας της πληροφορίας δεν μπορεί να οδηγήσει

αναγκαστικά σε μεγαλύτερη παγκόσμια δημοκρατία, αλλά, σε μια πιο ολοκληρωμένη θέση, για την ενίσχυση της ελευθερίας του πολιτικού λόγου [90].

Κεφάλαιο 6

Ελληνική Εμπειρία - Μελέτη Περίπτωσης - Πανελλήνιο Σχολικό Δίκτυο

Μία από τις βασικές ομάδες στις οποίες στοχεύει ό έλεγχος της πρόσβασης με βάση το περιεχόμενο είναι οι ανήλικοι. Η προστασία της ευαίσθητης παιδικής ηλικίας, αλλά και της εκπαιδευτικής διαδικασίας, που συνδέεται με αυτή, είναι οι δύο βασικοί παράμετροι οι οποίοι καθορίζουν στην περίπτωση αυτή την εφαρμογή του φιλτραρίσματος στο περιεχόμενο του Διαδικτύου.

Η προστασία των παιδιών από το να εκτεθούν σε ακατάλληλο ή επιβλαβές περιεχόμενο αλλά και το να αποτελέσουν μέρος τέτοιου περιεχομένου, στην περίπτωση της παιδικής πορνογραφίας, είναι μια παγκόσμια σταθερά, αποδεκτή σε όλες τις κοινωνίες, είτε αυτές είναι υπό το καθεστώς φιλελεύθερων δημοκρατικών κυβερνήσεων είτε υφίστανται πιο αυταρχικές και απολυταρχικές

πολιτικές. Από την άλλη το Διαδίκτυο, με τα προφανή του πλεονεκτήματα στην εφαρμογή του στο χώρο της εκπαίδευσης, μπορεί να συμβάλει στην πνευματική ανάπτυξη και την μορφωτική ολοκλήρωση των νέων ανθρώπων παρέχοντας ελεύθερα πληροφορίες και επικοινωνία.

Στην Ελλάδα το μεγαλύτερο δίκτυο που σχετίζεται άμεσα με τους νέους ανθρώπους και ένα από τα μεγαλύτερα γενικότερα στη χώρα, είναι το Πανελλήνιο Σχολικό Δίκτυο (ΠΣΔ).

6.1 Πανελλήνιο Σχολικό Δίκτυο

Το Πανελλήνιο Σχολικό Δίκτυο (www.sch.gr) είναι το προηγμένο Εκπαιδευτικό Εταιρικό δίκτυο του Υπουργείου Παιδείας, Θρησκευμάτων, Πολιτισμού και Αθλητισμού (ΥΠΘΠΑ), που διασυνδέει όλα τα σχολεία, τους εκπαιδευτικούς και πλήθος διοικητικών υπηρεσιών και εποπτευόμενων φορέων του ΥΠΘΠΑ. Πρόκειται για το μεγαλύτερο δημόσιο δίκτυο στη χώρα σε αριθμό χρηστών και έχει αναγνωριστεί διεθνώς ως ένα αξιόλογο εκπαιδευτικό δίκτυο που προάγει την αξιοποίηση των Τεχνολογιών της Πληροφορικής και των Επικοινωνιών (ΤΠΕ) στην ελληνική εκπαίδευση.

Το Πανελλήνιο Σχολικό Δίκτυο έχει συμπληρώσει δεκατρία χρόνια από την έναρξη της λειτουργίας του και με την επιτυχημένη υλοποίησή του έχει δημιουργήσει μία νέα γενιά καινοτόμων εκπαιδευτικών κοινοτήτων που χρησιμοποιούν καθημερινά τις Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ) στο έργο τους. Το σχολικό δίκτυο υποστηρίζει επίσης και το διοικητικό έργο της Εκπαίδευσης, καθώς το ΥΠΘΠΑ είναι από τους πρώτους φορείς του Δημοσίου στη χώρα μας που χρησιμοποιούν εφαρμογές ηλεκτρονικής διακυβέρνησης για τη διαχείριση της εκπαίδευσης, όπως π.χ. για τη συλλογή στοιχείων του μαθητικού και εκπαιδευτικού δυναμικού, για τον προγραμματισμό και την υλοποίηση των προσλήψεων των εκπαιδευτικών και τη μισθοδοσία τους, για τη διανομή των βιβλίων, κλπ.

Για να διαφυλαχθεί ο εκπαιδευτικός χαρακτήρας του δικτύου όλοι οι χρήστες του είναι πιστοποιημένα πρόσωπα ή εκπαιδευτικές ή διοικητικές οντότητες της Εκπαίδευσης. Συγκεκριμένα είναι Σχολεία, διοικητικές μονάδες του ΥΠΘΠΑ, εκπαιδευτικοί και μαθητές.

Μερικά από τα στοιχεία (μέχρι τον Μάιο του 2011) που τεκμηριώνουν την ευρύτατη χρήση και αξιοποίηση του σχολικού δικτύου είναι [97]:

- Συνδεδεμένα σχολεία: 16.618

- Συνδεδεμένες διοικητικές υπηρεσίες: 925
- Δείκτης ευρυζωνικότητας: 74,4%
- Εκπαιδευτικοί με προσωπικό λογαριασμό: 77.422
- Μαθητές Γυμνασίου με προσωπικό λογαριασμό: 51.483
- Μεταβολή της συνολικής δικτυακής κίνησης την τελευταία πενταετία: +80% ετησίως.
- Πλήθος ενεργών γραμματοκιβωτίων: 133.701
- Πλήθος φιλοξενούμενων εκπαιδευτικών ιστοσελίδων: 8.519
- Πλήθος ψηφιακών μαθημάτων: 3.526 από 893 σχολεία (σχολικό έτος 2010-11)
- Πλήθος εκπαιδευτικών ιστολογίων: 10.000 τα οποία διαβάζονται από περισσότερους από 155.000 μοναδικούς επισκέπτες ανά μήνα.
- Εκπαιδευτικές κοινότητες: 100
- Επισκεψιμότητα δικτυακής πύλης www.sch.gr: 220.000 μοναδικοί επισκέπτες ανά μήνα.
- Ιδιαίτερα υψηλή χρήση του ηλεκτρονικού ταχυδρομείου και των λιστών επικοινωνίας των υπηρεσιών του ΥΠΔΒΜΘ με τα σχολεία.

6.1.1 Αρχιτεκτονική του Δικτύου στο ΠΣΔ

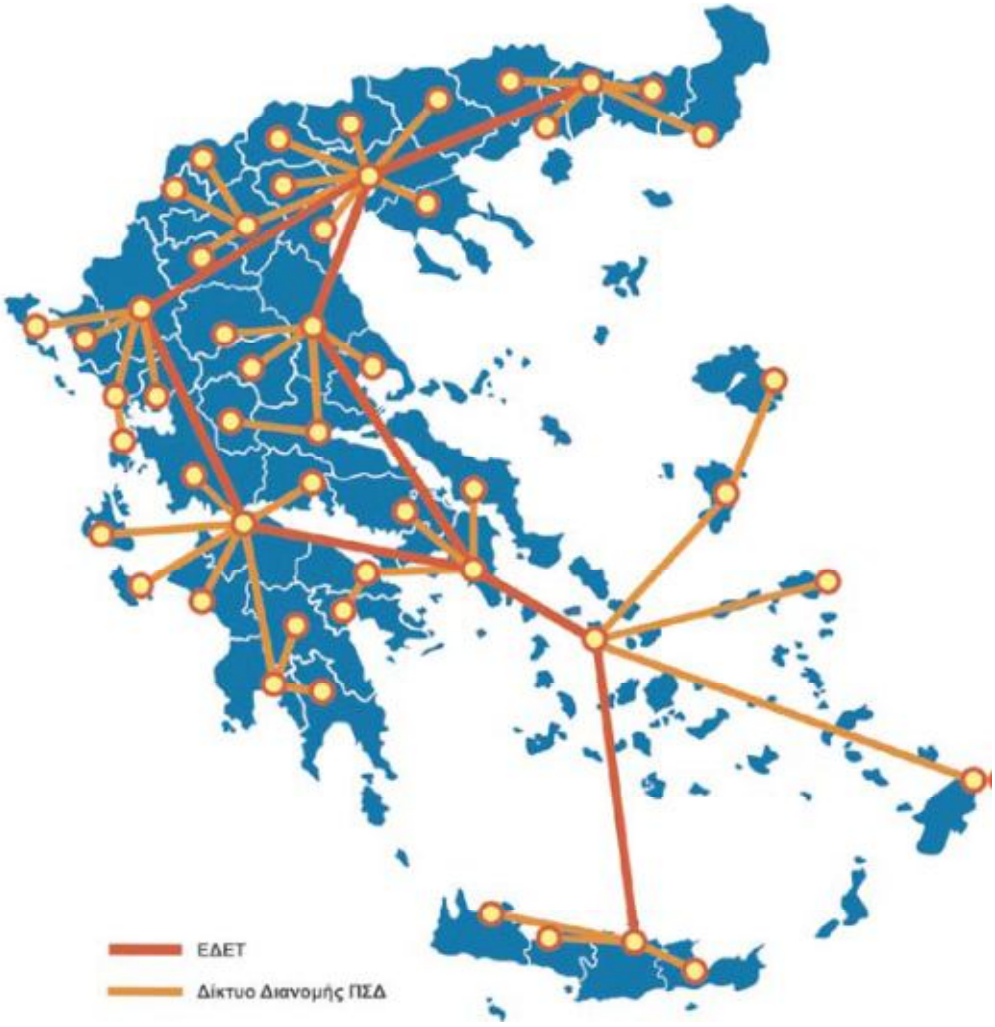
Το δίκτυο δομείται σε μία ιεραρχική δομή τριών επιπέδων [97]:

- Δίκτυο Κορμού: Ως δίκτυο κορμού χρησιμοποιείται το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ,), με το οποίο υπάρχει σήμερα διασύνδεση σε Αθήνα, Θεσσαλονίκη, Πάτρα, Ηράκλειο, Λάρισα, Ιωάννινα, Ξάνθη και Ερμούπολη.

- Δίκτυο Διανομής: Το σχολικό δίκτυο εγκαθιστά στην πρωτεύουσα κάθε νομού εξοπλισμό και εξασφαλίζει τη βέλτιστη πρόσβαση των σχολείων του νομού στο δίκτυο και στις υπηρεσίες του.

- Δίκτυο Πρόσβασης: Χρησιμοποιείται για να διασυνδέει άμεσα και με τις κατάλληλες τηλεπικοινωνιακές ζεύξεις τα σχολεία στον οικείο νομαρχιακό κόμβο. Με βάση συγκεκριμένα οικονομοτεχνικά χαρακτηριστικά επιλέγεται ο βέλτιστος τρόπος διασύνδεσης ανάμεσα σε:

    - Κύκλωμα ADSL
    - Ασύρματη ζεύξη (10 Mbps)
    - Μισθωμένο κύκλωμα (1-2 Mbps)
    - Ψηφιακό κύκλωμα ISDN (64/128 kbps)
    - Απλό κύκλωμα PSTN (56 kbps)
    - Κύκλωμα VDSL (10-15 Mbps, πιλοτικά)
    - Οπτικές συνδέσεις
    - Δορυφορικές ζεύξεις (μελλοντικά)



Σχήμα 6.1: Πανελλήνιο Σχολικό Δίκτυο

6.1.2 Παρεχόμενες Υπηρεσίες

Ένα μεγάλο πλήθος από ηλεκτρονικές υπηρεσίες παρέχονται και υποστηρίζονται σήμερα, από το Πανελλήνιο Σχολικό Δίκτυο όπως για παράδειγμα [97] :

- Ευρυζωνική πρόσβαση στο Διαδίκτυο.
- Πρόσβαση (dial-up) των εκπαιδευτικών στο Διαδίκτυο.
- Πύλη του Πανελληνίου Σχολικού Δικτύου (www.sch.gr).
- Μαθητική Πύλη (http://students.sch.gr).

- Δικτυακή Βιβλιοθήκη για το Εκπαιδευτικό Λογισμικό Ανοικτού Κώδικα (http://opensoft.sch.gr).

- Φιλοξενία Ιστοσελίδων.

- Εκπαιδευτικές Κοινότητες και Ιστολόγια (http://blogs.sch.gr).

- Ηλεκτρονικό Ταχυδρομείο.

- Ηλεκτρονική Τάξη (eclass.sch.gr).

- Ασύγχρονη Τηλεκπαίδευση(e-learning.sch.gr).

- Σύγχρονη Τηλεκπαίδευση και Τηλεδιάσκεψη (http://conf.sch.grs).

- Υπηρεσία Βίντεο (vod.sch.gr)

και πολλές άλλες, ανάμεσα στις οποίες ξεχωρίζουν οι :

1. Προώθηση της ασφαλούς χρήσης του Διαδικτύου (internet-safety.sch.gr) με οδηγίες και προτάσεις προς γονείς, εκπαιδευτικούς και μαθητές για την ασφαλή χρήση του Διαδικτύου, καθώς παρά την αδιαμφισβήτητη χρησιμότητά του υποκρύπτει και ορισμένους κινδύνους τους οποίους κάθε χρήστης ανακαλύπτει σταδιακά. Αυτοί οι κίνδυνοι αφορούν κυρίως στην έκθεση των παιδιών σε παράνομο ή ακατάλληλο περιεχόμενο, στην εξαπάτησή τους από άγνωστους ενήλικες οι οποίοι υποκρίνονται ότι είναι ανήλικοι ή στην άσκηση πίεσης για αποκάλυψη προσωπικών στοιχείων με την επιρροή που μπορεί να έχει ένας ενήλικος σε παιδιά.

2. Ασφαλής πρόσβαση στον Παγκόσμιο Ιστό, με την οποία το ΠΣΔ προστατεύει τους μαθητές από το παράνομο και ακατάλληλο περιεχόμενο παρέχοντας την υπηρεσία αποκλεισμού περιεχομένου. Αν οι μαθητές ή οι εκπαιδευτικοί συναντήσουν κάποια σελίδα με ακατάλληλο περιεχόμενο η οποία δεν αποκόπτεται από την υπηρεσία Ελεγχόμενης Πρόσβασης θα πρέπει να επικοινωνούν με τον διαχειριστή της υπηρεσίας για να ζητήσουν την απαγόρευση της συγκεκριμένης σελίδας. Αν εντοπίσουν σελίδα που ανήκει στην κατηγορία του παράνομου περιεχομένου τότε μπορούν να επικοινωνήσουν

με την Ελληνική Γραμμή Αναφοράς Παράνομου Περιεχομένου στο Internet (http://www.safeline.gr).

Η πρόσβαση στο Διαδίκτυο μέσα από το σχολείο πρέπει να γίνεται με την επίβλεψη του εκπαιδευτικού. Το ίδιο πρέπει να συμβαίνει και όταν τα παιδιά μπαίνουν στο Διαδίκτυο από το σπίτι, επειδή το πρόβλημα της ασφάλειας στο Διαδίκτυο είναι γενικότερο πρόβλημα και απαιτεί την ενημέρωση ολόκληρης της κοινωνίας και ιδιαίτερα των γονιών, οι οποίοι θα πρέπει να μπορούν να προστατεύσουν τα παιδιά τους όταν αυτά βρίσκονται στο σπίτι [97].

6.2 Υπηρεσία Ελέγχου Περιεχομένου στο Πανελλήνιο Σχολικό Διαδίκτυο

Η πρόσβαση στο σχολικό εργαστήριο, στο Διαδίκτυο και σε όλες τις υπηρεσίες που παρέχει το Πανελλήνιο Σχολικό Δίκτυο θα πρέπει να θεωρηθούν ως ένα αγαθό, που δίνεται στα μέλη της εκπαιδευτικής κοινότητας για την προαγωγή της γνώσης και τη διευκόλυνση της εκπαιδευτικής διαδικασίας. Παρά την αδιαμφισβήτητη χρησιμότητά του, το Διαδίκτυο υποκρύπτει και κάποιους κινδύνους. Το Πανελλήνιο Σχολικό Δίκτυο για να προστατεύσει τους μαθητές από το παράνομο και ακατάλληλο περιεχόμενο παρέχει την Υπηρεσία Ελεγχόμενης Πρόσβασης (Web filtering) στον παγκόσμιο ιστό. Με τον τρόπο αυτό απαγορεύεται η πρόσβαση σε σελίδες [97] :

- που προπαγανδίζουν την επιθετική συμπεριφορά, το μίσος και τη βία
- που προωθούν τα ναρκωτικά
- με τυχερά παιχνίδια
- με πορνογραφικό περιεχόμενο
- που προωθούν το ρατσισμό

Η απαγόρευση της πρόσβασης γίνεται σε κεντρικό σημείο του δικτύου και εφαρμόζεται για όλους συνολικά τους χρήστες του ΠΣΔ. Το σύνολο των ακατάλληλων σελίδων διατηρείται σε βάση δεδομένων και επικαιροποιείται τακτικά τόσο από ανάλογες βάσεις δεδομένων που διατίθενται δωρεάν στο διαδίκτυο, όσο και από τους ίδιους τους χρήστες του ΠΣΔ.

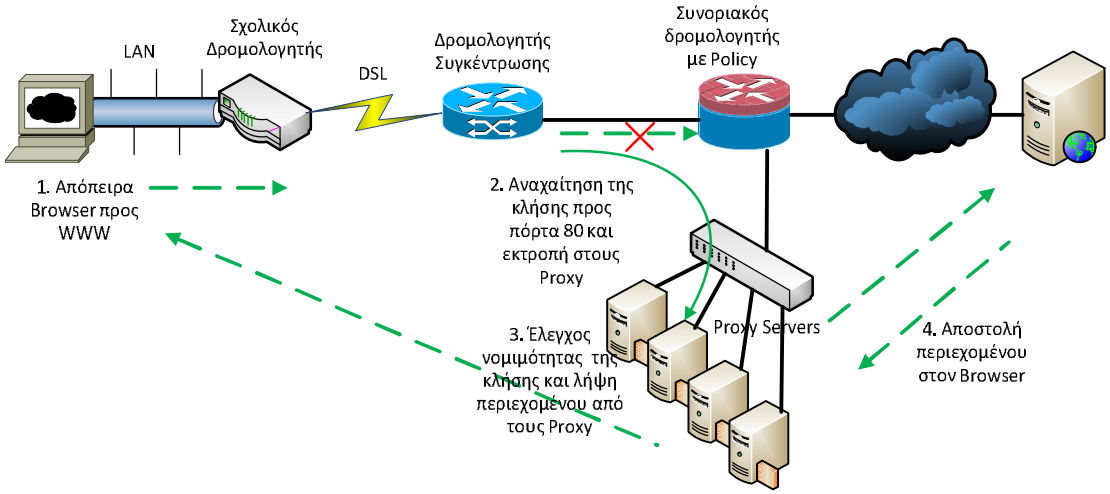
Η παρούσα αναφορά εξετάζει την τρέχουσα μορφή της υπηρεσίας και βασίζεται σε μεγάλο βαθμό στην «Μελέτη σχεδιασμού υπηρεσίας ελέγχου περιεχομένου WWW» [95], που πραγματοποιήθηκε τον Αύγουστο του 2012 από την Υπηρεσία Ελέγχου Περιεχομένου ΠΣΔ, που λειτουργεί στο Εθνικό Μετσόβιο Πολυτεχνείο (ΕΜΠ).

6.2.1 Περιγραφή Τρέχουσας Μορφής Υπηρεσίας

Η τρέχουσα μορφή της υπηρεσίας περιεχομένου υλοποιείται στον κεντρικό κόμβο λειτουργίας του ΠΣΔ στην Αθήνα. Εκεί βρίσκεται ο συνοριακός δρομολογητής του ΠΣΔ, η σύνδεση του ΠΣΔ με τον πάροχο του (ΕΔΕΤ) και καταλήγουν όλες οι γραμμές κορμού του.

Ο συνοριακός δρομολογητής αναδρομολογεί αυτομάτως τις αιτήσεις HTTP των χρηστών του ΠΣΔ σε μια συστοιχία εξυπηρετητών με τη χρήση της τεχνολογίας Cisco IP policy. Στους εξυπηρετητές λειτουργεί το ελεύθερο λογισμικό ανοιχτού κώδικα Squid ως transparent proxy server αναχαιτίζοντας με διαφανή τρόπο τις αιτήσεις των χρηστών. Οι χρήστες, δηλαδή, του ΠΣΔ δεν αντιλαμβάνονται την ύπαρξη του proxy server, ούτε χρειάζεται να προχωρήσουν σε ρύθμιση του, στους φυλλομετρητές τους (web browsers). Η καταλληλότητα ή όχι του περιεχομένου που ζητούν οι χρήστες κρίνεται από το λογισμικό SquidGuard, το οποίο διατηρεί βάση δεδομένων με ακατάλληλους ιστότοπους και ιστοσελίδες. Σε περίπτωση που το αίτημα κριθεί ακατάλληλο ο χρήστης ανακατευθύνεται σε μια ενημερωτική σελίδα, αλλιώς το Squid αναλαμβάνει να εξυπηρετήσει το αίτημα, φέρνοντας το σχετικό αντικείμενο από το διαδίκτυο.

Μια γενική εικόνα της διαδικασίας που ακολουθείται περιγράφεται στο ακόλουθο σχήμα:



Σχήμα 6.2: Διαδικασία αναδρομολόγησης κίνησης HTTP [95]

6.2.2 Squid

Το Squid (μεταφράζεται από τα Αγγλικά ως καλαμάρι) είναι ένας διακομιστής μεσολάβησης (web proxy) και ένας αυτόματος μηχανισμός (daemon) δημιουργίας κρυφής μνήμης σε μια ιστοσελίδα (web cache). Πρόκειται για Ελεύθερο λογισμικό/λογισμικό ανοιχτού κώδικα (ΕΛ/ΛΑΚ) με διάφορες χρήσεις, ανάμεσα στις οποίες είναι η επιτάχυνση ενός διακομιστή εξυπηρέτησης ιστοσελίδων (web server) με τη λειτουργία κρυφής μνήμης στα συχνά αιτήματα ιστοσελίδων, DNS και λοιπών αιτημάτων όταν μια ομάδα χρηστών μοιράζεται τους ίδιους δικτυακούς πόρους. Το Squid μπορεί να χρησιμοποιηθεί ως ασπίδα ασφαλείας, φιλτράροντας την κίνηση. Αν και το Squid χρησιμοποιείται κυρίως για αιτήματα μεταφοράς ιστοσελίδων (με το πρωτόκολλο http) αλλά και μεταφορές αρχείων (με το πρωτόκολλο ftp), έχει τη δυνατότητα να υποστηρίξει (με περιορισμούς) και διάφορα άλλα πρωτόκολλα όπως το TLS, SSL, Internet Gopher αλλά και το https [53].

Το Squid είχε αρχικά σχεδιαστεί να τρέχει σε συστήματα τύπου Unix, αλλά σήμερα τρέχει και σε λειτουργικά τύπου Windows. Το λογισμικό είναι ελεύθερο, διανέμεται με τη Γενική Άδεια Δημόσιας Χρήσης GNU και χρησιμοποιείται στα μεγαλύτερα εκπαιδευτικά δίκτυα διεθνώς όπως JANET (Αγγλία), GARR (Ιταλία), DFN (Γερμανία), SWITCH (Ελβετία), SURFnet (Δανία), NLANR (ΗΠΑ) [96].

6.2.3 Συστοιχία Εξυπηρετητών

Για την εξυπηρέτηση των αναγκών της υπηρεσίας έγινε προμήθεια 16 υπολογιστικών συστημάτων HP ProLiant DL380 G5 στα πλαίσια του έργου e-datacenter. Από αυτά, 8 χρησιμοποιούνται από την υπηρεσία, 2 χρησιμοποιούνται ως εφεδρικά και για δοκιμές, ενώ τα υπόλοιπα 6 έχουν δανειστεί σε άλλες υπηρεσίες του ΠΣΔ για την κάλυψη επειγουσών αναγκών. Κάθε ένα από τα συστήματα αυτά περιλαμβάνει ένα επεξεργαστή Intel Xeon E5420, 2 GB κεντρικής μνήμης, 3 δίσκους SAS σε διάταξη RAID1 (mirror) + hot spare και διπλό υποσύστημα τροφοδοσίας. Η εγκατάσταση των συγκεκριμένων συστημάτων έγινε στις αρχές του έτους 2010.

Στα συστήματα που χρησιμοποιούνται από την υπηρεσία έχει εγκατασταθεί η έκδοση 7.3 του λειτουργικού συστήματος FreeBSD και έχει παραμετροποιηθεί σύμφωνα με τα πρότυπα του Κέντρου Δικτύων του ΕΜΠ. Έχει ληφθεί ιδιαίτερη μέριμνα ώστε όλα τα συστήματα να είναι παραμετροποιημένα με τον ίδιο ακριβώς αυτοματοποιημένο τρόπο και να διαφέρουν μόνο σε

συγκεκριμένες παραμέτρους που αφορούν το καθένα από αυτά, όπως διεύθυνση IP, hostname κλπ. Με τον τρόπο αυτό εξασφαλίζεται η ομοιόμορφη συμπεριφορά τους, επιτυγχάνεται η διατήρηση του διαχειριστικού κόστους τους σε χαμηλά επίπεδα ασχέτως του πλήθους των μηχανών, δίνεται η δυνατότητα εύκολης και γρήγορης προσθήκης επιπλέον μηχανών όποτε αυτό θεωρηθεί σκόπιμο για τις ανάγκες της υπηρεσίας και δεν είναι αναγκαία η λήψη αντιγράφων ασφαλείας (backup) για κάθε σύστημα ξεχωριστά.

Πλέον του λειτουργικού συστήματος, έχουν εγκατασταθεί και χρησιμοποιούνται τα πακέτα λογισμικού Squid (έκδοση 2.7), SquidGuard (έκδοση 1.4) και Nginx (έκδοση 1.2).

Το Squid λειτουργεί ως διαμεσολαβητής (proxy server) για την εξυπηρέτηση των αιτημάτων HTTP των χρηστών του ΠΣΔ. Τα αιτήματα των χρηστών προωθούνται στη συστοιχία από τον κεντρικό δρομολογητή ως ροές πακέτων (packet flows) πρωτοκόλλου TCP με διευθύνσεις IP προορισμού εκτός ΠΣΔ και θύρα προορισμού 80. Το υποσύστημα δικτύου σε κάθε εξυπηρετητή είναι ρυθμισμένο καταλλήλως ώστε να αναγνωρίζει τις συγκεκριμένες ροές και να τις προωθεί στη διεργασία του Squid για τον περαιτέρω χειρισμό. Καθώς σε ώρες αιχμής κάθε εξυπηρετητής μπορεί να κληθεί να εξυπηρετήσει έως και μερικές εκατοντάδες αιτήματα HTTP το δευτερόλεπτο, η διεργασία του Squid έχει ρυθμιστεί έτσι ώστε να μην διατηρεί αντίγραφα των αιτημάτων (σελίδες HTML, εικόνες κλπ.) στον τοπικό δίσκο. Το παραπάνω κρίθηκε σκόπιμο, γιατί σε τέτοιους ρυθμούς η διαδικασία εγγραφής, αναζήτησης και ανάγνωσης από το δίσκο δημιουργούσε φαινόμενα κορεσμού και προσκαλούσε σοβαρές καθυστερήσεις στην εξυπηρέτηση των αιτημάτων. Εξάλλου, το εύρος ζώνης (bandwidth) των συνδέσεων του ΠΣΔ με το πάροχο του (ΕΔΕΤ) και στη συνέχεια με το διαδίκτυο είναι πλέον τόσο που τα οφέλη από τη λειτουργία του Squid ως caching proxy είναι μηδαμινά.

Το SquidGuard, που λειτουργεί σαν υποδιεργασία του Squid, διατηρεί τη βάση δεδομένων με τις ακατάλληλες σελίδες και αναλαμβάνει το ρόλο του διαιτητή επιτρέποντας ή μη την πρόσβαση στις σελίδες που ζητούν οι χρήστες. Η βάση δεδομένων είναι πανομοιότυπη για όλους τους εξυπηρετητές της συστοιχίας. Ο κάθε εξυπηρετητής διατηρεί το δικό του τοπικό αντίγραφο που ανανεώνεται αυτομάτως από κεντρικό σημείο. Η βάση περιλαμβάνει ανά κατηγορία ακατάλληλου περιεχομένου:

1. λίστα ονομάτων δικτυακών τόπων (hostnames, διευθύνσεις IP, domain names που περιέχουν αποκλειστικά ακατάλληλο περιεχόμενο.

2. λίστα διευθύνσεων ιστοσελίδων (URL) με ακατάλληλο περιεχόμενο που όμως φιλοξενούνται σε δικτυακούς τόπους που δεν περιλαμβάνουν αποκλειστικά ακατάλληλο περιεχόμενο.

3. λίστα με λέξεις κλειδιά και κανονικές εκφράσεις (regular expressions) που θεωρούνται ακατάλληλες και μπορεί να εμφανιστούν σε οποιοδήποτε σημείο της διεύθυνσης μιας ιστοσελίδας.

Η διαδικασία αξιολόγησης της καταλληλότητας ενός δικτυακού τόπου ή μιας ιστοσελίδας γίνεται από τους συντάκτες των παραπάνω λιστών. Η υπηρεσία ελέγχου περιεχομένου του ΠΣΔ χρησιμοποιεί αντίγραφα των συγκεκριμένων λιστών για ελέγξει την καταλληλότητα των σελίδων που ζητούν οι χρήστες του, ελέγχοντας σε πραγματικό χρόνο αν κάποιο από τα hostname, διεύθυνση IP, domain name ή URL της σελίδας ταυτίζεται με εγγραφή στη βάση. Σε καμία περίπτωση δεν γίνεται έλεγχος του περιεχομένου των σελίδων και των λοιπών αντικειμένων, όπως εικόνες, που ζητούν οι χρήστες και προσπάθεια αξιολόγησης της καταλληλότητας τους. Κάτι τέτοιο θα απαιτούσε πιθανώς πολλαπλάσιους υπολογιστικούς πόρους και εξελιγμένο λογισμικό που δεν είναι διαθέσιμο προς χρήση, τουλάχιστον με άδεια open source και χωρίς επιπλέον κόστος.

Επίσης, στη βάση διατηρούνται ορισμένες επιπλέον κατηγορίες περιεχομένου που δεν εμπίπτουν άμεσα σε αυτήν της ακατάλληλης για ανηλίκους. Οι κατηγορίες αυτές είναι:

1. Εξυπηρετητές στο διαδίκτυο που λειτουργούν ως open proxies και θα μπορούσαν να χρησιμοποιηθούν από τους χρήστες του ΠΣΔ για την παράκαμψη της υπηρεσίας ελέγχου περιεχομένου.

2. Παραβιασμένοι ιστότοποι ή ιστοσελίδες που έχουν μολυνθεί από επιτηδείους, φιλοξενούν επικίνδυνο υλικό (viruses, malware κλπ.) και τυχόν επίσκεψη σε αυτές θα μπορούσε να οδηγήσει σε μαζική μόλυνση υπολογιστών του ΠΣΔ.

3. Ιστότοποι ή ιστοσελίδες με ακατάλληλο υλικό που περιλαμβάνονται σε κάποια από όλες τις προηγούμενες κατηγορίες, αλλά προς το παρόν ακόμα δεν περιέχονται σε κάποια από τις λίστες που χρησιμοποιεί η υπηρεσία. Τέτοιες περιπτώσεις συνήθως αναφέρονται από τους χρήστες του ΠΣΔ και προστίθενται στη συγκεκριμένη ξεχωριστή κατηγορία.

4. Ιστότοποι ή ιστοσελίδες που κακώς αναφέρονται ως ακατάλληλες στις λίστες που χρησιμοποιεί η υπηρεσία. Τέτοιες περιπτώσεις συνήθως αναφέρονται από τους χρήστες του ΠΣΔ και προστίθενται στη συγκεκριμένη ξεχωριστή κατηγορία ώστε να εξαιρεθούν από τον αποκλεισμό.

Το Nginx λειτουργεί ως απλός εξυπηρετητής WWW στον οποίο καταλήγουν οι χρήστες όταν ζητούν να επισκεφτούν κάποια ακατάλληλη σελίδα. Φιλοξενεί μόνο μια στατική σελίδα που ενημερώνει το χρήστη για τους λόγους που δεν έχει πρόσβαση στην ιστοσελίδα που αρχικώς ζήτησε. Επιπλέον του παρέχει οδηγίες για τη διαδικασία που μπορεί να ακολουθήσει στην περίπτωση που θεωρεί ότι η αρχική ιστοσελίδα έχει κακώς κριθεί ακατάλληλη και επιθυμεί να αιτηθεί την άρση του περιορισμού. Η χρήση του λογισμικού Nginx σε σχέση με άλλα πιο δημοφιλή, όπως ο Apache HTTPd, κρίθηκε σκόπιμη για εξοικονόμηση πόρων του συστήματος.

Εικόνα 6.1: Ενημερωτική σελίδα για ακατάλληλο ιστότοπο.

Για την αποδοτικότερη λειτουργία της υπηρεσίας σε κάθε σύστημα λειτουργεί ξεχωριστός εξυπηρετητής ονοματοδοσίας (recursive caching name server), ο οποίος εξυπηρετεί αποκλειστικά τα αιτήματα του ίδιου του συστήματος, ως επί τω πλείστον προερχόμενα από το Squid. Χρησιμοποιείται το λογισμικό ISC BIND όπως διατίθεται προεγκατεστημένο από το λειτουργικό σύστημα [95].

6.2.4 Ρυθμίσεις Ανακατεύθυνσης Κίνησης στο Συνοριακό Δρομολογητή

Ο συνοριακός δρομολογητής του ΠΣΔ είναι ένας Cisco 7604. Ανάμεσα στα υπόλοιπα χαρακτηριστικά του είναι και η υποστήριξη της τεχνολογίας IP Policy, που επιτρέπει το χειρισμό μέρους της κίνησης που δρομολογείται μέσω της συσκευής με διαφορετικό τρόπο (από την συνήθη δρομολόγηση με βάση το πεδίο της διεύθυνσης προορισμού) εφόσον πληροί συγκεκριμένα κριτήρια που ορίζονται από το διαχειριστή της.

Η συγκεκριμένη τεχνολογία χρησιμοποιείται από την υπηρεσία ελέγχου περιεχομένου ως μηχανισμός διαφανούς ανακατεύθυνσης των αιτημάτων HTTP των χρηστών του ΠΣΔ που προορίζονται προς το διαδίκτυο. Συγκεκριμένα, οι ροές πακέτων που ικανοποιούν όλες οι ακόλουθες συνθήκες:

1. πρωτόκολλο TCP,

2. διεύθυνση (IP) αφετηρίας από το δίκτυο του ΠΣΔ,

3. διεύθυνση (IP) προορισμού εκτός δικτύου ΠΣΔ,

4. θύρα (port) προορισμού ίσο με 80

αντί να δρομολογηθούν προς το Διαδίκτυο, δρομολογούνται προς τη συστοιχία των εξυπηρετητών της υπηρεσίας ελέγχου περιεχομένου. Η κατανομή των αιτημάτων μεταξύ των οκτώ εξυπηρετητών της συστοιχίας γίνεται με βάση τα τρία τελευταία bits της διεύθυνσης IP προορισμού, δηλαδή του ιστότοπου που φιλοξενεί τη σελίδα που ζητά ο χρήστης. Με τον τρόπο αυτό κάθε ιστότοπος, εφόσον χρησιμοποιεί μία μόνο διεύθυνση IP θα εξυπηρετείται πάντα από τον ίδιο εξυπηρετητή της συστοιχίας. Η συγκεκριμένη συμπεριφορά είναι χρήσιμη στις περιπτώσεις που εμφανίζεται κάποιο πρόβλημα και απαιτείται εκσφαλμάτωση (debugging).

Τελικά, ο υπολογιστής του χρήστη καταλήγει, εν αγνοία του, να συνάπτει μία σύνδεση TCP με έναν από τους εξυπηρετητές της συστοιχίας, αντί με τον εξυπηρετητή της ιστοσελίδας που ζήτησε.

Για τις περιπτώσεις εξαιρέσεων, στις παραπάνω συνθήκες προστίθεται άλλη μία με την μορφή access list. Εάν η διεύθυνση (IP) προορισμού ταιριάζει με μία εγγραφή της συγκεκριμένης access list, τότε ακόμα και εάν ικανοποιεί τις αρχικές τέσσερις συνθήκες δεν ανακατευθύνεται. Οι

περιπτώσεις εξαιρέσεων που περιλαμβάνονται στη συγκεκριμένη access list χωρίζονται σε δύο κατηγορίες:

1. Δίκτυα που δεν περιέχουν ακατάλληλο περιεχόμενο, εξ ορισμού ή κατόπιν ελέγχου και είναι ιδιαίτερα δημοφιλή στους χρήστες. Για παράδειγμα, ελληνικά ή διεθνή ακαδημαϊκά ή ερευνητικά δίκτυα, υπηρεσίες του Υπουργείου Παιδείας και του Ελληνικού Κράτους, δίκτυα που προσφέρουν ενημερώσεις για λειτουργικά συστήματα (Microsoft updates) ή για λογισμικό προστασίας από ιούς (antivirus updates) κλπ. Η εξαίρεση τέτοιων περιπτώσεων γίνεται για την εξοικονόμηση πόρων της υπηρεσίας.

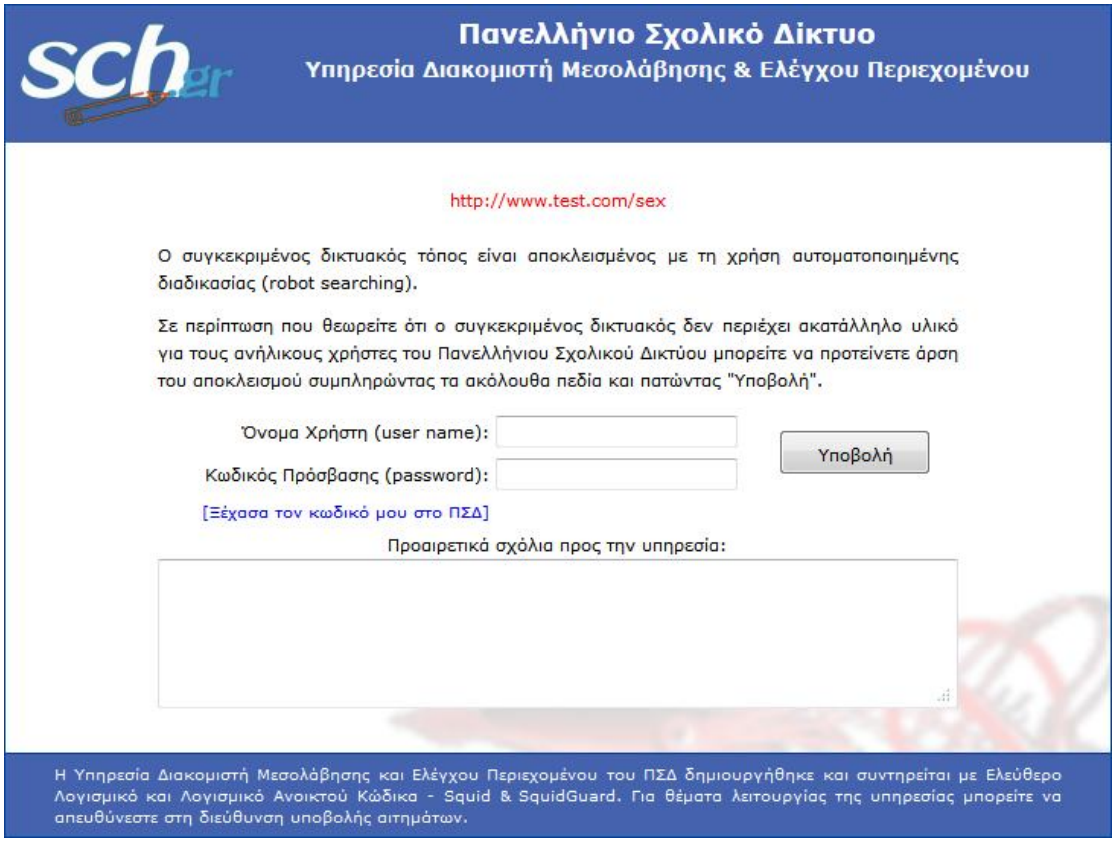
2. Συγκεκριμένοι δημοφιλείς ιστότοποι, με κατάλληλο περιεχόμενο, οι οποίοι θεωρούν τον αυξημένο αριθμό κλήσεων που δέχονται από τους εξυπηρετητές της υπηρεσίας ελέγχου περιεχομένου ως ένδειξη κακής χρήσης και απαγορεύουν την πρόσβαση από αυτούς. Αθροιστικά πρόκειται για μερικές δεκάδες περιπτώσεις που αυξάνονται με αργούς ρυθμούς με την πάροδο του χρόνου. Αρχικά, γινόταν προσπάθεια επικοινωνίας με τους διαχειριστές του κάθε ιστότοπου για την επίλυση της κάθε περίπτωσης. Το κόστος όμως σε ανθρώπινους πόρους από την πλευρά της υπηρεσίας ελέγχου περιεχομένου ήταν υπερβολικά υψηλό και συνεπώς ασύμφορο, οπότε και επιλέχθηκε η τρέχουσα λύση της παροδικής ή μόνιμης εξαίρεσης.

Το τρέχον σύστημα ανακατεύθυνσης και κατανομής της κίνησης HTTP επιλέχθηκε καθώς δεν κατέστη δυνατή η υλοποίηση της λύσης που περιελάμβανε τη χρήση ενός εξειδικευμένου μεταγωγέα επιπέδου 4/7 (Layer 4/7 switch). Η λύση του μεταγωγέα επιπέδου 4/7 θα προσέφερε δυνατότητα καλύτερης κατανομής του φορτίου της υπηρεσίας στους εξυπηρετητές της συστοιχίας, ασχέτως του πλήθους τους και δυνατότητα αυτόματης αναδρομολόγησης της κίνησης ενός εξυπηρετητή στους υπόλοιπους σε περίπτωση αστοχίας του. Όμως, η συγκεκριμένη λύση απαιτούσε και συγκεκριμένη δικτυακή τοπολογία εντός του ΠΣΔ, με ξεχωριστό δρομολογητή σε ρόλο αποκλειστικά συνοριακού (border router), κεντρικό δρομολογητή (core router) με τις συνδέσεις κορμού να καταλήγουν σε αυτόν και διασύνδεση των δύο μέσω του μεταγωγέα επιπέδου 4/7 με συνδέσεις ικανής χωρητικότητας ανάλογης αυτής της σύνδεσης με το διαδίκτυο (10 Gbps ή πολλαπλά 1 Gbps) [95].

6.2.5 Σύστημα Λογισμικού Εξυπηρέτησης Αιτημάτων Χρηστών

Για την εξυπηρέτηση των αιτημάτων των χρηστών της υπηρεσίας έχει υλοποιηθεί σύστημα λογισμικού προσβάσιμο μέσω WWW. Αποτελείται από δύο μέρη, ένα για τους τελικούς χρήστες και ένα για τους διαχειριστές της υπηρεσίας.

Το υποσύστημα που απευθύνεται στους τελικούς χρήστες είναι προσπελάσιμο από τη σελίδα που τους ενημερώνει ότι κάποιος δικτυακός τόπος δεν είναι διαθέσιμος λόγω ακατάλληλου περιεχομένου. Τους προσφέρει τη δυνατότητα να αιτηθούν την επανεξέταση της απαγόρευσης. Για την αποφυγή υποβολής άσκοπων αιτημάτων οι χρήστες καλούνται να ταυτοποιηθούν με username και password.



Εικόνα 6.2: Φόρμα υποβολής αιτήματος άρσης απαγόρευσης πρόσβασης

Το υποσύστημα για τους διαχειριστές της υπηρεσίας προσφέρει τη δυνατότητα εξυπηρέτησης των αιτημάτων των χρηστών. Καλύπτει τις περιπτώσεις αποχαρακτηρισμού ως ακατάλληλης μιας ολόκληρης δικτυακής περιοχής (π.χ. domain.com), ενός συγκεκριμένου δικτυακού τόπου (π.χ. hostname.domain.com) ή μιας μεμονωμένης ιστοσελίδας (π.χ. http://hostname.domain.com/path/page.html). Αντιστρόφως, καλύπτει και τις ανάλογες

περιπτώσεις χαρακτηρισμού περιοχών, τόπων και σελίδων ως ακατάλληλες. Επίσης, έχει τη δυνατότητα μαζικής εισαγωγής εγγραφών, καθώς και ελέγχου υποψήφιων εγγραφών. Οι νέες εγγραφές προωθούνται σε τακτά χρονικά διαστήματα αυτομάτως στους εξυπηρετητές της υπηρεσίας.

Εικόνα 6.3: Διαχειριστικό περιβάλλον υπηρεσίας ελέγχου περιεχομένου

Προς το παρόν φιλοξενείται σε υποδομή του Κέντρου Δικτύων ΕΜΠ και θα μπορούσε να αναπτυχθεί περαιτέρω καλύπτοντας και τις λειτουργίες που θα αναπτυχθούν, όπως την υποστήριξη για IPv6, τον μηχανισμό ελέγχου περιεχομένου μέσω DNS, τη διαχείριση τις λίστας εξαιρέσεων PROXY-BYPASS, κλπ.

6.2.6 Σύστημα Λογισμικού Ελέγχου Καλής Λειτουργίας Υπηρεσίας

Για τον έλεγχο της καλής λειτουργίας της υπηρεσίας και την παρακολούθηση διαφόρων παραμέτρων της χρησιμοποιείται η σχετική υποδομή του Κέντρου Δικτύων του ΕΜΠ. Η υποδομή αυτή περιλαμβάνει τα ακόλουθα μέρη:

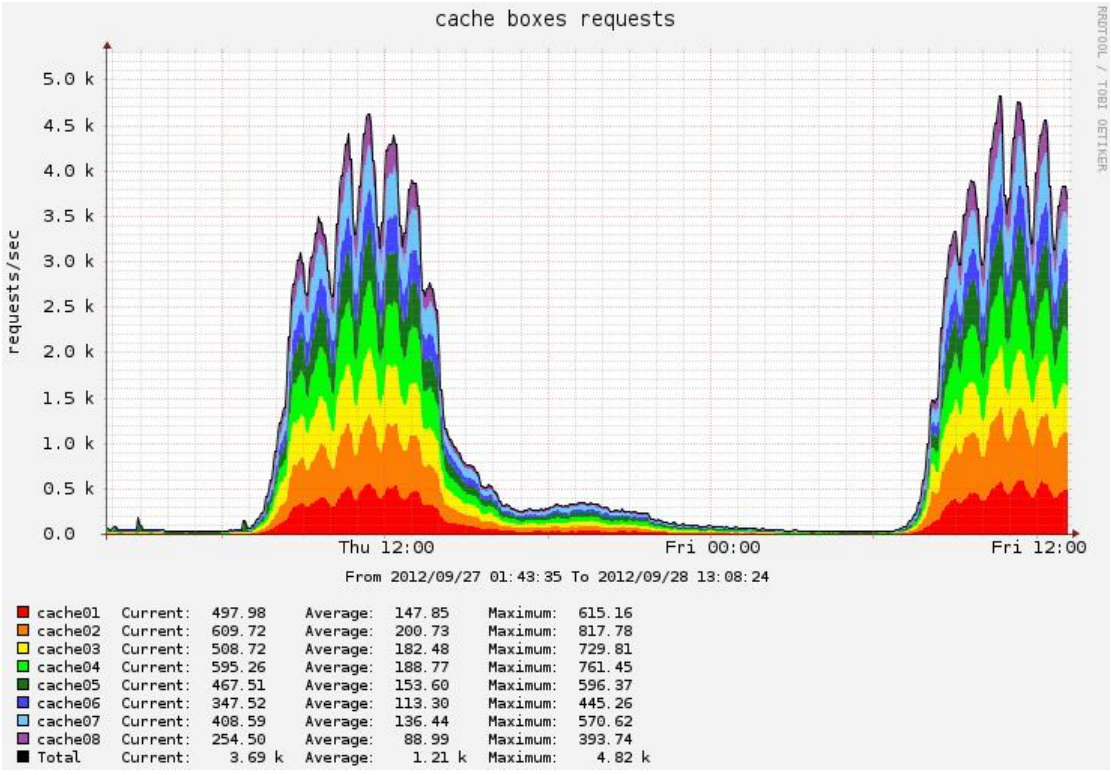
1. Λογισμικό Nagios για την παρακολούθηση της καλής λειτουργίας των εξυπηρετητών (υλικό, λειτουργικό σύστημα, λογισμικό Squid, δικτυακή σύνδεση κλπ.) και την άμεση

ενημέρωση των διαχειριστών της υπηρεσίας μέσω ηλεκτρονικού ταχυδρομείου σε περίπτωση δυσλειτουργίας.

2. Λογισμικό Cacti για την παρακολούθηση διαφόρων παραμέτρων των εξυπηρετητών και την αποτύπωσή τους σε γραφήματα (ημερήσια, εβδομαδιαία, μηνιαία, ετήσια) διαθέσιμα online [95].

6.2.7 Αναβάθμιση Συστήματος Αναδρομολόγησης με Χρήση Πρωτοκόλλου WCCP

Η αυτόματη αναδρομολόγηση των αιτημάτων HTTP των χρηστών του ΠΣΔ γίνεται με τη χρήση του μηχανισμού του IP policy στο συνοριακό δρομολογητή. Η συγκεκριμένη μέθοδος λειτουργεί απρόσκοπτα καλύπτοντας τις αυξημένες απαιτήσεις της υπηρεσίας χωρίς προβλήματα ή ιδιαίτερη επιβάρυνση του συνοριακού δρομολογητή. Επιπλέον, παρέχει ευέλικτο μηχανισμό εξαιρέσεων μέσω της access list PROXY-BYPASS. Η μέθοδος κατανομής του φορτιού των αιτημάτων στους οκτώ εξυπηρετητές της υπηρεσίας έχει ικανοποιητικά αποτελέσματα, αλλά όχι βέλτιστα, καθώς ορισμένοι από τους εξυπηρετητές αναλαμβάνουν σε σταθερή βάση την εξυπηρέτηση έως και υποδιπλασιάσου αριθμού αιτημάτων από τους υπόλοιπους (βλ. σχετικό διάγραμμα).



Εικόνα 6.4: Κατανομή αιτημάτων HTTP ανά εξυπηρετητή [95].

Το σοβαρότερο μειονέκτημα της μεθόδου του IP policy είναι ότι δεν προσφέρει μηχανισμούς για αυτόματη αντιμετώπιση προβλημάτων αστοχίας ενός ή περισσοτέρων εξυπηρετητών της υπηρεσίας. Στο τρέχον σχήμα, εάν κάποιος από τους εξυπηρετητές παρουσιάσει βλάβη (στο υλικό ή στο λογισμικό του) η κίνηση HTTP που του αναλογεί θα συνεχίσει να ανακατευθύνεται σε αυτόν χωρίς όμως να είναι δυνατή η εξυπηρέτησή της. Το αποτέλεσμα για τους τελικούς χρήστες είναι ότι δεν έχουν πρόσβαση στο συγκεκριμένο υποσύνολο του παγκόσμιου ιστού (WWW) μέχρι είτε να διορθωθεί η βλάβη, είτε να παρακαμφθεί ο συγκεκριμένος εξυπηρετητής. Τόσο η αντιμετώπιση της βλάβης, όσο και η παράκαμψη του συγκεκριμένου εξυπηρετητή γίνεται με παρέμβαση του διαχειριστή της υπηρεσίας στις ρυθμίσεις του συνοριακού δρομολογητή. Η ίδια διαδικασία ακολουθείται και σε κάθε περίπτωση προγραμματισμένης διακοπής για εργασίες στους εξυπηρετητές, π.χ. για αναβαθμίσεις.

Για την αντιμετώπιση του προβλήματος εξετάστηκε στο παρελθόν η λύση της χρήσης ενός μεταγωγέα επιπέδων 4/7 (Layer 4/7 switch). Ο μεταγωγέας θα αναλάμβανε τις λειτουργίες της ανακατεύθυνσης της κίνησης, της κατανομής της με καλύτερο τρόπο στους εξυπηρετητές και της αντιμετώπισης αστοχιών με αυτόματη ανακατανομή της κίνησης του προβληματικού κόμβου στους υπόλοιπους. Όμως, η δικτυακή τοπολογία (κεντρικός δρομολογητής – μεταγωγέας επιπέδων 4/7 – συνοριακός δρομολογητής) που απαιτούσε η συγκεκριμένη λύση δεν μπόρεσε να υλοποιήθηκε για διάφορους τεχνικούς και οικονομικούς λόγους.

Εναλλακτική λύση που είναι πλέον διαθέσιμη και προσφέρει τα ίδια πλεονεκτήματα είναι η χρήση του πρωτοκόλλου Web Cache Communication Protocol (WCCP). Το συγκριμένο πρωτόκολλο προτάθηκε και υλοποιήθηκε αρχικώς από την εταιρία Cisco, στη συνέχεια προτυποποιήθηκε και πλέον είναι διαθέσιμο σε συσκευές και λογισμικά τρίτων κατασκευαστών.

Σκοπός του πρωτοκόλλου WCCP είναι να προσφέρει μέσα από το ίδιο το λειτουργικό σύστημα της Cisco (IOS) λειτουργίες και δυνατότητες που αρχικά ήταν διαθέσιμες μόνο από εξειδικευμένες συσκευές, όπως οι μεταγωγείς επιπέδων 4/7. Έτσι από την έκδοση 12.1 και έπειτα του Cisco IOS, οι εκδόσεις 1 και 2 του πρωτοκόλλου WCCP είναι διαθέσιμες στις συσκευές της Cisco (δρομολογητές και μεταγωγείς).

Η έκδοση 1 του πρωτοκόλλου WCCP, υποστηρίζει αποκλειστικά την εξυπηρέτηση κίνησης HTTP (θύρα 80) από ένα δρομολογητή και ένα ή περισσότερους εξυπηρετητές.

Η έκδοση 2 υποστηρίζει:

- έως 32 δρομολογητές σε διάταξη cluster,
- οποιοδήποτε πρωτόκολλο IP (TCP ή UDP)
- έως 255 διαφορετικές υπηρεσίες ταυτόχρονα,
- ταυτοποίηση των συμμετεχόντων μερών με χρήση MD5 shared secret security.

Μία λύση που στηρίζεται στο πρωτόκολλο WCCP αποτελείτε από τα ακόλουθα μέρη:

1. Τον πελάτη WCCP (WCCP client ή WCCP engine), ρόλο που αναλαμβάνει ένας ή περισσότεροι εξυπηρετητές που τρέχουν λογισμικό proxy caching (όπως το Squid). Οι πελάτες αρχικά καταχωρούν την ύπαρξή τους και τις δυνατότητές τους, δηλαδή τις υπηρεσίες που είναι σε θέση να εξυπηρετήσουν (HTTP κλπ.) και σε τακτικά χρονικά διαστήματα ανακοινώνουν τη διαθεσιμότητά τους (μηνύματα «Here I Am»).

2. Τον εξυπηρετητή WCCP (WCCP server), ρόλο που αναλαμβάνει ένας ή περισσότεροι δρομολογητές ή μεταγωγείς. Καταχωρεί σε ομάδες ανά υπηρεσία τους πελάτες WCCP που έχουν ανακοινώσει την ύπαρξή τους, παρακολουθεί τη διαθεσιμότητά τους (από τα μηνύματα που λαμβάνει) και αναλόγως αναδρομολογεί με ομοιόμορφο τρόπο την κίνηση στους διαθέσιμους πελάτες. Στους δρομολογητές η αναδρομολογούμενη κίνηση από τον εξυπηρετητή WCCP προς τους πελάτες WCCP διοχετεύεται μέσω πρωτοκόλλου GRE (tunneling) ώστε το περιεχόμενο των αρχικών πακέτων IP να παραμείνει αναλλοίωτο. Στους μεταγωγείς υποστηρίζεται μηχανισμός αναδρομολόγησης επιπέδου 2 (Layer 2 redirection) αντί του καναλιού GRE [95],

6.3 Παροχή Υπηρεσίας Ελέγχου Περιεχομένου σε Τρίτους Μέσω DNS

Στους χρήστες που βρίσκονται εντός του ΠΣΔ εφαρμόζεται κεντρικά έλεγχος περιεχομένου για την εμπόδιση πρόσβασης σε σελίδες με ακατάλληλο ή επικίνδυνο περιεχόμενο. Το σύνολο των ακατάλληλων σελίδων διατηρείται σε ειδικά διαμορφωμένη βάση δεδομένων. Στόχος είναι η

δυνατότητα χρησιμοποίησης της βάσης δεδομένων από τρίτους που δεν βρίσκονται εντός του ΠΣΔ, για παράδειγμα από γονείς σε οικιακές συνδέσεις.

Στο ΠΣΔ έχουν αναπτυχθεί διαδικασίες για την συντήρηση και επικαιροποίηση της βάσης δεδομένων. Οι διαδικασίες αυτές αποτελούνται από αυτόματες ενημερώσεις από άλλες γνωστές και ευρέως χρησιμοποιούμενες βάσεις στο Διαδίκτυο, αλλά και από χειροκίνητες εισαγωγές (ή αντίθετα εξαιρέσεις) ύστερα από αιτήματα των χρηστών. Συνεπώς, προκειμένου η νέα υπηρεσία να έχει όσο το δυνατόν λιγότερο διαχειριστικό κόστος, είναι απαραίτητο να χρησιμοποιηθεί η υπάρχουσα βάση δεδομένων από την υπηρεσία ελέγχου περιεχομένου εντός του ΠΣΔ.

Εντός του ΠΣΔ, ο έλεγχος περιεχομένου βασίζεται στην αυτόματη αναδρομολόγηση των αιτήσεων HTTP των χρηστών του ΠΣΔ σε μια συστοιχία εξυπηρετητών proxy. Επειδή δεν υπάρχει αντίστοιχος τρόπος για αυτόματη δρομολόγηση αιτήσεων από χρήστες που βρίσκονται σε διαφορετικά δίκτυα, προτείνεται η χρήση της υπηρεσίας ονοματοδοσίας (DNS).

Στο Διαδίκτυο το κατανεμημένο σύστημα ονοματοδοσίας που ονομάζεται Domain Naming System (DNS) επιτρέπει την αναφορά σε κόμβους του δικτύου όχι με την IP διεύθυνσή τους (Internet Protocol address) αλλά με μνημονικά ονόματα (hostnames). Οι πληροφορίες ονοματοδοσίας διαχωρίζονται με βάση το Domain name σε διαφορετικές ζώνες και αποθηκεύονται σε διαφορετικούς εξυπηρετητές. Ο εξυπηρετητής Ονοματοδοσίας που είναι υπεύθυνος για κάποια συγκεκριμένη ζώνη, αυτός δηλαδή που διατηρεί την πρωτογενή πληροφορία, ονομάζεται authoritative name server. Ο εξυπηρετητής ο οποίος αναλαμβάνει την εύρεση της IP διεύθυνσης ενός hostname αναζητώντας τον κατάλληλο authoritative name server, ονομάζεται recursive/caching name server.

Ο στόχος είναι η εκμετάλλευση του πρωτοκόλλου DNS ώστε όταν κάποια αίτηση περιέχει hostname το οποίο θεωρείται ακατάλληλο (βρίσκεται δηλαδή στη βάση δεδομένων της υπηρεσίας ελέγχου περιεχομένου του ΠΣΔ), αντί να επιστρέφεται από τον εξυπηρετητή ονοματοδοσίας η πραγματική IP διεύθυνση του hostname, να επιστρέφεται η διεύθυνση εξυπηρετητή του σχολικού δικτύου. Με τον τρόπο αυτό, ο χρήστης θα οδηγείται σε ειδική σελίδα και θα ενημερώνεται ότι ο δικτυακός τόπος που θέλει να επισκεφθεί είναι ακατάλληλος.

Για την εφαρμογή της παραπάνω διαδικασίας:

- Χρειάζεται η δημιουργία και παραμετροποίηση ειδικού λογισμικού το οποίο θα λειτουργεί ως recursive/caching name server, το οποίο πριν επιστρέψει την πραγματική διεύθυνση ενός hostname θα ελέγχει αν ανήκει στη βάση δεδομένων της υπηρεσίας ελέγχου περιεχομένου.

- Χρειάζεται κάθε χρήστης που θέλει να χρησιμοποιήσει την υπηρεσία, να ορίζει χειροκίνητα στον υπολογιστή του, ως εξυπηρετητές ονοματοδοσίας, τους ειδικά διαμορφωμένους εξυπηρετητές που θα στηθούν για την νέα υπηρεσία. Για τις περιπτώσεις οικιακών δικτυακών συνδέσεων (π.χ. συνδέσεις ADSL) ο ορισμός του εξυπηρετητή ονοματοδοσίας μπορεί να οριστεί κεντρικά στο δρομολογητή της σύνδεσης (ADSL modem/router). Με τον τρόπο αυτό καλύπτονται όλες οι συσκευές στο σπίτι που χρησιμοποιούν τη συγκεκριμένη σύνδεση.

Καθώς θα χρησιμοποιηθεί η υπηρεσία ονοματοδοσίας για το φιλτράρισμα του περιεχομένου, από τις διαθέσιμες λίστες που βρίσκονται στη βάση δεδομένων του ΠΣΔ για τον έλεγχο περιεχομένου είναι δυνατό να χρησιμοποιηθεί μονάχα η λίστα ονομάτων ιστότοπων (hostnames, διευθύνσεις IP, domain names) που περιέχουν αποκλειστικά ακατάλληλο περιεχόμενο.

Για λόγους καλής λειτουργίας των recursive/caching name server και προκειμένου να μπορούν να αντεπεξέρθουν στο φορτίο, συνήθως αυτοί ρυθμίζονται έτσι ώστε να δέχονται αιτήσεις μονάχα από υπολογιστές που ανήκουν στο δίκτυό τους. Στην περίπτωση της υπηρεσίας αυτής, οι name server που θα στηθούν θα πρέπει να είναι «ανοιχτοί» σε αιτήματα από εξωτερικά δίκτυα. Ανάλογα με το πόσο δημοφιλής μπορεί να γίνει η υπηρεσία, μπορεί να αυξηθεί αρκετά το φορτίο στα μηχανήματα αυτά. Συνεπώς, θα πρέπει:

- Να προβλεφθεί κατά τη μελέτη και ανάπτυξη της υπηρεσίας η χρήση λογισμικού το οποίο θα μπορεί να υποστεί μεγάλο φορτίο.

- Να διαχωριστεί η νέα υπηρεσία ονοματοδοσίας από την υπάρχουσα, ώστε να μην επηρεαστεί η ποιότητα υπηρεσίας εντός του ΠΣΔ.

- Να εξεταστεί κατά πόσο είναι δυνατόν να περιοριστεί η πρόσβαση σε κόμβους που ανήκουν σε συγκεκριμένα δίκτυα (π.χ. σε δίκτυα μονάχα στην Ελλάδα) [95].

6.3.1 Παρόμοιες Υπηρεσίες στο Διαδίκτυο

Υπηρεσία παρόμοια με αυτή που προτείνεται στο υπάρχον κείμενο προσφέρεται από τον οργανισμό openDNS (http://www.opendns.com/). Πέρα από τη βασική και κρίσιμη μετάφραση ονομάτων (name resolution), το OpenDNS προσφέρει και κάποιες άλλες λειτουργίες, π.χ.:

- Διορθώνει λάθη πληκτρολόγησης. Αν για παράδειγμα ο χρήστης πληκτρολογήσει κατά λάθος το όνομα exemple.com αντί για το example.com, επιστρέφεται τελικά στο χρήστη μια σελίδα με προτάσεις ή με το σύνδεσμο για το δικτυακό τόπο τον οποίο ήθελε να επισκεφθεί ο χρήστης. Για τη λειτουργία αυτή χρειάζεται η συνεργασία ανάμεσα σε name server και web server. Στη πράξη, η λειτουργία αυτή προσφέρεται ήδη από διάφορους browser (για παράδειγμα τον chrome σε συνεργασία με τη μηχανή αναζήτησης της Google).

- Με την αξιοποίηση δεδομένων που συλλέγει ειδικό λογισμικό ασφαλείας, προστατεύει κατά του «phishing» (κακόβουλοι ιστότοποι που συστήνονται ως κάτι άλλο απ' αυτό που είναι, με σκοπό συνήθως να αποσπάσουν προσωπικά ευαίσθητα δεδομένα των χρηστών, όπως για παράδειγμα στοιχεία πιστωτικών καρτών).

Η υπηρεσία αυτή παρέχεται δωρεάν σε οικιακούς χρήστες, και επί πληρωμή σε μεγαλύτερους ή πολύ μεγάλους πελάτες, μαζί με την προσφορά επιπλέον χαρακτηριστικών, όπως ο γονικός έλεγχος (parental control) που ενδιαφέρει και στην περίπτωση που εξετάζεται.

Παρόμοια υπηρεσία προσφέρεται και από τη Norton. Πιο συγκεκριμένα, η υπηρεσία που ονομάζεται Norton DNS (https://dns.norton.com/dnsweb/) προσφέρει δημόσιους name servers με την παρακάτω πολιτική:

- Πολιτική 1 - Ασφάλεια: Αυτή η πολιτική εμποδίζει όλους τους τόπους που φιλοξενούν malware, phishing, και γενικότερα ιστοσελίδες με μη ασφαλές περιεχόμενο.

- Πολιτική 2 - Ασφάλεια + Πορνογραφία: Εκτός από τον αποκλεισμό των μη ασφαλών δικτυακών τόπων, αυτή η πολιτική εμποδίζει την πρόσβαση σε ιστοσελίδες που περιέχουν υλικό σεξουαλικού περιεχομένου.

- Πολιτική 3 - Ασφάλεια, Πορνογραφία και μη φιλικές προς οικογένειες ιστοσελίδες (non-Family Friendly). Η πολιτική αυτή απευθύνεται σε οικογένειες με μικρά παιδιά. Εκτός

από τον αποκλεισμό των μη ασφαλών ιστοσελίδων και των ιστοσελίδων με πορνογραφία, αυτή η πολιτική εμποδίζει την πρόσβαση σε ιστοσελίδες που διαθέτουν περιεχόμενο που απευθύνεται σε ενήλικες, με θέματα όπως το αλκοόλ, το έγκλημα, τα ναρκωτικά, τα τυχερά παιχνίδια, το κάπνισμα ή τη βία.

Σε κάθε διαφορετική πολιτική, διατίθεται ξεχωριστό ζεύγος από name server [95].

6.3.2 Περιγραφή Λύσης

Για την κάλυψη των απαιτήσεων που περιγράφηκαν στην προηγούμενη ενότητα, προτάθηκε το λογισμικό BIND σε συνδυασμό με τη χρήση της τεχνολογίας Response Policy Zones (RPZ).

Το BIND είναι το μακράν πιο ευρέως χρησιμοποιούμενο λογισμικό DNS στο Διαδίκτυο. Είναι λογισμικό ανοιχτού κώδικα που υλοποιεί τα πρωτόκολλα του Domain Name System για το Διαδίκτυο. Είναι μια εφαρμογή αναφοράς για τα πρωτόκολλα αυτά, αλλά είναι επίσης λογισμικό που χρησιμοποιείται ευρέως σε συστήματα παραγωγής, καθώς είναι κατάλληλο για χρήση σε μεγάλου όγκου και υψηλής αξιοπιστίας συστήματα.

Η έκδοση BIND 9.8.1 περιλαμβάνει το Response Policy Zone (RPZ) Rewriting, έναν μηχανισμό τροποποίησης των DNS απαντήσεων για αναδρομικές αιτήσεις (recursive queries), παρόμοιο σε λειτουργία με τις anti-spam DNS Blacklists. Με το μηχανισμό αυτό, η απάντηση σε κάποιο αίτημα ονοματοδοσίας μπορεί να αλλάξει και αντί για την επιστροφή της διεύθυνσης IP του hostname που ζητήθηκε, ο εξυπηρετητής ονοματοδοσίας είτε να αρνηθεί την ύπαρξη της δικτυακής υποπεριοχής (NXDOMAIN), είτε να αρνηθεί την ύπαρξη διευθύνσεων IP για τον συγκεκριμένο δικτυακό τόπο (NODATA), ή να επιστρέψει άλλη IP διεύθυνση.

Οι ζώνες RPZ είναι κοινές ζώνες DNS που περιέχουν εγγραφές DNS (RRsets) που θα μπορούσαν να χρησιμοποιηθούν σε οποιαδήποτε άλλη ζώνη ονοματοδοσίας. Προκειμένου να ενεργοποιηθεί ο μηχανισμός τροποποίησης, οι ζώνες αυτές ορίζονται με τη επιλογή response-policy option στο αρχείο ρυθμίσεων του BIND.

Υπάρχουν τέσσερα είδη εγγραφών στις ζώνες RPZ: QNAME, IP, NSIP, και NSDNAME. Από τα παραπάνω είδη, στην περίπτωσή που ενδιαφέρει την παρούσα μελέτη, μπορούν να χρησιμοποιηθούν οι εγγραφές IP και QNAME (που αφορούν ερωτήσεις A, AAAA και CNAME).

Συνεπώς, τα βήματα που χρειάζεται να γίνουν για την εγκατάσταση της υπηρεσίας είναι τα ακόλουθα [95]:

- Εγκατάσταση σε κατάλληλους εξυπηρετητές του λογισμικού BIND 9.8.1 ή νεότερου με δυνατότητα χρήσης RPZ με παράλληλη ρύθμιση για αποδοχή αναδρομικών αιτημάτων από εξωτερικά δίκτυα (εκτός ΠΣΔ). Τα δίκτυα από τα οποία θα επιτρέπεται να δρομολογηθούν αιτήματα ονοματοδοσίας προς τους εξυπηρετητές αυτούς μπορούν να περιοριστούν στον ελληνικό χώρο (ΠΣΔ,ΕΔΕΤ,GRIX), ρυθμίζοντας κατάλληλες access lists στους συνοριακούς δρομολογητές του ΠΣΔ.

- Δημιουργία ενός προγράμματος (script) που θα τρέχει περιοδικά, σε χρόνους που αντιστοιχούν στο χρονοδιάγραμμα αυτόματης ανανέωσης της βάσης δεδομένων της υπηρεσίας ελέγχου περιεχομένου του ΠΣΔ, το οποίο θα συλλέγει τα hostname που φιλοξενούν ακατάλληλες ιστοσελίδες και θα εισάγει αντίστοιχες εγγραφές (A,AAAA,CNAME) σε μια ειδική ζώνη ονοματοδοσίας.

- Η ζώνη ονοματοδοσίας θα προσφέρεται από τους εξυπηρετητές ονοματοδοσίας της υπηρεσίας και θα επαναφορτώνεται αυτόματα μετά από κάθε εκτέλεση του script.

- Λειτουργία web server στον οποίο θα ανακατευθύνονται μέσω DNS/RPZ οι χρήστες που έχουν ορίζει ως name server τους εξυπηρετητές της νέας υπηρεσίας, ο οποίος θα προσφέρει ειδική σελίδα που θα ενημερώνει το χρήστη ότι προσπάθησε να προσπελάσει ακατάλληλο ή επικίνδυνο περιεχόμενο. Αντίστοιχη υπηρεσία χρησιμοποιείται είδη για τον έλεγχο περιεχομένου εκτός του ΠΣΔ.

6.4 Υλοποίηση Υπηρεσίας για το Πρωτόκολλο HTTPS

Η τρέχουσα έκδοση της υπηρεσίας ελέγχου περιεχομένου του ΠΣΔ αναδρομολογεί τις κλήσεις που γίνονται μέσω του πρωτοκόλλου HTTP (θύρα TCP 80). Οι κλήσεις που γίνονται μέσω του πρωτοκόλλου HTTPS (Secure HTTP – θύρα TCP 433), όπως και τυχόν κλήσεις μέσω πρωτοκόλλου HTTP σε θύρες διαφορετικές της 80 δεν αναδρομολογούνται και κατά συνέπεια δεν ελέγχονται για ακατάλληλο περιεχόμενο.

Η συγκεκριμένη προσέγγιση, μέχρι στιγμής δεν έχει δημιουργήσει παράπονα από τους χρήστες του ΠΣΔ καθώς δεν έχουν εμφανιστεί περιπτώσεις ιστοσελίδων με ακατάλληλο περιεχόμενο που να διατίθενται μέσω θυρών διαφορετικών της 80. Εξαίρεση στον κανόνα αποτελούν οι ιστότοποι κοινωνικής δικτύωσης, όπως το Facebook, το Google+ κλπ., οι οποίοι πλέον σε μία προσπάθεια να διασφαλίσουν το απόρρητο της επικοινωνίας και των δεδομένων των χρηστών τους διαθέτουν τις υπηρεσίες μέσω του πρωτοκόλλου HTTPS. Οι συγκεκριμένες υπηρεσίες, κατόπιν απόφασης του ΠΣΔ, δεν είναι διαθέσιμες στους μαθητές των Δημοτικών σχολείων (παιδιά ηλικίας μικρότερης των 13 ετών). Ο συγκεκριμένος περιορισμός δεν έχει εφαρμοστεί μέσω της υπηρεσίας ελέγχου περιεχομένου καθώς όλες οι εκπαιδευτικές μονάδες, ανεξαρτήτου βαθμίδας, λαμβάνουν διευθύνσεις IP από κοινό χώρο διευθύνσεων και συνεπώς δεν είναι δυνατό να διαχωριστούν σε Δημοτικά σχολεία και λοιπά. Αντί αυτού, προτιμήθηκε η επιλεκτική εφαρμογή access list στους δρομολογητές των Δημοτικών σχολείων με αυτοματοποιημένο τρόπου μέσω της υπηρεσία Radius.

Η εκτίμηση που επικρατεί είναι πως και στο μέλλον δεν πρόκειται να εμφανιστούν σοβαρές περιπτώσεις ιστότοπων με ακατάλληλο περιεχόμενο που να διατίθενται μέσω πρωτοκόλλου HTTPS ή άλλης θύρας διαφορετικής της 80. Σε κάθε περίπτωση όμως, η υπηρεσία ελέγχου περιεχομένου του ΠΣΔ θα πρέπει να είναι σε θέση να αντιμετωπίσει τέτοιες περιπτώσεις, είτε στα πλαίσια της τυπικής λειτουργίας της, είτε με εναλλακτικούς τρόπους [95].

6.4.1 Τρόποι Ελέγχου Κίνησης HTTPS Μέσω Λογισμικού Squid

Η υπηρεσία ελέγχου περιεχομένου, όπως αναφέρθηκε και πιο πάνω λειτουργεί σε μορφή transparent proxy με τους εξυπηρετητές της υπηρεσίας να παρεμβάλλονται ανάμεσα στους φυλλομετρητές των χρηστών και τους ιστότοπους που ζητούν να επισκεφτούν. Οι συνδέσεις των χρηστών καταλήγουν στους εξυπηρετητές της υπηρεσίας και αυτοί με τη σειρά τους ξεκινούν νέες προς τους ιστότοπους. Όμως, οι συνδέσεις HTTPS έχουν ως βασικό χαρακτηριστικό τους ότι ο φυλλομετρητής του χρήστη δέχεται από τον ιστότοπο υπογεγραμμένο ψηφιακό πιστοποιητικό που αποδεικνύει την αυθεντικότητά του και εξασφαλίζει το απόρρητο της επικοινωνίας και την ακεραιότητα των δεδομένων που διακινούνται.

Σε περίπτωση που παρεμβληθεί ανάμεσα τους κάποιος τρίτος, έστω και οι εξυπηρετητές του ΠΣΔ, τίθενται θέματα εμπιστευτικότητας και παραβίασης απορρήτου επικοινωνιών και ως εκ τούτου θεωρείται κακή πρακτική (man in the middle attack). Από την κοινότητα του λογισμικού

Squid έχουν αναπτυχθεί ορισμένες τεχνολογίες που επιτρέπουν την αναδρομολόγηση συνδέσεων HTTPS σε περιβάλλον transparent proxy όπως η τεχνολογία «Squid - in - the - middle SSL Bump». Στην περίπτωση αυτή, το λογισμικό Squid παρουσιάζει στο χρήστη ένα δικό του ψηφιακό πιστοποιητικό και στη συνέχεια ξεκινάει νέα σύνδεση HTTPS με το ζητούμενο ιστότοπο. Το μειονέκτημα της συγκεκριμένης μεθόδου είναι ότι το ψηφιακό πιστοποιητικό του Squid δεν ταιριάζει με το όνομα του ιστότοπου που ζητάει ο χρήστης και στις περισσότερες περιπτώσεις κάθε σύγχρονος φυλλομετρητής θα παρουσιάσει μία ή περισσότερες προειδοποιήσεις (warnings) στο χρήστη, τις οποίες ο χρήστης θα κληθεί να αγνοήσει. Κάτι τέτοιο είναι εντελώς αντίθετο με την κουλτούρα που προσπαθεί να εμπεδώσει το ΠΣΔ στους νέους χρήστες του διαδικτύου για ασφαλή περιήγηση σε αυτό.

Για την ελαχιστοποίηση των προειδοποιήσεων των φυλλομετρητών αναπτύσσονται από την κοινότητα του λογισμικού Squid οι τεχνολογίες «Dynamic SSL Certificate Generation». Η πρώτη είναι διαθέσιμη στην έκδοση 3.2 και επιτρέπει την έκδοση ψηφιακών πιστοποιητικών σε πραγματικό χρόνο από Αρχή Πιστοποίησης που μπορεί διαθέτει εσωτερικά το λογισμικό Squid, αλλά από μόνη της δεν μπορεί να λειτουργήσει σε σχήμα transparent proxy. Η δεύτερη βρίσκεται υπό ανάπτυξη, θα είναι διαθέσιμη στην έκδοση 3.3 και χρησιμοποιείται για να μεταφέρει σε σχήμα transparent proxy το σωστό όνομα του τελικού ιστότοπου στην Αρχή Πιστοποίησης που θα παραγάγει το προσωρινό πιστοποιητικό [95].

6.4.2 Εναλλακτικοί Τρόποι Ελέγχου Κίνησης HTTPS

Εναλλακτικοί τρόποι αντιμετώπισης ιστότοπων με ακατάλληλο περιεχόμενο σε θύρες διαφορετικές της 80 είναι:

- Εφαρμογή περιορισμού πρόσβασης στους συγκεκριμένους ιστότοπους με την προθήκη κατάλληλης εγγραφής στην access list που υπάρχει στη σύνδεση του ΠΣΔ -ΕΔΕΤ του συνοριακού δρομολογητή. Η συγκεκριμένη access list μπορεί να δεχτεί δεκάδες, ίσως και εκατοντάδες, νέες εγγραφές, υπεραρκετές για τις λίγες περιπτώσεις που αναμένεται τυχόν να εμφανιστούν.

- Αξιοποίηση του μηχανισμού ελέγχου περιεχομένου μέσω πρωτοκόλλου DNS, που περιγράφηκε σε προηγούμενο κεφάλαιο, εντός ΠΣΔ με εγκατάστασή του στους εξυπηρετητές ονοματοδοσίας που χρησιμοποιούν οι τελικοί χρήστες του ΠΣΔ. Με τον

τρόπο αυτό, οι χρήστες δεν θα μπορούν να έχουν πρόσβαση στους ιστότοπους που αποκλείονται ασχέτως της θύρας που χρησιμοποιούν αυτοί.

Σημειώνεται ότι οι παραπάνω δύο προτεινόμενοι εναλλακτικοί τρόποι λειτουργούν για ολόκληρους ιστότοπους και όχι για μεμονωμένες ιστοσελίδες, δηλαδή δεν επιτρέπουν τον αποκλεισμό της πρόσβασης αποκλειστικά σε συγκεκριμένες ιστοσελίδες [95].

6.5 Συμπεράσματα

Το Πανελλήνιο Σχολικό Δίκτυο είναι το μεγαλύτερο δημόσιο δίκτυο στη χώρα σε αριθμό χρηστών και απευθύνεται στο πιο κρίσιμο και ευαίσθητο κοινό, τους μαθητές. Ο έλεγχος της προσπέλασης με βάση το περιεχόμενο σε ένα τέτοιο δίκτυο είναι αναμενόμενος και σε σημαντικό βαθμό επιθυμητός, προκειμένου να παρέχεται προστασία στους ανήλικους από τους κινδύνους που αφορούν κυρίως στην έκθεση τους σε παράνομο ή ακατάλληλο περιεχόμενο και στην εξαπάτηση τους από άγνωστους ενήλικες.

Η επιλογή που γίνεται για τον κεντρικό έλεγχο περιεχομένου του ΠΔΣ βασίζεται σε Ελεύθερο Λογισμικό ευρείας χρήσης, το Squid, έναν καλά διαμορφούμενο proxy & cache server που ανακατευθύνει το περιεχόμενο. Αποκλείονται ιστοσελίδες που έχουν σχέση με πορνογραφία και ειδικά παιδική, προπαγάνδα ναρκωτικών, προπαγάνδα βίας, μίσους, επιθετικής συμπεριφοράς και ρατσισμού, τυχερά παιχνίδια, πληροφορίες για παραβιάσεις ασφαλείας υπολογιστικών συστημάτων κα.. Η «μαύρη» λίστα προέρχεται από τη λίστα ακατάλληλων δικτυακών τόπων και σελίδων που δημιουργήθηκε και συντηρείται από τους δημιουργούς του επίσης Ελευθέρου Λογισμικού SquidGuard.

Η χρήση των συγκεκριμένων λογισμικών έχει σημαντικά πλεονεκτήματα, όπως το χαμηλό κόστος, την γρήγορη ανταπόκριση και τη δυνατότητα ποικιλόμορφης παραμετροποίησης. Η παροχή υπηρεσίας ελέγχου περιεχομένου σε τρίτους μέσω DNS και η δυνατότητα ελέγχου κίνησης HTTPS είναι επίσης σημαντικές παράμετροι. Η επιλογή τεχνικών που θα εξέταζαν σε βάθος το περιεχόμενο με καλύτερα πιθανόν αποτελέσματα είναι απαγορευτική για το συγκεκριμένο δίκτυο στην παρούσα φάση, κυρίως λόγο κόστους του απαραίτητου εξοπλισμό.

Κεφάλαιο 7
Συμπεράσματα

Η τεχνολογία ελέγχου προσπέλασης με βάση το περιεχόμενο είναι μια τεχνολογία εξαιρετικά ενδιαφέρουσα και ταχύτατα εξελισσόμενη που προκαλεί αντιπαραθέσεις σε σχέση με τον τρόπο και την αναγκαιότητα εφαρμογής της. Είτε πρόκειται για εφήβους στο σπίτι είτε για εργαζόμενους στο χώρο εργασίας ή ακόμη και απλά για πολίτες που επικοινωνούν, αναζητούν και διασκεδάζουν στο Διαδίκτυο, οι ηθικές, τεχνολογικές και οικονομικές επιπτώσεις των μηχανισμών ελέγχου, αποτελούν πρόκληση για οποιονδήποτε επιχειρηματολογεί υπέρ ή εναντίον της εφαρμογής τους.

Η θέση της λειτουργίας των μηχανισμών ελέγχου ποικίλει και εξαρτάται από τις διαθέσιμες τεχνικές δυνατότητες αλλά και την έκταση της εφαρμογής που είναι επιθυμητό να έχει. Έτσι κλιμακώνεται από το επίπεδο του τελικού χρήστη έως τα όρια μιας ευρύτερης περιοχής, όπως είναι η επικράτεια μιας χώρας. Σε κάθε περίπτωση πάντως, δύο είναι οι λειτουργίες που καλείται να επιτελέσει το φιλτράρισμα, η αναγνώριση του ανεπιθύμητου περιεχομένου και στη συνέχει ο αποκλεισμός του.

Η πρώτη βασική τεχνολογία αναγνώρισης είναι αυτή που βασίζεται σε λίστες, «μαύρες» ή «άσπρες», που περιέχουν κάποιο χαρακτηριστικό από το υλικό που είναι επιθυμητό να αποκλειστεί ή αυτό που μόνο πρέπει να μεταδοθεί αντίστοιχα. Οι λίστες μπορεί να περιέχουν IP ή

URL διευθύνσεις ή ακόμη και λέξεις κλειδιά, ανάλογα με το σε πιο επίπεδο κυμαίνεται η εφαρμογή που πραγματοποιεί τον έλεγχο. Η επιλογή αυτή εκμεταλλεύεται πολλές φορές, ειδικά στην περίπτωση του ελέγχου σε επίπεδο δικτύου, τις ήδη υπάρχουσες διαδικτυακές υποδομές με αποτέλεσμα να είναι οικονομική, γρήγορη και σχετικά αποτελεσματική. Παρότι είναι η πιο παλιά τεχνολογία αναγνώρισης περιεχομένου εξακολουθεί να χρησιμοποιείται ευρέως, κάποιες φορές για ένα γρήγορο πρώτο ξεκαθάρισμα της πληροφορίας, μια που μπορεί εύκολα να συνδυαστεί με τον αποκλεισμό του περιεχομένου μέσω της αναδρομολόγησης ή της απόρριψης των διακινούμενων πακέτων.

Η χρήση λέξεων ή φράσεων κλειδιών σε λίστες δεν αλλάζει την λογική της σύγκρισης για τον εντοπισμό του ακατάλληλου περιεχομένου, οδηγεί όμως αναπόφευκτα στον έλεγχο του ωφέλιμου φορτίου (payload), των προς επιθεώρηση διακινούμενων δεδομένων. Λαμβάνοντας υπόψη την ποικιλία, την μεταβλητότητα και τη διαδραστικότητα της φύσης του διακινούμενου υλικού στο Διαδίκτυο καθιερώνεται η επόμενη γενιά τεχνολογιών ελέγχου περιεχομένου, με πιο ευφυή και δυναμικά χαρακτηριστικά που απαιτούν και πετυχαίνουν σε μεγάλο βαθμό, τη σε βάθος επιθεώρηση και ανάλυση της μεταδιδόμενης πληροφορίας, προκειμένου να την κατατάξουν. Στην περίπτωση αυτή γίνεται χρήση «έξυπνων» αλγόριθμων, συστημάτων τεχνητής νοημοσύνης και τεχνολογίας ανάλυσης εικόνας και βίντεο, με σκοπό να αναγνωριστεί δυναμικά, πολλές φορές και σε πραγματικό χρόνο το ακατάλληλο περιεχόμενο. Οι απαιτήσεις σε υπολογιστικούς πόρους και κατά συνέπεια σε υλικοτεχνική υποδομή και επενδύσεις είναι μεγαλύτερες για αυτούς που επιθυμούν να εφαρμόσουν τον έλεγχο. Επιπλέον το πρόσθετο υπολογιστικό φορτίο που προκύπτει, μπορεί να προκαλεί κατά περίπτωση σημαντικές καθυστερήσεις.

Η εκ των προτέρων βαθμονόμηση και σήμανση του περιεχομένου και η εμπλοκή των τελικών χρηστών στην επιλογή του περιεχομένου που επιθυμούν να καταναλώσουν, με την έννοια του αυτοκαθορισμού, είναι μια επιλογή που συνδυαστικά ή αυτόνομα μπορεί να λειτουργήσει αποτελεσματικά στην διαδικασία του φιλτραρίσματος. Προς την κατεύθυνση αυτή αναμένεται να συμβάλει η περεταίρω καθιέρωση του σημασιολογικού ιστού. Πέρα από την απλή ετικετοδότηση των διακινούμενων δεδομένων, πολλές φορές από τρίτους, η ανάδειξη της σημασίας τους δίνει άλλη διάσταση στην επιλογή του περιεχομένου είτε από το τελικό χρήστη είτε από αυτόν που επιθυμεί να παρέμβει εξωτερικά.

Η μέθοδος αποκλεισμού περιλαμβάνει μια ποικιλία τεχνικών που κάποιες φορές είναι άμεσα συνδεδεμένες με την μέθοδο αναγνώρισης του περιεχομένου. Χρησιμοποιούνται τεχνολογίες που

επεμβαίνουν στην δρομολόγηση της πληροφορίας ή του αιτήματος για αυτήν. Υπάρχουν όμως και πιο δυναμικές τεχνικές όπως η επιθέσεις άρνησης παροχής υπηρεσιών (DDos) ή ακόμη και η χρήση βίαιων ή και κοινωνικών μεθόδων, όπως ο τερματισμός λειτουργίας εξυπηρετητών που φιλοξενούν το ανεπιθύμητο περιεχόμενο.

Η επιλογή της τεχνολογίας φιλτραρίσματος εξαρτάται άμεσα από τον σκοπό που έχει αυτός που επιδιώκει τον έλεγχο, αλλά και τα μέσα που διαθέτει. Η αξιολόγηση των μηχανισμών ελέγχου βασίζεται στα κριτήρια της αποτελεσματικότητα του και του κόστους εφαρμογής του. Η αποτελεσματικότητα καθορίζεται ως ο βαθμός επιτυχίας αποκλεισμού του πραγματικά ακατάλληλου περιεχομένου και η αποφυγή καταστάσεων υπερβολικού (over blocking) ή ελλιπούς (under blocking), φιλτραρίσματος με μπλοκάρισμα κατάλληλου ή προώθηση ακατάλληλου υλικού, αντίστοιχα.

Το θέμα του κόστους της εφαρμογής τεχνολογιών ελέγχου προσπέλασης με βάση το περιεχόμενο, είναι πολυδιάστατο. Όσο αφορά το οικονομικό κόστος, σίγουρα απαιτούνται κάποιες, μικρότερες ή μεγαλύτερες ανάλογα με την εφαρμογή, επενδύσεις σε υλικοτεχνική υποδομή. Επιπλέον η διαδικασία ελέγχου πολλές φορές επιβραδύνει την ταχύτητα διασύνδεσης και αυτό μεταφράζεται σε σπατάλη πόρων. Από την άλλη όμως ο έλεγχος περιεχομένου, σε εργασιακούς χώρους για παράδειγμα, μπορεί να αυξήσει την παραγωγικότητα ή να προστατεύσει οικονομικές δραστηριότητες που σχετίζονται με την υπεραξία της πνευματικής ιδιοκτησίας, καταστάσεις που πρέπει να συνεκτιμούνται στην οικονομική αξιολόγηση τέτοιων επιλογών.

Η πιο σημαντική παράμετρος όμως στην συνολική συζήτηση για τις τεχνολογίες φιλτραρίσματος του περιεχομένου στο Διαδίκτυο δεν αφορά το οικονομικό κόστος, αλλά την επίδραση τους σε μη υλικά αγαθά. Το όφελος από την προστασία ευαίσθητων κοινωνικά ομάδων, όπως είναι οι ανήλικοι, αλλά και το ρίσκο από τον περιορισμό βασικών ανθρωπίνων δικαιωμάτων, όπως η ελευθερία του λόγου, μετατοπίζουν το κέντρο βάρους των επιπτώσεων στο χώρο της ηθικής και της πολιτικής. Το Internet λόγω της αποκεντρωμένης και φιλελεύθερης δομής του, αποτελεί ιδανικό εργαλείο για επικοινωνία και ελεύθερη διάδοση πληροφοριών και ιδεών, αλλά παράλληλα και πρόσφορο έδαφος για ανεμπόδιστη ανάπτυξης παραβατικών δράσεων.

Ο αριθμός των κρατών που περιορίζουν την πρόσβαση στο περιεχόμενο του Διαδικτύου έχει αυξηθεί ραγδαία τα τελευταία χρόνια. Με επιχειρήματα ή προσχήματα όπως την εξασφάλιση δικαιωμάτων πνευματικής ιδιοκτησίας, την προστασία της εθνικής ασφάλειας, τη διατήρηση

των πολιτιστικών και θρησκευτικών αξιών και κυρίως την προστασία των παιδιών από την πορνογραφία, ειδικά την παιδική, πολλά κράτη εφαρμόζουν πρακτικές εκτεταμένου φιλτραρίσματος με σκοπό να περιορίσουν την αντίληψη ανομίας που υπάρχει για το μέσο.

Χαρακτηριστικότερο παράδειγμα κράτους που εφαρμόζει σε ευρεία κλίμακα έλεγχο περιεχομένου είναι η Κίνα, ακολουθούμενη από πλήθος άλλων χωρών, συνήθως του αναπτυσσόμενου κόσμου, όπου κυριαρχούν καθεστώτα με αυταρχικές τάσεις που επιδιώκουν τη καταστολή οποιασδήποτε αμφισβήτησης τους, παραβιάζοντας θεμελιώδη ανθρώπινα δικαιώματα. Αλλά και στο δυτικό κόσμο, με αφετηρία κυρίως την προστασία των παιδιών και της πνευματικής ιδιοκτησίας λειτουργούν μηχανισμοί ελέγχου, σε μικρότερο η μεγαλύτερο βαθμό, η νομική και ηθική κατοχύρωση των οποίων αποτελεί κέντρο μιας διεθνούς διαβούλευσης.

Παράλληλα, αν όχι ένα βήμα πιο μπροστά, με τις τεχνολογίες ελέγχου πρόσβασης εξελίσσονται και οι τεχνολογίες παράκαμψης αυτού του ελέγχου. Με κυρίαρχο κίνητρο την επιχειρηματολογία κατά του ελέγχου περιεχομένου και των δικαιωμάτων που αυτός παραβιάζει και βασικό πλεονέκτημα την φιλελεύθερη αποκεντρωμένη και κατανεμημένη δομή του Διαδικτύου, έχουν αναπτυχθεί πλήθος τεχνικών που να δίνουν διέξοδο στους περιορισμούς στην πρόσβαση που επιβάλλονται από άτομα, οργανισμούς ή κυβερνήσεις. Αυτές μπορεί να είναι αρκετά απλοϊκές, από την αλλαγή βασικών στοιχείων επικοινωνίας προκειμένου να «ξεγελάσουν» τον έλεγχο, μέχρι πιο εξεζητημένες. Η λογική που ακλουθείτε συνηθέστερα στις περιπτώσεις αυτές είναι η παράκαμψη μέσω διαμεσολάβησης. Όταν δηλαδή ένα τρίτο μέρος, διαδρομή, υπολογιστής ή πρωτόκολλο, αναλαβαίνει να μεταφέρει την απαγορευμένη πληροφορία.

Οι τεχνολογίες ελέγχου προσπέλασης με βάση το περιεχόμενο, αλλά και αυτές παράκαμψης τους, είναι ένα ιδιαίτερα δυναμικό κομμάτι της τεχνολογίας επικοινωνιών, που συνδέεται άμεσα με την μεταβαλλόμενη φύση των υπηρεσιών του Διαδικτύου. Η μελέτη των τεχνολογιών αυτών πρέπει πάντα να γίνεται σε συνδυασμό με τις κοινωνικές, πολιτικές και οικονομικές καταστάσεις από τις οποίες επιβάλλονται και τις οποίες επηρεάζουν. Ένα «καλό σύστημα φιλτραρίσματος» πρέπει να συνδυάζει και να συνυπολογίζει πολλές σημαντικές παραμέτρους, όπως τη διαλειτουργικότητα, τη συμβατότητα προς πολλές κατευθύνσεις, την αυτονομία του τελικού χρήστη, το σεβασμό της ελευθερίας της έκφρασης, της ιδεολογικής πολυμορφίας, της διαφάνειας και της ιδιωτικής ζωής,. Η ελευθερία του λόγου πρέπει να προστατεύεται μέσω τεχνολογικού σχεδιασμού και μέσω των διαχειριστικών και νομοθετικών ρυθμίσεων της τεχνολογίας. Σε κάθε περίπτωση, τόσο η τεχνολογία όσο και το νομικό υπόβαθρο της θα πρέπει

να είναι δομημένα με τέτοιο τρόπο ώστε το Διαδίκτυο να παραμείνει ένα μέσο που προάγει τις ατομικές ελευθερίες [1].

Βιβλιογραφία

[01] Australian Communication and Media Authority. «Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety». ACMA, 2008.

[02] Australian Communication and Media Authority. «Closed Enviroment Testing of ISP-Levele Internet Content Filtering». ACMA, 2008.

[03] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz,Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia. « Above the Clouds: A Berkeley View of Cloud Computing». UC Berkeley Reliable Adaptive Distributed Systems Laboratory, http://radlab.cs.berkeley.edu/, 2009

[04] M. Tariq Banday, Nisar A. Shah. «A Concise Study of Web Filtering», Sprouts:Working Papers on Information Systems, 10(31). http://sprouts.aisnet.org/10-31, 2010.

[05] Judit Bayer. «The Legal Regulation of Illegal and Harmful Content on the Internet». Central European University, Open Society Institute, 2003.

[06] Elisa Bertino, Elena Ferrari, Andrea Perego, Gian Piero Zarri. «Advanced Techniques for Web Content Filtering». Encyclopedia of Internet Technologies and Applications, Information Science reference, Hershey • New York, 2008

[07] Soren Billing. «Saudi Campaign to Clean Up YouTube». ITP.net, www.itp.net/564689-saudi-campaign-to-clean-up-youtube, 2009

[08] Constance Bitso, Ina Fourie, Theo Bothma. «Trends in transition from classical censorship to Internet censorship: selected country overviews». IFLA, FAIFE spotlight, 2012

[09] Henry Blodget. «State od the Internet : 2012». Bussines Insider, 2012.

[10] Vincent Bourgais, Heidi Seybert. «Internet access and use in 2012». Eurostat News Release, 2012.

[11] Yana Breindl, Joss Wright. «Internet Filtering Trends in Western Liberal Democracies: French and German Regulatory Debates». Workshop on Free and Open Communications on the Internet, 2012

[12] Peter Burrows. «Internet Censorship, Saudi Style». Business Week, http://www.businessweek.com/stories/2008-11-12/internet-censorship-saudi-style, 2008

[13] Cormac Callanan, Marco Gercke, Estelle De Marco, Hein Dries-Ziekenheiner. «Internet Blocking Balancing Cybercrime Responses in Democratic Societies». Aconite Internet Solutions, 2009.

[14] «Cisco Quick Product Reference Guide 2011», Cisco 2011.

[15] Hillary Rodham Clinton. «Remarks on Internet Freedom». http://www.state.gov/secretary/rm/2010/01/135519.htm, 21 Ιανουαρίου 2010.

[16] Baris Cus. «Information Filtering on Micro-blogging Services». Master's Thesis, Swiss Federal Institute of Technology Zurich, 2010.

[17] Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain. «Access Denied,The Practice and Policy of Global Internet Filtering». OpenNet, MIT Press, 2008.

[18] Ronald Deibert, Rafal Rohozinski. «Liberation vs. Control: The Future of Cyberspace».The Johns Hopkins University Press, Journal of Democracy, Volume 21, Number 4, Σελίδες 43-57, 2010.

[19] Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain. «Access Controlled,The Shaping of Power, Rights, and Rule in Cyberspace». OpenNet, MIT Press, 2010.

[20] Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain. «Access Contested, Security, Identity, and Resistance in Asian Cyberspace». OpenNet, MIT Press, Σελίδες 273-289, 2012.

[21] Maximillian Dornseif. «Government Mandated Blocking of ForeignWeb Content». Jan von Knop,Wilhelm Haverkamp, Eike Jessen (Editors): Security E-Learning, E-Services, Σελίδες 617-648, 2003.

[22] «The Anti-Counterfeiting Trade Agreement». European Commission, 2008.

[23] Elena Ferrari, Bhavani Thuraisingham. «Web and Information Security». London: IRM Press, Idea Group. Publ., 2006.

[24] Patricia Moloney Figliola. «Promoting Global Internet Freedom: Policy and Technology». CRS Report for Congress, Congressional Research Service, 2012.

[25] Simson Garfinkel. «Web Security, Privacy and Commerce, 2nd Edition». Cambridge, MA: O'Reilly & Associates, 1998.

[26] Davis Gossett, Jack D. Shorter. «Effectiveness of Internet Content Filtering». Journal of Information Technology Impact, Vol. 11, No. 2, Σελίδες 145-152, 2011.

[27] Stefanos Gritzalis, Lilian Mitrou. «Content Filtering Technologies and the Law». Securing Information and Communication Systems Principles, Technologies, and Applications,Steven M. Furnell, Sokratis Katsikas, Javier Lopez, Ahmed Patel, Artech House, Κεφάλαιο 12 , Σελίδες 243-265, 2008.

[28] Virginia Heffernan. «Granting Anonymity». New York Times Magazine, 17 Δεκεμβρίου 2010.

[29] Hose Maria Gomez Hidalgo, Enrique Puertas Sanz, Francisco Carrero Garcia, Manuel DeBuenaga Rodriguez. «Web Content Filtering». Advances in Computers, Τόμος 76, Σελίδες 257-306, 2009.

[30] Brian Hindley, Hosuk Lee-Makiyama. «Protectionism Online:Internet Censorship and International Trade Law». ECIPE Working Paper, 2009.

[31] Shuk Ying Ho, Siu Man Lui. «Exploring the Factors Affecting Internet Content Filters Acceptance». ACM SIG e-Com Exchange, Vol. 5, No. 1, Σελίδες 29–36, 2003.

[32] http://refer-points.blogspot.gr/2011/04/chapter-7-web-content.html# , Δεκέμβριος 2012

[33] «How To Bypass Internet Censorship». http://www.howtobypassinternetcensorship.org, 2011.

[34] http://el.wikipedia.org/wiki/SSL, Ιανουάριος 2013.

[35] Διαδικτυακή κοινότητα φοιτητών νομικής 2005, http://www.new-dimension.gr/e107_plugins/content/content.php?content.34, Ιανουάριος 2013.

[36] «Politically Motivated Cyber Attacks». Help Net Security, http://www.net-security.org/secworld.php?id=9957, 6 Οκτωβρίου 2010

[37] «Thai Website to Protect the King». BBC News, http://news.bbc.co.uk/2/hi/asia-pacific/7871748.stm, 2009

[38] «Telenor and KRIPOS introduce Internet child pornography filter». Telenor Norge), Telenor Press Release, http://presse.telenor.no/PR/200409/961319_5.html, 21 Σεπτεμβρίου 2004.

[39] http://en.wikipedia.org/wiki/Viacom_International_Inc._v._YouTube,_Inc., Ιανουάριος 2013.

[40] http://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act, Ιανουάριος 2013.

[41] http://eleftheriskepsii.blogspot.gr/2012/12/blog-post_3747.html, Ιανουάριος 2013.

[42] http://el.wikipedia.org/wiki/Stop_Online_Piracy_Act, Φεβρουάριος 2013.

[43] http://www.govtrack.us/congress/bills/112/s968/text, Φεβρουάριος 2013.

[44] http://judiciary.house.gov/hearings/pdf/112%20HR%203261.pdf, Φεβρουάριος 2013.

[45] http://portal.kathimerini.gr/4dcgi/_w_articles_kathworld_1_04/07/2012_450433, Φεβρουάριος 2013.

[46] http://www.lexology.com/library/detail.aspx?g=83358d53-fbbb-47da-b936-a0271439a750, Φεβρουάριος 2013.

[47] http://blog.dnhost.gr/2012/02/14/acta, Ιανουάριος 2013.

[48] http://en.wikipedia.org/wiki/PROTECT_IP_Act, Ιανουάριος 2013.

[49] http://internet-safety.sch.gr, Ιανουάριος 2013.

[50] EUROPA > Σύνοψη της νομοθεσίας της ΕΕ > Κοινωνία της πληροφορίας > ΔΙΑΔΙΚΤΥΟ, ΕΠΙΓΡΑΜΜΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΚΑΙ ΤΥΠΟΠΟΙΗΣΗ ΤΩΝ ΤΠΕ, http://europa.eu/legislation_summaries/information_society/internet/index_el.htm, Ιανουάριος 2013.

[51] http://en.wikipedia.org/wiki/Internet_censorship_in_Canada#Internet, Ιανουάριος 2013.

[52] http://www.newsbeast.gr/technology/arthro/353943/xekina-kai-stin-ellada-i-logokrisia-tou-internet/, Ιανουάριος 2013

[53] http://www.squid-cache.org/, Ιανουάριος 2013

[54] http://www.internetworldstats.com/, Ιανουάριος 2013

[55] http://www.newmediatrendwatch.com, Ιανουάριος 2013.

[56] http://www.dslprime.com/dslprime/42-d/4830-internet-transit-costs-down-50-in-last-year, Ιανουάριος 2013.

[57] http://www.w3.org/2001/sw/, Ιανουάριος 2013.

[58] http://el.wikipedia.org/wiki/Peer-to-peer, Ιανουάριος 2013.

[59] http://en.wikipedia.org/wiki/IPTV, Ιανουάριος 2013.

[60] http://www.w3.org/PICS/, Δεκέμβριος 2012.

[61] http://www.w3.org, Δεκέμβριος 2012.

[62] http://en.wikipedia.org/wiki/Resource_Description_Framework, Δεκέμβριος 2012.

[63] http://www.w3.org/RDF/, Δεκέμβριος 2012 .

[64] «Online content filtering: technology overview». I sieve Technologies, http://www.i-sieve.com/downloads/i_sieve_overview.pdf, Δεκέμβριος 2012.

[65] Sanja Kelly, Sarah Cook. «New Technologies, Innovative Represion: Growing Threats to Internet Freedom». Freedom House, Freefom on the Net, 2011

[66] Sanja Kelly, Sarah Cook, Mai Truong. «Freedom on the Net A Global Assesment of Internet and Digital Media». Freedom House, 2012.

[67] Joseph Migga Kizza. «Virus and Content Filtering». A Guide to Computer Network Security The Computer Communications and Networks, Σελίδες 331-350, 2009.

[68] Nikolaos Koumartzis. «BT's CleanFeed and Online Censorship in UK, Improvements for a more Secure and Ethically Correct System». University of the Arts London, εκδ. CreateSpace, 2008.

[69] Franc Kozamernik, Michael Mullane. «An Intoduction to internet Radio». EBU 2005

[70] John Markoff. «Iranians and Others Outwit Net Censors». New York Times, 30 Απριλίου 2009.

[71] Antony Mayfield. «What is Social Media».icrossing.co.uk/ebooks, 2008.

[72] Philip McCrea, Bob Smart, Mark Andrews. «Blocking Content on the Internet:a Technical Perspective». CSIRO, Mathematical and Information Sciences, 1998.

[73] Evgeny Morozov. «Whither Internet Control?».The Johns Hopkins University Press, Journal of Democracy, Volume 22, Number 2, Σελίδες 62-74, 2011,

[74] John Musser. «Web 2.0 Principles and Best Practices».O'Reilly Radar Team, 2006.

[75] Erica Naone. «Political Net Attacks Increase». Technology Review, 13 Μαρτίου 2009.

[76] Peter Nicoletti. «Content Filtering». Computer and Information Security Handbook, Elsevier, Σελίδες 723-744, 2009.

[77] Innocent Okeke. «Regulation and Censorship of the Internet». Bachelor's Thesis Guidelines, DP in Business Information Technology, Haaha Helia University of Applied Sciences, 2012.

[78] Maija Palmer. «Face Recognition Software Gaining a Broader Canvas». Financial Times, http://www.ft.com/cms/s/0/6e213416-653a-11df-b648-00144feab49a.html#axzz2NclIaf8O, 22 Μαΐου 2010.

[79] Jane Parry, Myles Gorton, Shirley Brown, Graham Titterington, Craig Skinner. «Internet content filtering», A Report to DCITA. 2003.

[80] «Internet Enemies Report 2012». Reporters Without Borders, 2012

[81] Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris, John Palfrey. «2010 Circumvention Tool Usage Report». Berkman Center for Internet and Society at Harvard University, 2010.

[82] Charlie Savage. «U.S. Tries to Make It Easier to Wiretap the Internet». New York Times, 27 Σεπτεμβρίου 2010.

[83] Heidi Seybert. «Internet use in households and by individuals in 2011». Eurostat, 2011.

[84] Denis Shestakov. «Sampling the National Deep Web». A. Hameurlain et al. (Eds.): DEXA , Part I, LNCS 6860, Σελίδες 331–340, 2011.

[85] Tom Simonite. «Surveillance Software Knows What a Camera Sees». MIT Technology Review, http://www.technologyreview.com/news/419171/surveillance-software-knows-what-a-camera-sees/1 Ιουνίου 2010.

[86] Gerri Sinclair, Julie Zilber, Ed Hargrave. «Regulating Content on the Internet: A New Technological Perspective». A Report for Industry Canada, http://www.ic.gc.ca, 2008.

[87] Matt Tett. «Content Filtering Technologies Overview».Enex Testlab, http://www.cso.com.au/article/393605/content_filtering_technologies_overview/, 2011.

[88] «The Complete Guide to Social Media». The Social Media Guys, 2010.

[89] Marco Vanetti, Elisabetta Binaghi, Barbara Carminati,Moreno Carullo, and Elena Ferrari. «Content-Based Filtering in On-Line Social Networks». Privacy and Security Issues in Data Mining and Machine Learning, Lecture Notes in Computer Science Volume 6549, Σελίδες 127-140, 2011.

[90] Barney Warf. «Global Internet Censorship». Global Geographies of the Internet, SpringerBriefs in Geography, The Author(s), Σελίδες 45-75, 2013.

[91] Barney Warf. «Geographies of global Internet censorship». GeoJournal,Springer Science+Business Media B.V., 201.

[92] Michael Wines. «In Restive Chinese Area, Cameras Keep Watch». New York Times, http://www.nytimes.com/2010/08/03/world/asia/03china.html?pagewanted=all&_r=0, Αύγουστος 2010.

[93] Sebastian Wolfgarten. «Investigating Large-Scale Internet Content Filtering». M.Sc. in Security & Forensic Computing, Dublin City University, 2006.

[94] «The State of Internet 2nd Quarter 2012 Report». Akamai, Volume 5, Number 2, 2012

[95] Δημήτριος Καλογεράς, Βασίλειος Χατζηγιαννάκης, Παναγιώτης Χριστιάς. «Μελέτη Σχεδιασμού Υπηρεσίας Ελέγχου Περιεχομένου WWW». «Σ Τ Η Ρ Ι Ζ Ω» - Οριζόντιο έργο υποστήριξης σχολείων, εκπαιδευτικών και μαθητών στο δρόμο για το ΨΗΦΙΑΚΟ ΣΧΟΛΕΙΟ, νέες υπηρεσίες Πανελλήνιου Σχολικού Δικτύου και Στήριξης του ΨΗΦΙΑΚΟΥ ΣΧΟΛΕΙΟΥ, ΕΠΣΕΥ, 2012

[96] Δημήτριος Καλογεράς. «Έλεγχος Περιεχομένου σε Εκπαιδευτικά Δίκτυα:Πολιτικές και Κατευθύνσεις που εφαρμόζει το Πανελλήνιο Σχολικό Δίκτυο για την προστασία των μαθητών από παράνομο και προσβλητικό περιεχόμενο στο Internet». Υπηρεσία Ελέγχου Περιεχομένου ΠΣΔ, Εθνικό Μετσόβιο Πολυτεχενείο, 2012

[97] Πανελλήνιο Σχολικό Δίκτυο. www.sch.gr, Ιανουάριος 2013

[98] http://ec.europa.eu/information_society/policy/ecomm/tomorrow/index_en.htm, Ιανουάριος, 2013

Παράρτημα Α

Αντιστοίχηση Ελληνικών - Αγγλικών

άμεσο μήνυμα :	instant messaging, IM
αναδρομικές αιτήσεις :	recursive queries
αναδρομολόγηση :	rerouting
ανεπιθύμητη ηλεκτρονική αλληλογραφία :	spam
ανιχνευτής :	crawler
Αόρατος Ιστός :	Deep Web
αποταξινόμηση :	deregistration
αριθμός θύρας :	port number
αυτό-διαβάθμιση :	self rating
αυτοκαθορισμός :	self regulation
βαθμονόμηση :	rating
γονικός έλεγχος :	parental control
δέντρα απόφασης :	decision trees

διαβάθμιση :	rating
Διαδίκτυο :	Internet
διακομιστής :	server
διακομιστής διαμεσολάβησης :	proxy server
διαμεσολαβητής:	proxy server
δίκτυο κορμού :	backbone
δρομολογητής :	router
δρομολογητής φιλτραρίσματος :	screening routers
εικονοστοιχείο :	pixel
εκσφαλμάτωση :	debugging
ελεύθερο λογισμικό :	free software
εταιρικό δίκτυο :	intranet
εξυπηρετητής :	server
εξυπηρετητής ονοματοδοσίας :	name server
εταιρικό δίκτυο :	intranet
ετικετοδότηση :	labeling
εύρος ζώνης :	bandwidth
ευρυζωνικός :	broadband
ιστοθέση :	website
ιστολόγιο :	blog
ιστοσελίδα :	webpage
ιστότοπος :	website
κατακερματισμός :	hashing
κατανεμημένο σύστημα ονοματοδοσίας :	Domain Name System DNS
κατηγοριοποιητής :	classifier
κεντρικός δρομολογητής :	core router
κ-κοντινότερων γειτόνων :	k-nearest neighbor
Κοινωνικά Μέσα :	Social Media
κορμός :	backbone

Κρυφός Ιστός :	Deep Web
Λογισμικό Ανοιχτού Κώδικα :	Open Source
λογοκρισία :	censorship
μεταγωγέας :	switch
μετάφραση ονομάτων :	name resolution
μηχανή αναζήτησης :	search engine
μικροιστολόγιο :	micro blog
μνημονικό ονόμα :	hostname
μπλογκόσφαιρα :	blogosphere
Ομότιμο Δικτύο :	Peer to Peer, P2P
Παγκόσμιος Ιστός :	World Wide Web, WWW
πάροχος :	provider
Πάροχος Υπηρεσιών Διαδικτύου :	Internet Service Provider, ISP
προειδοποίηση :	warning
προτυποποιώ :	standardize
πύλη πρόσβασης :	gateway
ροή πακέτων :	packet flow
Συλλέκτης :	Aggregator
συνοριακός δρομολογητής :	border router
ταμπλέτα :	tablet PC
τηλεδιάσκεψη :	teleconference
τηλεκπαίδευση :	distance learning
ΤΠΕ :	ICT
φιλοξενητής :	hosting server
φυλλομετρητής :	web browser

Παράρτημα Β
Αντιστοίχηση Αγγλικών – Ελληνικών Όρων

3G :	3η γενιά τεχνολογίας κινητής επικοινωνίας
4G :	4η γενιά τεχνολογίας κινητής επικοινωνίας
Access Control List (ACL) :	Λίστα Ελέγχου Πρόσβασης
Aggregator :	Συλλέκτης
antivirus :	λογισμικό προστασίας από ιούς
application gateway :	πύλη εφαρμογών
astrayment :	ακύρωση
authoritative name server :	έγκυρος εξυπηρετητής ονοματοδοσίας
automated :	αυτοματοποιημένη

Backbone Service Providers (BSP) :	Πάροχοι Υπηρεσιών Κορμού
backup :	αντίγραφα ασφαλείας
bandwidth :	εύρος ζώνης
Baysian :	κατηγοριοποιητής του Bayes
Bit Torrent :	πρωτόκολλο μεταφοράς δεδομένων μέσω του Διαδικτύου
blog :	ιστολόγιο
border router :	συνοριακός δρομολογητής
browser :	φυλλομετρητής
caching name server :	εξυπηρετητής ονοματοδοσίας
cached page :	προσωρινά αποθηκευμένες σελίδα
chat :	συνομιλία
chat room :	κανάλι συνομιλίας
classifier :	κατηγοριοποιητής
cluster :	συστάδα
copyright :	πνευματική ιδιοκτησία
core router :	κεντρικός δρομολογητής
crawler :	ανιχνευτής
daemon :	αυτόματος μηχανισμός
DDos attack :	Επίθεση κατανεμημένης άρνησης παροχής υπηρεσιών
debugging :	εκσφαλμάτωση
Deep Packet Inspection (DPI) :	σε βάθος έλεγχος δέσμης δεδομένων
Deep Web :	αόρατος ή κρυμμένος Ιστός
Denial of Service :	άρνηση παροχής υπηρεσιών
dial-up :	σύνδεση μέσω τηλεφωνικής κλήσης
Domain Name System (DNS) :	κατανεμημένο σύστημα ονοματοδοσίας
dynamic :	δυναμικός
enforced proxy :	εξαναγκασμένη διαμεσολάβηση
fiber to the home :	οπτική ίνα μέχρι το σπίτι
firewall :	ανάχωμα ασφαλείας

follower :	ακόλουθος (στο Twitter)
FTP :	Πρωτόκολλο Μεταφοράς Αρχείων
geo-location :	γεωγραφικός προσδιορισμός
hacker :	διαδικτυακός εισβολέας
hacking :	ηλεκτρονική πειρατεία
hardware :	υλικό (υπολογιστών)
hash functions :	συνάρτηση κατακερματισμού
hijacking :	πειρατεία
hostname :	μνημονικό όνομα υπολογιστή
HTTPS :	πρωτόκολλο SSL για Web υπηρεσίες
ICMP :	πρωτόκολλο για την ανταλλαγή μηνυμάτων λάθους
indexing :	χρήση ευρετηρίου
instant messaging (IM) :	άμεσο μήνυμα
intelligent :	ευφυή
interception :	παρακολούθηση
Internet :	Διαδίκτυο
IP address :	διεύθυνση πρωτοκόλλου Διαδικτύου
ISP :	Πάροχος Υπηρεσιών Διαδικτύου
jpeg :	πρότυπο απωλεστικής συμπίεσης εικόνων
k-Nearest neighbor :	κ-κοντινότεροι γείτονες
label bureau :	υπηρεσία ετικετοδότησης
layer :	επίπεδο
listing :	καταχώριση σε λίστα
live streaming :	ζωντανή μετάδοση
machine learning :	μηχανική μάθηση
malware :	κακόβουλο λογισμικό
man in the middle attack :	επίθεση με ενδιάμεσο υποκλοπέα
manipulation :	χειραγώγηση
micro blog :	μικροϊστολόγιο

mirroring :	δημιουργία αντιγράφου
monitoring :	παρακολούθηση
MP3 :	πρότυπο ψηφιακής κωδικοποίησης ήχου
MPEG-21 :	πρότυπο ενοποίησης πολυμεσικών εφαρμογών
name resolution :	μετάφραση ονομάτων
On Line Social Network :	σε απευθείας σύνδεση Κοινωνικό Δίκτυο
online :	σε απευθείας σύνδεση, επιγραμμικό
open source :	Λογισμικό ανοιχτού κώδικα
over blocking :	υπερβολικός αποκλεισμός
P2P :	Ομότιμο Δικτύο
packet flow :	ροή πακέτων
parental control :	γονικός έλεγχος
pass-by :	παράλληλα
pass-through :	σε σειρά
password :	συνθηματικό
payload :	ωφέλιμο φορτίο
PDA :	Προσωπικός Ψηφιακός Βοηθός
Peer to Peer :	Ομότιμο Δικτύο
phishing :	ηλεκτρονικό «ψάρεμα»
pixel :	εικονοστοιχείο
podcast :	κατά αίτηση διάθεση αρχείων βίντεο και ήχου
port :	θύρα
portal :	πύλη
proxy :	διακομιστής μεσολάβησης
proxy servers :	διακομιστής μεσολάβησης
rating :	αξιολόγηση
Really Simple Syndication (RSS) :	προτυποποιημένη μέθοδος ανταλλαγής ψηφιακού περιεχομένου
recursive caching name server :	αναδρομικός εξυπηρετητής ονοματοδοσίας

recursive name server :	αναδρομικός εξυπηρετητής ονοματοδοσίας
recursive queries :	αναδρομικές αιτήσεις
redirection :	αναδρομολόγηση
regular expressions :	κανονικές εκφράσεις
RGB :	πρότυπο χρώματος
router :	δρομολογητής
SaaS :	Λογισμικό (παρεχόμενο) ως Υπηρεσία
screening routers :	δρομολογητής φιλτραρίσματος
self regulation :	αυτορρύθμιση
Semantic Web :	Σημασιολογικός Ιστός
Shallow Packet Inspection :	επιφανειακός έλεγχος δέσμης δεδομένων
smart phone :	έξυπνο τηλέφωνο
SMTP :	πρωτόκολλο για την μετάδοση μηνυμάτων ηλεκτρονικού ταχυδρομείου
Social Media :	Κοινωνικά Μέσα
spam :	ανεπιθύμητη αλληλογραφία
spoofing :	πλαστογράφηση
Surface Web :	Επιφανειακός Ιστός
switch :	μεταγωγέας
tablet computers :	φορητός υπολογιστής με οθόνη αφής
tampering :	αλλοίωση
text categorization :	κατηγοριοποίηση κειμένου
time shifting :	χρονική μετατόπιση
transparency :	διαφάνεια
transparent proxy server :	διαφανής διακομιστής μεσολάβησης
tunneling :	διοχέτευση
under blocking :	ελλιπής αποκλεισμός
Uniform Resource Locators (URL) :	Ενιαίος Εντοπιστής Πόρων
user-generated :	δημιουργείται από το χρήστη

username :	όνομα χρήστη
video on demand :	βίντεο κατά παραγγελία
virtual hosting :	εικονική φιλοξενία
Voice over IP (VoIP) :	Διαδικτυακή τηλεφωνία
voluntary proxy :	δακομιστής μεσολάβησης σε εθελοντική βάση
warning :	προειδοποίηση
web :	Ιστός
web 2.0 :	Ιστός 2.0
web 3.0 :	Ιστός 3.0, Σημασιολογικός Ιστός
web browser :	φυλλομετρητής ιστού
Wi-Fi :	πρότυπο της IEEE για ασύρματα τοπικά δίκτυα
WiMAX :	τεχνολογία ασύρματης δικτύωσης
World Wide Web :	Παγκόσμιος Ιστός