



ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΜΗΜΑ ΑΡΧΕΙΟΝΟΜΙΑΣ & ΒΙΒΛΙΟΘΗΚΟΝΟΜΙΑΣ
ΜΕΤΑΠΤΥΧΙΑΚΟ

**Πρόγραμμα σπουδών: Διαχείριση και Ανάδειξη Πολιτιστικής
Πληροφορίας**

Αικατερίνη Σπυρίδων Μονόπωλη (Α.Μ.:ΜΑΒΜ201802)

*Διπλωματική Εργασία με θέμα: «Data filtering: Έλεγχος και διοχέτευση
δεδομένων στη σύγχρονη πολυπολιτισμική πραγματικότητα».*

Επιβλέπουσα καθηγήτρια: Κα. Κανελλοπούλου– Μπότη Μαρία
Κέρκυρα, 2021

Πρόλογος

Η ακολουθία και ο έλεγχος της ροής των πληροφοριών υπό τη σκέπη του νομοθετικού πλαισίου της κάθε χώρας υπαγορεύει τον τρόπο και την ωριμότητα της κάθε κοινωνικής δομής να ανταποκριθεί στην ευαίσθητη και πολυπαραγοντική θεματική της διαχείρισης, αξιοποίησης και προστασίας των προσωπικών δεδομένων των πολιτών της. Οι επιπτώσεις της διαχείρισης αυτής, είναι πολύπλευρες και αντικατοπτρίζονται σε κάθε έκφανσης της καθημερινής ζωής και δραστηριότητας των πολιτών. Με δεδομένο ότι οι σύγχρονες κοινωνίες εξελίσσονται μέσα από τον πολυπολιτισμικό τους χαρακτήρα, ο τρόπος και οι οπτικές διαχείρισης των προσωπικών δεδομένων των πολιτών, προσδίδει και άλλες διαστάσεις. Οι προεκτάσεις αυτές αποτυπώνονται υπό το πρίσμα των ατομικών ελευθεριών και με γνώμονα τη σύγχρονη κοινωνικοπολιτική ροή.

Εισαγωγή

Στην παρούσα έρευνα έχει καταβληθεί η προσπάθεια αποτύπωσης της πολύπλοκης πραγματικότητας των ροών των πληροφοριών που διακινούνται σε καθημερινή βάση και αφορούν τη σφαίρα της προσωπικής ζωής του κάθε ατόμου και πως αυτή παραβιάζεται υπό ορισμένες συνθήκες, εν γνώσει του ή εν αγνοία του.

Η αναγνώριση της δύναμης της πληροφορίας και η οικονομική και κοινωνική υπεροχή των κοινωνιών που επιλέγουν να τη διαχειριστούν, αποτελεί χαρακτηριστικό στοιχείο της σύγχρονης πραγματικότητας. Η αξιοποίηση των πληροφοριών αυτών των ατόμων, αλλά και των προσωπικών τους καταγραφών και δεδομένων, όπως αυτά καταχωρούνται σε βάσεις δεδομένων ή ευκολότερα στα «cookies» του υπολογιστή του χρήστη, είναι συνισταμένη με πολυπαραγοντικές οπτικές. Η αξιοποίηση αυτή πέραν των οικονομικών-απτών αποδείξεων στους δείκτες της εκάστοτε οικονομίας, αποτυπώνεται στο σχεδιασμό μακροπρόθεσμης στρατηγικής δράσεων προς αντιμετώπιση μαζικών μεταναστευτικών ροών και την αποφυγή συγκέντρωσης πληθυσμών σε συγκεκριμένες γεωγραφικές περιοχές ή χώρες. Η έρευνα αυτή αξιολογεί το νομοθετικό πλαίσιο της προστασίας των προσωπικών δεδομένων στους βασικούς γεωγραφικούς και οικονομικούς πόλους, σε μια προσπάθεια να καταδειχθεί η εξελισσιμότητα και η ευελιξία των κοινωνικών δομών ως προς τη διαχείρισης των δεδομένων των πολιτών τους, υπό το πρίσμα της διαφάνειας της δημόσιας διοίκησης.

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος	1
Εισαγωγή	2
ΠΕΡΙΕΧΟΜΕΝΑ.....	3
ΚΕΦΑΛΑΙΟ 1 Εισαγωγή	5
1.1 Πρόσβαση στην πληροφορία-Δικαίωμα ή Απαίτηση;.....	6
1.2 Η πραγματικότητα στην Ευρώπη, στην Ασία και τις Η.Π.Α.....	10
1.3 Νομοθεσία περί της ελεύθερης πρόσβασης στην πληροφορία.....	11
1.4 Ευρώπη	12
1.5 Ομάδα Εργασίας του άρθρου 29-Κανονισμός 2019/679.....	15
1.6 ΗΠΑ.....	16
1.7 Δυτική Αφρική – Το παράδειγμα του Μπενίν	24
1.8 Κίνα.....	25
1.9 Παραγουάη – Ζιμπάμπουε.....	30
ΚΕΦΑΛΑΙΟ 2 ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΑΝΗΛΙΚΟΤΗΤΑΣ.....	33
ΚΕΦΑΛΑΙΟ 3 ΜΕΣΑ ΨΗΦΙΑΚΗΣ ΠΛΗΡΟΦΟΡΙΑΣ.....	39
3.1 Η χρήση του διαδικτύου στη σύγχρονη εποχή-Το web 2.0.	39
3.2 Η χρήση των προσωπικών δεδομένων-διαδικτυακής πληροφορίας υπό το πρίσμα των ατομικών ελευθεριών.....	40
3.3 Επεξεργασία και αποθήκευση δεδομένων.	42
3.4 Απειλές σε περιβάλλον ιστού.	44
3.5 Κοινωνικά Δίκτυα-Social media.....	45
3.6 Προτάσεις	47
ΚΕΦΑΛΑΙΟ 4 Αποτύπωση της παγκόσμιας και ευρωπαϊκής πολυπολιτισμικής πραγματικότητας.....	50
4.1 Πολυπολιτισμική πραγματικότητα	51
4.2 Φιλτράρισμα δεδομένων (data filtering).....	54
4.3 Η πρόσβαση στην πληροφορία.	55
ΚΕΦΑΛΑΙΟ 5 Οπτικές διαχείρισης της πληροφορίας.....	62
5.1 Ριζοσπαστικοποίηση	62
5.2 11η Σεπτεμβρίου	66

ΕΠΙΛΟΓΟΣ.....	69
ΠΑΡΑΡΤΗΜΑ.....	71
ΒΙΒΛΙΟΓΡΑΦΙΑ	72
ΙΣΤΟΣΕΛΙΔΕΣ	72

ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

Ο αριθμός των χώρων που έχουν εγκρίνει νόμο για την κατοχύρωση της ελεύθερης πρόσβασης σε διοικητικά έγγραφα είναι ανοδικός. Η διαφάνεια είναι σήμερα στην κορυφή της ημερήσιας διάταξης για τις περισσότερες κυβερνήσεις και αποτελεί το στόχο πολλών κυβερνητικών σχημάτων και πεδίο διαμάχης των υπό διερεύνηση ομάδων (δημοσιογράφων κ.λπ.) (Prime minister's department broke the law delaying FOI request, watchdog finds, 2020). Η πρόσβαση των πολιτών στους νόμους για προστασία των προσωπικών δεδομένων και στη νομοθεσία για την ελευθερία στην πληροφόρηση, δεν αποτελεί υποκατάστατο της διαφάνειας, αλλά σηματοδοτεί την προθυμία μιας κυβέρνησης να λειτουργήσει υπό τον όρο της διαφάνειας. Η στροφή της δημόσιας διοίκησης σε δράσεις και διαδικασίες λήψης αποφάσεων όσο το δυνατόν πιο διαφανείς δημιουργεί τις βάσεις για ενεργή συμμετοχή των πολιτών στο δημοκρατικό βίο, διασφαλίζοντας την ισόρροπη εκπροσώπησή τους, εμποδίζοντας τους φορείς λήψης αποφάσεων σε παράνομη ή προνομιακή πρόσβαση σε πληροφορίες (Επίσημος ιστότοπος της Ευρωπαϊκής Ένωσης, 2020).

Ωστόσο οι φορείς δημόσιας διοίκησης εκμεταλλευόμενοι τα υπάρχοντα κενά διαφάνειας προσπαθούν να αντιστρέψουν τους όρους, επικαλούμενοι την προστασία των προσωπικών δικαιωμάτων των πολιτών που ήδη έχουν καταγραφεί. Οι δράσεις αυτές έχουν ως αποτέλεσμα τη δημιουργία κλίματος καχυποψίας, την άσκηση ελέγχου μέσω των επερωτήσεων, αλλά και τα επικριτικά σχόλια σε δημοσιεύσεις για ελλιπή διαφάνεια κατά την άσκηση της δημόσιας διοίκησης. Η παροχή υπηρεσιών και η διοχέτευση της πληροφορίας που συγκεντρώνουν οι δημόσιες υπηρεσίες και φορείς κρατικής εξουσίας είναι πλούσια και πολυσχιδής. Υπό το πρίσμα της εξυπηρέτησης του πολίτη και της διακυβέρνησης του κράτους διαπιστώνονται κενά διαφάνειας και καταστρατήγησης προσωπικών δεδομένων πολιτών από φορείς και άτομα που δεν φέρουν τις απαιτούμενες δικλείδες ασφαλείας και πιστοποίησης.

Πέρα από αυτά, το πεδίο εφαρμογής των νόμων περί προσωπικών δεδομένων δεν έχει ως στόχο μόνο την εξασφάλιση των πολιτών έναντι των παρεμβάσεων της δημόσιας διοίκησης και της ορθής διαφανούς διακυβέρνησης, αλλά κυρίως την προστασία τους σε κάθε συναλλαγή τους ηλεκτρονική ή μη, σε κάθε δραστηριότητα τους που ενέχει καταγραφή λήψη και επεξεργασία των προσωπικών τους δεδομένων. Η πλειονότητα των περισσότερων μελετών έχουν επικεντρωθεί στα κράτη όπου υπάρχουν τέτοιοι νόμοι, ειδικά στην Ευρώπη, Ασία και στην Αμερική, ενώ ελάχιστες έρευνες έχουν εκπονηθεί για την Αφρικανική Ήπειρο. Η παρουσίαση συνοπτικά της επικρατούσας νομοθετικής δράσης σε διάφορες χώρες του

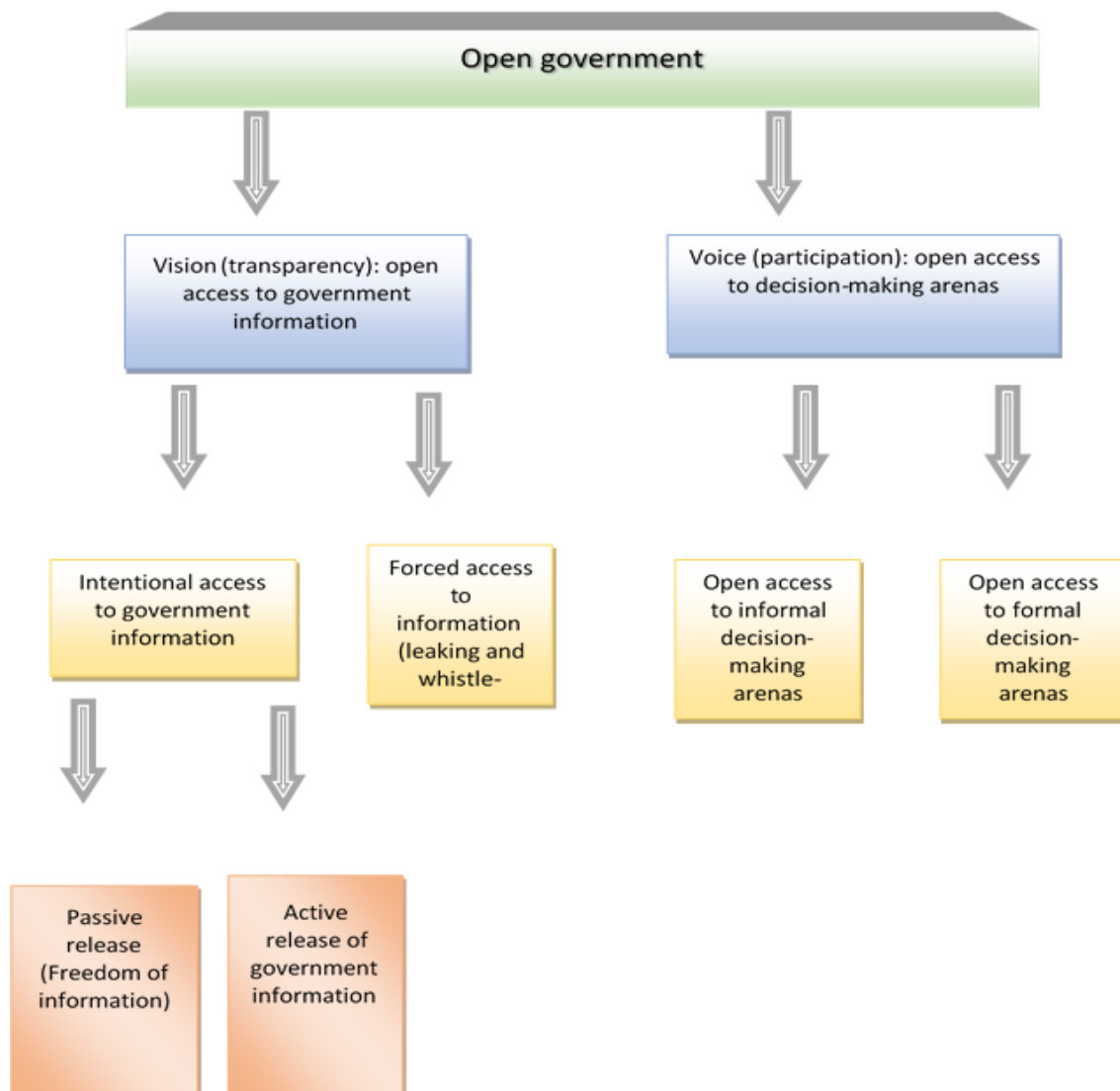
πλανήτη οδηγεί στη λήψη συμπερασμάτων για την πορεία που έχει γίνει στον τομέα της προστασίας των προσωπικών δεδομένων ανά την υφήλιο.

1.1 Πρόσβαση στην πληροφορία-Δικαίωμα ή Απαίτηση;

Η πρόσβαση στην πληροφορία προστατεύεται από το δίκαιο της κάθε χώρας η οποία έχει θεσπίσει ένα πλέγμα νομοθετημάτων, προκειμένου να διασφαλίσει την ελεύθερη πρόσβαση των χρηστών στην πληροφορία κατά τις συνδιαλλαγές τους με ιδιωτικούς αλλά και κρατικούς φορείς, να κατοχυρώσει τις προσωπικές τους πληροφορίες όπως αυτές αποθηκεύονται κατά τις καθημερινές τους δραστηριότητες αλλά κυρίως να διασφαλίσει ότι την πρόσβαση σε αυτές από τρίτους. Η κατοχύρωση των νόμων περί ελεύθερης πρόσβασης στην πληροφορία έχει ως στόχευση, πέραν της προστασίας των ατομικών ελευθεριών και τη διασφάλιση της διαφάνειας στις δράσεις και ενέργειες της δημόσιας διοίκησης. Υπό το πρίσμα αυτό, η σύγχρονη πραγματικότητα απαιτεί τη διαφάνεια στη διοίκηση και υπαγορεύει ένα κίνημα καθαρότητας στις κυβερνητικές δράσεις. Η διάκριση στην έννοια της ανοιχτής διακυβέρνησης επικουρεί την ορθή και σαφή νομοθετική πρόβλεψη των νόμων περί προστασίας των προσωπικών δεδομένων των πολιτών (Sáez-Martín, López-Hernandez and Caba-Perez, 2017).

Η έννοια της ανοιχτής διακυβέρνησης μπορεί να διακριθεί από την αρχή κατοχύρωσης των νόμων περί ελεύθερης πρόσβασης στην πληροφορία, σε δύο κατηγορίες στην «παθητική διαφάνεια» και στην «ενεργητική διαφάνεια» (Mabillard and Pasquier, 2016, σ. 72–73), (Meijer, Curtin and Hillebrandt, 2012, σ. 14). Στο κάτωθι σχήμα παρουσιάζεται το όραμα της ελεύθερης πρόσβασης στην επίσημη πληροφόρηση και της συμμετοχικής διαφάνειας, η οποία προϋποθέτει την ελεύθερη πρόσβαση στη διαδικασία λήψης των αποφάσεων. Στο ιδανικό περιβάλλον της ανοιχτής διακυβέρνησης, υπάρχει μια συνεργατική σχέση μεταξύ διαφάνειας και συμμετοχής: η διαφάνεια εγγυάται ότι το κοινό αποκτά πρόσβαση σε πληροφορίες σχετικά με την κυβέρνηση και η συμμετοχή παρέχει στο κοινό, πρόσβαση στην ίδια κυβέρνηση και στις δράσεις της. Σε αυτό το σχήμα αναλύονται τα δύο σχέδια ενίσχυσης της πρόσβασης στην πληροφορία, τα οποία αλληλοτροφοδοτούνται. Προϋπόθεση για την ύπαρξη συμμετοχικής δράσης από τους χρήστες της πληροφορίας, είναι η ύπαρξη ενός βασικού βαθμού πρόσβασης στην πληροφόρηση, ως το ελάχιστο επίπεδο διαφάνειας. Οι ιδιώτες μπορούν να επιδιώξουν να επηρεάσουν τις αποφάσεις πολιτικής μόνο εάν γνωρίζουν ποιες αποφάσεις λαμβάνονται και αντίστροφα, η διαφάνεια μπορεί να προκύψει από τη διαδικασία συμμετοχής. Το μοντέλο της ανοιχτής πρόσβασης στην πληροφόρηση είναι επίκαιρο και προωθείται από αρκετά κράτη υπό το πρίσμα της γενικής

παραδοχής των δικαιωμάτων και ελευθεριών των πολιτών-χρηστών και υποκειμένων των πληροφοριών τους. Η διάθεση ωστόσο για περαιτέρω παροχή πληροφορίας στους πολίτες, με στόχο την ενίσχυση της συμμετοχικής τους δράσης και η ανοιχτή πρόσβαση τους σε βάσεις δεδομένων και στατιστικά στοιχεία που τηρούν και συλλέγονται προς εξαγωγή συμπερασμάτων και ανάλυσης συμπεριφορών στα πλαίσια κοινωνικοπολιτικών μελετών, διαφοροποιεί και κωλυσιεργεί τις αρχικές αβυσσικές προθέσεις.



Εικόνα 1: Σχέδια ενίσχυσης πρόσβασης στην πληροφορία
(Meijer, Curtin and Hillebrandt, 2012, σ. 14).

Η γνώση των πληροφοριών που αποθηκεύονται και διακινούνται σε διαύλους και κανάλια επικοινωνίας, είναι ένα νεωτερικό και ανεξερεύνητο περιβάλλον για τον μέσο χρήστη-πολίτη. Η διαδικτυακή έκρηξη νέων τεχνολογιών έχει δημιουργήσει ένα νέο πλέγμα κοινωνικής ζωής και πληροφοριών που διακινούνται μέσω της τεχνολογίας. Οι πολίτες χρησιμοποιούν μηχανισμούς ανατροφοδότησης σε πλατφόρμες αιτήσεων πληροφοριών και δεδομένων, σε επίσημα και ανεπίσημα κανάλια. Οι πολίτες απαιτούν πληροφορίες και οι κυβερνήσεις χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης ως εργαλεία για την ενημέρωση του κοινού σχετικά με την απόδοσή τους.

Με αρωγό την τεχνολογία οι κυβερνήσεις υιοθετούν καινοτομίες τεχνολογίας πληροφοριών και επικοινωνιών¹, που διευκολύνουν με ηλεκτρονικά μέσα την επεξεργασία, τη μετάδοση και την προβολή πληροφοριών. Η ραγδαία χρήση των καινοτομιών ICT καθορίζει την τρόπο διαχείρισης και διοχέτευσης της πληροφορίας και επανατροφοδοτεί πληροφοριακά συστήματα και βάσεις δεδομένων που συνεχώς εξελίσσονται, ενώ επαναδομείται ο τρόπος με τον οποίο αλληλεπιδρούν οι χρήστες με τα δεδομένα, ο τρόπος πληροφόρησης τους από πλατφόρμες ανεπίσημες ή μη, καθώς και από τα μέσα κοινωνικής δικτύωσης (Davies and Fumega, 2014). Ωστόσο, οι ICT επηρέασαν όχι μόνο τις δραστηριότητες των χρηστών αλλά και τον τρόπο με τον οποίο οργανώνεται η στρατηγική προώθησης της διαφάνειας, από πλευράς των κυβερνήσεων και στη συνέχεια καταπολέμησης της διαφθοράς.

Το crowdsourcing² ως πρακτική αξιοποίησης των ιδεών ατόμων ή ομάδων ατόμων, αμειβόμενων ή μη, που συνδέονται με στόχο την ανταλλαγή και συγκέντρωση ιδεών. Κίνητρο δύναται να είναι οικονομικό για τη συγκέντρωση στοιχείων της αγοράς για την προώθηση προϊόντων μιας εταιρείας ή ιδεολογικός στο πλαίσιο παροχής πληθώρας ιδεών και απόψεων, μέσω της συνδεσιμότητας και ευελιξίας που προσφέρει το web 2 (Jennifer Alsever, 2020). Το crowdsourcing σε ανοιχτές κυβερνητικές πύλες δεδομένων παρέχει στους πολίτες πρόσβαση σε κρατικά σύνολα δεδομένων, καθώς επίσης η εφαρμογή «open gov» αποτέλεσε το θεμέλιο λίθο στη διακίνηση των δεδομένων των επισήμων φορέων, επιτρέποντας την ελεύθερη πρόσβαση των πολιτών σε αυτά και επικουρεί την καταπολέμηση της διαφθοράς. Τα κινητά τηλέφωνα θεωρούνται ευρέως ως ισχυρά εργαλεία κατά της διαφθοράς και η

¹ICT:Information and communications technology, <http://uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict>, (Ημερομηνία πρόσβασης:15-02-2021).

²Crowdsourcing:“the activity of giving tasks to a large group of people or to the general public, for example,by asking for help on the internet”, <https://dictionary.cambridge.org/dictionary/english/crowdsourcing>, <https://crowdsourcingweek.com/what-is-crowdsourcing/>, (Ημερομηνία πρόσβασης:15-02-2021).

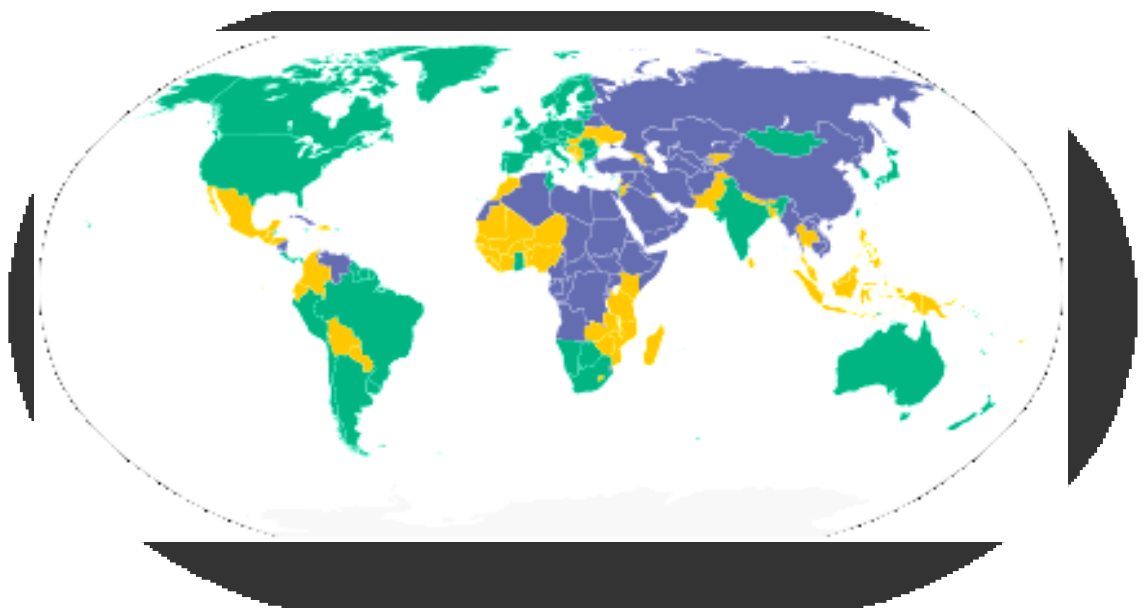
πολύπλευρη χρήση τους ευνοεί την άμεση και ευέλικτη πρόσβαση σε βάσεις δεδομένων (Davies and Fumega, 2014). Η τεχνολογία πληροφοριών και επικοινωνιών (ICT) παρέχει τα μέσα για την αναδιάρθρωση της επιχείρησης επιτρέποντας στην κάθε επιχειρηματική μονάδα την άμεση πρόσβαση του χρήστη στις παροχές της και ενισχύοντας την αποδοτικότητα και την παραγωγικότητα της. Η χρήση των νέων αυτών τεχνολογιών μειώνει το κόστος συναλλαγής, αυτοματοποιεί την πρόσβαση του χρήστη και του επιτρέπει να αναζητά, να ενημερώνεται για προϊόντα και υπηρεσίες, ενώ παράλληλα συγκρίνει και επικουρεί την ανταλλαγή απόψεων, την τεχνογνωσία, την παροχή υπηρεσιών σε τοπικό, εθνικό αλλά και παγκόσμιο επίπεδο. Η παγκοσμιοποίηση είναι το από και εμφανές παράδειγμα (Serrat, 2017). Αντίστοιχη και η δήλωση του Tim Berners-Lee, του εφευρέτη του World Wide Web “*You affect the world by what you browse*” (Dennis, 2021).

Τα διαφορετικά κίνητρα που ωθούν στην υιοθέτηση αυτών των τεχνολογιών διαμορφώνουν αντίστοιχα τον τρόπο με τον οποίο αυτές εφαρμόζονται στην πράξη, με ανάλογες επιπτώσεις στην καταπολέμηση της διαφθοράς και στην προαγωγή της ελεύθερης πρόσβασης. Ωστόσο, αξίζει να αναφερθεί η ευελιξία δράσεων και σχηματισμών κατά τη διαχείριση των ροών δεδομένων από επίσημα κανάλια επικοινωνίας με δυνατότητα νεωτερικών μετασχηματισμών που προάγουν την ελευθεριότητα στη διαχείριση των επίσημων δεδομένων. Η νεωτερικότητα κατά τη διαχείριση των ροών πληροφορίας τόσο από επίσημα όσο από ανεπίσημα κανάλια, έδωσε νέα ώθηση στην διαχείριση των δεδομένων που σηματοδοτείται από ραγδαία έκρηξη της πληροφορίας. Η νομοθετική πρόβλεψη ακολούθησε την καινοτομία ως συνηθίζεται να ακολουθεί τις συμπεριφορές, αφήνοντας στο μεσοδιάστημα κενά στην προστασία των προσωπικών δεδομένων των ατόμων-χρηστών.

1.2 Η πραγματικότητα στην Ευρώπη, στην Ασία και τις Η.Π.Α.

Οι νόμοι περί προσωπικών δεδομένων κατοχυρώνουν τόσο την πρόσβαση στην πληροφορία όσο και την παρεμπόδιση της πρόσβασης σε αυτή, προστατεύοντας το αντικείμενο της πληροφορίας, το είδος της, τον τρόπο εξόρυξης της και την αποθήκευση της για μελλοντική χρήση. Η κατοχύρωση των δικαιωμάτων πρόσβασης στην πληροφορία αποτελεί μέλημα των σύγχρονων κρατών μελών, που είτε ρυθμίζουν το υφιστάμενο νομικό τους πλαίσιο, είτε θεσμοθετούν από την αρχή για να προστατεύσουν το έννομο αγαθό της ανθρώπινης ελευθερίας και του δικαιώματος της ανθρώπινης ελεύθερης έκφρασης (Union, 2009). Σε παγκόσμια κλίμακα υφίστανται χώρες που έχουν ήδη θεσμοθετήσει την αλλαγή στο νομικό τους πλαίσιο, όπως οι Ευρωπαϊκές χώρες, με την έκδοση σχετικών οδηγιών αλλά και οι Ηνωμένες Πολιτείες Αμερικής.

Η ύπαρξη ωστόσο του νομοθετικού πλαισίου δεν συνεπάγεται την εφαρμογή του στο ακέραιο. Η κατοχύρωση των μηχανισμών επιβολής και ελέγχου είναι ιδιαίτερα λεπτή και δεν συνεπάγεται εκ προοιμίου τη διάθεση από κρατικούς φορείς να υποβληθούν στον έλεγχο των στοιχείων και των ροών πληροφορίας που διαχειρίζονται. Οι ρυθμιστικές διατάξεις σε μεγάλο βαθμό έρχονται να διευκολύνουν την εφαρμογή του νόμου, ωστόσο σε ορισμένες περιπτώσεις δεν επιτυγχάνεται αυτό πλήρως με αποτέλεσμα πλημμελή προστασία και λανθασμένες κινήσεις. Ωστόσο είναι θεμιτή η αναφορά και η περιήγηση στο νομοθετικό πλαίσιο που διέπει τις κυρίαρχες χώρες του πλανήτη, ως ενδεικτική μελέτη των διαφορετικών διαστάσεων που ενέχει η διαχείριση του νομοθετικού πλαισίου της πρόσβασης στην πληροφορία, ως δικαίωμα των πολιτών (Beezy and Lucas, 2018).



Εικόνα2:Country ratings from Freedom House's Freedom in the World 2020 survey, concerning the state of world freedom in 2019.[38] Free (84) Partly Free (64) Not Free (51) (<https://freedomhouse.org>)

1.3 Νομοθεσία περί της ελεύθερης πρόσβασης στην πληροφορία

Η αναγκαιότητα νομοθετικής πρόβλεψης είναι αποτέλεσμα της εξελικτικής κοινωνικής διαδικασίας στην πορεία της καθημερινής διακίνησης τεράστιου όγκου πληροφοριών και προσωπικών δεδομένων. Η ενσωμάτωση των διατάξεων και Οδηγιών στο πλαίσιο του Ευρωπαϊκής νομοθεσίας μπορεί να θεωρηθεί για ορισμένες κοινωνίες ως κατευθυντήρια απαίτηση προσαρμογής στις επιταγές της κοινωνικής πολιτικής και οικονομικής ορθότητας. Ωστόσο, αρκετές χώρες προγενέστερα της υπαγόρευσης της κοινής ευρωπαϊκής πολιτικής και πορείας, διέκριναν την αναγκαιότητα προσαρμογής του νομοθετικού τους πλαισίου. Η κινητοποίηση αυτή είναι αποτέλεσμα πολλών παραγόντων και οφείλεται σε μια συστάδα καταστάσεων κοινωνικών, πολιτικών αλλά και οικονομικών (Schudson, 2018).

Η προστασία των προσωπικών δεδομένων των πολιτών των κρατών, στενά συνυφασμένη με την εξασφάλιση ελεύθερης πρόσβασης στην πληροφορία, εντάσσεται σε μια γενικότερη προσπάθεια διαφάνειας στη διοίκηση και τις διοικητικές διαδικασίες που αφορούν στη διαχείριση του κράτους, τους μηχανισμούς επιβολής ελέγχου, τη συλλογή και καταγραφή των δεδομένων των πολιτών. Από την άλλη πλευρά, η ραγδαία συσσώρευση πληροφορίας από ιδιωτικές επιχειρήσεις, έχει οδηγήσει σε σαφείς εκτιμήσεις της εμπορικής αξίας της πληροφορίας που διακινείται με κάθε τρόπο και μέσο. Το ρητό “Η γνώση είναι δύναμη” είναι πιο επίκαιρο από ποτέ (Michener, 2015).

Η ανάγκη για διαφάνεια στις δράσεις της δημόσιας διοίκησης, σηματοδοτεί τις εξελισσόμενες απαιτήσεις των πολιτών για διαφανείς πολιτικοοικονομικές δράσεις. Η προστασία του δικαιώματος των πολιτών μπορεί να θεωρηθεί από τις σημαντικότερες επιδράσεις των Freedom of Information Laws (FOI), ακόμη και όταν αυτοί οι νόμοι χρησιμοποιούνται ως μέσο διοχέτευσης αμφιβολιών κλονισμού της αξιοπιστίας σε βάρος της δημόσιας διοίκησης. Ο έλεγχος των πληροφοριών μπορεί να έχει ως αποτέλεσμα τη διερεύνηση σκανδάλων, τονώνοντας το αίσθημα της εμπιστοσύνης των πολιτών προς το κράτος δικαίου. Επιπροσθέτως η ύπαρξη εξελιγμένου δικτύου μη κυβερνητικών οργανώσεων (ΜΚΟ), με έντονο ενδιαφέρον για διαφάνεια στη δημόσια διοίκηση, αυξάνει την πίεση στους φορείς να προστατεύσουν τους πολίτες τους και να προάγουν τη διαφάνεια, παίρνοντας και τα εύσημα για το έργο τους. Η πολιτική διαχείριση των δράσεων τους

συσπειρώνει τους υποστηρικτές τους, με εμφανή αποτελέσματα στην κοινωνικοοικονομική δομή της κάθε χώρας που δραστηριοποιούνται. Επιπλέον με τη σταδιακή μείωση της ανισορροπίας μεταξύ κυβέρνησης και άλλων θεσμικών επιπέδων πολίτες μπορούν να αυξήσουν την ικανότητα και την αποτελεσματικότητα των ροών πληροφοριών, οι οποίες μπορούν να κινούνται αμφίδρομα το ίδιο αποτελεσματικά. Παράδειγμα αυτού η σταδιακή ανάπτυξη της κυβερνητικής δεκτικότητας της Κίνας, αναφορικά με τη νομοθεσία που προστατεύει την ελεύθερη πρόσβαση στην πληροφορία και με την πάροδο του χρόνου στη διαμόρφωση πιο ευέλικτων μοντέλων (Mabillard, Kakroni and Cottier, 2018).

Η ανοιχτή διακυβέρνηση, ως τρόπος ενίσχυσης της διαφάνειας στη δημόσια διοίκηση, εφαρμόζεται από ανοικτές κυβερνητικές πρωτοβουλίες με στόχο τη βελτίωση της λογοδοσίας και την καταπολέμηση της διαφθοράς. Ωστόσο, δεν υφίσταται πλήρης συναίνεση αναφορικά με τις συστατικές διαστάσεις της ανοιχτής διακυβέρνησης και τον τρόπο με τον οποίο γίνονται αντιληπτές από τους δημόσιους διαχειριστές σε διαφορετικά πλαίσια λειτουργίας τους. Αφορμή αποτελεί το παράδειγμα της Ισπανίας όπου κατόπιν σχετικής έρευνας που διεξήχθη σε τοπικές της κυβερνήσεις, διαπιστώθηκε ότι οι δημόσιοι διευθυντές που εργάζονται σε πρωτοβουλίες ανοιχτής διακυβέρνησης, αντιλαμβάνονται την εξωστρέφεια των οργανισμών τους στον τομέα αυτό μέσω τριών διαφορετικών πρισμάτων: (α) τις δημοκρατικές αξίες συνυπευθυνότητας, (β) την τεχνολογική καινοτομία και (γ) τη διαθεσιμότητα και πρόσβαση σε πληροφορίες. Αυτή η νέα κατηγοριοποίηση των προοπτικών της ανοιχτής διακυβέρνησης παρέχει πολύτιμη συμβολή στην επιστημονική συζήτηση σχετικά με το τι είναι η ανοιχτή διακυβέρνηση (Open Government) και πώς αυτή η νέα στρατηγική δημόσιας διαχείρισης γίνεται αντιληπτή από τους διαχειριστές της τοπικής αυτοδιοίκησης (Criado and Gil-garcia, 2019).

1.4 Ευρώπη

Με την έναρξη εφαρμογής του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ)³, (Ιγγλεζάκης, 2018), (Μήτρου, 2017), (Παναγοπούλου-Κουντατζή, 2017) όπως αυτός έχει τεθεί σε ισχύ από το Μάη του 2018, το σύνολο των εταιριών εντός και εκτός της Ευρώπης υπόκεινται στον ενιαίο κανονισμό προστασίας των φυσικών προσώπων, όταν απευθύνονται, αποθηκεύουν, χρησιμοποιούν και επεξεργάζονται δεδομένα πολιτών της Ευρώπης (Kadelbach, 2013). Τα δεδομένα των χρηστών-πελατών, που διακινούνται, αφορούν

³Κανονισμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27-04-2016, General Data

όλες τις εκφάνσεις της κοινωνικοοικονομικής τους ζωής και η παραβίαση τους έχει αντίκρισμα τόσο κοινωνικό όσο και οικονομικό. Η κοινωνική διάσταση της παραβίασης αποτελεί τη θεμελιώδη συλλογιστική για την έναρξη της προστασίας του ατόμου απέναντι σε επιδόξους παραβάτες της σφαίρας της προσωπικής ζωής του πολίτη. Η ευχέρεια πρόσβασης στη σφαίρα της ιδιωτικής ζωής και των δεδομένων που στοιχειοθετούν την κοινωνική και ατομική δραστηριότητα του ατόμου, αποτελεί παραβίαση των ουσιωδών δικαιωμάτων της αυτοδιάθεσης και του απορρήτου και της ελεύθερης ανάπτυξης της προσωπικότητας του κάθε ατόμου. Η δημοσιοποίηση, η καταγραφή και αποθήκευση των δεδομένων προσωπικού χαρακτήρα του ατόμου, ενέχει σαφή παραβίαση της σφαίρας της ιδιωτικής ζωής του και κινδύνους με αντίκτυπο στην κοινωνική συνοχή.

Εκτός αυτού, το οικονομικό όφελος από τη διαχείριση της πρόσβασης και την αποθήκευση των δεδομένων προσωπικού χαρακτήρα του ατόμου, επιφέρει κέρδος σε επιχειρήσεις που χρησιμοποιούν και διακινούν τις ροές πληροφοριών. Η προστασία των ατομικών ελευθεριών κρίνεται επιβεβλημένη καθώς στη σημερινή πραγματικότητα, η κερδοφορία των επιχειρήσεων δεν έχει αντίκρισμα μόνο χρηματικό, αλλά ανταποκρίνεται και στη ροή των δεδομένων και πληροφοριών. Οι πληροφορίες διακινούνται πολύ πιο εύκολα και μαζικά από τα αγαθά, με αποτέλεσμα την άσκηση πιέσεων στις κυβερνήσεις για τη θεσμοθέτηση ορίων και περιορισμών χρήσης τους, με έμφαση στο διασυνοριακή ροή δεδομένων. Χαρακτηριστικό είναι ότι η διασυνοριακή ροή δεδομένων παγκοσμίως σύμφωνα με την αναφορά του MGI⁴ εκτιμάται σε 2.8 τρισεκατομμύρια δολάρια το 2014 (Yakovleva and Irion, 2020, σ. 4). Η διακίνηση των ροών πληροφοριών, ξεπερνά τα στενά συνοριακά όρια του κάθε κράτους και πλέον λογίζεται ως παγκόσμια. Μέσα στο πλαίσιο αυτό, κρίθηκε επιβεβλημένη η θέσπιση ενιαίου νομοθετικού πλαισίου που θα ρυθμίζει τη διακίνηση των ροών των πληροφοριών μέσω νόμιμων διαύλων, που θα υπόκεινται στον έλεγχο νομιμότητας από τις ελεγκτικές αρχές του κάθε κράτους, υπό την κοινή εναρμόνιση της νομοθετικής διαδικασίας.

Η Ελλάδα με το Ν. 4624/2019, ευθυγράμμισε το νομοθετικό της πλαίσιο με τον ΓΚΠΔ κατά την Οδηγία 2016/680 της Ευρωπαϊκής Ένωσης περί προστασίας των δεδομένων προσωπικού χαρακτήρα. Η κατοχύρωση των εμπορικών συναλλαγών απαιτήσε την αλλαγή αυτή, θέτοντας το άτομο-πολίτη της Ευρώπης, απέναντι σε εμπορικές εταιρείες παγκόσμιας εμβέλειας και υπό τη σκέπη της αμερικανικής αγοράς. Οι Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ), έχοντας ως πολιτική τον έλεγχο των δεδομένων των πολιτών, κινούνται προς την

⁴ McKinsey Global Institute (MGI).

κατεύθυνση αυτή και στις περιπτώσεις συναλλαγών ευρωπαϊών πολιτών. Η τυχόν παραβίαση των προσωπικών δεδομένων των ευρωπαϊών πολιτών, θέτει τις εταιρείες απέναντι στη Ευρωπαϊκή προστασία ακόμη και αν η έδρα των εταιρειών αυτών βρίσκεται σε έδαφος των ΗΠΑ (Yakovleva and Irion, 2020, σ.3), (Ευρωπαϊκό Κοινοβούλιο, 2016, αρθρ. 7, 8). Η ειδοποιός αυτή διαφορά έναντι των προγενέστερων νομοθετικών κειμένων, παρέχει την πλήρη και ενιαία προστασία του ατόμου έναντι κάθε παραβίασης των προσωπικών του δεδομένων, θέτοντας ως κυρίαρχο στόχο την προστασία αυτή και παραγκωνίζοντας τυχόν διαδικαστικές λεπτομέρειες που θα μπορούσαν να θέσουν τον Κανονισμό Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ανενεργό.

Ο καθορισμός διακριτών γραμμών για την προστασία του υποκειμένου των δεδομένων κάτοικων της Ευρωπαϊκής Ένωσης, όταν αυτοί συναλλάσσονται με άλλες εταιρείες εκτός Ε.Ε., καθεμία από τις οποίες υπόκεινται στην νομοθεσία του κράτους που εδρεύει, όπως για παράδειγμα οι Ηνωμένες Πολιτείες Αμερικής, όπου εδρεύουν οι πιο δημοφιλείς εφαρμογές κοινωνικής δικτύωσης (facebook, amazon, instagram), δομεί ένα πλαίσιο λειτουργίας οριοθετώντας κανόνες χρήσης, ρητής και διακριτής δήλωσης συγκατάθεσης επεξεργασίας των προσωπικών δεδομένων του φυσικού προσώπου-υποκειμένου αυτών. Στόχος είναι να αποκλειστεί και να διωχθεί ο παραβάτης σε περιπτώσεις μη συμμόρφωσης, ή σε περιπτώσεις αποθήκευσης, καταγραφής, επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όπως αυτά καταγράφονται με τη χρήση αλγορίθμων στις εν λόγω εφαρμογές. Στο παρασκήνιο των εφαρμογών υφίστανται ένα πλέγμα δράσεων, με οικονομικό κίνητρο και δυνατότητες διάθεσης των δεδομένων που αποθηκεύονται άπειρες. Θέτοντας τη διαμάχη και τον προβληματισμό για προσκόμματα κατά τη διασυνοριακή μεταφορά δεδομένων των εμπορικών συναλλαγών και κινήσεων σε διεθνές επίπεδο, υφίσταται αντίλογος αναγνωρίζοντας την αναγκαιότητα καθορισμού του νομοθετικού πλαισίου, εντός του οποίου θα κινούνται τα κράτη μέλη της Ευρωπαϊκής Ένωσης, οι Ηνωμένες Πολιτείες Αμερικής, ως η βασική κινητήριος δύναμη της διασυνοριακής ροής πληροφοριών και των λοιπών κρατών ανά τον κόσμο. Ο καθορισμός των βάσεων δράσης και διοχέτευσης των δεδομένων δημιουργεί θεσμικές διαμάχες, καθόσον οι οικονομικοί κύκλοι έχουν ως στόχο την ασφάλεια των συναλλαγών και την αποτελεσματική και απρόσκοπτη διασυνοριακή ροή των δεδομένων (Aaronson, 2015), σε αντίθεση με τους θεσμικούς νομοθετικούς πυλώνες του κάθε κράτους, που στοχεύουν στην προστασία των ατομικών ελευθεριών των πολιτών τους αλλά και των συναλλασσόμενων γενικότερα (Reyes, 2011), (Ευρωπαϊκό Κοινοβούλιο, 2016, αρθρ. 7, 8).

1.5 Ομάδα Εργασίας του άρθρου 29-Κανονισμός 2019/679

Οι βασικές κατευθύνσεις του ΓΚΠΔ αποτυπώνονται στον Ν.4624/2019 και συναντώνται στις κατευθυντήριες της Ομάδας Εργασίας του Άρθρου 29 σχετικά με την συγκατάθεση βάσει του κανονισμού 2019/679. Ειδικότερα, στον Ν.4624/2019, καθορίζονται τα όρια και οι προϋποθέσεις υπό τις οποίες ο υπεύθυνος επεξεργασίας μπορεί να έχει στην κατοχή του προσωπικά δεδομένα του υποκειμένου, το είδος, τις προϋποθέσεις τήρησης αυτών και τον τρόπο λήψης τους. Ο καθορισμός αυτός θέτει σαφείς υποχρεώσεις για τον υπεύθυνο επεξεργασίας με την ανάληψη προσωπικής του ευθύνης, για την εξασφάλιση ρητής και συγκεκριμένης συγκατάθεσης καθώς και την εξεύρεση των επιμέρους λύσεων λήψης της συγκατάθεσης αυτής. Η διασφάλιση της επιλογής απόρριψης ή αποδοχής των προσφερόμενων όρων χωρίς ζημιά ή συνέπειες για το υποκείμενο των δεδομένων, αποτελεί βασική παράμετρο εξασφάλισης της διαχείρισης των δεδομένων προσωπικού χαρακτήρα του υποκειμένου. Η αποτύπωση αυτή πρέπει να είναι σαφής και με τρόπο που θα εφεύρει ο υπεύθυνος επεξεργασίας που επιδιώκει την πρόσβαση στα δεδομένα του υποκειμένου. Η τυχόν παράνομη, παράτυπη ή ανεπαρκής λήψη της συγκατάθεσης του υποκειμένου, ουσιαστικά αφαιρεί το δικαίωμα στον υπεύθυνο επεξεργασίας, χρήσης, επεξεργασίας και αποθήκευσης των δεδομένων (VerLoren van Themaat and Reuder, 2018, αρθρ. 7–8). Επιπλέον η Οδηγία 2002/58/EK ορίζει σαφώς τις δικλίδες ασφαλείας για την προστασία του ατόμου κατά τις ηλεκτρονικές επικοινωνίες του, την ηλεκτρονική αλληλογραφία (e-mail), τις εμπορικές τακτικές προώθησης (αρθ. 4,7 ΓΚΠΔ), καθώς και τις διαδικτυακές μεθόδους παρακολούθησης, με τη χρήση cookies και εφαρμογών λογισμικού. Με τον τρόπο αυτό κατοχυρώνεται η δραστηριότητα του ατόμου σε ψηφιακό περιβάλλον, ως στοιχεία του προσωπικού του πεδίου κίνησης και οριοθετείται η διακριτή προστασία του ατόμου κατά την ψηφιακή του δραστηριότητα (European Commission, 2002), είτε επαγγελματικά είτε στη σφαίρα της ιδιωτικής του ζωής.

Χαρακτηριστικά αναφέρεται η Γνώμη 03/2016 (WP 240), με τη συνοπτική έκθεση για δημόσια διαβούλευση σχετικά με την αξιολόγηση και την αναθεώρηση των οδηγιών e-Privacy (European Commission, 2002), ως αλληλεπιδρώντα νομοθετήματα για την επανεξέταση της εξέλιξης της κοινωνικής και οικονομικής ζωής των πολιτών (Ομάδα Εργασίας του άρθρου 29 για την προστασία των δεδομένων, 2014). Ιδιαίτερη μνεία γίνεται στις περιπτώσεις όπου η ανισορροπία ισχύς του υποκειμένου με τον υπεύθυνο επεξεργασίας είναι δεδομένη, όπως για παράδειγμα κατά την υποβολή αιτήματος του ατόμου με αποδέκτη δημόσια αρχή. Στις εν λόγω περιπτώσεις η απαίτηση ύπαρξης απόλυτης συγκατάθεσης του

υποκειμένου των δεδομένων προσωπικού χαρακτήρα, κρίνεται απαραίτητη και διασφαλίζει τη διαδικασία⁵. Η διαπιστωμένη ανισορροπία ισχύος του υπευθύνου επεξεργασίας, δεν είναι θεμιτό να αποτελέσει τροχοπέδη κατά τη λήψη συγκατάθεσης υπό το φόβο τυχόν επιπτώσεων-κυρώσεων. Η παροχή έγκυρης νομικής βάσης-συσχέτισης για την επεξεργασία δεδομένων προσωπικού χαρακτήρα του ατόμου, σε σχέση με το δημόσιο φορέα δεν επιτρέπεται, ενώ η όποια καταπάτηση των δεδομένων του υποκειμένου πραγματοποιείται και αντισταθμίζεται από τον επιδιωκόμενο προς αυτό σκοπό (Board, 2020). Αντίστοιχα κρίνεται σκόπιμη η ενημέρωση του υποκειμένου των δεδομένων για τους επιδιωκόμενους σκοπούς χρήσης, ως περαιτέρω διασφάλιση του λόγου για τον οποίο κρίνεται ότι πρέπει να παραβιαστεί το προσωπικό δικαίωμα της αυτοδιάθεσης του ατόμου, έναντι εταίρου σκοπού (π.χ. οικονομικού) του υπευθύνου επεξεργασίας. Η έννοια της συγκατάθεσης του υποκειμένου (Ομάδα Εργασίας του άρθρου 29 για την προστασία των δεδομένων, 2014, σ.16), ενέχει τη σαφή και απλή διατύπωση του προς τον υπεύθυνο επεξεργασίας, καθώς και την εμφάνιση του σκοπού επεξεργασίας που καθιστά αναγκαία τη λήψη των προσωπικών δεδομένων του υποκειμένου και αποτελεί δικλείδα ασφαλείας για την ουσιαστική προστασία της σφαίρας της ιδιωτικής ζωής του ατόμου.

1.6 ΗΠΑ

Στις Η.Π.Α. η προστασία των προσωπικών δεδομένων και η εξασφάλιση της ελεύθερης πρόσβασης των πολιτών στην πληροφορία, τίθεται απέναντι στο κράτος και με προστατευτική διάθεση προς τον πολίτη. Συγκεκριμένα έχει αναχθεί σε συνταγματικό δικαίωμα, από το 1973, με την απόφαση *Grisworldv. Connecticut*, κατά την οποία συζητήθηκε ο όρος της προστασίας της ιδιωτικής ζωής, με αφορμή τη δικαστική συζήτηση της υπόθεσης για την απαγόρευση χρήσης αντισυλληπτικών από έγγαμα ζευγάρια.⁶ (Bottis, 2009, σ.810).

Ο πολίτης κινείται και προστατεύεται στο ακέραιο έναντι παρεμβάσεων του κρατικού μηχανισμού σε τυχόν παραβίαση των προσωπικών του δεδομένων. Οι συνισταμένες αυτού πολλές, αλλά η βασική κινητήριος δύναμη στρέφεται γύρω από την απόλυτη προστασία του πολίτη έναντι στον κρατικό παρεμβατισμό. Οι οποιεσδήποτε παραβιάσεις ιδιωτών προς τον ιδιώτη, αντιμετωπίζονται υπό το πρίσμα της ελευθεριότητας και της ανοιχτής πρόσβασης

⁵Αρθ.6 παρ.1 ε'Γ.Κ.Π.Δ.

⁶381 U.S. 479 (1965).

στην πληροφορία. Η υποστήριξη της ελευθερίας του λόγου και της ελευθερίας του Τύπου συνδυάστηκαν σε μια δικαιολογημένη θεώρηση, με στόχο την καθιέρωση του δικαιώματος πρόσβασης των πολιτών στις πληροφορίες που τηρούν δημόσιοι φορείς (DLA Piper, 2017), (Kontargyris, 2018).

Η προστασία των δεδομένων και της ιδιωτικής ζωής στο Κράτος των πολιτών όπως αυτή έχει κατοχυρωθεί από τα κράτη μέλη της Ευρωπαϊκής Ένωσης δεν ταυτίζεται πλήρως με την θεμελιώδη λογική διαχείρισης των ιδιωτικών πληροφοριών των αμερικανών πολιτών, σε σύγκριση με την προστασία που παρέχεται στα ευρωπαϊκά κράτη (Union, 2009). Η λογική της διακίνησης της πληροφορίας ιδιωτικής ή μη και η προστασία του πολίτη όπως παρέχεται από το αμερικανικό δικαϊκό σύστημα, δε συνάδει με την θεμελιακή προστασία της ιδιωτικής ζωής των ευρωπαίων πολιτών ακόμη και στις περιπτώσεις που διακινούν ιδιωτικές πληροφορίες τους για εμπορικούς σκοπούς, με ιδιωτικές επιχειρήσεις με έδρα τις ΗΠΑ, όπως προαναφέρθηκε.

Η Ομοσπονδιακή Επιτροπή Εμπορίου των ΗΠΑ (FTC)⁷ έχει δικαιοδοσία για ένα ευρύ φάσμα εμπορικών οντοτήτων υπό την εξουσία της για την πρόληψη και την προστασία των καταναλωτών από αθέμιτες ή παραπλανητικές εμπορικές πρακτικές, συμπεριλαμβανομένων των περιπτώσεων προσβολής της ιδιωτικής ζωής και της ασφάλειας των δεδομένων. Η FTC⁸ εκδίδει κανονισμούς, επιβάλλει συγκεκριμένους νόμους περί απορρήτου και εφαρμόζει δράσεις ερευνώντας προληπτικά και κατασταλτικά τη δραστηριότητα των εταιριών, εντός των ορισθέντων ορίων προστασίας των καταναλωτών. Η σφαίρα δραστηριοποίησης τους δεν εξαντλείται με τον έλεγχο παραβίασης των δικαιωμάτων απορρήτου των καταναλωτών μέσω της συλλογής, χρήσης, διανομής ή μη επαρκούς προστασίας των πληροφοριών τους, αλλά συνίσταται και στον έλεγχο τυχόν παραβίασης του πλαισίου προστασίας της ιδιωτικής ζωής των καταναλωτών της FTC ή ορισμένων εθνικών νόμων και κανονισμών περί απορρήτου, και λοιπών παραβιάσεων των δικαιωμάτων των καταναλωτών που βλάπτουν τους καταναλωτές στα κράτη τους. Η θεσμοθέτηση της ως ανεξάρτητη αρχή, προσδίδει τη διαφάνεια και την εγκυρότητα που απαιτείται για τη δράση της, προς επίτευξη των ιδρυτικών της στόχων απέναντι σε κυβερνητικά κανάλια και οργανισμούς. Ως πρωτοπόρος στην άμεση εκδήλωση εποπτικών και κατασταλτικών δράσεων ανά περίπτωση φροντίζει να παρέχει κατευθυντήριες στους καταναλωτές-χρήστες. Η διαχείριση των πληροφοριών τους

⁷<https://www.ftc.gov/>(Ημερομηνία πρόσβασης 14-05-2020).

⁸<https://www.usa.gov/federal-agencies/federal-trade-commission>. (Ημερομηνία πρόσβασης 11-03-2020).

καταγράφεται σε αντίστοιχη βάση δεδομένων, όπως αυτά κατηγοριοποιούνται και αποτελεί την αρχή για την προστασία τους. Πέραν από διαφοροποιήσεις των δεδομένων που προστατεύονται ανά είδος και σπουδαιότητα, ως ευαίσθητα προσωπικά δεδομένα, λογίζονται τα προσωπικά δεδομένα υγείας, οικονομικά δεδομένα, δεδομένα πιστοληπτικής ικανότητας, βιομετρικά δεδομένα, προσωπικές πληροφορίες που συλλέγονται σε απευθείας σύνδεση από παιδιά κάτω των 13 ετών (αριθμοί κοινωνικής ασφάλισης και άλλα κυβερνητικά αναγνωριστικά στοιχεία), αριθμοί πιστωτικών καρτών και οικονομικών λογαριασμών, ιατρικά ή ιατρικά στοιχεία, ασφαλιστική ταυτότητα, διαπιστευτήρια λογαριασμού στο διαδίκτυο, ψηφιακές υπογραφές και / ή βιομετρικά στοιχεία) (DLA Piper, 2017).

Ανά Πολιτεία ισχύουν ειδικότερες προστατευτικές διατάξεις οι οποίες ενισχύουν το γενικότερο προφίλ προστασίας του καταναλωτή έναντι των παρεμβάσεων στα προσωπικά του δεδομένα. Συγκεκριμένα στην πολιτεία της Καλιφόρνια, από 1η Ιανουαρίου 2020, η California Consumer Privacy Act (CCPA)⁹ εφαρμόζει και εισάγει σαφείς ορισμούς και ευρεία ατομικά δικαιώματα, περιορισμούς στη συλλογή, χρήση και αποκάλυψη προσωπικών πληροφοριών (Kari Paul, 2020). Ο κάτοικος της συγκεκριμένης πολιτείας, απολαμβάνει της προστασίας της California Consumer Privacy Act (CCPA) και την καθοδήγηση σε περιπτώσεις παραβιάσεων. Αντίστοιχα προστατεύονται υπό προϋποθέσεις και οι επιχειρήσεις, με κριτήρια εισοδηματικά και με βάση την προσφορά τους στον οικονομική δραστηριότητα της πολιτείας (Information National Freedom of Coalition., 2020). Τα εισοδηματικά κριτήρια εναπόκεινται στην εμπορική δραστηριότητα της επιχείρησης εντός ή σε σχέση-εξάρτηση με την πολιτεία της Καλιφόρνιας.

Στην περίπτωση που οι παραβιάσεις αφορούν ιδιώτες ακόμη και αν το άτομο βρίσκεται προσωρινά εκτός της πολιτείας, παρέχεται στην ιστοσελίδα του οργανισμού αναλυτική περιγραφή των δικαιωμάτων του καταναλωτή και οι εναλλακτικές δράσεις του σε περιπτώσεις παραβίασης των προσωπικών του δεδομένων ή χρήσης τους χωρίς άδεια. Συγκεκριμένα το δικαίωμα “opt-out”, αναφέρεται στην απαγόρευση χρήσης των δεδομένων του χρήστη για εμπορικούς σκοπούς, με εξαίρεση τις περιπτώσεις που υφίσταται συναίνεση, μεταγενέστερα της απαγορευτικής δήλωσης του, καθώς και εξειδικεύεται ο τρόπος άσκησης του δικαιώματος αυτού, παρέχοντας σαφείς κατευθύνσεις προς το χρήστη. Για παράδειγμα ο χρήστης-καταναλωτής έχει το δικαίωμα να ειδοποιηθεί, πριν ή στο σημείο που οι επιχειρήσεις συλλέγουν τα προσωπικά του στοιχεία, το είδος προσωπικών πληροφοριών που συλλέγονται (ονοματεπώνυμο, ημερομηνία γέννησης κ.λπ.), τον τρόπο χρήσης και τυχόν

⁹<https://www.oag.ca.gov/privacy/ccpa> (Ημερομηνία πρόσβασης 10-05-2020).

διάθεσης αυτών. Στις περιπτώσεις που εμπίπτουν στις απαγορευτικές και καταχρηστικές ενέργειες από την επιχείρηση ή τον οργανισμό κρατικό ή μη, που προέβη στην παραβίαση των δεδομένων προσωπικού χαρακτήρα φυσικού προσώπου ή επιχείρησης υπό τις προαναφερθείσες προϋποθέσεις, υπάρχει η νομική οδός με την κατάθεση μήνυσης σε βάρος των επιχειρήσεων για τις περισσότερες παραβιάσεις CCPA. Ειδικότερα στις περιπτώσεις υποκλοπής κρυπτογραφημένων προσωπικών στοιχείων, ως αποτέλεσμα των ελλείψεων της επιχείρησης να διατηρήσει ικανό επίπεδο ασφαλείας για τους συναλλασσόμενους με αυτήν χρήστες, προβλέπεται προστασία και καταδίκη των επιχειρήσεων.

Στην περίπτωση που το φυσικό ή νομικό πρόσωπο επιθυμεί να αποζημιωθεί για βλάβη που υπέστη ως αποτέλεσμα της πρόθεσης ή της αμέλειας της επιχείρησης, ακολουθείται συγκεκριμένη διαδικασία που υπαγορεύει την πρότερη ενημέρωση της επιχείρησης, για ποιες ενότητες CCPA παραβίασε και τη θέση προθεσμίας συμμόρφωσης των 30 ημερών, προκειμένου η επιχείρηση να διαβεβαιώσει με γραπτή δήλωση της τον ιδιώτη ότι έχει διορθωθεί το σφάλμα που είχε ως αποτέλεσμα τη βλάβη, όπως αυτή καταγγέλλεται. Στην περίπτωση αυτή που ακολουθείται η διαδικασία της έγγραφης δήλωσης ως προς τη συμμόρφωση με τις υποδείξεις της CCPA και επακόλουθη διόρθωση των όποιων ελλείψεων ή παραβιάσεων, δεν υφίσταται περαιτέρω δικαίωμα υποβολής αγωγής αποζημίωσης σε βάρος της επιχείρησης για το λόγο αυτό, με εξαίρεση τις περιπτώσεις που η επιχείρηση συνεχίσει να παραβιάζει το CCPA αντίθετα με τη δήλωσή συμμόρφωσής της.

Για όλες τις άλλες παραβιάσεις του CCPA, αποκλειστικά ο Γενικός Εισαγγελέας μπορεί να υποβάλει αγωγή εναντίον επιχειρήσεων, ο οποίος δεν εκπροσωπεί μεμονωμένους καταναλωτές, αλλά με αφορμή τα παράπονα καταναλωτών και άλλες πληροφορίες, συγκεντρώνει πληροφοριακό υλικό και εντοπίζει μοτίβα κακής συμπεριφοράς που μπορεί να οδηγήσουν σε έρευνες και ενέργειες εκ μέρους των συλλογικών νομικών συμφερόντων των κατοίκων της Καλιφόρνια. Συνεπώς η αρμοδιότητα του Γενικού Εισαγγελέα εναπόκειται στην προστασία και διατήρηση της συνολικής νομοθετικής ευταξίας και δεν καλείται για την κάθε μεμονωμένη περίπτωση παραβίασης των δεδομένων προσωπικού χαρακτήρα ιδιώτη, πάρα μόνο όταν οι δράσεις αυτές έχουν οργανωμένο και το συνολικό χαρακτήρα (*California Consumer Privacy Act (CCPA)*, 2019).

Σύμφωνα με το CCPA οι επιχειρήσεις οφείλουν και οι πολίτες δικαιούνται να γνωρίζουν, κάθε λεπτομερές στοιχείο για τη συλλογή των προσωπικών τους πληροφοριών, το είδος των δεδομένων που συλλέγονται καθώς και το σκοπό της συλλογής τους (χρήση, επεξεργασία από τον πάροχο ή άλλο φορέα). Υπό αυτό το πρίσμα και προκειμένου να

εξασφαλιστεί η διαφάνεια κατά τη διαχείριση των προσωπικών δεδομένων των πελατών τους, οι επιχειρήσεις υποχρεούνται να δημοσιεύουν την πολιτική απορρήτου που υιοθετούν, όπου γίνεται αναφορά στις κατηγορίες των προσωπικών πληροφοριών που συλλέγονται, τους σκοπούς χρήσης, τις κατηγορίες υπηρεσιών, τους παρόχους και άλλα τρίτα μέρη στα οποία αποκαλύπτονται ή πωλούνται πληροφορίες και ατομικά δικαιώματα των ατόμων (π.χ. πρόσβαση, διαγραφή, δεδομένα φορητότητας). Ο σύνδεσμος "do not sell my information", αποτελεί μια σελίδα όπου οι καταναλωτές μπορούν να αποχωρήσουν από την πώληση των προσωπικών τους πληροφοριών¹⁰ υπό μια διαδικασία εξαίρεσης κατά την οποία ο καταναλωτής δεν είναι υποχρεωμένος να δημιουργήσει λογαριασμό, παρέχοντας τα προσωπικά του στοιχεία. Τα στοιχεία που αποθηκεύονται για το σκοπό αυτό, οφείλουν να είναι τα απολύτως αναγκαία για τη συμπλήρωση του αιτήματος εξαίρεσης και με χρονικό ορίζοντα τουλάχιστον 12 μηνών πριν ζητηθεί από τον καταναλωτή να συμμετάσχει στην πώληση των προσωπικών του στοιχείων. Παράλληλα στο πλαίσιο εξασφάλισης των δεδομένων που παρέχονται, η επιχείρηση οφείλει να διασφαλίσει ότι τα άτομα που χειρίζονται ερωτήσεις καταναλωτών σχετικά με τις πρακτικές απορρήτου ή συμμόρφωσης, ενημερώνονται για το ισχύον νομοθετικό πλαίσιο και γνωρίζουν πώς να κατευθύνουν τους καταναλωτές να ασκήσουν τα δικαιώματά τους.

Σε κάθε περίπτωση ακόμη και εν αγνοία των επιχειρήσεων που διαχειρίζονται προσωπικά δεδομένα των χρηστών τους διαβλέπεται η ευθύνη της επιχείρησης για την ορθή και κατάλληλη συλλογή τους, αλλά και για την ασφαλή φύλαξη των δεδομένων και πληροφοριών που ορθά και νομότυπα έχουν αποθηκευτεί. Η ευθύνη αυτή βαραίνει εξ ολοκλήρου την κάθε επιχείρηση συλλογής, τόσο κατά τους κανονισμούς του αμερικανικού δικαίου και των επιμέρους διατάξεων που διέπουν την Πολιτεία της Καλιφόρνια, όσο και κατ' αντιστοιχία το λοιπό νομικό πλέγμα των ευρωπαϊκών χωρών. Το βάρος απόδειξης μετατοπίζεται στον οργανισμό ή την επιχείρηση για να συμμορφωθεί ή να αντικρούσει την όποια καταγγελία δημιουργεί δικαίωμα αγωγής για παραβιάσεις του CCPA. Λογικό επακόλουθο αυτού είναι η δημιουργία των προσωπικών δεδομένων, ως αγαθού εμπορεύσιμου και άξιου προστασίας. Η άνθηση εταιριών που εξασφαλίζουν στην κάθε επιχείρηση τον έλεγχο των δεδομένων που διακινεί και βεβαιώνει την ασφαλή διακίνηση τους προστατεύοντας από παραβιάσεις ασφαλείας, είναι γεγονός. Οι επιπτώσεις ενός κενού ασφαλείας στην επιχείρηση έχει αντίκτυπο στο κύρος τις συναλλαγές της, ανεξαρτήτως του

¹⁰<https://www.clarip.com/data-privacy/do-not-sell-my-personal-information/> (Ημερομηνία πρόσβασης 14-05-2020).

είδους αυτής. Το όποιο κενό ασφαλείας δύναται να προκαλέσει τριγμούς ακόμη και στον κοινωνικό ιστό, όταν διακυβεύεται η αξιοπιστία της εταιρείας, όπως για παράδειγμα της εταιρείας που διαχειρίζεται τα δεδομένα αποτελεσμάτων των εκλογών (*Cybersecurity Legislation 2020*, 2020). Πέραν αυτών υφίστανται και επιπρόσθετοι νόμοι περί προστασίας της ιδιωτικής ζωής στην Πολιτεία της Καλιφόρνια όπως για παράδειγμα California's "Shine the Light Law" που έχουν νομοθετηθεί και ισχύουν και επιβάλλουν πρόσθετες υποχρεώσεις προειδοποίησης (DLA Piper, 2017).

Τον Ιούνιο του 2018, το Οχάιο έγινε το πρώτο αμερικανικό κράτος που πέρασε νομοθεσία για την ασφαλή ασφάλεια στον κυβερνοχώρο. Ως μια πρώτη νομοθετική προσπάθεια κατατέθηκε με νομοσχέδιο της Γερουσίας της Καλιφόρνια 27 για την αντιμετώπιση της «χρηματιστηριακής λίστας», της συλλογής και της πώλησης των προσωπικών πληροφοριών των ατόμων. Τα στοιχεία αυτά χρησιμοποιούνται ως πηγή άντλησης πληροφοριών για εμπορικούς σκοπούς, τροφοδότησης σε καμπάνιες μάρκετινγκ, συμπεριλαμβανομένων των ανεπιθύμητων μηνυμάτων, του τηλεμάρκετινγκ και του ανεπιθύμητου ταχυδρομείου. Οι μεσίτες λίστας συλλέγουν προσωπικά στοιχεία από πολλές πηγές, όπως επιχειρηματικές συναλλαγές, κάρτες εγγύησης και καταχωρήσεις λαχείων. Σε αρκετές των περιπτώσεων οι επιχειρήσεις δεν ενημερώνουν τα άτομα για την καταχώρηση και την επεξεργασία των προσωπικών δεδομένων τους ή για την πώληση αυτών σε εταιρείες που επιθυμούν να κατηγοριοποιήσουν το αγοραστικό κοινό, αλλά και σε χρηματιστές που καταρτίζουν μελέτες αγοραστικής δυναμικής των εταιριών που κινούνται στο χρηματιστήριο. Η πληροφόρηση για την άνοδο ή πτώση της δυναμικής της εταιρίας μπορεί να αποσταθεροποιήσει τους δείκτες και να μεταβάλει την αγοραστική δύναμη της, με συνέπειες στους οικονομικούς της δείκτες (California S.B. 27, 2020). Η αρχική πρόβλεψη του νομοσχεδίου περιελάμβανε αυστηρές διατάξεις για το σύνολο των επιχειρήσεων με στόχο την προστασία του χρήστη-καταναλωτή. Ωστόσο κατά την τελική τροποποίηση εξαιρέθηκαν από τις διατάξεις του εν λόγω νόμου οι εταιρείες που εφαρμόζουν πολιτικές απορρήτου και παρέχουν στους καταναλωτές την επιλογή, να εξαιρεθούν από την αποκάλυψη των προσωπικών τους στοιχείων σε τρίτους για σκοπούς μάρκετινγκ. Στις περιπτώσεις αυτές, η εταιρεία δεν υποχρεούται να παρέχει στον καταναλωτή τις λεπτομέρειες σχετικά με τις πληροφορίες που κοινοποιήθηκαν και σε ποιόν, αλλά απλώς απαιτείται να ενημερώνει τους καταναλωτές για μια δωρεάν μέθοδο, με την οποία μπορούν να εξαιρεθούν της διαδικασίας. Η τελική αυτή ευνοϊκή ρύθμιση καταδεικνύει έμπρακτα τη σπουδαιότητα της διαχείρισης των προσωπικών δεδομένων των χρηστών από τις επιχειρήσεις και την ασύδοτη χρήση τους,

μέχρι τη θεσμοθέτηση ισχυρού νομικού πλαισίου, που θα κατοχυρώνει τους χρήστες που αγνοούν την αξία των προσωπικών τους πληροφοριών για τις επιχειρήσεις και θα τους κατευθύνει ως προς την άσκηση των δικαιωμάτων τους, με ευρύτερο στόχο τον περιορισμό της πώλησής των προσωπικών δεδομένων τους (Thomas and Hoofnagle, 2011).

Στον αντίποδα ωστόσο, οι τεχνικές και οι πιέσεις της αγοράς που αντιμετωπίζει την προσωπική πληροφορία ως το πλέον εμπορεύσιμο προϊόν, υπαγορεύουν ένα νομικό πλαίσιο συνυφασμένο στην πολιτική της ελευθεριότητας και της ελεύθερης διακίνησης της πληροφορίας ακόμη και αν αυτή θίγει τα προσωπικά δεδομένα του χρήστη. Οι ΗΠΑ όπως καταδεικνύουν οι δράσεις τους δεν επιδιώκουν τον ψηφιακό προστατευτισμό και υποστηρίζουν την ελευθεριότητα στην διάδοση της ψηφιακής πληροφορίας. Ο στόχος της μεγιστοποίησης του κέρδους είναι υπαρκτό δέλεαρ για τις επιχειρήσεις και τους οργανισμούς που διακινούν πληροφορίες για εμπορικούς σκοπούς. Οι περιορισμοί χρήσης στην πώληση και μεταφορά αντίκεινται στη λογιστική του εμπορίου, όπου η πληροφορία πρέπει να διακινείται ελεύθερα, χωρίς περιορισμούς και σε κάθε περίπτωση το αντίκτυπο είναι οικονομικό (Yakovleva and Irion, 2020, σ.3).

Ο αντίλογος στην ελευθεριότητα της διακίνησης των πληροφοριών έρχεται από την κινεζική αγορά, όπου υποστηρίζει ότι η δραστηριότητα των ΗΠΑ συνίσταται στην υποβόσκουσα στόχευση να διαδώσουν και να κυριαρχήσουν μέσω της κουλτούρας, των συνηθειών τους, που φροντίζουν μέσω των εφαρμογών facebook, twitter κ.λπ., να προωθούν σε όλο και μεγαλύτερο μέρος του πλανήτη. Η ψηφιακή ελευθεριότητα συνίσταται σε έμμεση ψηφιακή υποβολή των συνηθειών και του τρόπου ζωής και σκέψης σε ευρύτερη κλίμακα.¹¹ Η προπαγανδιστική νοοτροπία υπαγορεύει, κατά τον αντίλογο της ανταγωνιστικής κινεζικής αγοράς, την προώθηση όχι μόνο των αμερικανικών προϊόντων, αλλά κυρίως της αμερικανικής κουλτούρας, ώστε το αγοραστικό κοινό πέραν των ΗΠΑ να επεκταθεί και να υιοθετήσει κοινές συνήθειες και καταναλωτική νοοτροπία.

Εκτός των ανωτέρω το νομοθετικό πλαίσιο των ΗΠΑ προσαρμόζεται, όσο το επιτρέπουν οι συνθήκες, με την θέσπιση στην Πολιτεία της Καλιφόρνια, από την 1η Ιανουαρίου 2020, της πρώτης νομοθεσίας των ΗΠΑ σχετικά με το Ίντερνέτ των πραγμάτων. Το Ίντερνέτ των πραγμάτων παρέχει δυνατότητες επεξεργασίας πληροφοριών που επιτρέπουν στους υπολογιστές να αισθάνονται, να ενσωματώνουν, να παρουσιάζουν και να αντιδρούν σε όλες τις πτυχές του φυσικού κόσμου, ανταποκρινόμενοι στις ανάγκες του χρήστη τους. Η

¹¹<https://www EFF.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall> (Ημερομηνία πρόσβασης:05-03-2020).

σύγχρονη πραγματικότητα είναι αυτό που θεωρούνταν «ουτοπικό» κατά την προηγούμενη δεκαετία. Η μετάβαση από «διασυνδεδεμένους υπολογιστές» σε «διασυνδεδεμένα πράγματα», με την ανάπτυξη νέων εφαρμογών και υπηρεσιών, υποστηρίζουν τη διαλειτουργικότητα μεταξύ ετερογενών συσκευών και εντάσσουν το χρήστη σε μια πραγματικότητα όπου διαχειρίζεται τα αντικείμενα και αλληλεπιδρά με αυτά, καταγράφοντας τα δεδομένα που του είναι χρηστικά (Chaqfeh and Mohamed, 2012).

Ήδη από το 2015 με την εναρκτήρια ομιλία του CEO της Samsung Electronics στη CES 2015, είχε διαφανεί η δυναμική του νέου προϊόντος που θα αναπτύξει το δίκτυο σε επίπεδο χρήστη, μεταξύ των συσκευών που διαχειρίζεται, διευκολύνοντας την καθημερινότητά του. Το «ιντερνέτ των πραγμάτων» (Scott R. Peppet, 2008), έχει τις προοπτικές να μεταμορφώσει την κοινωνία, την οικονομία και τον τρόπο με τον οποίο ζούμε τις ζωές μας», ανέφερε ο κ. Yoon. «Είναι δική μας αρμοδιότητα, ως βιομηχανία, να κάνουμε πραγματικότητα, όλα όσα υπόσχεται το ιντερνέτ των πραγμάτων (*Η Εναρκτήρια ομιλία του CEO της Samsung Electronics στη CES 2015*, 2014). Η εξελικτική αυτή τροπή χρήσης των συσκευών έχει πολλές συνιστώσες. Το νομοθετικό πλαίσιο όπως θεσμοθετήθηκε με την έλευση του έτους, προβλέπει ότι οι κατασκευαστές των περισσότερων συνδεδεμένων με Bluetooth συσκευών, θα πρέπει να εφαρμόσουν χαρακτηριστικά ασφαλείας «κατάλληλα» για τη φύση και τη λειτουργία της συσκευής και συνδυασμένα με τις πληροφορίες που μπορεί να συλλέγει, να περιέχει ή να μεταδίδει η συσκευή, ενώ παράλληλα να είναι εξοπλισμένα με εφαρμογές έναντι της μη εξουσιοδοτημένης πρόσβασης, καταστροφής, χρήσης, τροποποίησης ή αποκάλυψης των πληροφοριών που περιέχουν. Η εφαρμογή των πρωτοκόλλων ασφαλείας εναπόκειται στην κάθε επιχείρηση, η οποία οφείλει να ενημερώνει το χρήστη για τυχόν έλλειψη στον τομέα αυτό και να προσαρμόζει ικανό επίπεδο ασφαλείας της.

Παράλληλα οι συνθήκες τις σύγχρονης καθημερινότητας αναπροσαρμόζονται συνεχώς και οι πολίτες υπό τους αυξημένους ρυθμούς κοινωνικής ζωής, απαιτούν άμεσα πληροφορίες από τις κυβερνήσεις και τους φορείς. Οι κυβερνήσεις αναγνωρίζοντας τα πλεονεκτήματα που προσφέρει η διακίνηση πληροφοριών με τη χρήση κοινωνικών μέσων και εργαλείων, δραστηριοποιούνται αξιοποιώντας τα τεχνολογικά επιτεύγματα προς το σκοπό αυτό. Το κοινό ενημερώνεται έγκυρα και έγκαιρα σχετικά με την απόδοσή τους, οι δημόσιες υπηρεσίες υιοθετούν πιο εξελιγμένες τεχνολογίες (blockchain, κβαντική πληροφορική, τεχνητή νοημοσύνη) για να κάνουν τις υπηρεσίες τους πιο καινοτόμες και πιο ευέλικτες και προσαρμόζοντας για το σκοπό αυτό, τις υπάρχουσες κοινωνικές δομές και λειτουργίες της

δημόσιας διαχείρισης (Criado and Gil-garcia, 2019). Υπό το πρίσμα αυτό οι αμφίπλευρες κινήσεις διαχείρισης των πληροφοριών των χρηστών-πολιτών, τόσο από κρατικούς φορείς, όσο και από ιδιωτικές επιχειρήσεις, έχουν ανάγκη ενιαίου ρυθμιστικού πλαισίου που καθορίζει με σαφήνεια τις προϋποθέσεις παρέμβασης συλλογής και διαχείρισης των προσωπικών δεδομένων των πολιτών τους (Aaronson, 2015).

1.7 Δυτική Αφρική– Το παράδειγμα του Μπενίν

Οι περισσότερες χώρες υιοθέτησαν το νομοθετικό πλαίσιο για τη διαφάνεια κατά τη δεκαετία του 1990 και στις αρχές του 21^{ου} αιώνα. Με εξαίρεση τη Σουηδία (όπου εγκρίθηκε ένας νόμος ήδη από το 1776), η Φινλανδία και οι Ηνωμένες Πολιτείες (ΗΠΑ), οι περισσότερες χώρες της Ευρώπης, οι χώρες της Βόρειας Αμερικής, Μεξικό, Ινδία, Αυστραλία, Νέα Ζηλανδία, έχουν κωδικοποιήσει την προστασία της ελευθερίας της πληροφόρησης (FOI). Παράλληλα ορισμένες χώρες, όπως η Κίνα, το Hong Kong, η Αργεντινή, η Νιγηρία, ήδη ανέγνωσαν την επερχόμενη αλλαγή στην ροή των πληροφοριών που καθιστά την νομοθετική πρόβλεψη αναγκαία και έχουν προσαρμόσει το εσωτερικό τους δίκαιο, αντικρούοντας τις όποιες αντιδράσεις είχαν αρχικά ανακύψει στο εσωτερικό τους (Meijer, Curtin and Hillebrandt, 2012). Ωστόσο κατά το παράδειγμα της Κίνας, αν και υφίσταται το νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων των πολιτών, αυτό καθίσταται ανίσχυρο, χωρίς τη ρητή πρόβλεψη των απειλούμενων ποινών για τους παραβάτες και σαφή διάκριση των δικαιωμάτων των χρηστών. Υπό το πλαίσιο αυτό, η στοχευμένη και σαφής θεσμοθέτηση κρίνεται επιβεβλημένη, κατά την οποία να ορίζεται ισχυρή απαξία και πρόβλεψη καταδίκης- ποινής για τον παραβάτη.

Παράλληλα υφίστανται περιπτώσεις χωρών όπου δεν έχει θεσπιστεί νόμος για την πρόσβαση στην πληροφορία (Access to Information–ATI), όπως για παράδειγμα στην Αφρική, η οποία κατέχει στο μεγαλύτερο μέρος της το υψηλότερο ποσοστό απουσίας νομοθετικής πρόβλεψης. Στην Ινδία τον Ιούνιο του 2018 διοργανώθηκε διεθνής καμπάνια ενημέρωσης για τα δικαιώματα πρόσβασης στην πληροφορία (Nayanimia, 2019), ενώ ο νόμος για το δικαίωμα της πληροφόρησης (RTI) τέθηκε σε ισχύ το 2005. Ανάλογα με το πολιτισμικό πλαίσιο, η έννοια της προστασίας των προσωπικών δεδομένων ανά την κάθε χώρα, μπορεί είτε να αντιμετωπίζεται ως εγγενής αξία, η οποία χρήζει εξ ορισμού νομικής προστασίας από το θεσμικό κράτος, είτε ως ένας μηχανισμός που εξασφαλίζει την ισχυρή αξία και δράση του οργάνου. Η τελευταία αυτή προοπτική προϋποθέτει την ύπαρξη διαφάνειας κατά τις διαδικασίες εφαρμογής και εκπλήρωσης του στόχου της δημόσιας

διοίκησης, που δεν είναι άλλος από την προστασία των προσωπικών δεδομένων των πολιτών. Η θέση και η εκπλήρωση των νομοθετικά προβλεπόμενων συνθηκών προϋποθέτει την αυξημένη συμμετοχή των πολιτών καθώς και εμπιστοσύνη στη δημόσια διοίκηση και τις εκφάνσεις της (Mabillard, KakpoviandCottier, 2020).

Χαρακτηριστικό αποτελεί το παράδειγμα του Μπενίν-κρατίδιο της Δυτικής Αφρικής, με πολυτάραχη εσωτερική ιστορία, ως ενδεικτικό της αυξημένης διαβούλευσης που τελείται από κρατικούς φορείς και κοινωνικούς παράγοντες ως προς την θέσπιση της νομοθεσίας που θα κατοχυρώσει την ελευθερία πρόσβαση στην πληροφόρηση. Το Μπενίν υπήρξε πρώην γαλλική αποικία και αποτέλεσε πόλο έλξης για απανταχού αποικιοκράτες, δεχόμενο πλήθους πολιτισμικών επιρροών, κυρίως γαλλικών, σε όλους τους τομείς του δικαίου. Αξίζει να σημειωθεί ότι ανεξαρτητοποιήθηκε από τη Γαλλία, την 1^η Αυγούστου 1960. Συνυπολογίζοντας ότι το Μπενίν έχει Σύνταγμα από τις 2 Δεκεμβρίου του 1990, με το πολίτευμα της Προεδρικής Δημοκρατίας, συμπεραίνεται η άρρηκτη σύνδεση των ιστορικών και πολιτικών δεδομένων, με τον τρόπο αντιμετώπισης και χειρισμού των ατομικών ελευθεριών (Ronen, Dov, Robin, Law, 2021). Η διαχείριση της ελευθερίας πρόσβασης στην πληροφορία, απαιτεί κοινωνική και πολιτική βούληση και ριζοσπαστική διάθεση προστασίας του αγαθού της ελεύθερης πρόσβασης στην πληροφορία.

1.8 Κίνα

Στις 7 Μαΐου 1999, στα πλαίσια βομβαρδισμού του NATO στη Γιουγκοσλαβία (Επιχείρηση Συμμαχικής Δύναμης), συντονίστηκαν αμερικανικές βόμβες άμεσης επίθεσης των ΗΠΑ με προορισμό τη Σερβική πόλη του Βελιγραδίου, οι οποίες δεν έφτασαν στον προορισμό τους, αλλά από λάθος ένδειξη στις συντεταγμένες θέσεις του στόχου τους που τους έδωσε το GPS, έπληξαν την πρεσβεία της Λαϊκής Δημοκρατίας της Κίνας,. Αποτέλεσμα ήταν ο θάνατος τριών Κινέζων διπλωματών, ο τραυματισμός υπαλλήλων της Πρεσβείας και η ολοσχερής καταστροφή του κτιρίου (Pariser, 2011, σ. 141–143).

Η επίσημη ανακοίνωση του NATO της 08/05/1999 ήταν η κάτωθι:

«Following its meeting this afternoon the North Atlantic Council wishes to express its deep regret for the tragic mistake of the bombing of the Chinese Embassy in Belgrade.

The sincere sympathy and condolences of all members of the Alliance go to the victims, their families and the Chinese government.

NATO never has, and never will, intentionally target civilians. Extraordinary care is taken to avoid damage to other than legitimate military and military-related targets. The

bombing of the Chinese Embassy was a deeply regrettable mistake. We continue to review the circumstances surrounding the incident and we will make available any further information as soon as possible.

NATO will continue to pursue its goals: to stop the ethnic cleansing in Kosovo and ensure the Kosovars can return to their homes in peace and security.

NATO is prepared to suspend its air strikes once Belgrade has unequivocally accepted the five key conditions set down by the North Atlantic Council for a peaceful settlement of the conflict.

NATO will continue to support all attempts at a diplomatic solution which respect these conditions. Our mistaken attack against the Chinese Embassy should not diminish or derail these efforts building on the results of the recent G8 meeting».¹²

Η αντίδραση του κινέζων πολιτών ήταν σφοδρή, με αντιδράσεις και συγκεντρώσεις διαμαρτυρίας κατά της αποτρόπαιης αυτής πράξης των Ηνωμένων Πολιτειών. Η ανακοίνωση του NATO καθώς και η απολογητική ανακοίνωση των Ηνωμένων Πολιτειών μεταδόθηκε στον κινεζικό λαό, μόλις τέσσερις ημέρες αργότερα, επιτρέποντας τις εντάσεις να κορυφωθούν. Το περιστατικό αυτό αποτελεί από παράδειγμα της μονομερούς μετάδοσης της πληροφορίας και της λογοκριτικής συμπεριφοράς της πολιτικής εξουσίας χωρών και κυβερνήσεων. Η διάδοση της πληροφόρησης, όσο και η αποτροπή αυτής, έχει στη σημερινή εποχή της αμέσους ενημέρωσης εξέχουσα θέση και η αποτροπή αυτής, επίσης σημαίνουσα θέση. Το Chinese Firewall αποδεικνύεται σε κάθε περίπτωση με τη λογική διεκδίκησης των συμφερόντων υπέρ της ασφάλειας στον κυβερνοχώρο (Yakovleva and Irion, 2020, σ. 3). Το φιλτράρισμα δεδομένων υπό τη μορφή του αποκλεισμού των κοινωνικών δικτύων και της Google, κατευθύνει τη γνώση και την ενημέρωση του ατόμου υπό το πρίσμα της κοινωνικής ευταξίας (Zittrain and Edelman, 2003), με χαρακτηριστική την απαγόρευση του καρτούν Internet Police, ως παράδειγμα προς αποφυγή.

Από την άλλη πλευρά, τα ανωτέρω εξελίσσονται κατά τη διάρκεια συνεχούς επίδειξης της τεχνολογικής υπεροχής της κινεζικής ψηφιακής τεχνολογίας¹³, με τη δημιουργία επεξεργαστών όπως η Huawei, που δύναται να χρησιμοποιηθούν σε αλγόριθμο, σχεδιασμένο να αναγνωρίζει ένα πρόσωπο μέσα σε ένα κινούμενο πλήθος δεκάδων χιλιάδων ανθρώπων, σε λίγα δευτερόλεπτα. Η αποτύπωση της κίνησης του ατόμου εντός του χώρου, όπως αυτό

¹²<https://www.nato.int/docu/pr/1999/p99-076e.htm>, (Ημερομηνία πρόσβασης: 02-09-2019).

¹³<http://www.wuzhenwic.org/> (Ημερομηνία πρόσβασης: 02-09-2019).

καταγράφεται από κλειστά κυκλώματα καμερών, δημιουργεί μια προσωποποιημένη βάση δεδομένων υπό τις ευλογίες της κρατικής εξουσίας. Η εν λόγω τεχνολογία προκαλεί τις κυβερνήσεις του δυτικού κόσμου όπως και των αμερικάνων επιστημόνων αναγνωρίζοντας, το πλεονεκτήματα της ψηφιακής εξέλιξης στον τομέα αυτό, καθώς και την ευθεία προσβολή της προσωπικής ελευθερίας του ατόμου (Alan Weedon and Samuel Yang, 2019).

Ειδικότερα το τείχος προστασίας της Λαϊκής Δημοκρατίας της Κίνας, δεν επιτρέπει εφαρμογές όπως Twitter, το Google και το Facebook να λειτουργούν στην εδαφική τους αρμοδιότητα, μπλοκάροντας την οποιαδήποτε πηγή πληροφοριών, η οποία μπορεί να προκαλέσει ανισορροπία στις κοινωνικές δομές. Εξάιρεση αυτού αποτελεί το Χονγκ Κονγκ, ως μέρος της συμφωνίας «μία χώρα, δύο συστήματα», όπου λειτουργεί έξω από το «τείχος προστασίας» και έχει διαθέσιμες υπηρεσίες όπως το Twitter, το Google και το Facebook, με τους τοπικούς ISP¹⁴-παρόχους να τίθενται απέναντι στην άμεση κρατική λογοκρισία στο ανοιχτό Διαδίκτυο (*China and the Internet*, 2014). Προς την κατεύθυνση αυτή η Δημοκρατία της Κίνας έχει αναπτύξει εφαρμογές περιορισμένης χρήσης για τους πολίτες της, αντίστοιχες του twitter¹⁵, αντιτασόμενη στην προπαγανδιστική χρήση των αμερικανικών τύπου εφαρμογών, ως ένας τρόπος αποφυγής διάδοσης των ιδεών και της αμερικανικής κουλτούρας και νοοτροπίας (O'Brien, 2019). Το φιλτράρισμα των πληροφοριών που παρέχονται από τις εφαρμογές που διαχειρίζονται εκατομμύρια χρήστες ανά τον κόσμο, είναι ενδεικτικό της πρόθεσής για έλεγχο στα δεδομένα και τις πληροφορίες που διακινούνται. Η αποτύπωση των αναζητήσεων και του πλήθους των αποτελεσμάτων που αναρτώνται προς το χρήστη, είναι ενδεικτικό του ελέγχου που ασκείται κατά τη διακίνηση της πληροφορίας.

Επιπλέον το Tik Tok¹⁶, είναι μια από τις μεγαλύτερες και ταχύτερα αναπτυσσόμενες παγκόσμιες πλατφόρμες κοινωνικών δικτύων που ξεκινούν από το Πεκίνο, μέσω της οποίας εποπτεύεται σε μεγάλο βαθμό το περιεχόμενό του. Οι διαδεδομένες οδηγίες γενικής εποπτείας του Tik Tok απαγορεύουν ρητά οποιοδήποτε περιεχόμενο επικρίνει την κινεζική κυβέρνηση, όπως περιεχόμενο που σχετίζεται με την κινεζική δίωξη των εθνοτικών μειονοτήτων, ενώ κράτη όπως οι Ηνωμένες Πολιτείες παρατηρούν την εξάπλωση της εφαρμογής και του αντίκτυπου που έχει ιδίως στις νεαρές ηλικίες και απειλούν με

¹⁴<https://www.isp.com/> (Ημερομηνία πρόσβασης: 12-10-2019).

¹⁵LIHKG (Unofficial Chinese: Cantonese Yale: Lihndāng) is a multi-category forum website based in Hong Kong. The website has gained popularity since the launch in 2016, and is often referred to as the Hong Kong version of Reddit. (<https://en.wikipedia.org/wiki/LIHKG>, Ημερομηνία πρόσβασης: 02-09-2019).)

¹⁶<https://www.tiktok.com> (Ημερομηνία πρόσβασης: 02-09-2019).

απαγορεύσεις χρήσης, κατά την προσπάθεια να περιορίσουν τη χρήση της εφαρμογής ή στην περίπτωση που δεν είναι αυτό εφικτό, τη διαχείριση του. Ο καλύτερος τρόπος για να επιτευχθεί ο στόχος αυτός, είναι μέσω της αγοράς της εφαρμογής και ελέγχου της χρήσης και των πληροφοριών που διαδίδονται μέσω αυτής (Carvajal Nikki, 2020).

Η Κίνα στην προσπάθειά της να ενισχύσει τη δυναμική της κατά την εφαρμογή της πολιτικής χρήσης του διαδικτύου στο εξωτερικό, αλλά και εντός των συνόρων της, εφαρμόζει διεισδυτική πρακτική χρήσης κακόβουλου λογισμικού και επιθέσεων DDoS, που υποστηρίζονται από το κράτος. Προωθεί με τον τρόπο αυτό το φιλτράρισμα και την επιτήρηση των δεδομένων προσωπικού χαρακτήρα του πελάτη. Προβλέπει οικονομικές κυρώσεις, στην προσπάθεια να περιοριστεί η ελευθερία λόγου μέσω διασυνοριακών διαύλων επικοινωνίας, ασκώντας πίεση στους ιδιωτικούς φορείς να ενεργήσουν ως παγκόσμια πολιτιστική αστυνομία (O'Brien, 2019). Προς απόδειξη των ανωτέρω και σε εφαρμογή του συστήματος κοινωνικής πίστης, δύνανται να συγκεντρωθούν ψηφιακά 1,4 δισεκατομμύρια πολίτες σε πραγματικό χρόνο, με βάση μια ποικιλία μετρήσεων που σχετίζονται με την κοινωνική συμπεριφορά και την πιστότητα προς το πολιτικό καθεστώς της Κίνας Κεντρικό στοιχείο του συστήματος είναι περίπου 200 εκατομμύρια κάμερες CCTV σε εθνικό επίπεδο, οι οποίες τροφοδοτούν δεδομένα σε ένα δίκτυο παρακολούθησης που υποστηρίζεται από αλγόριθμους τεχνητής νοημοσύνης και μηχανικής μάθησης. Ανά πάσα στιγμή υφίσταται δυνατότητα παρακολούθησης και καταγραφής των κινήσεων ατόμων στα πλαίσια προληπτικών δράσεων, ιδίως αυτών που θεωρούνται απειλές. Ο έλεγχος των εισερχομένων πληροφοριών είναι αυστηρός, όπως και η ανατροφοδότηση από καταγεγραμμένες πληροφορίες που συλλέγονται. Αυτή η στρατηγική παρακολούθησης ομάδων ατόμων και μειονοτήτων υλοποιείται πλήρως στο Xinjiang (Falkenheim, Victor C. and Hsieh, 2018) και αποτελεί μέρος της πολιτιστικής γενοκτονίας της Κίνας, της μειονότητας των Ουιγούρων (Encyclopaedia, 2020), (Washington Post, 2020).

Παράλληλα η κυβέρνηση διατηρεί λογοκρισία σε όλα τα μέσα που μπορούν να προσεγγίσουν ένα ευρύ κοινό. Αυτό περιλαμβάνει τηλεόραση, έντυπα μέσα μαζικής ενημέρωσης, ραδιόφωνο, τέχνες, κινηματογράφος, θέατρο, γραπτά μηνύματα, άμεσα μηνύματα, βιντεοπαιχνίδια, λογοτεχνία και το διαδίκτυο. Δίνεται η αποκλειστική ευχέρεια σε Κινέζους αξιωματούχους να έχουν πρόσβαση σε μη λογοκριμένες πληροφορίες μέσω ενός εσωτερικού συστήματος εγγράφων (James Griffiths, 2017). Η χρήση της τεχνολογίας και των εφαρμογών καταγραφής προσώπου σε συνδυασμό με την κατάρτιση βάσεων δεδομένων για την κατηγοριοποίηση και τον εντοπισμό των κατοίκων ανά περιοχή, αναπτύσσεται στην Κίνα

με την επιδίωξη να αποτελέσει η πρακτική αυτή ένα συνεχές κύμα καταγραφής και αξιοποίησης των προσωπικών δεδομένων, διαμορφώνοντας έτσι διεθνείς κατευθυντήριες γραμμές για τον ψηφιακό αυταρχισμό. Η στόχευση είναι σαφής και αξιοποιείται για την επίτευξη του στόχου αυτού στο έπακρο η υφιστάμενη και διαθέσιμη τεχνολογία και τεχνογνωσία.

Η ασάφεια του νομοθετικού πλαισίου για την προστασία των δεδομένων προσωπικού χαρακτήρα στη Λαϊκή Δημοκρατία της Κίνας (Λ.Δ.Κ.), είναι ενδεικτική της διάθεσης για ύπαρξη κατευθυντήριων γραμμών, χωρίς ωστόσο πραγματικό αντίκρισμα. Οι κανόνες σχετικά με την προστασία των προσωπικών δεδομένων και την ασφάλεια των δεδομένων, αποτελούν μέρος ενός πολύπλοκου πλαισίου και εντοπίζονται σε διάφορους νόμους και κανονισμούς, χωρίς να υφίσταται ρητή απαγορευτική διάταξη με απειλή ποινής και κυρώσεων για τους παραβάτες αυτής (DLA Piper, 2017).

Την 1η Ιουνίου 2017 τέθηκε σε ισχύ ο νόμος για την ασφάλεια στον κυβερνοχώρο της Λαϊκής Δημοκρατίας της Κίνας και έγινε ο πρώτος εθνικός νόμος για την προστασία του κυβερνοχώρου και της προστασίας της ιδιωτικής ζωής των δεδομένων. Ωστόσο εξακολουθεί να υφίσταται αβεβαιότητα ως προς τον τρόπο με τον οποίο θα εφαρμοστεί ο νόμος για την ασφάλεια στον κυβερνοχώρο της ΛΔΚ και ποια πρακτικά μέτρα πρέπει να ληφθούν για την επίτευξη της συμμόρφωσης με το κανονιστικό περιβάλλον που εξακολουθεί να εξελίσσεται ταχέως. Σχέδια κατευθυντήριων γραμμών δημοσιεύονται, στα οποία ωστόσο εκλείπουν τα εθνικά πρότυπα που θα βοηθήσουν περαιτέρω τους οργανισμούς να συμμορφωθούν με τις υποχρεώσεις προστασίας δεδομένων που επιβάλλονται, βάσει του ισχύοντος νομοθετικού πλαισίου για την ασφάλεια στον κυβερνοχώρο (Carvajal Nikki, 2020). Η αμφίπλευρη και αντιφατική διαχείριση της διάδοσης της πληροφόρησης μέσω της τεχνολογίας και της χρήσης του διαδικτύου, από τη μια πλευρά ενισχύθηκε ως πρωτοπόρα, δίνοντας φορολογικές ελαφρύνσεις σε εταιρείες υψηλής τεχνολογίας και σχεδιάστηκαν εφαρμογές που έτυχαν παγκόσμιας αποδοχής. Ωστόσο από την άλλη πλευρά, η διάδοση αυτή της πληροφόρησης, σύμφωνα με την πολιτική του Κομμουνιστικού Κόμματος, θεωρήθηκε ως μη ελεγχόμενη και απειλητική, για τη σταθερότητα της χώρας και αξιολογήθηκε ως αναγκαία η θέση περιορισμών και επιπρόσθετων ελέγχων στη ροή της πληροφόρησης (*China and the Internet*, 2014).

Το ποινικό δίκαιο της ΛΔΚ απαγορεύει την πώληση, την παράνομη παροχή ή την παράνομη πρόσβαση στις προσωπικές πληροφορίες των πολιτών. Οι διατάξεις για την προστασία των προσωπικών δεδομένων των τηλεπικοινωνιών και των χρηστών του

διαδικτύου, εφαρμόζονται στους παρόχους υπηρεσιών τηλεπικοινωνιών και διαδικτύου. Αντίστοιχα οι κατευθυντήριες για τη διαχείριση δεδομένων ισχύουν για τα τραπεζικά χρηματοπιστωτικά ιδρύματα, που είναι εγκατεστημένα στο έδαφος της ΛΔΚ με άδεια λειτουργίας από τις ρυθμιστικές αρχές των τραπεζών της ΛΔΚ, ενώ καθορίζονται οι υποχρεώσεις για την ενίσχυση της ασφάλειας των πληροφοριών σχετικά με την πρόσβαση στη βάση δεδομένων για πληροφορίες σχετικά με τις χρηματοπιστωτικές πιστώσεις. Παράλληλα ο νόμος περί προστασίας των προσωπικών δεδομένων των καταναλωτών της Κίνας, περιλαμβάνει υποχρεώσεις προστασίας δεδομένων που ισχύουν για τα περισσότερα είδη επιχειρήσεων που ασχολούνται με τους καταναλωτές, αλλά και τις κυρώσεις για παραβίαση των δικαιωμάτων και των συμφερόντων τους (DLA Piper, 2017).

Σε μια προσπάθεια εναρμόνισης της νομοθεσίας της σε σχέση με την προσπάθεια προστασίας και νομιμοποίησης του ταχέως αναπτυσσόμενου τομέα του διαδικτύου της χώρας και ύπαρξης δικλίδων ασφαλείας για τη μεταφορά πολύτιμων κινεζικών δεδομένων στο εξωτερικό, οι συλλέκτες δεδομένων κρίνεται επιβεβλημένο να προστατεύουν τα προσωπικά στοιχεία του ατόμου και δεν μπορούν να αποκτήσουν, να αποκαλύψουν ή να πραγματοποιήσουν συναλλαγές τέτοιων δεδομένων αυτών, χωρίς συγκατάθεσή του υποκειμένου. Το σαφές νομοθετικό πλαίσιο θεσπίζει σαφείς και αυστηρές ποινές για τους παραβιάσεις και καθορισμένα δικαιώματα για τους πολίτες, ωστόσο το άκαμπτο δικαστικό σύστημα, περιορίζει τη δικανική κρίση κατά την εκτίμηση ερμηνευτικών διατάξεων στο ισχύον νομοθετικό πλαίσιο (Wu, 2020), (Pernot-Leplay, 2020).

1.9 Παραγωγή – Ζιμπάμπουε

Οι ρυθμιστικοί νόμοι για την προστασία της ελευθερίας της πληροφορίας έχουν μια ειδοποιό διαφορά σε σχέση με τους λοιπούς ποινικούς, οικονομικούς νόμους. Η θέσπιση και τήρησή τους είναι εμφανής στην κοινωνική πραγματικότητα, σε αντίθεση με τους νόμους που προστατεύουν την ελευθερία της πληροφορίας, οι οποίοι δεν είναι εμφανές αν τηρούνται ή όχι και αν τυγχάνουν της πλήρους εφαρμογής στην καθημερινότητα των πολιτών τους. Η προσαρμογή του νομοθετικού πλαισίου, καταδεικνύει τη διάθεση συμμόρφωσης των κυβερνήσεων στις διεθνείς επιταγές με γνώμονα τα ανθρωπιστικά ιδεώδη, ενώ παράλληλα οι διεθνείς φορείς καλύπτονται ως προς την τήρηση ενιαίας νομοθεσίας, ωστόσο χωρίς ουσιαστική εφαρμογή τους στην πράξη (Michener, 2011). Χαρακτηριστικό παράδειγμα αποτελούν η Παραγωγή και η Ζιμπάμπουε.

Η Παραγουάη έχει γίνει η 100^η χώρα στον κόσμο που έχει κατοχυρώσει την προστασία της ελευθερίας της πληροφόρησης, ως ένα γεγονός ορόσημο για την θεσμοθέτηση της προστασίας των πολιτών της, αλλά και ως καθοριστική κίνηση διαφάνειας. Το πρώτο ανεξάρτητο Σύνταγμα της Παραγουάης, το οποίο τέθηκε σε ισχύ το έτος 1980, καθορίζει τη νομική βάση για την κατοχύρωση των νόμων περί προστασίας της ελευθερίας στην πληροφόρηση, οι οποίοι ψηφίστηκαν στην Παραγουάη το έτος 1766 και προέβλεπαν την παραχώρηση στο κοινό, πρόσβαση σε κυβερνητικά έγγραφα. Έτσι από τα τέλη της δεκαετίας του '70, υπάρχει μια σταθερή έγκριση των νόμων προστασίας της ελευθερίας στην πληροφόρηση, οι οποίοι εγγυώνται την πρόσβαση του κοινού σε κυβερνητικά αρχεία, θεσμοθετώντας παράλληλα και ορισμένες ως προς αυτό εξαιρέσεις. Ωστόσο η νομοθετική αυτή πρόβλεψη αν και θεμελιώνει την προστασία του δικαιώματος της ελεύθερης πρόσβασης στην πληροφορία, δεν κατοχυρώνει αυτοδικαίως την άμεση εφαρμογή του. Τα διλήμματα που καλούνται να διαχειριστούν οι κυβερνήσεις στην προσπάθειά τους να γεφυρώσουν το χάσμα της νομοθεσίας περί ελευθερίας της πληροφόρησης και τις πράξεις διαφάνειας που καλούνται να εφαρμόσουν τα θεσμικά όργανα, αποτυπώνεται διαφορετικά στην πράξη (Meijer, Curtin and Hillebrandt, 2012), (Michener, 2011, σ.148).

Ο Νόμος για την πρόσβαση των πολιτών της Ζιμπάμπουε στην πληροφόρηση και την προστασία της ιδιωτικής ζωής (AIPPA), είχε θεσπιστεί το 2003 από το Κοινοβούλιο της. Είναι σε μεγάλο βαθμό συγκρίσιμος με τα νομοθετήματα πολλών δυτικών δημοκρατιών, ωστόσο οι διαδικασίες εφαρμογής του βρίσκουν αγκυλώσεις. Οι περιοριστικά αναφερόμενες ως εξαιρέσεις του νόμου, εφαρμόζονται καταχρηστικά και έχουν μεταλλαχθεί σε κανόνα εφαρμογής του, μεταλλάσσοντας την αρχική έννοια και σκοπό θέσπισής του (Michener, 2011, σ. 148-149), (Banisar, 2004), (Kenneth Bradley, 2020).

Η AIPPA προέβλεπε ένα σύστημα προληπτικής δημοσίευσης, σύμφωνα με το οποίο ένας δημόσιος οργανισμός πρέπει να δημοσιεύει πληροφορίες, είτε ζητούνται είτε όχι, εάν σχετίζονται με κίνδυνο σοβαρής βλάβης για την υγεία ή την ασφάλεια των μελών του κοινού, τον κίνδυνο σημαντικής βλάβης στο περιβάλλον καθώς και με θέματα εθνικής ασφάλειας. Με τον τρόπο αυτό η AIPPA, όχι μόνο κατεύθυνε την πρόσβαση στην πληροφόρηση, αλλά είχε καταστεί μέσο ελέγχου του τύπου, επιβάλλοντας πρόστιμα για την χρήση και αναμετάδοση της πληροφορίας που διακινείται εντός της χώρας. Η τακτική αυτή είχε ως αποτέλεσμα την απομάκρυνση μελών του διεθνή τύπου και την ανοιχτή αντιπαράθεση τους με κυβερνητικά κλιμάκια σε ένδειξη της δυσaráρεσκειάς τους. Υπό το πλαίσιο αυτό, η επεμβατική διάθεση του κράτους απείχε από την αρχή της διαφάνειας κατά τη διαχείριση των πληροφοριών των

πολιτών τους και παρείχε την ευχέρεια στο κράτος να περιορίσει τη δραστηριότητα του τύπου και να παρακολουθεί στενά αυτούς που εμπλέκονται σε κάθε εκδήλωση διαφορετικής, μη λογοκριμένης άποψης ή δημοσίευσης. (The Constitution Unit, 2011), (Committee to Protect Journalists, 2011).

Με τη Νο 1/2020 Διακήρυξη για την προστασία της ελεύθερης πρόσβασης των πολιτών στην πληροφορία, στην οποία καθορίζονται οι προϋποθέσεις πρόσβασης στην πληροφορία, καταργήθηκε από την 1η Ιουλίου 2020, ο προηγούμενος νόμος για την πρόσβαση στην πληροφόρηση και την προστασία της ιδιωτικής ζωής του 2003 (AIPPA). Το νομοσχέδιο για την ελευθερία της πληροφόρησης καθορίζει τη διαδικασία πρόσβασης σε πληροφορίες που κατέχουν δημόσιοι φορείς ή πληροφορίες που κατέχει οποιοδήποτε άτομο, οι οποίες είναι απαραίτητες για την άσκηση ή την προστασία του δικαιώματός του. Ορίζει επίσης τη θέσπιση προαιρετικών και υποχρεωτικών μηχανισμών- διαδικασιών, με στόχο την εξασφάλιση του δικαιώματος πρόσβασης των πολιτών σε πληροφορίες, προκειμένου να διευκολύνεται η άμεση πρόσβαση του πολίτη σε πληροφορίες και να προάγεται η διαφάνεια και η αποτελεσματική διακυβέρνηση (Zimbabwe, 2020).

Από τα ανωτέρω προρρηθέντα καθίσταται κατανοητό ότι παρά το γεγονός ότι μέχρι το 1997, 22 χώρες, μεταξύ των οποίων και η Παραγουάη, είχαν εγκρίνει νόμους FOI, δεν συνεπάγεται αυτοδικαίως την εφαρμογή τους στην κοινωνική πραγματικότητα. Βέβαια δεν υποβαθμίζεται το γεγονός ότι η θέσπιση νομοθετικού πλαισίου για την προστασία της ελεύθερης διάδοσης πληροφορίας, κατοχυρώνει ένα μοντέλο διαχείρισης της πρόσβασης στην πληροφορία, προάγει τη διαφάνεια στη δημόσια διοίκηση και επιταχύνει την ανάπτυξη του και σε λοιπές χώρες, όπου αναγνωρίζεται η σπουδαιότητα ύπαρξής τους και οι ευκαιρίες πρόσβασης που παρέχονται στο ευρύ κοινό (Toby McIntosh, 2014).

ΚΕΦΑΛΑΙΟ 2 ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΑΝΗΛΙΚΟΤΗΤΑΣ

Η αυξανόμενη χρήση του διαδικτυακού τρόπου επικοινωνίας ιδιαίτερα κατά τις νεαρές ηλικίες, έχει μεταλλάξει το είδος της εκπαίδευσης που δέχονται οι ανήλικοι και γενικότερα το είδος της πληροφορίας που προσλαμβάνουν. Η ονομασία τους ήδη από το 2001 ως «ψηφιακοί αυτόχθονες» (Davies and Eynon, 2018), (Τσαλική, 2013) προμήνυε την εξέλιξη της νέας γενιάς στη διαχείριση της πληροφορίας. Η ραγδαία αυτή αύξηση χρήσης της τεχνολογίας κατά την επίτευξη και διάδοση της πληροφορίας, με τις αλλαγές που επιφέρει αυτή στην καθημερινή ζωή των εφήβων, κατέδειξε ένα νέο πεδίο δράσης και ανάπτυξης νέων μορφών εγκληματικότητας. Η αναγκαιότητα διαφύλαξης της ανηλικότητας και η προστασία των ανηλίκων χρηστών από κακόβουλες επιθέσεις, εγείρεται ως μείζουσα θεματική. Ειδικότερα η αναγκαιότητα προστασίας των δικαιωμάτων των παιδιών και η διαφύλαξης της ανηλικότητας τους, ορίζεται ρητά στη Σύμβαση του Ο.Η.Ε. για τα δικαιώματα του παιδιού 20/11/89, όπως κυρώθηκε με το Νόμο 243 του 1990. Χαρακτηριστικά αναφέρεται ότι το δικαίωμα των παιδιών στην ιδιωτικότητα, ορίζοντας ότι: «Κανένα παιδί δεν μπορεί να αποτελέσει αντικείμενο αυθαίρετης ή παράνομης επέμβασης στην ιδιωτική του ζωή, στην οικογένεια του, στην κατοικία του ή στην αλληλογραφία του, ούτε παράνομων προσβολών της τιμής και της υπόληψής του» (άρθρο 16).

Η αρχή της μη διάκρισης (άρθρο 2). Όλα τα παιδιά είναι ίσα. Έχουν δικαίωμα να τα αντιμετωπίζουν χωρίς διακρίσεις λόγω της φυλής, του φύλου, της γλώσσας, της θρησκείας, των απόψεων, της περιουσίας, της κατάστασης, των ιδιαίτερων αναγκών ή της εμφάνισής τους.

Η ρήτρα του συμφέροντος του παιδιού (άρθρο 3). Όταν οι μεγάλοι παίρνουν αποφάσεις που αφορούν τα παιδιά, πρέπει να υπολογίζουν πριν από όλα το συμφέρον των παιδιών. Η Πολιτεία πρέπει να προστατεύει και να φροντίζει τα παιδιά, αν οι γονείς τους δεν μπορούν να το κάνουν.

Το δικαίωμα στη ζωή (άρθρο 6) Τα παιδιά έχουν δικαίωμα στη ζωή, την επιβίωση και την ανάπτυξη.

Ελευθερία γνώμης (άρθρο 12). Τα παιδιά έχουν δικαίωμα να εκφράζουν ελεύθερα τις απόψεις τους.

Οι μεγάλοι πρέπει να ακούν και να παίρνουν σοβαρά υπόψη τους τη γνώμη των παιδιών για θέματα που τα αφορούν, ανάλογα με την ηλικία και την ωριμότητά τους. Πληροφόρηση (άρθρο 17). Τα παιδιά έχουν δικαίωμα να μαθαίνουν τι συμβαίνει γύρω τους από τα μέσα ενημέρωσης (εφημερίδες, ραδιόφωνο, τηλεόραση, ηλεκτρονικά μέσα). Η

Πολιτεία πρέπει να ενθαρρύνει τα μέσα να διαδίδουν χρήσιμες πληροφορίες και να προστατεύουν τα παιδιά από ότι μπορεί να τα βλάψει¹⁷.

Περαιτέρω οι βασικές αρχές που διέπουν την προστασία προσωπικών δεδομένων των παιδιών μπορούν να συνοψιστούν ως κάτωθι:

Το μείζον συμφέρον του παιδιού, η προστασία και φροντίδα για την ευημερία των παιδιών, το δικαίωμα στην ιδιωτική ζωή (*Νόμος που κυρώνει τη σύμβαση για τα δικαιώματα του παιδιού*, 1990, κεφ. 16).

Αντιπροσώπευση: Το δικαίωμα αυτό, όπως προβλέπεται στο άρθρο 1510 Αστικού Κώδικα, περιλαμβάνει, μεταξύ άλλων, την εκπροσώπηση του ανηλίκου σε κάθε υπόθεση ή δικαιοπραξία, που αφορούν το πρόσωπό του ή την περιουσία του.

Σύγκρουση του μείζονος συμφέροντος του παιδιού με το δικαίωμα στη προστασία δεδομένων.

Προσαρμογή στο βαθμό ωριμότητας του παιδιού.

Δικαίωμα συμμετοχής (Ομάδα Εργασίας του άρθρου 29 για την προστασία των δεδομένων, 2014) - Γνωμοδότηση 2/2009 για την προστασία προσωπικών δεδομένων παιδιών (WP 160).

Σε διεθνή κλίμακα, η προστασία των δικαιωμάτων των παιδιών και η κατοχύρωση τους σε περιπτώσεις παραβίασης αυτών, προβλέπεται από τις νομοθετικές πράξεις των κρατών όπως αυτές εναρμονίζουν τη νομοθεσία τους βάση Οδηγιών της Ε.Ε. αλλά και βάσει της αγοράς και πρωτοβουλιών αυτορρύθμισης. Παράδειγμα πρωτοβουλιών αυτορρύθμισης συναντώνται στην Αμερική, όπου η Ομοσπονδιακή Επιτροπή Εμπορίου (FTC) προβλέπει συγκεκριμένες μεθόδους εξακρίβωσης ηλικίας και εξασφάλισης της γονικής συγκατάθεσης, σε περιπτώσεις που προσωπικά δεδομένα παιδιών πρόκειται να κοινοποιηθούν σε τρίτους. Η σαφήνεια των νομοθετημάτων και οι επαπειλούμενες ποινές, υπαγορεύουν και αποτρέπουν την κάθε παραβίαση από κακόβουλο χρήστη-πάροχο. Ειδικότερα για την εξασφάλιση της ενηλικότητας του χρήστη, η οποία αποτελεί υποχρέωση του παρόχου, έχουν θεσμοθετηθεί συγκεκριμένες μέθοδοι, από τις οποίες κατά κανόνα επιλέγονται εκείνες που εξυπηρετούν καλύτερα τους παρόχους-διαχειριστές των πληροφοριών των χρηστών. Ενδεικτικά αναφέρονται:

- Εκτύπωση και υπογραφή του ασκούντος τη γονική μέριμνα εντύπου, το οποίο διατίθεται μέσω του ιστότοπου.
- Χρήση πιστωτικής ή χρεωστικής κάρτας του ασκούντος τη γονική μέριμνα

¹⁷<http://www.0-18.gr/paidikiprostasia/paidikiprostasia>(Ημερομηνία πρόσβασης: 02-09-2019).

- Χρήση ταυτότητας
- Επικοινωνία του ασκούντος τη γονική μέριμνα με υπεύθυνο του παρόχου των υπηρεσιών μέσω τηλεφωνικού κέντρου.
- Επικοινωνία του ασκούντος τη γονική μέριμνα με υπεύθυνο του παρόχου των υπηρεσιών μέσω τηλεδιάσκεψης-βιντεοκλήσης κλπ. (Macenaite and Kosta, 2017)

Ένας από τους πλέον διαδεδομένους τρόπους ταυτοποίησης της ανηλικότητας, ιδιαίτερα όταν ο πάροχος συλλέγει προσωπικά δεδομένα του παιδιού μόνο για εσωτερικούς σκοπούς, είναι η μέθοδος της κινητής κλίμακας. Κατά τη διαδικασία αυτή αποστέλλεται μήνυμα ηλεκτρονικό ταχυδρομείου στο γονέα και ο πάροχος εξασφαλίζει την γονική συγκατάθεση για τη χρήση στοιχείων του ανηλίκου ή αντίστοιχα εξακριβώνει την ενηλικότητα του χρήστη.

Η διαδικασία αυτή προτιμάται από τους περισσότερους παρόχους υπηρεσιών της κοινωνίας της πληροφορίας, ως η λιγότερο κοστοβόρα μέθοδος, η πλέον γρήγορη, ενώ παράλληλα βοηθά τους γονείς να γίνονται ενήμεροι και να συμμετέχουν στη διαδικτυακή δραστηριότητα των παιδιών τους. Στην περίπτωση που ο πάροχος θελήσει να συλλέξει επιπλέον δεδομένα να τα μεταβιβάσει ή κοινοποιήσει σε τρίτον, επιβάλλεται η περαιτέρω επικύρωση των στοιχείων ταυτότητας με υποβολή γραπτού εντύπου, ή μέσω τηλεδιάσκεψης-βιντεοσυνομιλία κλπ, με τρόπο ικανό να πιστοποιήσει την ενηλικότητα του χρήστη (Κελάλη, 2018, σ.87), (Macenaite and Kosta, 2017). Ως ένα από τα μειονεκτήματα της χρήσης της εν λόγω μεθόδου, είναι ότι μπορεί εύκολα να παρακαμφθεί με τη χρήση ψευδών στοιχείων ή ακόμη η αυτοταυτοποίηση δεν συνεπάγεται την ενηλικότητα ή την γονική συγκατάθεση στις περιπτώσεις ανηλίκων χρηστών. Παράλληλα η ψευδής καταγραφή της ηλικίας των παιδιών, τα εξοικειώνει στη μη συμμόρφωση με τους κανόνες που θέτονται και τα ωθεί να βρίσκουν λύσεις για τους παρακάμπουν (John Carr, 2015).

Στο άρθρο 8 του Γενικού Κανονισμού για την Προστασία Δεδομένων, αναφέρονται οι προϋποθέσεις που ισχύουν για τη συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών και ειδικότερα στην παρ. 2 αυτού ορίζεται ρητά ότι: *«Ο υπεύθυνος επεξεργασίας καταβάλλει εύλογες προσπάθειες για να επαληθεύσει στις περιπτώσεις αυτές ότι η συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία»*.

Πέραν των ανωτέρω, το πλέγμα των ανά περίπτωση ζητημάτων που καλείται να λύσει ο εκάστοτε πάροχος απαιτεί συντονισμένη και ενιαία αντιμετώπιση για την άντληση της πληροφορίας με τον ασφαλέστερο τρόπο, τόσο για την επιχείρηση, όσο και για τον χρήστη. Η εγκατάσταση κωδίκων μεθοδολογίας για τους παρόχους της σε περιπτώσεις παραβίασης των

κανόνων χρήσης, θα μπορούσε να αποτελέσει την ενιαία βάση αντιμετώπισης της εν λόγω δυσλειτουργίας, με τη συλλογή των απολύτως απαραίτητων προσωπικών δεδομένων, κατόπιν μηχανισμών ενημέρωσης των δεδομένων που συλλέγονται και αποθηκεύονται.

Τα ερωτήματα που εγείρονται συνίστανται ως προς τις μεθόδους εξασφάλισης της επαληθεύσιμης συγκατάθεσης, την αναζήτηση αυτής καθώς και ειδικότερα ζητήματα που ανακύπτουν ως προς την άπαξ άντληση της συγκατάθεσης καθώς και αν υφίσταται ανάγκη επαλήθευσης ανά τακτά χρονικά διαστήματα. Επίσης προβληματισμός εγείρεται στις περιπτώσεις που ο πάροχος αναζητά πληροφορίες για ανήλικο χρήστη και ειδικότερα η αμφιλεγόμενη συλλογιστική ως προς την απαίτηση στη γονική συγκατάθεση, υπό το δικαίωμα συμμετοχής του ανηλίκου και τον περιορισμό των προσωπικών του ελευθεριών στο μέτρο που επιτρέπει την έκφραση της ελεύθερης βούλησης του (Κελάλη, 2018, σ.74).

Η Πράξη του 1998 για την προστασία της ιδιωτικότητας των παιδιών στο διαδίκτυο¹⁸, στρέφεται προς δυο κατευθύνσεις:

- Την προστασία της ιδιωτικότητας σε παιδιά κάτω των 13 ετών
- Την ενεργό συμμετοχή των γονιών
- Ως δεδομένα προσωπικού χαρακτήρα εννοείται κάθε πληροφορία που μπορεί να οδηγήσει σε ταυτοποίηση όπως: όνομα και όνομα χρήστη, όπως περιέχεται σε αναγνωριστικά cookies
- Ταχυδρομική διεύθυνση
- Πληροφορίες ηλεκτρονικής επικοινωνίας
- Αριθμός τηλεφώνου
- Αριθμός κοινωνικής ασφάλειας
- Διεύθυνση IP Internet Protocol
- Φωτογραφίες, βίντεο, ακουστικά αρχεία, που περιέχουν τη φωνή του παιδιού
- Πληροφορίες γεωεντοπισμού για να ταυτοποιηθεί η οδός και η πόλη

Πληροφορίες για το παιδί ή τους γονείς του που ο πάροχος συλλέγει ηλεκτρονικά και συνδυάζει με κωδικούς αναγνώρισης (Children's online privacy protection act of 1998 (COPPA) 15 U.S.C. §§6501-6506 όπως τροπ. το 2002)¹⁹, (Federal Trade Commission, 2002).

Η ελεγχόμενη και σαφής αναφορά στα στοιχεία που αναζητούνται ως τα απαραίτητα αναγνωστικά ταυτοποίησης, συσχετίζονται με τα στοιχεία που παρατύπως αντλούνται και αποτελούν τη βάση για προσβολή της προσωπικής ελευθερίας των χρηστών κατά την

¹⁸Children's online privacy protection act of 1998 (COPPA).

¹⁹<https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>(Ημερομηνία πρόσβασης: 05-09-2019).

διακίνηση, αποθήκευση και άντληση της πληροφορίας με την χρήση τεχνολογικών μέσων. Κρίνεται σκόπιμο να επισημανθεί ότι οι διαδικασίες αυτοματοποίησης και άντλησης των προσωπικών δεδομένων, τόσο ενηλίκων αλλά κυρίως ανηλίκων, αφορούν στις περιπτώσεις ηλεκτρονικής διακίνησης των προσωπικών δεδομένων τους, όπου η αυτοπρόσωπη και ενυπόγραφη λήψη συγκατάθεσης τους, δεν συναντάται.

Χαρακτηριστικό παράδειγμα διαχείρισης των προσωπικών δεδομένων ανηλίκων είναι η τακτική που ακολουθείται από παρόχους στις εταιρείες με χρήστες κατά βάση ανηλίκους, όπως η Disney.com, που προσφέρει περιεχόμενο φιλικό προς όλη την οικογένεια. Συγκεκριμένα η Disney.com δεν επιτρέπει σε χρήστες κάτω των 13 ετών να γραφούν συνδρομητές σε newsletters or emails, αποφεύγοντας με τον τρόπο αυτό η υποχρέωση αναζήτησης γονικής συναίνεσης, ακόμη και αν αυτό συνεπάγεται τη μείωση της επισκεψιμότητας στην ιστοσελίδα του συγκεκριμένου παρόχου.

Άλλοι πάροχοι επιλέγουν να ακολουθήσουν μια περιορισμένης χρήσης Πολιτική Απορρήτου με βάση την οποία γνωστοποιούνται τα στοιχεία που συλλέγονται κατά τη χρήση των υπηρεσιών του παρόχου, σε μια προσπάθεια να ελαχιστοποιήσουν τα προσωπικά δεδομένα που συλλέγουν από παιδιά και προκειμένου να μειώσουν την έκθεσή τους σε αστική ή άλλη ευθύνη υπό την COPPA. Για παράδειγμα, το Cartoon Network,²⁰ ένα δημοφιλές κανάλι στις ΗΠΑ, συλλέγει διευθύνσεις ηλεκτρονικού ταχυδρομείου μόνο προς επιβεβαίωση της δημιουργίας λογαριασμού και κατόπιν αποθηκεύει σε προστατευμένη μορφή με μοναδικό σκοπό την ανάκτηση του κωδικού πρόσβασης από τον χρήστη. Επιπλέον επιστούν την προσοχή στους χρήστες θέτοντας με σαφήνεια τις διαδικασίες που ακολουθούνται σε περίπτωση καταγραφής των προσωπικών δεδομένων των ενηλίκων αλλά και των ανηλίκων, παρέχοντας μια διαδικτυακή πύλη υποβολής αιτημάτων παραπόνων-διαπιστώσεων, προβλέποντας ειδικότερα την υπαγωγή στο Νόμο περί απορρήτου καταναλωτών της Καλιφόρνια για επιχειρήσεις και χρήστες εταιριών που εδρεύουν και δραστηριοποιούνται στην εν λόγω περιοχή.

Η Nintendo²¹ στη σελίδα των ενημερωτικών ερωτημάτων αναφέρει ρητά ότι οι παρεχόμενες της Υπηρεσίες δεν προσφέρονται σε χρήστες κάτω των 13 ετών, χωρίς τη συγκατάθεση του γονέα, με τη χρήση του λογαριασμού του ηλεκτρονικού ταχυδρομείου. Σε κάθε περίπτωση η δημιουργία του λογαριασμού στον εν λόγω πάροχο (Nintendo Network

²⁰<https://www.cartoonnetwork.com/legal/privacy.html>(Ημερομηνία πρόσβασης: 06-09-2019).

²¹<https://www.nintendo.com.au/help/account-registration>(Ημερομηνία πρόσβασης: 02-09-2019).

ID), συνδέεται με το λογαριασμό στο Facebook, Twitter, Google ή Apple, για τους οποίους είναι απαραίτητη η ηλικία χρήστη άνω των 13 ετών. Η σύνδεση του εν λόγω παρόχου με το προφίλ ενηλικιότητας ή μη του χρήστη σε δημοφιλείς εφαρμογές, καταδεικνύει την ανάγκη για ενιαία βάση και θεώρηση της αξιοπιστίας των δεδομένων που παρέχονται από το χρήστη, ιδίως στις περιπτώσεις εξακρίβωσης της ηλικίας του. Στην πράξη, οι περισσότεροι πάροχοι υπηρεσιών κοινωνίας της πληροφορίας έχουν εφαρμόσει ένα σύστημα αυτό-επιβεβαίωσης ηλικίας, απαιτώντας από τους χρήστες να εισάγουν την ημερομηνία γέννησης και κατά την τρέχουσα πρακτική, επιλέγουν να συνδέσουν το χρήστη με υπάρχον προφίλ σε δημοφιλείς εφαρμογές στις οποίες να ελέγχεται παράλληλα η ενηλικιότητα του χρήστη. Για παράδειγμα στην περίπτωση που ο χρήστης είναι κάτω των 13 ετών απαγορεύεται η δημιουργία λογαριασμού στο Facebook (Κελάλη, 2018, σ. 88–89) και έτσι αποκλείεται η χρήση και των συνδεδεμένων με το προφίλ αυτό, εφαρμογών και ιστοσελίδων.

Οι κατευθυντήριες αυτές, ως αποτυπώνονται στις νομοθετικές πράξεις του κάθε κράτους υπαγορεύουν το πλαίσιο λειτουργίας του παρόχου, ωστόσο προβληματισμοί εγείρονται ως την πρακτικοποίηση της μεθόδου εξακρίβωσης της ανηλικότητας, εντοπίζοντας τα σημεία που υφίστανται διαδικαστικές ανωμαλίες. Ειδικότερα ως προαναφέρθηκε, ο κάθε πάροχος επιλέγει την τακτική εξακρίβωσης της ηλικίας στο διαδίκτυο που επιθυμεί να ακολουθήσει με προσωπική του ευθύνη. Η κάθε μέθοδος που επιλέγεται, δεν εξασφαλίζει εκ προοιμίου τη διαχείριση των περιπτώσεων σε ενιαία βάση. Η αυτό-ταυτοποίηση παρακάμπτεται, καθώς δεν μπορεί να εξακριβωθεί η ενηλικιότητα του χρήστη-αποστολέα του μηνύματος. Ωστόσο η χρυσή τομή μεταξύ της ανάγκης διατήρησης της ανωνυμίας του χρήστη και του δικαιώματος του αυτό, υπό το πρίσμα της ελευθερίας έκφρασης της ιδιωτικότητας του δεν έχει ακόμη βρεθεί, καθώς η χρήση των υπηρεσιών αυτών απαιτεί κατά κανόνα την παροχή προσωπικών δεδομένων των χρηστών και αποτελεί τρόπο έκφρασης και κοινωνικότητας, ανεξαρτήτου ηλικίας (Παναγοπούλου-Κουτνατζή, 2010, σ.27 επ.), (Εφημερίδα της Ευρωπαϊκής Ένωσης, 2007), (Τυπογραφείο, 2019).

ΚΕΦΑΛΑΙΟ 3 ΜΕΣΑ ΨΗΦΙΑΚΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

3.1 Η χρήση του διαδικτύου στη σύγχρονη εποχή-To web 2.0.

Το web 2.0. υφίσταται και υποστηρίζει τις δραστηριότητες των χρηστών του διαδικτύου βασιζόμενο στη δημιουργία περιεχομένου, μέσω διαμοιρασμού και συνεργασίας. Η χρήση υπερσυνδέσμων (hyperlinking), αποτελεί τη βάση του web 2.0. Οι χρήστες μπορούν να προσθέσουν νέο περιεχόμενο, να εμφανίσουν νέους συσχετισμούς, αναπτύσσοντας τη διακλάδωση του διαδικτύου και επεκτείνοντας την πληροφορία, οδηγώντας με τον τρόπο αυτό και άλλους χρήστες στην οργανική ανάπτυξη του δικτύου (O'Reilly, Tim and Battelle, 2009). Το πλεονέκτημα της εξατομίκευσης της πληροφορίας που παρέχεται από το χρήστη και αξιοποιείται από το δίκτυο αποτελεί τη βάση της τεχνητής νοημοσύνης (Shanker, 2019), με τη χρήση αλγορίθμων διαχείρισης της πληροφορίας, καθώς και με τον τρόπο που η εξέλιξη αυτή αλληλεπιδρά στις κοινωνικές και νοητικές λειτουργίες του ατόμου.

Το Yahoo, το Google's breakthrough in search, eBay, Amazon είναι ενδεικτικά παραδείγματα χρήσης του web 2.0, το οποίο ανταποκρίνεται με τον καλύτερο δυνατό τρόπο στις απαιτήσεις των χρηστών. Παρέχεται αμεσότητα στην αναζήτηση της πληροφορίας, ανταποκρίνεται στις επιθυμίες των χρηστών, προσφέροντας υπηρεσίες αγοράς-πώλησης αρκετά ελκυστικές, διαφημίζοντας παράλληλα το περιεχόμενο τους από τους ίδιους τους χρήστες και μέσω των κριτικών τους. Οι εφαρμογές ανοιχτής πρόσβασης παρέχονται φαινομενικά δωρεάν στο χρήστη, ωστόσο έχουν καθιερώσει τη λογική της "διαδικτυακής αγοράς". Η διαδικτυακή αγορά παρέχει πληθώρα των προϊόντων υλικών ή άυλων, καλύπτοντας το καταναλωτικό κενό των χρηστών τους. Επιπλέον το web 2.0. καινοτομεί, παρέχοντας τη βασική διαδικτυακή εγκυκλοπαίδεια στον χρήστη. Μέσω της εφαρμογής αυτής παρέχεται στο χρήστη η ευχέρεια να διορθώσει, να προσθέσει και ουσιαστικά να τροποποιήσει το περιεχόμενο της εγκυκλοπαίδειας, που είναι διαθέσιμο στους λοιπούς διαδικτυακούς επισκέπτες, ενισχύοντας έτσι την έννοια της διαδραστικότητας. Επίσης ιστοσελίδες, όπως το del.icio.us και το Flickr, όπου μπορεί καθένας να μοιραστεί τον κατάλογο των διευθύνσεων που έχει επισκεφτεί (bookmarks), αλλά και τις φωτογραφίες του, με την αντίστοιχη ετικέτα (tag), έχουν συμβάλει αποφασιστικά στην αναδιαμόρφωση του διαδικτυακού τοπίου. Το "tagging", όπως έχει καθιερωθεί στη γλώσσα του διαδικτύου, η θέση δηλαδή επισήμανσης στις αναζητήσεις του χρήστη, κατηγοριοποιεί τις πληροφορίες αναζήτησης του χρήστη, με στόχο την ελαχιστοποίηση του χρόνου αναζήτησης και επίτευξης

του επιθυμητού αποτελέσματος, το οποίο δεν είναι άλλο από την πρόσβαση στην πληροφορία (Thomas and Hoofnagle, 2011).

Όλα τα ανωτέρω, ως βασικές λειτουργίες του web 2.0, έχουν οδηγήσει τους χρήστες σε μια διαδικτυακή πραγματικότητα εξυπηρέτησης των αναγκών τους, αλλά και τις κρατικές υπηρεσίες στην διαδικτυακή εξυπηρέτηση των πολιτών, δημιουργώντας τον ψηφιακό πολίτη (e-citizen) (RodríguezBolívar, 2017). Η ενημέρωση των πολιτών γίνεται σε αρκετές των περιπτώσεων αποκλειστικά διαδικτυακά, με τους διαύλους επικοινωνίας και δημοσιογραφικής κάλυψης να διαφοροποιούνται από τους παραδοσιακές μορφές δημοσιογραφίας και πληροφόρησης. Η γνώση και η ενημέρωση των χρηστών παρέχεται από πληθώρα πηγών δημοσιογραφικών ή μη, με τη χρήση των μέσων κοινωνικής δικτύωσης ή blog. Έτσι ο οποιοσδήποτε έλεγχος που θα μπορούσε να ασκηθεί από επίσημες μεθόδους ελέγχου της πληροφόρησης, έχει ανατραπεί, με το διαδίκτυο να έχει δημιουργήσει ένα καινούργιο δυναμικό κοινό, που ζητά και του παρέχονται αντίστοιχα διαφημιζόμενες πληροφορίες (Pearson, 2013, σ. 220).

Επιπροσθέτως η διεθνής πολιτική πραγματικότητα έχει εισάγει την πολιτική παρακολούθησης λογαριασμών με την εφαρμογή των αντιτρομοκρατικών νόμων μέσω cloud και των λογαριασμών διακίνησης της πληροφόρησης με την καταγραφή και παρακολούθηση των συνομιλιών των πολιτών (Pearson, 2013, σ. 221). Βέβαια αξίζει να σημειωθεί ότι στην Ελλάδα το ισχύον νομοθετικό πλαίσιο εντός της Ευρωπαϊκής Ένωσης. η πρόσβαση σε κάθε πληροφορία ή στοιχείο του τηλεπικοινωνιακού απορρήτου, ως ορίζεται στις αρχικές διατάξεις και στις τροποποιήσεις του Ν. 2225/1994, η άρση του απορρήτου και την καταγραφή τηλεφωνικών ή άλλων συνομιλιών πολιτών επιτρέπεται σε κακουργηματικού χαρακτήρα πράξεις κατόπιν αιτιολογημένης διάταξης του Εισαγγελέα Εφετών-βουλεύματος, σε περιοριστικά αναφερόμενες περιπτώσεις αδικημάτων, γεγονός που φανερώνει την προστατευτική διάθεση του νομοθέτη (Ν. 2225/1994 όπως τροπ., 2016).

3.2 Η χρήση των προσωπικών δεδομένων-διαδικτυακής πληροφορίας υπό το πρίσμα των ατομικών ελευθεριών.

Η διαχείριση και αποθήκευση ατομικών δεδομένων ταυτότητας, κατοικίας, σε πλατφόρμες και μέσα κοινωνικής δικτύωσης, αποτελεί έναν τρόπο μη παραδοσιακό άντλησης δεδομένων. Η έλλειψη των πληροφοριών σχετικά με τους ιδιόκτητες αλγορίθμων που χρησιμοποιούν οι εταιρείες κοινωνικών μέσων για την επεξεργασία προσωπικών δεδομένων και η ταξινόμηση των χρηστών με βάση τη συμπεριφορά τους, μπορεί να οδηγήσουν τον

ερευνητή σε αποκλίσεις, οι οποίες αν προβλεφθούν μπορούν να παρακαμφτούν με τις αντίστοιχες μεταβλητές. Η αξιοπιστία των αυτοαναφερόμενων πληροφοριών σχετικά με τα κοινωνικά μέσα είναι επίσης αμφισβητήσιμη (Παναγοπούλου-Κουτνατζή, 2013).

Στο χώρο των κοινωνικών δικτύων, η ατομική δήλωση στο προφίλ του χρήστη δεν επιδέχεται δικλείδες ασφαλείας και πιστοποιητικά αυθεντικότητας. Η απουσία ταυτοποίησης περιορίζεται στην αυτοταυτοποίηση χωρίς έλεγχο πληρότητας ή πλαστότητας των δεδομένων, που αποθηκεύονται για ένα άτομο και λαμβάνοντας υπόψη ότι ένα μεγάλο ποσοστό των χρηστών έχουν ψεύτικους λογαριασμούς ή ανενεργούς εσκεμμένα ή ακόμη και λόγω θανάτου τους. Το Facebook έχει υπολογίσει ότι το τέταρτο τρίμηνο του 2018, οι ψεύτικοι λογαριασμοί και οι διπλοί λογαριασμοί αποτελούσαν περίπου το 5% και το 11% των μηνιαίων ενεργών χρηστών παγκοσμίως αντίστοιχα (States, United Commission, 2015).

Η χρήση δεδομένων προερχόμενα από τα μέσα κοινωνικής δικτύωσης, δημιουργεί εύλογη ανησυχία για την προστασία της ιδιωτικής ζωής του ατόμου, υπό το πρίσμα της δεοντολογικής χρήσης τους. Για παράδειγμα, τα διαθέσιμα δεδομένα θέσης από τα μέσα κοινωνικής δικτύωσης, ακόμη και σε συγκεντρωτική μορφή, μπορούν να χρησιμοποιηθούν για την παρακολούθηση των κινήσεων ευάλωτων ομάδων, όπως εκτοπισθέντων ατόμων, προερχόμενα τόσο από ανθρωπιστικές οργανώσεις, όσο και από εγκληματικές οργανώσεις. Επίσης, τα δεδομένα αυτά μπορούν να χρησιμοποιηθούν για την παρακολούθηση των συμπεριφορών των χρηστών, με τρόπους που θα μπορούσαν να επηρεάσουν και να προσβάλλουν τις πολιτικές τους ελευθερίες. Από την άλλη πλευρά, υπό το φως της έντονης επαγρύπνησης των κοινωνιών για την προστασία των ευάλωτων πληθυσμιακών ομάδων, από την μαζική διασπορά του κορονοϊού, καθώς και με γνώμονα τη διασφάλιση και αποφυγή οικονομικής κατάρρευσης των κοινωνιών, χρησιμοποιούνται εφαρμογές που εντοπίζουν τη κίνηση και θερμοκρασία του ανθρώπινου σώματος, ιδίως όταν αυτή υπερβαίνει το όριο που χαρακτηρίζει το άτομο ως φορέα covid-19. Οι κοινωνίες της Κίνας, έχουν δώσει το εναρκτήριο λάκτισμα για τη χρήση των εφαρμογών επιτήρησης ατόμων που έχουν χαρακτηριστεί ως ύποπτα ή επιβεβαιωμένα κρούσματα και επιβάλλεται να παραμένουν εντός της οικίας τους, χωρίς αυτό να αποκλείει τη χρήση τους και από άλλες χώρες, παρακάμπτοντας τους όποιους ενδοιασμούς για την προστασία των προσωπικών δεδομένων των πολιτών τους (Dukakis, 2020), (COVID-19 effect: China now shows delivery person's body temperature on the app, 2020), (Murdock, 2020).

Ωστόσο σε κάθε περίπτωση, η ανάλυση των δεδομένων των μέσων κοινωνικής δικτύωσης, θέτει σοβαρά ζητήματα προστασίας δεδομένων, λαμβάνοντας υπόψη ότι οι

χρήστες δεν συνειδητοποιούν τι είδους στοιχεία συλλέγουν, επεξεργάζονται και μοιράζονται με τις εταιρείες αυτές αλλά και με τρίτους, κατά τη ροή της αλυσιδωτής διακίνησης της πληροφορίας (Spyratos, Spyridon, Yildiz *et al.*, 2019), (Pariser, 2011, σ. 195–199). Η αμφιλεγόμενη τακτική των κοινωνιών παρακάμπτει, στην εν λόγω περίπτωση τις προσωπικές ελευθερίες μιας ομάδας ή μεμονωμένων πολιτών, προκειμένου να προστατεύσει το σύνολο του πληθυσμού από αμελείς και μη συνεργάσιμους φορείς του κορονοϊού. Η προβληματική είναι εμφανής, όπως και το κέρδος από την καταπάτηση των προσωπικών δεδομένων του ατόμου υπέρ του κοινωνικού συνόλου, το οποίο κατά γενική ομολογία είναι αμφισβητήσιμο.

Υπό τη θεωρητική αυτή βάση, η χρήση της τεχνολογίας των έξυπνων συσκευών, έχει ως στόχο να εξυπηρετήσει τις ανάγκες του χρήστη και να εξατομικεύσει τις παρεχόμενες σε αυτόν υπηρεσίες. Η χρήση και αξιοποίηση των προσωπικών δεδομένων του ατόμου, έχει ένα στόχο-την παροχή εξατομικευμένων υπηρεσιών, ανά σκευή χρήσης. Η έννοια της εξατομικεύσης μέσω τεχνητών έξυπνων τεχνικών έχει εφαρμοστεί σε διάφορους τομείς, ειδικά όταν ο στόχος είναι η ενίσχυση μιας υπηρεσίας ή ενός προϊόντος που ταιριάζει απόλυτα στις αντίστοιχες απαιτήσεις ενός ανθρώπινου χρήστη (Rouse, 2020). Οι συσκευές αυτές λειτουργούν σε ένα πλήρως αυτοματοποιημένο περιβάλλον, αξιολογούν τις συνθήκες, αλληλεπιδρούν με άλλες συσκευές, εκτελούν λειτουργίες διαχείρισης και μετάδοσης δεδομένων. Η χρήση εφαρμογών και συσκευών, της αναδυόμενης αυτής τεχνολογίας, ως αποκαλείται Ambient Intelligence (AmI) μπορεί να οριστεί ως εξής: «Η περιβαλλοντική νοημοσύνη (AmI) είναι το στοιχείο ενός διεισδυτικού περιβάλλοντος υπολογιστών που του επιτρέπει να αλληλεπιδρά και να ανταποκρίνεται κατάλληλα στους ανθρώπους και τις ανάγκες τους στο περιβάλλον αυτό²²», (Bylykbashi *et al.*, 2018), (Brown, 2019).

3.3 Επεξεργασία και αποθήκευση δεδομένων.

Οι περισσότερες περιπτώσεις απειλών μέσω διαδικτύου²³, έχουν ως βάση τη δυνατότητα, που παρέχουν οι μηχανές αναζήτησης, με τη χρήση cookies, παροχής προσωποποιημένων πληροφοριών στους χρήστες. Η καταγραφή και αποθήκευση δεδομένων στο ιστορικό αναζήτησης, οδηγεί σε πληροφορίες, οι οποίες ενώ αρχικά χρησιμοποιήθηκαν με στόχο την εξυπηρέτηση του χρήστη, εξοικονομώντας χρόνο, στη συνέχεια αποθηκεύοντας

²²<https://searchenterpriseai.techtarget.com/definition/ambient-intelligence-AmI> (Ημερομηνία πρόσβασης: 02-09-2020).

²³e-theft, e-fraud, identity theft

τις προτιμήσεις του, αξιοποιήθηκαν από εταιρείες για εμπορικούς σκοπούς (Palmer, 2001), (Krafft, Gamer and Zweig, 2019). Η εκτίμηση για την πιθανότητα αγοράς ενός προϊόντος ή μιας υπηρεσίας με βάση τα ενδιαφέροντα του χρήστη, ενδιαφέρει την κάθε εταιρεία. Η δημιουργία ενός καταναλωτικού προφίλ χρήστη αποτελεί καινοτόμο δυνατότητα του web 2.0 και έχει ως στόχο αυτή ακριβώς την κατηγοριοποίηση των δεδομένων (Dutton and Graham, 2014). Στη συνέχεια η συλλογή και επεξεργασία των προσωπικών δεδομένων κίνησε το ενδιαφέρον κακόβουλων χρηστών, προς άντληση τυχόν ευαίσθητων προσωπικών δεδομένων άλλων χρηστών ως στόχοι κυβερνο-επιθέσεων. Η αποθήκευση αλλά και η επεξεργασία των δεδομένων προσωπικού χαρακτήρα ξεκίνησε ως προτέρημα του διαδικτύου και έχει εξελιχθεί σε έναν τρόπο καταγραφής των διαδικτυακών κινήσεων του ατόμου. Η ιδιωτικότητα της αναζήτησης μέσω διαδικτύου είναι πλέον παρελθόν. Με τη μεθοδική καθοδήγηση δημιουργίας προφίλ χρήστη για την είσοδο στο λογαριασμό της Google και τη χρήση των εφαρμογών της, όπως Google drive, ή Google maps, με αντίστοιχο έλεγχο της τοποθεσίας του χρήστη κατά την είσοδο στην εφαρμογή, ουσιαστικά χρησιμοποιείται η υπηρεσία με κόστος, την παροχή των προσωπικών δεδομένων του κάθε χρήστη της (Pariser, 2011), (Bujlowetal., 2017).

3.4 Απειλές σε περιβάλλον ιστού.

Οι βασικές απειλές που συναντώνται σε περιβάλλον ιστού μπορούν να συγκεντρωθούν στην παρακάτω κατηγοριοποίηση, όπως αυτή έχει διαμορφωθεί από τις επικρατούσες συνθήκες της παγκόσμιας πραγματικότητας κατά τη χρήση του διαδικτύου (Smith *et al.*, 2019, σ. 45):

Botnet	A Botnet infection occurs when a hacker transmits instructions to other computers for the purpose of controlling them, and then using them for various purposes such as spam distribution or phishing
Computer virus	A computer virus is a computer program that piggybacks or attaches itself to application programs or other executable system software; the virus subsequently activates, sometimes causing severe damage to computer systems or files
Cyberterrorism	Cyber terrorism occurs when terrorists cause virtual destruction in online computer systems
E-fraud	E-fraud is the use of online techniques by a perpetrator to commit fraud. Popular forms of e-fraud include spoofing, phishing, and online credit card fraud
E- theft	E- theft occurs when a perpetrator hacks into a financial institution, e.g. a bank and diverts funds to accounts accessible to the criminal. To prevent e-theft, most major banks severely limit what clients can do online
Hacking	Hacking occurs when a perpetrator gains unauthorized access to data on a computer system
Online credit card fraud	Online credit card fraud is illegal online acquisition of a credit card number and use of it for unauthorized purposes such as fraudulent purchases
Phishing	Phishing occurs when the perpetrator sends fictitious emails to individuals with links to fraudulent websites that appear official and thereby cause the victim to release personal information to the perpetrator
Software piracy	Software piracy is the theft of intellectual assets associated with computer programs
Spam	Spam refers to unsolicited email; spam is illegal if it violates the Can-Spam Act of 2003, such as by not giving recipients an opt-out method

Spoofing	Spoofing is use of email to trick an individual into providing personal information that is later used for unauthorized purposes
----------	--

3.5 Κοινωνικά Δίκτυα-Social media

Η πλειονότητα του πληθυσμού παγκοσμίως, έχει εντάξει τη χρήση των διαδικτυακών μέσων επικοινωνίας στην καθημερινή δραστηριότητά του. Αν κάποιος δεν έχει δημιουργήσει λογαριασμό στα μέσα κοινωνικής δικτύωσης, λογίζεται ως διαδικτυακά αποκλεισμένος. Η έννοια των μέσων κοινωνικής δικτύωσης, συνίσταται στο facebook, twitter, instagram, snapchat, messenger, (EU science hub, 2018), ως τα πιο δημοφιλή κοινωνικά δίκτυα, τα οποία δίνουν το σφυγμό του μεγαλύτερου μέρους των χρηστών του διαδικτύου. Αντιστοίχως σε αυτά παρατηρούνται τα περισσότερα κρούσματα παραβατικής συμπεριφοράς. Η επιθετική τακτική ότι θύματα και θύτες, διαδικτυακού εκφοβισμού, (cyberbullying), θα παρουσιαστούν στην ιστοσελίδα στο facebook του σχολείου με τα περισσότερα μέλη, είναι σαφής. Το φαινόμενο της ευρείας χρήσης των μέσων κοινωνικής δικτύωσης, έχει προκαλέσει το ενδιαφέρον των μελετητών και λάβει τεράστιες διαστάσεις. Παρότι δεν υφίσταται οπτική επαφή κατά την online επικοινωνία, μεταξύ των χρηστών-μελών της ομάδας, ή αλλιώς πρόκειται για computer-mediated communication (CMC), η κοινωνική αναγνώριση, το αίσθημα ότι το άτομο ανήκει κάπου και είναι αποδεκτό από την ομάδα, αποτελεί ισχυρό κίνητρο, ιδιαίτερα στους νεαρές ηλικίες. Η εν λόγω συμπεριφορά δύναται να δικαιολογηθεί, καθόσον κατά την επικοινωνία μέσω διαδικτύου, δεν υφίστανται οι κοινωνικοί ρόλοι που ενδεχομένως να αποκλείσουν το ένα άτομο από την ομάδα, λόγω οικονομικής ευμάρειας, ούτε οι κοινωνικοί κανόνες που καθορίζουν τις ανθρώπινες συμπεριφορές. Η ισοπεδωτική αντιμετώπιση των χρηστών και η αμεσότητα της επικοινωνίας τους δημιουργεί μια αλληλεπίδραση μοναδική και έχει κατακτήσει τους χρήστες των μέσων κοινωνικής δικτύωσης (Markus Kaakinen, MSocSci, Teo Keipi, DrSocSci, Pekka Ra'sa'nen, DrSocSci, 2017, σ.1-2).

Η ηθελημένη από πλευράς του χρήστη παράδοση προσωπικών του στοιχείων, πραγματοποιείται στα πλαίσια της κοινωνικοποίησης του, ωστόσο το σύστημα αποθηκεύει δεδομένα ως βοήθημα της προσωποποιημένης χρήσης των συστημάτων κοινωνικής δικτύωσης και με στόχο την παροχή άμεσων και στοχευμένων πληροφοριών στο χρήστη, ανάλογα με τα ενδιαφέροντά του. Η παροχή προσωποποιημένων υπηρεσιών (Personalization) δεν έχει απαραίτητα αρνητικό χαρακτήρα. Από τη στιγμή ωστόσο που τα δεδομένα και

προσωπικά στοιχεία του χρήστη αποθηκεύονται σε εφαρμογές ή στο διαδίκτυο, ως ένας τρόπος διαφήμισης συγκεκριμένων προϊόντων, που μπορούν να ενδιαφέρουν το χρήστη, ανοίγουν οι ασκοί του Αίολου (Zimmer, 2010, σ.885). Από την άλλη πλευρά, η χρήση των δεδομένων και του λογαριασμού-προφίλ στα κοινωνικά δίκτυα ενός ατόμου, παρέχει πλήρη εικόνα αυτού και συνυπολογίζεται για την πρόσληψη σε μια θέση εργασίας, ή τη διερεύνηση εγκλημάτων κατά την ανάλυση του προφίλ του υπόπτου (profiling) (Ledingham and Mills, 2015, σ.4). Οι κινήσεις και οι συνήθειες του ατόμου, αφήνουν ηλεκτρονικά ίχνη και αποτυπώνουν το χαρακτήρα και την προσωπικότητά του (Ledingham and Mills, 2015, σ.6).

Οι κίνδυνοι ωστόσο ελλοχεύουν, καθώς μια παραποιημένη φωτογραφία ενός μαθητή ή ενός υπαλλήλου, μπορεί να στιγματίσει τον έφηβο ή να έχει ως αποτέλεσμα να χάσει ο υπάλληλος την προαγωγή του. Η κακόβουλη χρήση της επιρροής των μέσων κοινωνικής δικτύωσης, ασκεί ασφυκτική πίεση στους χρήστες, που γίνονται στόχος. Μια επεξεργασμένη φωτογραφία με ακατάλληλο περιεχόμενο φοιτήτριας, που την εμφανίζει σε καυτές πόζες, και ανεβαίνει στο προφίλ του πανεπιστημίου, μπορεί να οδηγήσει σε ψυχολογική κατάρρευση, ακόμη και σε αυτοκτονία της (Ανασταστας, 2018), (Ponna, 2020). Χαρακτηριστική είναι η διασύνδεση των ατόμων με αυτισμό με περιπτώσεις διαδικτυακών εγκλημάτων, είτε ως θύτες, λόγω των ικανοτήτων τους, είτε ως θύματα, λόγω της αναπτυξιακής και κοινωνικής ιδιαιτερότητας που αντιμετωπίζουν.

Η πιο διαδεδομένη διαδικτυακή απειλή, η σεξουαλική εκβίαση (sextortion) (Στεφανου, 2020), (Kennedy, 2020,σ.155-182), είναι μια τακτική που εξαπλώνεται με γοργούς ρυθμούς στην κοινωνική πραγματικότητα, με συγκεκριμένη μεθοδολογία δράσης. Ο κακόβουλος χρήστης άνδρας ή γυναίκα, επιδιώκει συνομιλία μέσω chat, και κερδίζοντας την εμπιστοσύνη του χρήστη, τον παρασύρει στα πλαίσια του διαδικτυακού σεξ να στείλει γυμνές ή ημίγυμνες φωτογραφίες ή να κάνει διάφορες σεξουαλικές πράξεις μέσω κάμερας (Sameer Hinduja, 2016). Αφού κλείσουν την επαφή μέσω του διαδικτύου, η γυναίκα/άντρας θύτης επανέρχεται με μήνυμα και απειλεί τον συνομιλητή του, ότι εάν δεν πληρώσει ένα ποσό (στην αρχή χαμηλό), τότε η βιντεοσκόπηση ή οι φωτογραφίες που του έχουν σταλεί, θα κοινοποιηθούν σε όλους τους φίλους και επαφές του θύματος. Οι θύτες βρισκόμενοι χωροταξικά σε οποιονδήποτε μικρό ή μεγάλο χώρο, συνδεδεμένοι σε υπολογιστές-διαδίκτυο, αποκομίζουν τεράστια κέρδη με στόχο τους χρήστες των μέσων κοινωνικής δικτύωσης. Συνήθως θύματά τους είναι ανήλικοι χρήστες του διαδικτύου, καθώς δεν δύνανται να διακρίνουν τους κινδύνους που κρύβονται πίσω από την κοινοποίηση προσωπικών τους δεδομένων στον ψηφιακό κόσμο. Η θυματοποίηση σε περιπτώσεις σεξουαλικής εκβίασης,

δημιουργεί αίσθημα ντροπής, ενοχής και φόβου, ακόμη και οδηγεί σε τάσεις αυτοκαταστροφής. Σε περιπτώσεις που ικανοποιηθεί το πρώτο αίτημα τους, οι δράστες επανέρχονται με μεγαλύτερες απαιτήσεις, ενώ ο εντοπισμός τους είναι εξαιρετικά δύσκολος, καθώς τα στοιχεία που δίνουν στην επικοινωνία με το θύμα τους είναι ψεύτικα και ανεπαρκή (Ανάσταστας, 2018), (FBI, 2015), (National Crime Agency, 2020), (Thorn, 2017).

Σύμφωνα με στοιχεία που συλλέχθηκαν από έρευνα που διενεργήθηκε το 2017, υπό την επίβλεψη του Οργανισμού Διαχείρισης Περιστατικών Σεξουαλικής Εκβίασης, σε 2.097 άτομα που έπесαν θύματα, το 83% των ερωτηθέντων, ήταν γυναίκες και σχεδόν οι μισοί (46%) ήταν ανήλικοι (17 ετών ή νεότεροι). Αξίζει να σημειωθεί ότι 3 στους 5 (60%) γνώριζε τον δράστη στην πραγματική ζωή πριν από τη θυματοποίηση, ενώ το 40% τους γνώρισε στο διαδίκτυο. Με άλλα λόγια, οι περισσότερες περιπτώσεις περιελάμβαναν μια ρομαντική σχέση στον πραγματικό κόσμο όπου τραβήχτηκαν φωτογραφίες ή βίντεο και στη συνέχεια ένας συνεργάτης τις χρησιμοποίησε για να χειραγωγήσει ή να ταπεινώσει τον άλλο. Οι υπόλοιπες περιπτώσεις αφορούσαν συνομιλία και διαδικτυακή επικοινωνία του χρήστη, με αποτέλεσμα μια προσωπική εικόνα που στάλθηκε ή λήφθηκε να χρησιμοποιηθεί για να απαιτήσει περαιτέρω σεξουαλικό περιεχόμενο ή δραστηριότητα (Thorn, 2017).

Η επαφή μεταξύ δραστών και θυμάτων πραγματοποιήθηκε σε πολλά μέσα: κοινωνικά δίκτυα (54%), εφαρμογές ανταλλαγής μηνυμάτων (41%), εφαρμογές φωνητικών κλήσεων βίντεο (23%), e-mail (12%), εφαρμογές γνωριμιών (9%) ακόμη και πλατφόρμες παιχνιδιών (4%). Περίπου το 70% τόσο στις προσωπικές όσο και στις διαδικτυακές σχέσεις, παρείχαν εν γνώσει τους σεξουαλική εικόνα στον δράστη, το 40% παρείχε την εικόνα ελεύθερα για να διατηρήσει τη σχέση, επειδή τους άρεσε το άλλο άτομο ή επειδή δεν πίστευαν ότι ήταν μεγάλη υπόθεση. Στο 45% των περιπτώσεων, οι εικόνες αποκτήθηκαν από τους δράστες χωρίς τη γνώση ή τη συγκατάθεση του χρήστη. Στο 18% των περιπτώσεων, καταγράφηκαν εικόνες κάμερας web. Στο 9%, λήφθηκαν χωρίς άδεια από κινητό τηλέφωνο. Στο 8%, ήταν ψεύτικες ή προϊόν Photoshop. Τέλος, στο 5% είχαν πρόσβαση μέσω εισβολής στον υπολογιστή ή στην κινητή συσκευή του (Sameer Hinduja, 2016).

3.6 Προτάσεις

Μέσα από μια μακρά περίοδο διαδικτυακής αθωότητας, διανύουμε την διαδικτυακή ωρίμανση. Η συνειδητοποίηση της επικινδυνότητας και των επιπτώσεων τους στην πνευματική υγεία του ατόμου και την σωματική του ακεραιότητα κρίνεται ως επιτακτική. Η

λελογισμένη χρήση του διαδικτύου, με γνώση των κινδύνων του, είναι ένα μέτρο αντίστασης στο χείμαρρο των πληροφοριών που κατακλύζει το διαδικτυακό χώρο.

Η συνειδητοποίηση ότι το εμπόδιο της σημερινής εποχής δεν είναι η πρόσβαση στην πληροφορία αλλά η αξιολόγησή της, διακρίνοντας την αλήθεια και τη σπουδαιότητα της από την πληθώρα των παρεχόμενων πληροφοριών, κρίνεται επιβεβλημένη. Στη συνέχεια η επιλογή αξιόπιστων παρόχων πληροφορίας, καθώς και η ενημέρωση για τους κινδύνους και η άρνηση αιτημάτων φιλίας από άγνωστα άτομα είναι ένας τρόπος προφύλαξης. Συνίσταται να αποφεύγεται η καταχώρηση και δημοσιοποίηση δεδομένων προσωπικού χαρακτήρα που μπορούν να οδηγήσουν σε ταυτοποίηση, όπως όνομα και όνομα χρήστη, ταχυδρομική διεύθυνση, πληροφορίες ηλεκτρονικής επικοινωνίας (e-mail), αριθμό τηλεφώνου, διεύθυνση κατοικίας, πληροφορίες γεωεντοπισμού- για να ταυτοποιηθεί η οδός και η πόλη κατοικίας του χρήστη. Οι ενέργειες του χρήστη είναι θεμιτό, να βασίζονται στην ορθή και συνετή χρήση του διαδικτύου και γι' αυτό κρίνεται αναγκαία η ενημέρωση των χρηστών για τους κινδύνους που έχουν ανακύψει (Κελάλη, 2018, σ. 78).

Η μη αποθήκευση των κωδικών κάρτας στην κρυφή μνήμη- cache του υπολογιστή ή του κινητού τηλεφώνου, καθώς και η διαγραφή του ιστορικού σε τακτά χρονικά διαστήματα, ενδεχομένως περιορίζει τις παρεμβολές. Ωστόσο οι τακτικές αυτές απομακρύνουν παροδικά την όποια απειλή, χωρίς να δύναται ουσιαστική λύση στην προστασία των ατομικών δικαιωμάτων των πολιτών. Το δαιδαλώδες δίκτυο επιτρέπει, λόγω της πολυπλοκότητας των συνδέσμων του και της διαδραστικότητας των χρηστών του, να παραμένουν ακάλυπτα πολλά σημεία ασφαλούς πλοήγησης, στα οποία μπορεί ο επιτήδειος κακόβουλος χρήστης (hacker) να εισέλθει και να προκαλέσει βλάβη, είτε στο λειτουργικό σύστημα του μέσου πλοήγησης, είτε στην καταστρατήγηση του ανωνύμου της συνομιλίας μέσω μηνυμάτων και υποκλοπής δεδομένων προσωπικού χαρακτήρα. Επίσης η διαβούλευση και ο προβληματισμός στρέφεται σε ομάδες χρηστών που λόγω ηλικίας και συναισθηματικής ή νοητικής ανωριμότητας, δε δύνανται να εκτιμήσουν τον κίνδυνο που προέρχεται από την αλόγιστη χρήση προσωπικών τους στοιχείων κατά την πλοήγηση στο διαδίκτυο (Bujlow *et al.*, 2017). Η προστασία των ανηλίκων αποτελεί κοινωνική προτεραιότητα. Η σαφής νομοθετική και αυστηρή θεσμοθέτηση συντελείται κατόπιν διαπίστωσης της παραβατικής συμπεριφοράς, προς συμμόρφωση του δράστη και προστασίας του κοινωνικού συνόλου. Η υπάρχουσα νομοθεσία καλύπτει τις βασικές διατάξεις με την προστασία του Νόμου περί προσωπικών δεδομένων όπως αυτός έχει τροποποιηθεί και ισχύει. Στα αδικήματα που τελούνται μέσω διαδικτύου, οι βλάβες που συντελούνται δύναται να είναι από ελαφριές ως καταστροφικές για το άτομο και

φυσικά για τον ανήλικο. Το σύστημα αυτοεπιβεβαίωσης της ηλικίας του χρήστη με την δήλωση ότι είναι άνω των δεκαοχτώ ετών, ή άνω των δεκατριών ετών, εύκολα παρακάμπτεται. Η αναγκαιότητα εύρεσης άλλων τρόπων εξακρίβωσης της ηλικίας και ο αποκλεισμός ανηλίκων από την έκθεση σε ακατάλληλο για το ανώριμο της ηλικίας τους περιεχόμενο, είναι πιο επίκαιρη από ποτέ.

Από την άλλη οπτική, η πρόληψη και η καλλιέργεια πληροφοριακής παιδείας των χρηστών κάθε ηλικίας, από τους γονείς για να συμβουλευθούν τα παιδιά τους, ως τον κάθε ενήλικα χρήστη των κοινωνικών δικτύων, συμβάλει στη δημιουργία προστατευτικού κλοιού. Ενίσχυση της θετικής χρήσης της τεχνολογίας, με την αξιοποίηση των εργαλείων αναζήτησης της πληροφορίας προς πλήρωση του αρχικού σκοπού του διαδικτύου και της ελεύθερης διακίνησης της πληροφορίας. Επίσης η ανάγκη ενημέρωσης και συντονισμού των γονέων και των εκπαιδευτικών για εντοπισμό περιστατικών διαδικτυακού εκφοβισμού σεξουαλικού ή μη, (cyberbullying ή sextortion) με τη δημιουργία ιστοσελίδας ή ανάλογου blog στο σχολείο, όπου ο καθένας μπορεί να καταθέτει ανάλογα περιστατικά, υπό την επίβλεψη εξειδικευμένων εκπαιδευτικών (π.χ. του καθηγητή πληροφορικής ως διαχειριστή), μπορεί να εντοπίσει περιστατικά παραβίασης προσωπικών δεδομένων. Είναι σαφές ότι η τεχνολογία τρέχει με ιλιγγιώδεις ρυθμούς. Η πλειονότητα των χρηστών δεν είναι προετοιμασμένοι να την διαχειριστούν και δεν γνωρίζουν τους κινδύνους που ελλοχεύουν. Η ηθική κατά τη χρήση και διαχείριση της πληροφορίας δεν έχει διαλευκανθεί, λαμβάνοντας υπόψη ότι το διαδίκτυο αποτελεί τον μεγαλύτερο συλλέκτη δεδομένων. Η πληροφορία διαχέεται ελεύθερα, ωστόσο οι όποιοι περιορισμοί της αναγκάζουν το χρήστη σε υποχωρήσεις στις ρυθμίσεις ασφαλείας, ακόμη και αυτές τελούνται από τις αυτοματοποιημένες ρυθμίσεις της εφαρμογής. Η ωφέλεια ή η κατάχρηση χρήσης του διαδικτύου εναπόκεινται στον χρήστη καθώς και η αδήριτη ανάγκη προστασίας του ιδίως σε περιπτώσεις ανηλίκων. Το κριτήριο με βάση το οποίο αξιολογούνται οι επιλογές ως ορθές ή μη, τοποθετείται με βάση την πρόκληση βλάβης σε άλλον χρήστη. Η χρήση τομή δηλαδή της ελευθερίας του ατόμου, της αυτοδιάθεσής του, έναντι και της ελευθερίας των άλλων (Παναγοπούλου-Κουτνατζή, 2013).

ΚΕΦΑΛΑΙΟ 4 Αποτύπωση της παγκόσμιας και ευρωπαϊκής πολυπολιτισμικής πραγματικότητας.

Ο πολυπολιτισμικός χαρακτήρας των κοινωνιών εμφανίζεται σε χρονικές περιόδους της ιστορικής διαδρομής του ανθρώπου συνυπολογίζοντας τις συνθήκες που οδηγούν στην μετακίνηση πληθυσμών και πόσο συχνά αυτές συναντώνται ιστορικά. Υπό το πρίσμα αυτό οι σύγχρονες πολυπολιτισμικές κοινωνίες δεν αποτελούν νέο φαινόμενο. Η διαφοροποίηση που παρατηρείται και αναπροσαρμόζει τη διαχείριση των μετακινούμενων ομάδων έγκειται στο ιστορικό πλαίσιο, το πολιτισμικό υπόβαθρο και την αλληλεπίδραση ανάμεσα στις συστατικές πολιτισμικές ομάδες και στις κοινωνικές δομές των κοινωνιών στις οποίες επιθυμούν να ενταχθούν (Δραγώνα, 2015, σ. 11–12)

Οι σύγχρονες κοινωνίες εμφορούμενες από τις αρχές του κράτους δικαίου και με γνώμονα τις θεμελιώδεις ανθρώπινες αξίες ισότητας και ελευθερίας των ατόμων, έχουν αμβλύνει τις ανισότητες μεταξύ των ατόμων ανεξαρτήτου καταγωγής, φυλής, θρησκείας. Η αποκαθήλωση των τυραννικών καθεστώτων, η κατάργηση της δουλείας, το Ολοκαύτωμα, έθεσαν νέες βάσεις στην κοινωνική διαστρωμάτωση και παρουσίασαν τη δυσχερή διαχείριση της διαφορετικότητας των κοινωνικών ομάδων που επιθυμούν να ενταχθούν στην ήδη ισορροπημένη κοινωνική δομή. Οι κοινωνικές ομάδες αναζητούν το χώρο τους σε κάθε κοινωνική διαστρωμάτωση και επιθυμούν να διαχειρίζονται ισότιμα τόσο από την υπόλοιπη κοινωνία, όσο και από το κράτος τη θεσμική ομάδα του κάθε κράτους, υπό τις αρχές της ισότητας των ευκαιριών και των πολιτισμικών δικαιωμάτων των μειονοτήτων. Η ένταξή τους και ο τρόπος που επιζητούν την καταξίωση και την αφομοίωση τους στην κοινωνική δομή, δημιουργεί προβληματισμό ως προς την ανεκτικότητα της κοινωνίας στο διαφορετικό στην αποδοχή ή την απορρόφηση του από αυτήν. Η πρόκληση της ανισορροπίας αυτής στις κοινωνικές δομές, ενδεχομένως να μην είναι δυνατό να εξαλειφθεί με αποτέλεσμα την αντίδραση από συντηρητικές δυνάμεις της. Η αποδοχή της διαφορετικότητας και η αμφίπλευρη παραδοχή μιας διαφοροποιημένης πραγματικότητας, υπό το πρίσμα της παγκόσμιας κοινωνίας και παγκοσμιοποίησης, απαιτεί χρόνο και κοινωνική δεκτικότητα (Villa and Magri, 2020).

Στο πλαίσιο αυτό εντάσσεται η γενικότερη αντίδραση των κοινωνιών και των ομάδων στην πολιτισμική ετερότητα, ως βάση της εκδήλωσης ξενοφοβικών εξάρσεων που γειτνιάζουν ως συμπεριφορές με το ρατσισμό. Η ξενοφοβία εκδηλώνεται ως αποκλεισμός ή διαχωρισμός μιας ομάδας, ως ένας «μηχανισμός απόκρουσης» του άλλου ατόμου. Διακρίνεται ωστόσο από τον ρατσισμό, κατά τον οποίο κριτήριο αποκλεισμού είναι εκείνο

της φυλετικής ή εθνικής υπεροχής, αλλά και από τον εθνικισμό, στον οποίο το διακυβευόμενο είναι η διατήρηση των αξιών, κανόνων και πρακτικών της εθνικής ιδεολογίας. Το μεταναστευτικό φαινόμενο όπως εξελίσσεται σε διαφορετική κοινωνικό-οικονομική βάση ανά χρονική συγκυρία σε διεθνές πλαίσιο, η απορρύθμιση της αγοράς εργασίας, οι επισφαλείς συνθήκες εργασίας, σε συνδυασμό με το πλεόνασμα προσφερόμενου ανθρωπίνου δυναμικού, όπως αυτό συνδέει τη 'μαύρη' οικονομία με την παράνομη μετανάστευση, αναπροσαρμόζουν τους όρους και την ευπροσήγορη διάθεση υποδοχής των κοινωνιών απέναντι στις μεταναστευτικές ροές. Τα άτομα επιδιώκουν να καλύψουν τις θέσεις εργασίας υπό πιο εύελictους όρους εργασίας και μισθούς, αλλά και να ενσωματωθούν στην υπάρχουσα κοινωνική δομή βρίσκοντας τη θέση τους σε αυτή (Λιαλιούτη *et al.*, 2017).

Υπό το πρίσμα αυτό, αναδεικνύεται η σημασία της κατάρτισης αποτελεσματικών μεταναστευτικών πολιτικών, μελετώντας τις μεταναστευτικές τάσεις κινητικότητας των πληθυσμών διεθνώς, αξιοποιώντας τις παραδοσιακές μεθόδους άντλησης στατιστικών στοιχείων μετακίνησης πληθυσμών, λαμβάνοντας παράλληλα υπόψη όχι μόνο τα παραδοσιακά δεδομένα απογραφής του πληθυσμού αλλά και τις σύγχρονες μεθόδους άντλησης δεδομένων, όπως αυτά εξάγονται από πλατφόρμες μέσω κοινωνικής δικτύωσης (Shanker, 2019, σ.18).

4.1 Πολυπολιτισμική πραγματικότητα

Η πολυπολιτισμική πραγματικότητα όπως αυτή αποτυπώνεται από τις αυξανόμενες ροές μεταναστευτικών κυμάτων μεγάλων αποστάσεων και κλίμακας προς την ευρωπαϊκή δύση, λόγω ποικίλων και διαφορετικών παραγόντων, έχουν ως κύριο χαρακτηριστικό τη μαζικότητα εκδήλωσής τους (Sebastian Morris, 2005). Οι μετακινήσεις πληθυσμιακών ομάδων λόγω περιβαλλοντικών αλλαγών και ακραίων καιρικών φαινομένων, αποτελεί ένα σύνηθες φαινόμενο που έχει ως αποτέλεσμα τη ριζική αλλαγή στην καθημερινότητα των ατόμων. Ο παράγοντας αυτός σε συνδυασμό με τη γεωπολιτική αστάθεια και τη συγκρουσιακή κατάσταση σε γεωγραφικές περιοχές κυρίως της Ανατολής, αποτελεί μια ισχυρή κινητήριο δύναμη που ωθεί τον πληθυσμό προς τη μεταναστευτική οδό. Κατά γενική ομολογία, η αύξηση των μεταναστευτικών ροών οφείλεται στη αδυναμία των ατόμων να αντιμετωπίσουν την ανισότητα, την ανεργία, τη φτώχεια, την πολιτική και κοινωνική αστάθεια. Η ανασφάλεια των ατόμων και οι ρωγμές που προκαλούνται στις κοινωνικές δομές, είναι ένας σημαντικός παράγοντας μαζικής μετακίνησης του πληθυσμού με την ελπίδα εύρεσης καλύτερων συνθηκών διαβίωσης. Οι πιο ασφαλείς χώρες, ως χώρες τελικής

εγκατάστασης, δέχονται μαζικές εισροές ατόμων που έχουν ανάγκη διεθνούς προστασίας και περικλείονται από τις διατάξεις του ασύλου. Επιπλέον οι σημαντικές δημογραφικές μεταβολές (OECD, 2020, σ. 2–4), όπως αναμένεται να λάβουν χώρα τις επόμενες δεκαετίες, εξαιτίας της παγκόσμιας τάσης γήρανσης του πληθυσμού, ωθεί τις κοινωνίες στην επιλογή και εξεύρεση νεαρότερου ανθρώπινου δυναμικού, ανάλογα με τη ζήτηση στην αγορά εργασίας των οικονομιών τους. Το φαινόμενο αυτό συναντάται σε διαφορετικές χρονικές περιόδους της ιστορικής διαδρομής του ανθρώπου. Αξίζει να αναφερθεί ότι κατά το χρονικό διάστημα 1945-1961 οι αρχές της Αυστραλίας επέλεξαν να ανατροφοδοτήσουν το εργατικό δυναμικό τους με λευκούς ανθρώπους, στα πλαίσια της «White Australia Policy» ακόμη και ανειδίκευτους, τους οποίους εκπαίδευαν και στη συνέχεια απασχολούσαν στην παραγωγική διαδικασία των οικονομιών τους. Η επιδίωξή τους να μην αναμειχθεί ο πληθυσμός τους, διατηρώντας την καθαρότητά τους, καθόριζε την πολιτική επιλογής των ατόμων που θα εισέρχονταν στην χώρα τους (National museum of Australia, 2020), (Λημνιός-Σέκερης, 2015), (Betts, 2014).

Οι διαδικασίες επιλογής των ατόμων που θα απασχοληθούν και θα δικαιολογήσουν την παραμονή τους στην χώρα υποδοχής εξαιτίας της εργασίας τους, πραγματοποιούνται με τη χρήση εξελιγμένων πληροφοριακών συστημάτων και υπαγορεύονται από συστήματα επιλογής και ενσωμάτωσης της μετανάστευσης με τη χρήση αλγορίθμων. Αυτές τις βάσεις δεδομένων αλλά και κάθε βάση δεδομένων που χρησιμοποιείται για την ταυτοποίηση του ατόμου, κατόπιν αιτήματος και ρητής συγκατάθεσής του (European Commission, 2020), διαχειρίζονται προσωπικά δεδομένα και πληροφορίες τους, με στόχο την καταγραφή και την περαιτέρω νομιμοποίηση της παραμονής τους στη χώρα που αιτούνται. Στις βάσεις αυτές δεδομένων, υπό τον αυστηρό έλεγχο καταγραφής εισόδου νομιμότητας του ατόμου, παραγκωνίζονται τα προσωπικά δεδομένα των ατόμων, στη λογική της εξυπηρέτησης του αιτήματός τους και την ύπαρξη της αμέριστης συγκατάθεσής τους. Είναι θεμιτό να αναζητηθεί μέχρι σε ποιο σημείο είναι θεμιτή και δεοντολογικά ορθή η χρήση και παρείσφρηση στα προσωπικά δεδομένα των ατόμων που αιτούνται διεθνή προστασία ή επιθυμούν να αναγνωριστούν ως πρόσφυγες και να τύχουν των ευεργετικών διατάξεων του νομοθετικού πλαισίου. Στις ΗΠΑ μεταξύ των προσωπικών στοιχείων που δύνανται να χρησιμοποιηθούν είναι οι αντλούμενες πληροφορίες από τα μέσα κοινωνικής δικτύωσης, τα δεδομένα θέσης, το προφίλ του χρήστη κλπ. Η χρήση των βιομετρικών δεδομένων αποτελεί κανόνα για αιτήσεις άδειας και θεώρησης, είτε αιτούνται για εύρεση εργασίας, είτε κατοικίας. Μπορεί επίσης να ζητηθούν παρόμοιες πληροφορίες που αφορούν συγγενείς ή και φίλους του αιτούντα,

προκειμένου να ελεγχθούν οι κοινωνικές επαφές του αιτούντα και η ύπαρξη βιοτικών δεσμών και δεσμών συγγενείας του²⁴. Εγείρεται προβληματισμός σχετικά με τη συλλογή και επεξεργασία προσωπικών δεδομένων καθώς οι κοινωνικές πλατφόρμες μετατρέπονται στα μέσα αξιολόγησης, κατόπιν της έγκρισης και της ανάγκης του αιτούντα μετανάστη για νομιμοποίησή του στη χώρα που τον έχει υποδεχτεί.

Παράδειγμα χαρακτηριστικό αποτελεί το διαδικτυακό σύστημα E-Verify, που επιτρέπει στους εγγεγραμμένους εργοδότες να επιβεβαιώνουν την επιλεξιμότητα των υπαλλήλων τους, προκειμένου να πραγματοποιήσουν την πρόσληψή τους και να εργαστούν στις Ηνωμένες Πολιτείες. Οι εργοδότες, μέσω του E-Verify, επαληθεύουν την ταυτότητα του ατόμου και δηλώνουν ότι θα του παράσχουν εργασία, αντιστοιχίζοντας ηλεκτρονικά πληροφορίες, όπως αυτές αντλούνται από βάσεις δεδομένων που παρέχονται από τη Διοίκηση Κοινωνικής Ασφάλισης (SSA) και το Υπουργείο Εσωτερικής Ασφάλειας (DHS). Η διαδικασία αυτή συλλέγει και επεξεργάζεται τα προσωπικά στοιχεία που έχουν αποθηκευτεί στις εν λόγω βάσεις δεδομένων για το άτομο που επιλέγεται και μεταπίπτουν στην εφαρμογή αυτή, εμφανίζοντας εγγραφές σε παράλληλες βάσεις δεδομένων. Οι εφαρμογές αυτές λειτουργούν κατόπιν εθελοντικής γενικής συγκατάθεσης για τη συλλογή και χρήση των προσωπικών πληροφοριών του ατόμου. Σημειώτέο ότι η συγκατάθεση αυτή είναι απόλυτη και δεν μπορεί το άτομο να θέσει περιορισμούς διάρκειας ή κατηγορίας των υπό επεξεργασία δεδομένων του. Επίσης το E-Verify διατηρεί τις πληροφορίες που υπέβαλε ο συμμετέχων για μια δεκαετία από την ημερομηνία κατά την οποία ο συμμετέχων ολοκλήρωσε τη διαδικασία επαλήθευσης, με εξαίρεση τις περιπτώσεις που διεξάγεται δικαστική διαδικασία ή έρευνα και για όσο χρόνο διαρκεί αυτή. Κατά τη διαδικασία αξιολόγησης των συλλεγόμενων στοιχείων το E-Verify, έχει την ευχέρεια να στείλει σε συνεργαζόμενες πλατφόρμες της E-Verify για σκοπούς επαλήθευσης, στοιχεία των συμμετεχόντων στην επιχειρηματική διαδικασία επιλογής και να συνδεθεί με άλλους οργανισμούς, όπως οργανισμούς DHS. Η διοίκηση κοινωνικής ασφάλισης (SSA), το Υπουργείο Εξωτερικών το Τμήμα Δικαιοσύνης καθώς και το Τμήμα Γραφείου Μεταναστών και Δικαιωμάτων των Εργαζομένων.

Η δημιουργία του «Μεταναστευτικού προφίλ» θεωρείται αναγκαία και κατοχυρώνεται από διεθνείς συμφωνίες, υπό το πρίσμα της εθνικής και ευρωπαϊκής ασφάλειας των κοινωνιών από τις μαζικές και ανεξέλεγκτες μεταναστευτικές ροές. Η κατηγοριοποίηση των δεδομένων και η διαχείρισή τους κρίνεται ως επιβεβλημένη και απαιτείται κυρίως από τις χώρες-πύλες εισόδου στην ευρωπαϊκή κοινότητα. Η καταχώρηση

²⁴<https://www.e-verify.gov>, (Ημερομηνία πρόσβασης: 05-09-2020).

στο SIS II (European Commission, 2020), με διασύνδεση πέραν των ευρωπαϊκών κρατών και άλλων κρατών που έχουν προχωρήσει και συνυπογράψει τη συμφωνία των διακινούμενων δεδομένων, θεωρείται ο πλέον σύγχρονος τρόπος προληπτικής δράσης των κυβερνήσεων (European Commission, 2020). Το SIS II επιτρέπει την ανταλλαγή πληροφοριών σε ασφαλές περιβάλλον στα πλαίσια εθνικού ελέγχου των συνόρων σε τελωνειακές και αστυνομικές αρχές, στην προσπάθεια να διασφαλιστεί η ελεύθερη κυκλοφορία των ανθρώπων εντός της Ε.Ε. Η αναγκαιότητα αυτή δεν μπορεί να παραγκωνίσει τους ηθικούς προβληματισμούς που ανακύπτουν σχετικά με το είδος των πληροφοριών που απαιτείται να χρησιμοποιηθούν και κατά πόσο η προστασία που απολαμβάνουν οι μόνιμοι κάτοικοι στον τομέα αυτό πρέπει να επεκταθεί και στους μετανάστες (European Commission, 2020, σ. 13), (Amanda, 2018).

4.2 Φιλτράρισμα δεδομένων (data filtering)

Το φιλτράρισμα δεδομένων εξ' ορισμού περιλαμβάνει τη λήψη των πληροφοριών αναζήτησης για το χρήστη, που δεν είναι χρήσιμες για τον αναγνώστη με βάση τις προτιμήσεις του (cookies). Με τον τρόπο αυτό τα αποτελέσματα της αναζήτησης είναι «προσωποποιημένα», με απώτερη συνέπεια την λήψη άμεσων και ασφαλέστερων αποφάσεων-επιλογών (Pariser, 2011, σ. 212). Οι αναφορές και τα αποτελέσματα ερωτημάτων, όπως αυτά προκύπτουν από αναζήτηση σε εργαλεία βάσης δεδομένων, οδηγούν συχνά σε μεγάλα, πολύπλοκα και άχρηστα για το χρήστη, σύνολα δεδομένων. Τα περιττά ή αμερόληπτα κομμάτια δεδομένων μπορούν να προκαλέσουν σύγχυση ή αποπροσανατολισμό του χρήστη ('Definition - What does Data Filtering mean?', 2020) και να δυσχεραίνουν την αναζήτησή του. Στόχος είναι η παροχή των καλύτερων δυνατών υπηρεσιών-αποτελεσμάτων στο λιγότερο δυνατό χρόνο. Η παροχή εξατομικευμένων υπηρεσιών υπαγορεύει ταχύτητα και ακρίβεια για το αποτέλεσμα αναζήτησης του χρήστη. Με δεδομένη την αθρόα και ανεξάντλητη διάθεση πληροφοριών, ο κίνδυνος υπερφόρτωσης με άχρηστα για το χρήστη δεδομένων είναι υπαρκτός και η ανάγκη για διαλογή αυτών αναγκαία.

Σε άλλες περιπτώσεις, το φιλτράρισμα των δεδομένων λειτουργεί προστατευτικά προς το χρήστη και όχι μόνο προς εξυπηρέτησή του. Η αποτροπή ευρύτερης πρόσβασης σε ευαίσθητες πληροφορίες, με τον έλεγχο των εισερχόμενων εντολών και την κατεύθυνση ή αποφυγή τους, δημιουργεί προστατευτικό πλαίσιο για το χρήστη. Για παράδειγμα, ένα πρόγραμμα φιλτραρίσματος δεδομένων θα μπορούσε να απομακρύνει τους αριθμούς κοινωνικής ασφάλισης, τους αριθμούς πιστωτικών καρτών και άλλα αναγνωριστικά από σύνθετα σύνολα δεδομένων πελατών που εισέρχονται στην εργασία ενός υπαλλήλου ή ακόμη

στη συσκευή του κινητού του. Η πρακτική «φέρτε τη δική σας συσκευή» (BYOD), επιτρέπει στους διαχειριστές να διαμορφώσουν τη δική τους βάση δεδομένων, στοχεύοντας στην αύξηση της παραγωγικότητας και τη μείωση του κόστους στις μικρομεσαίες επιχειρήσεις. Το BYOD ενθαρρύνει τους υπαλλήλους της εταιρείας να εργάζονται στη συσκευή που επιλέγουν, εξασφαλίζοντας την πρόσβαση τους σε εταιρικά e-mail και βάσεις δεδομένων στον προσωπικό τους υπολογιστή²⁵. Ωστόσο το φιλτράρισμα δεδομένων μπορεί να θεραπεύσει τα ανακύπτοντα προβλήματα ασφαλείας που σχετίζονται με τις πληροφορίες που οι εργαζόμενοι χρησιμοποιούν από τον προσωπικό τους υπολογιστή ή το κινητό τηλέφωνο κατά την εργασία τους και δύνανται να θέσουν σε κίνδυνο τα ευαίσθητα επιχειρηματικά συστήματα της εταιρείας. Ακόμη και τα ίχνη που αφήνουν τα δεδομένων αποθηκεύονται και δύνανται να αξιοποιηθούν παράλληλα ενώ στη συνέχεια, αν δεν είναι πλέον χρήσιμα, “ξεπλένονται” (data laundering), (Pariser, 2011, σ.212). Το φιλτράρισμα δεδομένων αφορά σε ένα ευρύ φάσμα στρατηγικών ή λύσεων για τη βελτίωση των συνόλων δεδομένων. Τα σύνολα δεδομένων εξευγενίζονται, σύμφωνα με τις απαιτήσεις του χρήστη, προσωποποιώντας τις ανάγκες του, αποκλείοντας τα δεδομένα που μπορεί να είναι επαναλαμβανόμενα, άσχετα ή ακόμη και ευαίσθητα. Το φιλτράρισμα δεδομένων ουσιαστικά είναι το αποτέλεσμα της μείωσης του περιεχομένου «θορύβου», κατ’ αντιστοιχία με την επεξεργασία των ηχητικών δεδομένων. Ο «θόρυβος μέτρησης» δύναται να καλύψει τα σημαντικά χαρακτηριστικά των δεδομένων και να περιορίσει τη χρησιμότητά τους, παρεκκλίνοντας από την αρχική στοχοθεσία-την άμεση και αποτελεσματική εξεύρεση της πληροφορίας που αναζητά ο χρήστης (Byun *et al.*, 2013).

4.3 Η πρόσβαση στην πληροφορία.

Η διαχείριση και αποθήκευση προσωπικών δεδομένων, δεδομένων ταυτότητας, κατοικίας σε πλατφόρμες και μέσα κοινωνικής δικτύωσης αποτελεί έναν μη παραδοσιακό τρόπο άντλησης δεδομένων. Η έλλειψη των πληροφοριών σχετικά με τους ιδιόκτητες αλγορίθμους που χρησιμοποιούν οι εταιρείες μέσων κοινωνικής δικτύωσης για την επεξεργασία των προσωπικών δεδομένων και την ταξινόμηση των χρηστών με βάση τη συμπεριφορά τους, μπορεί να οδηγήσει τον ερευνητή σε αποκλίσεις, οι οποίες αν

²⁵<https://www.thebalancecareers.com/bring-your-own-device-byod-job-policy-4139870>,
<https://www.techradar.com/news/computing/what-is-byod-and-why-is-it-important-1175088>
(Ημερομηνία πρόσβασης: 05-05-2020).

προβλεφθούν μπορούν να παρακαμφθούν με τις αντίστοιχες μεταβλητές. Η αξιοπιστία των αυτοαναφερόμενων πληροφοριών σχετικά με τα κοινωνικά μέσα είναι επίσης αμφισβητήσιμη, ωστόσο σε συνδυασμό με τις παραδοσιακές μεθόδους άντλησης πληροφοριών, είναι ιδιαίτερα αποδοτική (Shanker, 2019,σ.18). Στο χώρο των μέσων κοινωνικής δικτύωσης, ο κάθε χρήστης παραχωρεί στοιχεία από το φάσμα ιδιωτικότητας του, αμφιβόλου αξιοπιστίας, δίχως να υφίσταται η δυνατότητα επαλήθευσής τους. Από την ηλικία του, ως τις ασχολίες και το κοινωνικό του υπόβαθρο, οι όποιες αναφορές είναι πλήρως αμφισβητήσιμες και αναξιόπιστες. Χαρακτηριστικό παράδειγμα αυτής της αποτύπωσης είναι η αδυναμία εξακρίβωσης της ηλικίας των χρηστών, ιδίως όταν πρόκειται για ανήλικο χρήστη. Η αυτό-ταυτοποίηση παρακάμπτεται με τη δήλωση ενηλικιότητας από το χρήστη. Η ανυπαρξία κοινών τακτικών εξακρίβωσης της ηλικίας στο διαδίκτυο, εμφανίζει τη δυσκολία ισορροπίας μεταξύ της ανάγκης διατήρησης της ανωνυμίας του χρήστη, την ανάγκη επαλήθευσης της ηλικίας του καθώς και της ελεύθερης έκφρασης της προσωπικότητάς του. Η οποιαδήποτε αποθήκευση των δεδομένων του, μπορεί εφόσον ο χρήστης στοχοποιηθεί από επίδοξο hacker, να υποκλαπεί (identity theft), ενώ δεν είναι υφίσταται έλεγχος εγκυρότητας των δεδομένων που αποθηκεύονται για τον κάθε χρήστη. Ένα μεγάλο ποσοστό των χρηστών έχουν ψεύτικους λογαριασμούς ή ανενεργούς, όπως προκύπτει από στατιστικά δεδομένα του facebook, με αποτέλεσμα, το τέταρτο τρίμηνο του 2018, οι ψεύτικοι λογαριασμοί και οι διπλοί λογαριασμοί, να αποτελούν περίπου το 5% και το 11% των μηνιαίων ενεργών χρηστών παγκοσμίως αντίστοιχα (Spyratos, Spyridon, Yildiz *et al.*, 2019), (Paper, Lakhani and Wolf, 2003).

Από την άλλη πλευρά, η πλατφόρμα του Facebook έχει το πλεονέκτημα της χρήσης των δεδομένων που αποθηκεύει χωρίς περιορισμούς από το διαθέτη προς το χρήστη. Τα στοιχεία αυτά δύνανται και χρησιμοποιούνται από τους ερευνητές χωρίς χρειάζεται να αντιμετωπίσουν τα νομικά και τεχνικά ζητήματα άντλησής τους, στα πλαίσια της προστασίας των προσωπικών δεδομένων των χρηστών και της ελεύθερης ή μη διάθεσης των προσωπικών τους δεδομένων. Η συστηματική χρήση μη παραδοσιακών δεδομένων για υποστήριξη ερευνητικών προγραμμάτων για την ανάπτυξη συμπεριφορικών μοντέλων πολιτισμικής και κοινωνικής δράσης ομάδων ατόμων, σταδιακά θα οδηγήσει τους ερευνητές να διαπραγματευτούν συμφωνίες με εταιρείες κοινωνικών μέσων ενημέρωσης με στόχο την παροχή μεγαλύτερο έλεγχο για τον τρόπο παραγωγής και προεπεξεργασίας των δεδομένων που αντλούν από τις εφαρμογές τους. Ο μακροπρόθεσμος σχεδιασμός της κοινωνικό-οικονομικής πολιτικής και διακυβέρνησης της μετανάστευσης είναι ένα σαφές πεδίο έρευνας

που αντλεί αυξανόμενα στοιχεία για τις μετακινήσεις πληθυσμών. Η πρόθεση συγκέντρωσης σε μια γεωγραφική περιοχή μιας ομάδας ατόμων με κοινά ιδεολογικά στοιχεία, κοινωνικό πολιτική βάση αλλά και κοινό θρησκευτικό υπόβαθρο, είναι ένα σημείο αιχμής για τον ερευνητή που στοχεύει στην παροχή έγκαιρων και έγκυρων δεδομένων φυλετικής μετακίνησης και συγκέντρωσης πληθυσμιακών ομάδων ανά περιοχές. Επιπροσθέτως, οι ανοιχτές πηγές άντλησης της πληροφόρησης εύκολα μετατρέπονται σε αναξιόπιστες και η απαίτηση για αξιόπιστη πληροφορία, είναι ολοένα και πιο σημαντική, αν ληφθεί υπόψη ότι τα fake news αναδύονται για διχάσουν και να δοκιμάσουν κοινωνίες και τις κυβερνήσεις (“‘Fake news’: Greece rejects Turkey’s claims its forces killed a migrant trying to cross border”, 2020). Τα δεδομένα αυτά μπορούν να χρησιμοποιηθούν για την παρακολούθηση των συμπεριφορών των χρηστών με τρόπους που θα μπορούσαν να επηρεάσουν τις πολιτικές τους ελευθερίες, την ιδιωτικότητά τους, καθώς και το δικαίωμα τους στη λήθη (Παναγοπούλου-Κουτνατζή, 2013).

Υπό αυτό το πρίσμα, γίνεται κατανοητό ότι η χρήση δεδομένων από κοινωνικά μέσα δημιουργεί διάφορες ανησυχίες για την προστασία της ιδιωτικής ζωής και τη δεοντολογία του νομοθετικού πλαισίου που την κατοχυρώνει. Τα ανοιχτά διαθέσιμα δεδομένα θέσης από τα κοινωνικά μέσα, ακόμη και σε συγκεντρωτική μορφή, μπορούν να χρησιμοποιηθούν για την παρακολούθηση των κινήσεων ευάλωτων ομάδων, τη συγκέντρωση δεδομένων καταναλωτικής κίνησης των χρηστών με στόχο τη διαφήμιση, αλλά και τον έλεγχο συγκεκριμένων ομάδων χρηστών με κοινό κοινωνικοπολιτικό υπόβαθρο, περιθωριακών ομάδων, ανθρωπιστικών αλλά και εγκληματικών και λοιπών οργανώσεων με στόχο την ριζοσπαστικοποίηση των μελών τους και το φανατισμό. Ειδικότερα, στα πλαίσια της εκπόνησης μελετών για την αποτύπωση των μεταναστευτικών ροών παγκοσμίως αλλά και εντός της Ευρωπαϊκής Ένωσης, καθώς και στα πλαίσια σχεδιασμού της μεταναστευτικής πολιτικής της, γίνονται προσπάθειες να αποτυπωθεί η κινητικότητα των ατόμων ανά μεταβλητές και σταθερά δεδομένα, που θα αποτυπώνουν την πραγματικότητα σε ρεαλιστική βάση (The Global Compact for Safe, 2020).

Η καταγραφή και μετακίνηση πραγματοποιείται στις συνοριακές γραμμές της κάθε χώρας, στα προξενεία αυτής, στις αστυνομικές υπηρεσίες καθώς και στους οργανισμούς εξυπηρέτησης μεταναστών και καταγράφεται σε μελέτες και στατιστικές κίνησης των πληθυσμιακών ομάδων. Πέρα των επίσημων καναλιών επικοινωνίας, υφίστανται πληθώρα μετακινήσεων που δεν αποτυπώνονται, δεν μελετώνται και αποτελούν την λανθάνουσα μετακίνηση πληθυσμών, όπως η προσωρινή μετανάστευση και η κυκλική μετανάστευση, η

οποία με την εγκατάστασή της στη χώρα προορισμού εμφανίζεται ως δεδομένη. Και στις δύο κατηγορίες οι λεπτομέρειες που συλλέγονται είναι μηδαμινές. Στις χώρες στου τελικού προορισμού συλλέγονται τα στοιχεία που δηλώνουν οι μετακινούμενοι τα οποία πολλές φορές δεν μπορούν να εξακριβωθούν ως προς την ορθότητά τους. Οι παραδοσιακές μέθοδοι ωστόσο άντλησης πληροφοριών, θεωρούνται πιο αξιόπιστες αφού περνούν από επίσημες διαύλους επικοινωνίας. Από την άλλη πλευρά οι μη παραδοσιακές ή εναλλακτικές μέθοδοι συλλογής πληροφοριών καταγράφουν ποικίλες λεπτομέρειες που δεν μπορούν να ανευρεθούν μέσω επίσημων δίαυλων επικοινωνίας. Η δωρεάν πρόσβαση σε εφαρμογές κοινωνικού δικτύου, δίνει την ευκαιρία σε κάθε χρήστη να εμφανιστεί με την ταυτότητα και τα στοιχεία που προσδίδει ο ίδιος στον εαυτό του, με στόχο τη διασκέδαση του, την εξεύρεση φίλων, ατόμων με ίδια ενδιαφέροντα ή αντιλήψεις, αλλά να περιηγηθεί παρατηρώντας τις συμπεριφορές άλλων (Hughes *et al.*, 2016).

Ο αλγόριθμος που καταγράφει και προτείνει τους πιθανούς φίλους στο facebook, εξετάζει τα ενδιαφέροντα τις κοινές φιλίες και ομάδες και κατηγοριοποιεί τους χρήστες προτείνοντας τους άλλους χρήστες ως πιθανές επαφές. Η ευρεία διάδοση των μέσων κοινωνικής δικτύωσης στηρίζεται σε αυτή την επεξεργασία και κατηγοριοποίηση των δεδομένων των χρηστών του και αντλεί τη δυναμική της από τη δημοφιλία χρήσης της στον πληθυσμό ανά χώρα. Οι εφαρμογές χρήσης των κοινωνικών δικτύων, επιδιώκουν και αναζητούν την πρόσβαση σε όσον δυνατόν περισσότερους χρήστες όλων των ηλικιών, των κοινωνικών ομάδων και θρησκειών ακόμη και των πιο δύσκολα προσπελάσιμων τμημάτων του πληθυσμού και περιοχών του κόσμου. Η καταγραφή των κινήσεων και των κλήσεων από το κινητό τηλέφωνο του χρήστη, δίνοντας στίγμα της τοποθεσίας στην οποία βρίσκεται, αφενός είναι δυνατόν να τον βοηθήσει σε περίπτωση που κλαπεί το κινητό του τηλέφωνο, αφετέρου καταγράφονται τα σύνολα των δεδομένων των κινήσεων και κλήσεων του, τηρώντας το προσωπικό του ιστορικό αρχείο δεδομένων. Οι εφαρμογές χρήσης θέτουν αυτά υπό επεξεργασία, ώστε να προτείνουν προσωποποιημένα διαφημιστικά μηνύματα και να μεγιστοποιούν τις παρεχόμενες υπηρεσίες (Krafft, Gamer and Zweig, 2019). Τα δεδομένα αυτά, προσβάσιμα στην εταιρία κινητής τηλεφωνίας δύνανται να αποτελέσουν τη βάση για μελέτες κινητικότητας των πληθυσμών, θέτοντας σε λεπτές ισορροπίες την προστασία της ατομικής ελευθερίας του ατόμου²⁶. Από μια διαφορετική οπτική, η χρήση των δεδομένων

²⁶<https://inimareng.ee/en/open-to-the-world/tracking-trans-nationalism-with-mobile-telephone-data/>
(Ημερομηνία πρόσβασης 03-10-2020).

αυτών για ερευνητικούς σκοπούς προάγει την ελευθερία της σκέψης, του πνεύματος και τη νεωτερικότητα στην εξαγωγή ερευνητικών συμπερασμάτων. Ωστόσο η χρήση τους ως μεγάλα δεδομένα (big data) ιδιωτικών εταιριών, από παρόχους εταιριών κινητών τηλεφώνων, εταιρίες ταχυμεταφορών και όχι ως προσωπικά δεδομένα χρηστών, καθιστά το πλαίσιο διαπραγμάτευσης για την παροχή τους εφικτό. Με τον τρόπο αυτό, υπερσκελίζονται τυχόν νομικά εμπόδια που απέκλειαν τη χορήγησή και επεξεργασία τους ως συγκεντρωτικά στοιχεία προσωπικών δεδομένων.

Συγκεκριμένα η τεχνική πλατφόρμα του facebook αποθηκεύει δεδομένα για τη δημιουργία του προφίλ του χρήστη σύμφωνα με αυτοαναφερόμενα στοιχεία κατοικίας. Η κατοικία και η τοποθεσία φαγητού και διακοπών αποθηκεύονται και διανέμονται για ερευνητικούς σκοπούς όπως αντίστοιχα και οι άλλες πλατφόρμες κοινωνικής δικτύωσης. Η τακτική χρησιμοποίησης των πληροφοριών αυτών από τους επίσημους φορείς με στόχο το σχεδιασμό των στρατηγικών αποτύπωσης των μεταναστευτικών ροών παγκοσμίως, καταδεικνύει την ανάγκη για πλούσια και πηγαία πληροφόρηση ακόμη και αν αυτή υπόκειται σε αμφισβητήσιμα αυτοαναφορικά στοιχεία του χρήστη²⁷.

Ας μην παραλειφθεί το γεγονός ότι η διαχείριση των πληροφοριών που διακινούνται στο διαδίκτυο δεν αξιοποιείται από ιδιωτικές εταιρίες για την κάλυψη εμπορικών συμφερόντων των πολυεθνικών διαφημιστικών εταιριών. Η διοχέτευση των προσωπικών δεδομένων των χρηστών και κατ' επέκταση των συλλογικοτήτων παρέχεται και ενθαρρύνεται από επίσημους δίαυλους επικοινωνίας, με στόχο προληπτικά και κατασταλτικά μέτρα αποφυγής εγκληματικότητας, όπως αυτή οργανώνεται από μεταναστευτικές ροές (Shanker, 2019, σ.18). Ο έλεγχος των ατόμων που εισέρχονται σε ευρωπαϊκό έδαφος και η καταγραφή τους αποτελεί βασικό μέλημα της ευρωπαϊκής πολιτικής στα πλαίσια διαφύλαξης της εύρυθμης κοινωνικής και οικονομικής δομής των ευρωπαίων πολιτών. Ενδεικτικό αυτής της πολιτικής αποτελεί η υιοθέτηση από την Ευρωπαϊκή Επιτροπή λειτουργιών και διαδικασιών προστασίας των προσωπικών δεδομένων των ατόμων, προς ενίσχυση και ανάλυση των υφιστάμενων δικλείδων ασφαλείας κατά την είσοδο και καταγραφή των μετακινούμενων ατόμων σε ευρωπαϊκό έδαφος. Το 2019 η μεταρρύθμιση της νομοθεσίας της Ευρωπαϊκής Ένωσης για το σύστημα πληροφοριών Σένγκεν ενίσχυσε το ρόλο των τεχνολογιών αναγνώρισης προσώπου, δακτύλου και DNA, ενώ εισήγαγε επίσης ισχυρότερους κανόνες προστασίας των προσωπικών δεδομένων των μετακινούμενων ατόμων. Η καταγραφή στη

²⁷https://ec.europa.eu/knowledge4policy/migration-demography_en, <https://gmdac.iom.int/> (Ημερομηνία πρόσβασης 25-02-2020).

βάση δεδομένων Συστήματος Πληροφοριών Σένγκεν (SIS) χρησιμοποιώντας αναγνωριστικά έγγραφα ταυτοποίησης, η καταχώρηση μοναδικών αριθμών βάσης ανά μετακινούμενο άτομο, με τη συλλογή βιομετρικών δεδομένων δακτυλικών και παλαμικών αποτυπωμάτων αλλά και βιολογικού υλικού DNA για αστυνομική και δικαστική συνεργασία, ωθεί στη συλλογή και διοχέτευση ολόένα και αυξανόμενου όγκου πληροφοριών. Οι πιθανότητες διπλών ή λανθασμένων καταχωρήσεων εκμηδενίζονται, κατόπιν των διαδικασιών ελέγχου του συστήματος καταχώρησης. Οι αλγοριθμικές συνιστάμενες επικουρούν το διακλαδικό έλεγχο των δεδομένων που παρέχονται στο σύστημα, διευκολύνουν την ταυτοποίησή και την κατηγοριοποίησή τους. Στις περιπτώσεις που υφίστανται διαθέσιμα δεδομένα δακτυλικών αποτυπωμάτων, παρέχουν ειδοποιήσεις που σχετίζονται με αγνοούμενους, ενώ παράλληλα εγγυούνται την αξιοπιστία και καταλληλότητα χρήσης των παρεχόμενων προσωπικών δεδομένων (Ιστότοπος Ευρωπαϊκής Ένωσης, 2019).

Ωστόσο η καταγραφή και η χρήση των στοιχείων του προσώπου ως αναγνωριστικό ταυτότητας θέσης δημιουργεί ασυνέχεια ιδιωτικότητας στην κοινωνική δράση του κάθε ατόμου (Privacy discontinuity). Εγείρονται αμφιβολίες ως προς την αναγνώριση της θέσης και κίνησης των ατόμων ως στοιχείο της αποθήκευσης δεδομένων σε μια βάση αναγνώρισης στοιχείων-ατόμων, παρέχοντας με τον τρόπο αυτό απεριόριστη δύναμη και ευχέρεια αποτύπωσης των κινήσεων σε υπολογιστικά συστήματα. Η κίνηση των πολιτών στο εμπορικό κέντρο με τη χρήση βραχιολιού εντοπισμού, παρέχει ακριβή στοιχεία για τα καταστήματα στα οποία εισέρχεται, το είδος των ρούχων που αγοράζει καθώς και ποια από αυτά περιεργάζεται χωρίς να τα αγοράσει. Τα ελκυστικά πλεονεκτήματα και μηδαμινή χρέωση τους, διευκολύνει το άτομο, το οποίο για παράδειγμα αναρτά την φωτογραφία στο facebook με την επίδειξη του βραχιολιού που φέρει ο χρήστης. Το άτομο που περιφερόταν στο χώρο του εμπορικού κέντρου γίνεται αποδέκτης μηνυμάτων για την αγορά των προϊόντων, επισυνάπτοντας πλήρη στοιχεία εξυπηρέτησης, πλήρως προσαρμοσμένα στις προτιμήσεις του. Η καταγραφή και έλεγχος της κίνησης ατόμων, ο εντοπισμός των ατόμων όπως καταγράφεται από τις συσκευές, μετατρέπει το Internet στο «Internet of things». Αντίστοιχα το Google μπορεί να παρέχει στοιχεία θέσης και κίνησης πλήρως ενημερωμένα και διαμορφούμενα ανάλογα με τους αλγόριθμους αναζήτησης του κάθε χρήστη (Pariser, 2011, σ. 195–199).

Από την άλλη πλευρά, η χρήση των εφαρμογών αναγνώρισης προσώπου (Facial Recognition APIs & Software), είναι άκρως δελεαστική. Ο χρήστης αποδεσμευμένος από τους κωδικούς και τη χρήση καρτών για την πραγματοποίηση των αγοραστικών του

κινήσεων, μπορεί να απολαμβάνει την ευκολία και την αξιοπιστία της ταυτοποίησης προσώπου, δίχως τον κίνδυνο της υποκλοπής των προσωπικών του κωδικών ή καρτών. Οι πιο έγκυρες και διαδεδομένες εφαρμογές στον τομέα αυτό, διαφημίζουν την αξιοπιστία της ταυτοποίησης, με σεβασμό στα προσωπικά δεδομένα του χρήστη, σε συνδυασμό με τα οφέλη της αναγνώρισης προσώπου. Η χρήση των επιτευγμάτων αυτών μπορεί εύκολα να καταχραστεί με απτά παραδείγματα αυταρχικών καθεστώτων που συλλέγουν και κατηγοριοποιούν απευθείας τις κινήσεις του ατόμου²⁸.

²⁸<https://rapidapi.com/blog/top-facial-recognition-apis/> (Ημερομηνία πρόσβασης 25-02-2020).

ΚΕΦΑΛΑΙΟ 5 Οπτικές διαχείρισης της πληροφορίας

Η συγκέντρωση πληροφοριών για άτομα, στοιχεία ταυτότητας, κατοικίας, κινήσεις διαμονής, αγορές μέσω διαδικτύου, κοινωνικές επαφές και γενικότερα στοιχεία τα οποία, όπως ανωτέρω παρουσιάστηκε, εύκολα μοιράζεται ο χρήστης σε εφαρμογές κοινωνικών δικτύων, δύνανται με την κατάλληλη χωροθέτηση να υποστηρίξουν μαζικές ιδεολογίες και να κινητοποιήσουν κοινωνικές ομάδες, στοχοποιώντας αντίπαλες. Η κοινωνική δομή εύκολα εκτρέπεται και επηρεάζεται υπό το πρίσμα μιας υποτυπώδους κρίσης, βασιζόμενη σε ψευδείς ειδήσεις. Η ροή των πληροφοριών και η διάδοση τους εγκυμονεί κινδύνους και ρέπει την ομαδική καθοδήγηση σε μονοπάτια ακραία. Υπό αυτό το πρίσμα, ο νομοθέτης καλείται να ενεργοποιήσει το πλέγμα δράσεων προκειμένου να διαφυλάξει την κοινωνική δομή και ευταξία από εκκολαπτόμενο εκτροχιασμό.

5.1 Ριζοσπαστικοποίηση

Η λέξη *ριζοσπαστισμός*, και η έννοια της ριζοσπαστικοποίησης, δηλώνει τη δυναμική ενός κινήματος-κόμματος ή μιας ιδεολογίας, που αμφισβητεί την μετριότητα του συστήματος στο οποίο ανήκει, αντικρούοντας τους ισχύοντες κοινωνικούς κανόνες. Καθορίζει το μέτρο και τα όρια των πράξεων, υπερβαίνοντας τα με δηλώσεις αυξημένης προσήλωσης ακόμη και με τρόπο που αυτές απαιτούν την υιοθέτηση ακραίων τρόπων εκδήλωσής (Παπαδημητρίου, 2017, σ.9-33). Τα στάδια της βίαιης ριζοσπαστικοποίησης μπορούν να κατηγοριοποιηθούν ως ακολούθως, χωρίς ωστόσο να συνεπάγεται ότι η ριζοσπαστικοποίηση έχει ως μοναδική επαγωγή τον εξτρεισμό και τη βίαιη κατ' ανάγκη προσήλωση στο στόχο της κοινωνική υποταγής της ομάδας (Kemea brochure, 2016).

Τρομοκρατία

Βίαιος εξτρεμισμός

Νομιμοποίηση της βίας

Ανάληψη δράσης

Ένταξη σε Οργάνωση/Ομάδα

Ταύτιση με ριζοσπαστική ιδεολογία

Προσλαμβανόμενο αίσθημα αδικίας

Ως ένας γενικός ορισμός της ριζοσπαστικοποίησης θα μπορούσε να είναι ο κάτωθι: «ριζοσπαστικοποίηση είναι μια διαδικασία ανάπτυξης εξτρεμιστικών πεποιθήσεων, συναισθημάτων και συμπεριφορών. Οι εξτρεμιστικές πεποιθήσεις είναι βαθιές πεποιθήσεις,

που αντιτίθενται στις θεμελιώδεις αξίες της κοινωνίας, τους νόμους της δημοκρατίας και τα οικουμενικά ανθρώπινα δικαιώματα υποστηρίζοντας την υπεροχή μιας συγκεκριμένης ομάδας (φυλετικές, θρησκευτικές, πολιτικές, οικονομικές, κοινωνικές κ.λπ.)». Οι ορισμοί της ριζοσπαστικοποίησης συνήθως επικεντρώνονται σε δύο διαφορετικές εστίες: (i) στη βίαιη ριζοσπαστικοποίηση, όπου δίνεται έμφαση στην ενεργή επιδίωξη ή αποδοχή της χρήσης βίας για την επίτευξη του τιθέμενου στόχου, και (ii) σε μια ευρύτερη αίσθηση ριζοσπαστικοποίησης, όπου δίνεται έμφαση στην ενεργό επιδίωξη ή αποδοχή αλλαγών που προωθούνται στην κοινωνία, οι οποίες μπορεί να θέσουν σε κίνδυνο τη δημοκρατία, χωρίς αυτή να συνεπάγεται την απειλή ή χρήση βίας για την επίτευξη των τιθέμενων αυτών στόχων (Borum, 2011, σ. 8–12). Η έννοια της ριζοσπαστικοποίησης είναι πολύπλευρη και συγχέεται τις περισσότερες φορές με την τρομοκρατία ή θεωρείται πρώιμο στάδιο τρομοκρατικών δράσεων. Η ριζοσπαστικοποίηση ως η διαδικασία ανάπτυξης εξτρεμιστικών ιδεολογιών και πεποιθήσεων διαφοροποιείται από τον τρόπο έκφρασης της βίας και τη διαδικασία εμπλοκής σε τρομοκρατία ή βίαιες εξτρεμιστικές ενέργειες. Η υιοθέτηση ριζοσπαστικής ιδεολογίας δεν συνεπάγεται ότι αυτές θα εκφραστούν με βίαιες εξάρσεις. Η πιθανότητα οι αντιδράσεις να περιορίζονται στην ιδεολογική αντιπαράθεση και μόνο είναι υπαρκτή (Borum, 2011, σ.29-30).

Από την άλλη πλευρά, «Ο εξτρεμισμός αναφέρεται σε πολιτικές ιδεολογίες που αντιτίθεται στις βασικές αξίες και αρχές μιας κοινωνίας». Η έννοια του εξτρεισμού δεν αντιτίθεται σε συγκεκριμένη πολιτική ή κοινωνική ιδεολογία, αλλά αντιθέτως, υποστηρίζει κάθε ιδεολογία, που αναφέρεται στη φυλετική ή θρησκευτική υπεροχή και αντιτίθεται στον πυρήνα, στις αρχές της δημοκρατίας και των καθολικών ανθρωπίνων δικαιωμάτων, ως στοιχεία της κοινωνικής ιδεολογίας και συνοχής. (Neumann, 2010, σ. 873–893).

Αυτή η τάση ωθεί στη βίαιη έλλειψη σεβασμού στην ανθρώπινη ζωή, λογίζοντας την απώλεια της, ως μια παράπλευρη, ελάσσονος σημασίας απώλεια, τόσο για το θύτη όσο και για το θύμα. Παράλληλα εγείρονται σαφή ερωτηματικά για τις μεθόδους αποτελεσματικής στρατολόγησης των θυτών. Το ιδεολογικό υπόβαθρο υποστηρίζει και δικαιολογεί την κάθε δράση του ατόμου, που θεωρείται αναγκαία προς επίτευξη του τιθέμενου στόχου. Μετά τα γεγονότα της 11ης Σεπτεμβρίου 2001 (*CNN Ελλάδας*, 2018), με την εμφάνιση του φαινομένου της λεγόμενης “νέας τρομοκρατίας” και της σύνδεσης της με το θρησκευτικό εξτρεισμό, το φαινόμενο της ριζοσπαστικοποίησης αποτυπώνεται ως ένας ακραίος τρόπος εκδήλωσης των θρησκευτικών ή μη ιδεολογιών, προκαλώντας με τη χρήση βίας, το ενδιαφέρον του κοινού (Borum, 2011).

Σε πρώιμο στάδιο οι ενδείξεις που μπορούν να εξελιχθούν σε πλήρη αποδοχή της φιλοσοφίας εκδήλωσης ακραίων συμπεριφορών, εμφανίζονται σε εφήβους και μπορούν να ταυτιστούν με τη φυσιολογική αντιδραστική συμπεριφορά ενός εφήβου, χωρίς ωστόσο να θεωρηθούν ως παρεκκλίνουσες. Η διαδικτυακή συμπεριφορά του εναλλάσσεται με την παρακολούθηση σελίδων με συγκεκριμένο περιεχόμενο, ενώ η στάση του απέναντι σε διαφορετικά άτομα ή ομάδες ατόμων, μεταβάλλεται, παρατήρηση η οποία δεν αξιολογείται εκ προοιμίου ως ανησυχητική (*Signs of radicalisation*, 2020), (*Protecting children from radicalisation*, 2020). Η θεωρητική βάση του οικοδομήματος των συλλογικοτήτων αυτών, έχει ερείσματα κοινωνικά και ψυχολογικά, τα οποία ενεργοποιούνται υπό κοινούς παρονομαστές των μελών τους. Το αίσθημα των κοινών ιδεών, του κοινωνικού και πολιτικού υπόβαθρου, των ακραίων ή μη αντιλήψεων σε συγκεκριμένα θέματα, προσελκύει το ενδιαφέρον των αρχηγών τους που στρατολογούν νέα μέλη. Προκειμένου να πολλαπλασιαστεί ο αντίκτυπος των δράσεων της ομάδας και να διαδοθεί η υποστηρίζουσα ιδεολογία τους ο προσηλυτισμός νέων μελών των συλλογικοτήτων αυτών, εν πρώτης απευθύνεται στο άμεσο περιβάλλον του χρήστη. Η μεθοδολογία προσέγγισης των νέων μελών στοχεύει στην εύρεση και προσέγγιση και προσηλυτισμό ατόμων-χρηστών των οποίων το προφίλ προσομοιάζει με τις αντιλήψεις της ομάδας. Ο έλεγχος στις κοινές επαφές-στοιχεία του, είναι στη διάθεση της ομάδας, μέσω των εφαρμογών κοινωνικής δικτύωσης και λαμβάνοντας υπόψη ότι η πλειονότητα των χρηστών αυτοπροσδιορίζεται εκθέτοντας προσωπικές τους ιδέες και δεδομένα απευθείας, επεκτείνοντας την αναζήτηση σε εναλλακτικούς τρόπους άντλησης δεδομένων όπως αυτά καταγράφονται στις εφαρμογές κοινής δικτύωσης (McCauley and Moskalenko, 2008). Η Ευρώπη αντιμετωπίζει μια υψηλή και εξελισσόμενη τρομοκρατική απειλή, όπως αποδεικνύεται από την αύξηση των τρομοκρατών τα τελευταία χρόνια, με επιθέσεις, θανάτους και καταδικαστικές αποφάσεις για τρομοκρατία. Το 2016, συνολικά αναφέρθηκαν 142 απόπειρες και τελεσμένες τρομοκρατικές επιθέσεις. Κατά το 2017, 16 επιθέσεις έπληξαν οκτώ διαφορετικά κράτη μέλη ενώ περισσότερα από 30 περιπτώσεις απέτυχαν (European Union, 2017). Η ριζοσπαστικοποίηση όπως αυτή οδηγεί σε βίαιο εξτρεμισμό και τρομοκρατία, δεν είναι περιορισμένο φαινόμενο σε ένα μόνο κράτος μέλος αλλά επεκτείνεται στην ευρωπαϊκή γειτονιά ως σύνολο, γεγονός που επιτάσσει την αναπροσαρμογή των πολιτικών δράσης ανά περίπτωση. Το αυξανόμενο ρεύμα με στόχευση σε ριζοσπαστικές εξάρσεις, δεν έχει καταγραφεί με επίσημα στοιχεία του αριθμού των ριζοσπαστικοποιημένων ατόμων που ζουν και βρίσκονται στα κράτη μέλη της Ευρωπαϊκής Ένωσης (Dankert, 2017). Ωστόσο, από τα συλλεχθέντα στοιχεία σε εθνικό

επίπεδο των κρατών μελών, προκύπτει ότι περίπου 20.000 άτομα, βρίσκονται στη Γαλλία, ενώ στο Ηνωμένο Βασίλειο υπάρχουν πληροφορίες για πάνω από 20.000 άτομα. Αντίστοιχα οι γερμανικές αρχές ασφαλείας, έχουν αναφέρει 11.000 Salafists²⁹ (Joas Wagemakers, 2016), με ροπή στη βία και το τρομοκρατικό φάσμα, μεταξύ των οποίων ένα μικρότερο ποσοστό εκτιμάται ως ιδιαίτερα «επικίνδυνο». Αξίζει να σημειωθεί ότι σύμφωνα με τις διαθέσιμες αξιολογήσεις απειλών, παρατηρείται μια αυξητική τάση του δεξιού εξτρεμισμού που προωθεί τον αντιδημοκρατισμό, τη μισαλλόδοξα και διχαστικά μηνύματα, που τροφοδοτούν το βίαιο εξτρεμισμό και οδηγούν στην πόλωση (European Commission, 2018), (Widiawati, 2020).

Στην προσπάθεια να μελετηθεί η ανθρώπινη αυτή συμπεριφορά, ως φαινόμενο που καταδεικνύει μεγάλη απαξία στην ανθρώπινη ζωή, υφίσταται εκτεταμένη βιβλιογραφία και έρευνα για τον λόγο και την αιτία της πρόκλησης των εξτρεμιστικών και ριζοσπαστικών εξάρσεων, αναλύοντας τις ψυχολογικές καταβολές του ατόμου. Η αστάθεια στην κοινωνική συνοχή αποτυπώνεται σε ακραίες εκδηλώσεις βίας, με κοινωνικό και πολιτικό υπόβαθρο. Εκτιμάται ότι η βίαιη συμπεριφορά είναι αποτέλεσμα ψυχολογικών μηχανισμών που θέτουν τους ανθρώπους στην ευάλωτη θέση να πιστεύουν στη ριζοσπαστικοποιημένη ιδεολογία και αντιστρόφως, υφίστανται ψυχολογικοί μηχανισμοί που εμποδίζουν τους ανθρώπους να συμμετάσχουν σε αυτήν (Trip *et al.*, 2019), (Neumann, 2013). Μέσα στο πλαίσιο αυτό και με στόχο την πρόληψη των βίαιων εξάρσεων, οι κυβερνήσεις τείνουν να χαράζουν την πολιτική τους, συλλέγοντας στοιχεία θέσης και κίνησης των πολιτών τους, με στόχο την άμεση ενημέρωσή τους για τις κινήσεις τους, τις επαφές τους, την όποια μετεγκατάστασή τους, ιδίως στις περιπτώσεις ξένων τρομοκρατών.

Οι δυνατότητες που παρέχει η τεχνολογία παράλληλης διακίνησης μη ανιχνεύσιμων και αθρόων πληροφοριών σε κανάλια επικοινωνίας με βαθμό εμπιστευτικότητας, επιτρέπει τη δημιουργία ομάδων χρηστών με κοινές αντιλήψεις. Η πυραμοειδής διάρθρωσή τους, σε συνδυασμό με την ευελιξία και αμεσότητα που προσφέρει το διαδίκτυο, προσελκύει νέους χρήστες-οπαδούς, ενισχύοντας τη δυναμική της ομάδας κατά την οργάνωση των δράσεων των υφιστάμενων μελών της. Η χρήση των μέσων κοινωνικής δικτύωσης και η έρευνα στο προφίλ του χρήστη, επικουρούν τον προσηλυτισμό νέων χρηστών, ως μια ασφαλής μέθοδος επικοινωνίας και προσέγγισης, αποφεύγοντας το εμπόδιο της ανωνυμίας. Οι αναρτήσεις του χρήστη με ακραίο ή ριζοσπαστικό περιεχόμενο, οι κοινωνικοπολιτικές του πεποιθήσεις,

²⁹ «Σαλαφισμός είναι ένας κλάδος του σουνιτικού Ισλάμ, του οποίου οι σύγχρονοι οπαδοί ισχυρίζονται ότι μιμούνται τους «ευσεβείς προκάτοχους»

δραστηριοποιούν τους διαχειριστές της ομάδας, να ελέγξουν το προφίλ του και στη συνέχεια να τον προσεγγίσουν. Η ανωνυμία που προσφέρουν τα μέσα κοινωνικής δικτύωσης και η ελευθερία έκφρασης των απόψεων του χρήστη, επιτρέπει σε έναν επίδοξο διαχειριστή ομάδας να διακρίνει την όποια συσχέτισή του χρήστη με το ιδεολογικό προφίλ της (Ledingham and Mills, 2015, σ.6), (Kennedy, 2020, σ.223-237). Επιπλέον η συναισθηματική εγγύτητα και η κοινή αποδοχή των θέσεων της ομάδας, προσφέρει συναισθηματική ικανοποίηση και ενθάρρυνση στο άτομο που συμμετέχει σε αυτήν και ενστερνίζεται τις κοινές θέσεις των μελών της, πραγματώνοντας την έννοια της ιδέας του “ubuntu”, ήτοι την έννοια της φράσης κατά την αφρικανική ιδεολογία, «το να υπάρχουν σημαίνει να ανήκεις» (στην ομάδα) (Κανελλοπούλου-Μπότη, 2012). Η σφυρηλάτηση συλλογικών ταυτοτήτων και αντιλήψεων μεταξύ των μελών της ομάδας αποτελεί τη βάση επίτευξης διαρκούς και βίαιης κινητοποίησης των μελών της. (Joel Busher, 2015).

Πέραν αυτού, η καταγραφή των δεδομένων θέσης του χρήστη, δύναται να διευκολύνει τη στοχοθεσία δράσεων σε ένα συγκεκριμένο τόπο και την έναρξη διασύνδεσης με άλλους ενεργούς πυρήνες δράσης, συσπειρώνοντας ταχύτατα τα μέλη της ομάδας, με τη χρήση κρυπτογραφημένων κωδικών επικοινωνίας. Οι μετακινήσεις των ηγετών των ομάδων αυτών, ανά περιοχή, σηματοδοτούν για τα λοιπά μέλη τους την συσπείρωσή τους ανά περίπτωση, ενεργοποιώντας το ανενεργό μέχρι τη στιγμή αυτή, πλέγμα διασύνδεσής τους. Η τυχόν απομόνωση τους κατά το διάστημα εγκλεισμού τους σε σωφρονιστικό ίδρυμα και η διακριτική παρακολούθηση των μετακινήσεών τους, από επίσημους φορείς, μπορεί να συντελέσει προληπτικά ως ειδικό προειδοποιητικό σήμα για μια επικείμενη βίαιη εκδήλωση της ομάδας. Στο παράδειγμα των οργανωμένων ομάδων με χαρακτηριστικό, τη θρησκευτική τους ιδεολογία, η ανακατεύθυνση των πληθυσμιακών ομάδων-μελών και η χειραγώγησή τους από τα ηγετικά στελέχη, είναι στενή και άμεση, καταδεικνύοντας την άρρηκτη σχέση εξάρτησης των μελών, που τους οδηγεί σε ακραίες εκδηλώσεις βίας με ριζοσπαστικές εξάρσεις, μόλις δοθεί το εναρκτήριο σήμα (European Commission, 2020), (European Commission, 2018).

5.2 11η Σεπτεμβρίου

Η 11^η Σεπτεμβρίου αποτελεί την απαρχή της σύγχρονης τρομοκρατικής δράσης, όπως αυτή αποτυπώθηκε ακραία με την ριζοσπαστική επίθεση και αποτέλεσμα το αδιάκριτο θάνατο 2.998 ατόμων. Η ζημιά που προκλήθηκε πέρα από το κόστος της ανθρώπινης ζωής εκτιμάται και σε οικονομικά μεγέθη. Το 30% των γραφείων στο Κάτω Μανχάταν

καταστράφηκαν, το κόστος διάσωσης των αγνοουμένων, των τραυματιών αλλά και η καταστροφή των περιουσιακών στοιχείων των εταιριών, υπολογίζεται πάνω από 22δισ. δολάρια. Χαρακτηριστικό αυτών είναι ότι η οικονομική ζημία αποτυπώθηκε από την Wall Street με το άνοιγμα της μειωμένη περί τα 1,3 τρις. δολάρια (15% της χρηματιστηριακής της αξίας). Μακροπρόθεσμα και οι τομείς των αερομεταφορών είχαν υποστεί πλήγμα με τη μείωση των εσόδων τους, πλήττοντας τους οικονομικούς δείκτες της χώρας. Ωστόσο πέρα των οικονομικών μεγεθών που καταδεικνύουν το μέγεθος της οικονομικής και κοινωνικής καταστροφής, η ύπαρξη του κλίματος φόβου, ήταν η αρχή για την καλλιέργεια μιας κουλτούρας φόβου. Στόχος είναι η πρόκληση φόβου στους κόλπους της κοινωνίας που ανατροφοδοτεί τα ριζοσπαστικά φαινόμενα και τις ακραίες εξάρσεις βίας και διαχέεται αδιακρίτως. Οι επιθέσεις με χρήση άνθρακα στις εβδομάδες που ακολούθησαν της 11^{ης} Σεπτεμβρίου που είχαν ως αποτέλεσμα να διακοπεί προσωρινά η λειτουργία της Βουλής της Γερουσίας, είναι ενδεικτικές της διάθεσης να αναπτυχθεί η κουλτούρα φόβου και κοινωνικής αναστάτωσης στο μεγαλύτερο μέρος του πληθυσμού (Criado and Gil-garcia, 2019, σ. 426).

Με γνώμονα τα ανωτέρω, κρίθηκε επιβεβλημένη η αναπροσαρμογή των διατάξεων και των μέτρων ασφαλείας που λαμβάνουν οι κυβερνήσεις για τους πολίτες τους. Στις περιπτώσεις αυτές που το δημόσιο συμφέρον υπερτερεί, η προσωπική προστασία των ατομικών ελευθεριών παρακάμπτεται και αμβλύνεται η όποια παραβίαση στη σφαίρα των προσωπικών δεδομένων τηλεφωνικών κλήσεων, καταγραφής κίνησης και δεδομένων θέσης, αυξάνοντας την επιτήρηση των πολιτών αλλοδαπών ή ημεδαπών (Images, 2020). Υπό το φως της αναταραχής προς εξασφάλιση της κοινωνικής ηρεμίας και συνοχής και προκειμένου να αντιμετωπιστεί η περιρρέουσα ανασφάλεια των πολιτών έναντι στην αδιάκριτη βία, η κυβερνητική πρόθεση αποτυπώθηκε στο Patriot Act (Government, 2020), με το οποίο το Κογκρέσο έδωσε στο FBI και την NSA (Cybersecurity, 2020) νέες δυνατότητες να συλλέγουν και να μοιράζονται δεδομένα. Συγκεκριμένα, παρέχονταν η ευχέρεια στις υπηρεσίες πληροφοριών αναζήτησης αρχείων βιβλιοθήκης του ατόμου, του ιστορικού αναζήτησης του στο διαδίκτυο με μικρή δικαστική επίβλεψη και παραγκωνίζοντας τις δικλίδες ασφαλείας υποχρεωτικής απόδειξης και δικαιολόγησης του είδους και του λόγου της διερεύνησης ή διασύνδεσης του ατόμου με συγκεκριμένη ερευνούμενη υπόθεση. Συνέχεια αυτού, το 2008 δόθηκε η ευχέρεια, κατόπιν νομοθετικής πρόβλεψης (Foreign intelligence surveillance Act of 1978 Amendments Act of 2008-FISA) στις αμερικανικές αρχές να παρακολουθούν αμερικανικές τηλεφωνικές κλήσεις, μηνύματα κειμένου και μηνύματα ηλεκτρονικού ταχυδρομείου αμερικανών πολιτών, αλλά και ατόμων εκτός Η.Π.Α., υποχρεώνοντας τις

εταιρείες παροχής τηλεπικοινωνιακής κάλυψης σε συνεργασία (Arrigo, 2018), στοχοποιώντας ξένους υπηκόους ως ύποπτους για τρομοκρατία.

Η πράξη επέκτεινε επίσης τη διάταξη «μοναχικός λύκος» του Νόμου για τη μεταρρύθμιση των πληροφοριών και την πρόληψη της τρομοκρατίας του 2004, το οποίο επέτρεψε στο Foreign Intelligence Surveillance Court (FISC)³⁰, να επιτρέψει την επιτήρηση και τις φυσικές αναζητήσεις που απευθύνονται σε αλλοδαπούς υπηκόους που «εμπλέκονται σε διεθνή τρομοκρατία ή δραστηριότητες προετοιμασίας για διεθνείς τρομοκράτες» (Duignan, 2001). Παράλληλα οι ΗΠΑ, στον απόηχο του τρομοκρατικού χτυπήματος, επέλεξαν να αυστηριοποιήσουν το επίπεδο εποπτείας και επιτήρησης, με στόχο την πρόληψη, τον εντοπισμό και τη δίωξη της διεθνούς νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας, αλλά κυρίως και τον έλεγχο των αλλοδαπών οι οποίοι ενδεχομένως αποτελέσουν τον πυρήνα για μια νέα τρομοκρατική επίθεση. Η εξεύρεση των πόρων που τροφοδότησε το χτύπημα αυτό κρίθηκε ως βασικό μέλημα και αποτυπώθηκε σε ένα αυστηρό νομοθέτημα που θα υποχρεώνει τις επιχειρήσεις να αναφέρουν και να παρέχουν επαρκή στοιχεία του κλάδου των χρηματοοικονομικών υπηρεσιών τους, προκειμένου να αποφευχθεί η πιθανή νομιμοποίηση εσόδων από παράνομες δραστηριότητες (Government, 2020).

Γίνεται εύκολα διακριτό, ότι η ιδεολογία του φόβου, η ανάγκη διαφύλαξης της δημόσιας σταθερότητας κατά το χρονικό διάστημα αυτό καθώς και η αναγκαιότητα αποτροπής διάπραξης παρόμοιων περιστατικών, οδήγησαν τις ΗΠΑ στην ενεργοποίηση του νομοθετικού τους οπλοστασίου για την προστασία των πολιτών τους, έναντι της προστασίας των ατομικών και προσωπικών δεδομένων και ελευθεριών των μεταναστών και ατόμων που μπορούν να θεωρηθούν ύποπτα για τρομοκρατία. Το γεγονός της 11^{ης} Σεπτεμβρίου και η διαχείριση του από τις ΗΠΑ, αν και δεν αποτελεί το παράδειγμα ψύχραιμης εκδήλωσης των απαιτούμενων ενεργειών, ωστόσο μπορεί να περιγραφεί ως μια κατάσταση «κρίσης», και αποτελεί ενδεικτικό της άμεσης διασύνδεσης και ανάπτυξης του πληροφοριακού δικτύου των δεδομένων που διακινούνται και δύνανται ανά πάσα στιγμή να αντληθούν και να αξιοποιηθούν αναφορικά με συγκεκριμένα άτομα ή ομάδες ατόμων χρησιμοποιώντας για το σκοπό αυτό κάθε πρόσφορο τεχνολογικό μέσο (Roger, 2018), (Degeling *et al.*, 2010).

³⁰<https://www.fisc.uscourts.gov/> (Ημερομηνία πρόσβασης 13-02-2020).

ΕΠΙΛΟΓΟΣ

Η διασταλτική χρησιμότητα του διαδικτύου και η επεκτατική του δράση σε όλο το φάσμα της ανθρώπινης δραστηριότητας στη σύγχρονη εποχή, καθιστά την ανάγκη αναπροσαρμογής του νομοθετικού πλαισίου που διέπει τη χρήση του, επιτακτική. Η πληροφορία πλέον δεν διακινείται αποκλειστικά με τις παραδοσιακούς μεθόδους αλλά διαχέεται από τα διαδικτυακά κανάλια επικοινωνίας. Ο προβληματισμός για την αποτελεσματικότητα της προστασίας του χρήστη είναι υπαρκτός. Η διαδραστικότητα και η ταχύτητα διαμοιρασμού των δεδομένων των χρηστών, καθιστά τους κατόχους αυτής, ανίσχυρους να ελέγξουν ακόμη και τα προσωπικά στοιχεία που διαμοιράζουν άθελα τους ή μη. Από την άλλη πλευρά, οι επιχειρήσεις έχοντας εντοπίσει την κερδοφόρα πτυχή της διακίνησης της πληροφοριών έχουν δραστηριοποιηθεί για την αξιοποίησή τους στο έπακρο προς όφελός τους.

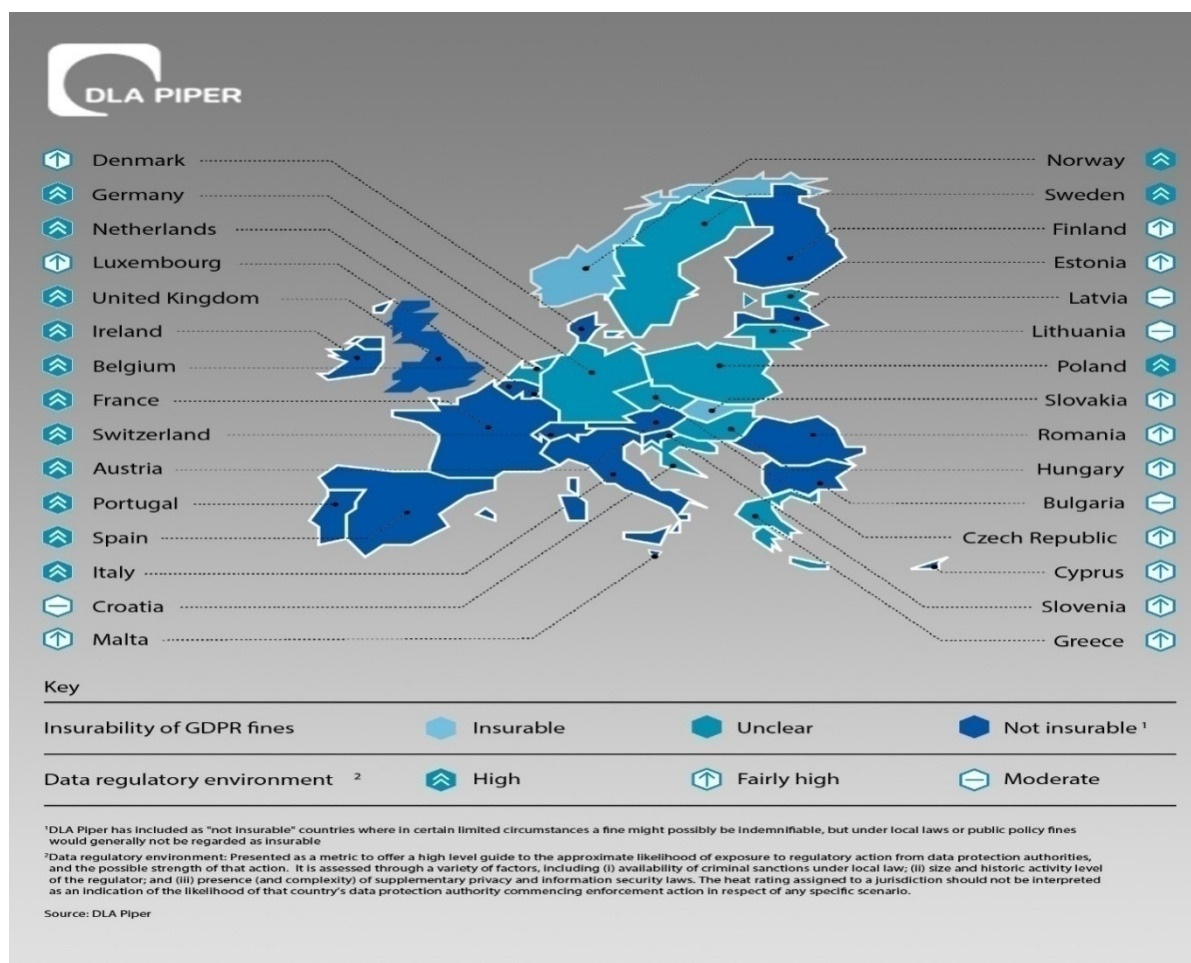
Στο αντίποδα οι κυβερνητικές πηγές συσσωρεύουν λόγω του θεσμικού στους ρόλου, το σύνολο των πληροφοριών που διακινούνται από τους χρήστες, τις οποίες επιλέγουν να μοιραστούν προς εξυπηρέτησή τους και να παράσχουν πρόσβαση, στο πλαίσιο της ηλεκτρονικής διακυβέρνησης και ευελιξίας. Ο τρόπος που οι πληροφορίες αυτές αξιοποιούνται από κρατικούς διαύλους επικοινωνίας, υποδηλώνει και καθορίζει τις μακροπρόθεσμες στρατηγικές δράσεις, με κύριο παράγοντα τη μελέτη και πρόβλεψη των μεταναστευτικών ροών, ως ένα υπαρκτό φαινόμενο παγκοσμίως. Οι κοινωνικοοικονομικές ανισορροπίες που μπορούν να προκληθούν από την αθρόα μεταναστευτική κίνηση, αποτελούν ισχυρό παράγοντα αποσταθεροποίησης για τις κοινωνίες. Αντίστοιχα αποτελέσματα μικρότερης έκτασης και έντασης δύναται να προκαλέσει ο αντίκτυπος και η φοβοκρατία, ένεκα της εμφάνισης ριζοσπαστικών εξάρσεων. Η διαχείριση των φαινομένων αυτών υπαγορεύει άμεσες και αποτελεσματικές δράσεις από το σύνολο των κυβερνήσεων που πλήττονται, με σύμπραξη περισσότερου του ενός κράτους. Η κοινή μελέτη και η άντληση των εν λόγω ζητημάτων, υπαγορεύει μεθοδεύσεις και συλλογή πληροφοριών για άτομα, τη δράση τους, τα δεδομένων θέσης και τηλεφωνικών κλήσεων τους, με στόχο την προάσπιση της κοινωνικής ευνομίας.

Σε κάθε περίπτωση, η θέσπιση ισχυρών και εφαρμόσιμων περιορισμών χρήσης των δεδομένων που διαμοιράζονται από τους χρήστες του διαδικτύου εκούσια ή ακούσια, κατοχυρώνει την ελευθερία της έκφρασης, της αυτοδιάθεσης και αποτελεί τον πυρήνα των συνταγματικών κατοχυρωμένων ελευθεριών ανάπτυξης της προσωπικότητας του ατόμου. Η κατοχύρωση αυτή, είναι θεμιτό τεθεί σε ενιαία βάση για το σύνολο των ιδιωτικών ή κρατικών

φορέων, με απώτερο στόχο τη διαφύλαξη της ιδιωτικότητας του ατόμου σε κάθε έκφανση της προσωπικότητάς του.

Το εν λόγω νομοθετικό πλέγμα κρίνεται θεμιτό να επικουρείται από τις Αρχές προστασίας δεδομένων προσωπικού χαρακτήρα, οι οποίες δύνανται να εντείνουν τις δράσεις τους και να καλλιεργήσουν τη φιλελεύθερη νοοτροπία προστασίας των δεδομένων προσωπικού χαρακτήρα, προωθώντας μέσω διασυννοριακών δράσεων, τη διεξαγωγή κοινών ερευνών τόσο στα κράτη μέλη της Ευρωπαϊκής Ένωσης αλλά και εκτός αυτής, στοχεύοντας στην αμερόληπτη εφαρμογή του νομοθετικού πλαισίου σε κάθε περίπτωση, υποδεικνύοντας μεταξύ άλλων και στις επιχειρήσεις, την υποχρέωση αναπροσαρμογής των πρακτικών τους, προκειμένου να περιφρουρηθεί η ασφάλεια των δεδομένων τους και να θεμελιώσουν με τον τρόπο αυτό την προστασία της ιδιωτικής ζωής ως ανταγωνιστικό πλεονέκτημα.

ΠΑΡΑΡΤΗΜΑ



Εικόνα 3: Το ρυθμιστικό περιβάλλον προστασίας των δεδομένων στην Ευρώπη

<https://www.dlapiper.com/de/austria/insights/publications/2020/05/third-edition-of-guide-on-the-insurability-of-gdpr-fines-across-europe/>

ΒΙΒΛΙΟΓΡΑΦΙΑ

Aaronson, S. (2015) *Why Trade Agreements are not Setting Information Free*, *World Trade Review*. doi: 10.1017/S1474745615000014.

Amanda, A. (2018) *Protect, serve and deport*, *NIVERSITY OF CALIFORNIA PRESS*. Available at: <http://dx.doi.org/10.1016/j.cirp.2016.06.001><http://dx.doi.org/10.1016/j.powtec.2016.12.055><https://doi.org/10.1016/j.ijfatigue.2019.02.006><https://doi.org/10.1016/j.matlet.2019.04.024><https://doi.org/10.1016/j.matlet.2019.127252><http://dx.doi.o>.

Arrigo, B. A. (2018) 'Foreign Intelligence Surveillance Act', *The Sage Encyclopedia of surveillance, security and privacy*. doi: 10.4135/9781483359922.n177.

Banisar, D. (2004) 'Freedom of information and access to government record laws around the world', σ. 1–96.

Beezy, B. M. C. and Lucas, S. A. (2018) 'Compliance with the eu's general data protection regulation and us discovery law', σ. 1–17. Available at: https://www.inta.org/Advocacy/Documents/2017/Article - Compliance with the EU_S General Data Protection Regulation and US Discovery Law.pdf.

Betts, K. J. (2014) 'Multicultural muddles transforming a white Australia: Issues of Racism and immigration', (January 2012).

Board, E. D. P. (2020) 'Κατευθυντήριες γραμμές 5/2020 σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679', σ. 1–40.

Borum, R. (2011) 'Radicalization into Violent Extremism I: A Review of Social Science Theories', *Journal of Strategic Security*, 4(4), σ. 7–36. doi: 10.5038/1944-0472.4.4.1.

Bottis, M. C. (2009) *Η προστασία της ιδιωτικής ζωής και η ευρωπαϊκή νομοθεσία για τα προσωπικά δεδομένα σκέψεις σε σχέση με την πορεία της προστασίας της ιδιωτικής ζωής στις ΗΠΑ*. Bottis, Maria C.

Brown, T. L. (2019) 'Ambient Intelligence Changes the Office Environment', in Gordon, P. A. and Overbey, J. A. (eds) *Advances in the Technology of Managing People: Contemporary Issues in Business*. Emerald Publishing Limited, σ. 149–160. doi: 10.1108/978-1-78973-073-920191013.

Bujlow, T. *et al.* (2017) 'A Survey on Web Tracking: Mechanisms, Implications, and

Defenses’, *Proceedings of the IEEE*, 105(8), σ. 1476–1510. doi: 10.1109/JPROC.2016.2637878.

Bylykbashi, K. *et al.* (2018) ‘Implementation and evaluation of an ambient intelligence testbed’, *International Journal of Web Information Systems*. Emerald Publishing Limited, 14(1), σ. 123–135. doi: 10.1108/IJWIS-12-2017-0082.

Byun, C. *et al.* (2013) ‘Twitter data collecting tool with rule-based filtering and analysis module’, *International Journal of Web Information Systems*, 9(3), σ. 184–203. doi: 10.1108/IJWIS-04-2013-0011.

California Consumer Privacy Act (CCPA) (2019) *State of California Department of Justice*. Available at: <https://www.oag.ca.gov/privacy/ccpa> (Accessed: 11 September 2020).

California S.B. 27, S. the L. L. (2020) *California, ‘Shine the Light’ Law*, <https://epic.org/>. Available at: <https://epic.org> (Accessed: 15 September 2020).

Carvajal Nikki, K. C. (2020) ‘Trump issues orders banning TikTok and WeChat from operating in 45 days if they are not sold by Chinese parent companies’, *CNN*. Available at: <https://edition.cnn.com/2020/08/06/politics/trump-executive-order-tiktok/index.html>.

Chaqfeh, M. A. and Mohamed, N. (2012) ‘Challenges in middleware solutions for the internet of things’, *Proceedings of the 2012 International Conference on Collaboration Technologies and Systems, CTS 2012*, (May), σ. 21–26. doi: 10.1109/CTS.2012.6261022.

China and the Internet (2014) *Frontline*. Available at: <https://www.pbs.org/wgbh/pages/frontline/shows/red/roundtable/internet.html> (Accessed: 25 September 2020).

*CNN Ελλάδα*ς (2018) ‘11η Σεπτεμβρίου 2001: Η μέρα που άλλαξε τον κόσμο’, p. 1. Available at: <https://www.cnn.gr/news/kosmos/story/146266/11i-septemvrioy-2001-h-mera-poy-allaxe-ton-kosmo> (Accessed: 1 June 2020).

Committee to Protect Journalists (2011) *Zimbabwe hikes media fees under draconian media law*, *Committee to Protect Journalists*. Available at: <https://cpj.org/2011/01/zimbabwe-hikes-media-fees-under-draconian-media-la/> (Accessed: 10 February 2020).

Criado, J. I. and Gil-garcia, J. R. (2019) ‘Creating public value through smart technologies and strategies and beyond’, 32(5). doi: 10.1108/IJPSM-07-2019-0178.

Cybersecurity (2020) <https://www.nsa.gov/What-We-Do/Cybersecurity/>. Available at:

<https://www.nsa.gov/What-We-Do/Cybersecurity/> (Accessed: 16 December 2020).

Cybersecurity Legislation 2020 (2020). Available at: <https://www.ncsl.org/> (Accessed: 18 September 2020).

Dankert, A. C. (2017) *Europe under Pressure*. Bd. 9. Deutsche Nationalbibliothek.

Davies, H. C. and Eynon, R. (2018) ‘Is digital upskilling the next generation our “pipeline to prosperity”?’ , *New Media and Society*, 20(11), σ. 3961–3979. doi: 10.1177/1461444818783102.

Davies, T. and Fumega, S. (2014) ‘Mixed incentives : Adopting ICT innovations for’, (4), σ. 1–24. Available at: <http://www.cmi.no/publications/file/5172-mixed-incentives.pdf>.

‘Definition - What does Data Filtering mean?’ (2020) *techopedia*. Available at: <https://www.techopedia.com/definition/26202/data-filtering> (Accessed: 6 August 2020).

Degeling, M. *et al.* (2010) ‘On the vagueness’, (Morris 2012), σ. 1–20.

DLA Piper (2017) ‘DATA PROTECTION Full Handbook’, (April 2017).

Duignan, B. (2001) ‘USA PATRIOT Act’, <https://www.britannica.com/topic/USA-PATRIOT-Act>. 1st edn. Available at: <https://www.britannica.com/topic/USA-PATRIOT-Act>.

Dukakis, A. (2020) ‘China rolls out software surveillance for the COVID-19 pandemic, alarming human rights advocates’, *abc.net.au.news*. Available at: <https://abcnews.go.com/International/china-rolls-software-surveillance-covid-19-pandemic-alarming/story?id=70131355>.

Dutton, W. H. and Graham, M. (2014) ‘Reconfiguring Access and the Societal Implications of the Internet’, σ. 28.

Encyclopaedia, T. editors of (2020) ‘Uighur’, *Britannica*. britannica. Available at: <https://www.britannica.com/topic/Uighur>.

European Commission (2002) ‘Οδηγία 2002/58/ εκ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου’, *Επίσημη Εφημερίδα Των Ευρωπαϊκών Κοινοτήτων*. Available at: http://ec.europa.eu/justice/data-protection/law/files/recast_20091219_el.pdf.

European Commission (2018) *High-Level Commission Expert Group on Radicalisation*. doi: 10.2837/050920.

European Commission (2020) *Schengen Information System*. Available at:

https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en (Accessed: 2 January 2021).

European Union (2017) *Terrorism situation and trend report*. doi: 10.2813/237471.

“‘Fake news’: Greece rejects Turkey’s claims its forces killed a migrant trying to cross border’ (2020) *abc.net.au.news*. Available at: <https://www.abc.net.au/news/2020-03-05/turkey-says-greek-forces-killed-migrants-trying-to-cross-border/12026950>.

Falkenheim, Victor C. and Hsieh, C.-M. (2018) ‘Xinjiang’, *Britannica*. britannica. Available at: <https://www.britannica.com/place/Xinjiang>.

Federal Trade Commission (2002) ‘Protecting Children’ s Privacy Under COPPA : a Survey on Compliance’, (April).

Government, O. website of the U. S. (2020) *USA PATRIOT Act, An official website of the United States Government*. Available at: <https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act> (Accessed: 11 December 2020).

Hughes, C. *et al.* (2016) *Inferring Migrations: Traditional Methods and New Approaches based on Mobile Phone, Social Media, and other Big Data: Feasibility study on Inferring (labour) mobility and migration in the European Union from big data and social media data, Report for the European Commission*. Available at: https://eprints.soton.ac.uk/408499/1/KE0216632ENN_002.pdf.

Images, D. A. (2020) *5 Ways September 11 Changed America*, <https://www.history.com/news/september-11-changes-america>.

Information National Freedom of Coalition. (2020) *California FOIA Laws*. Available at: <https://www.nfoic.org/coalitions/state-foi-resources/california-foia-laws> (Accessed: 12 March 2021).

James Griffiths (2017) *The ideological war playing out on China’s internet*, CNN. Available at: <https://edition.cnn.com/2017/10/15/asia/china-party-congress-internet-censorship/index.html> (Accessed: 10 August 2020).

Jennifer Alsever (2020) *What is Crowdsourcing?*, CBS NEWS. Available at: <https://www.cbsnews.com/news/what-is-crowdsourcing> (Accessed: 19 February 2021).

Joas Wagemakers (2016) ‘Salafism’. doi: <https://doi.org/10.1093/acrefore/9780199340378.013.255>.

Joel Busher (2015) ‘What part do social networks play in radicalisation?’, <https://www.radicalisationresearch.org/>. Available at: <https://www.radicalisationresearch.org/debate/busher-social-networks/>.

John Carr, D. (2015) *The relevant text – and age verification puts in an appearance*. Available at: <https://johncarr.blog/2015/12/16/the-relevant-text-and-age-verification-puts-in-an-appearance/> (Accessed: 5 April 2021).

Kadelbach, S. (2013) ‘Charter of Fundamental Rights of the European Union (2000)’, *Max Planck Encyclopedia of Public International Law*, σ. 391–407. doi: 10.1093/law:epil/9780199231690/e1864.

Kari Paul (2020) *California’s groundbreaking privacy law takes effect in January. What does it do?*, <https://www.theguardian.com/>. Available at: <https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do> (Accessed: 11 September 2020).

Kemea brochure (2016) *ΔΡΑΣΕΙΣ ΚΑΤΑ ΤΗΣ ΡΙΖΟΣΠΑΣΤΙΚΟΠΟΙΗΣΗΣ ΚΑΙ ΤΟΥ ΕΞΤΡΕΜΙΣΜΟΥ*. Αθήνα.

Kennedy, J. P. (2020) *Counterfeit products online*, *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. doi: 10.1007/978-3-319-78440-3_46.

Kenneth Bradley, I. K. S. C. W. (2020) ‘Zimbabwe’, *Britannica. Encyclopædia Britannica*. Available at: <https://www.britannica.com/place/Zimbabwe>.

Kontargyris, X. (2018) *IT Laws in the Era of Cloud-Computing*, *IT Laws in the Era of Cloud-Computing*. doi: 10.5771/9783845295626.

Krafft, T. D., Gamer, M. and Zweig, K. A. (2019) ‘What did you see? A study to measure personalization in Google’s search engine’, *EPJ Data Science*. The Author(s), 8(1). doi: 10.1140/epjds/s13688-019-0217-5.

Ledingham, R. and Mills, R. (2015) ‘A preliminary study of autism and cybercrime in the context of international law enforcement’, *Advances in Autism*, 1(1), σ. 2–11. doi: 10.1108/AIA-05-2015-0003.

Mabillard, V., Kakpovi, B. G. and Cottier, B. (2018) ‘Access to information in Benin: a case study’, *International Review of Administrative Sciences*, (June). doi: 10.1177/0020852318762039.

Mabillard, V. and Pasquier, M. (2016) 'Transparency and trust in government (2007 - 2014): A comparative study', *NISPA Journal of Public Administration and Policy*, 9(2), σ. 69–92. doi: 10.1515/nispa-2016-0015.

Macenaite, M. and Kosta, E. (2017a) 'Consent for processing children's personal data in the EU: following in US footsteps?', *Information and Communications Technology Law*. Taylor & Francis, 26(2), σ. 146–197. doi: 10.1080/13600834.2017.1321096.

Macenaite, M. and Kosta, E. (2017b) 'Consent for processing children's personal data in the EU: following in US footsteps?', *Information and Communications Technology Law*, 26(2), σ. 146–197. doi: 10.1080/13600834.2017.1321096.

Markus Kaakinen, Teo Keipi, Pekka Rasanen, A. O. (2017) *Cybercrime Victimization and Subjective Well-Being: An Examination of the Buffering Effect Hypothesis Among Adolescents and Young. FINLAND.* doi: https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1089%2Fcyber.2016.0728?_sg%5B0%5D=R7ITqz-TVrJt86xTlsw0j_hq1we0kx77bu00X6gznelKy4DvB0blr30wYKRFTWfF10cQ6VXEbbNioO2-H9aCi4uXwg.fiHqD4YuMb4b72e8aX1wEZj5-ZcI4lz0noguLcCUp4H0-QwAshcftICosiM2j2_7qZJO0u5Es_wT8qnW0_JtxQ.

McCauley, C. and Moskalenko, S. (2008) 'Mechanisms of political radicalization: Pathways toward terrorism', *Terrorism and Political Violence*, 20(3), σ. 415–433. doi: 10.1080/09546550802073367.

Meijer, A. J., Curtin, D. and Hillebrandt, M. (2012) 'Open government: connecting vision and voice', *International Review of Administrative Sciences*, 78(1), σ. 10–29. doi: 10.1177/0020852311429533.

Michener, G. (2011) 'FOI laws around the world', *Journal of Democracy*, 22(2), σ. 145–159. doi: 10.1353/jod.2011.0021.

Michener, G. (2015) 'How Cabinet Size and Legislative Control Shape the Strength of Transparency Laws', *Governance*, 28(1), σ. 77–94. doi: 10.1111/gove.12075.

National Crime Agency (2020) *Sextortion (webcam blackmail)*, nationalcrimeagency.gov.uk. Available at: <https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail> (Accessed: 16 October 2020).

National museum of Australia (no date) *End of the White Australia policy*. Available at: <https://www.nma.gov.au/defining-moments/resources/end-of-white-australia-policy> (Accessed: 2 February 2021).

Nayanima, B. (2019) 'NCPRI rejects RTI law amendments, calls them "regressive"', *theprint*. Available at: <https://theprint.in/india/governance/ncpri-rejects-rti-law-amendments-calls-them-regressive/265665/>.

Neumann, P. R. (2010) 'Prisons and Terrorism: Radicalisation and De-radicalisation in 15 Countries'.

Neumann, P. R. (2013) 'The trouble with radicalization', *International Affairs*, 89(4), σ. 873–893. doi: 10.1111/1468-2346.12049.

O'Brien, D. (2019) *China's Global Reach: Surveillance and censorship beyond the Great Firewall*, <https://www.eff.org/>. Available at: <https://www.eff.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall>.

O'Reilly, Tim and Battelle, J. (2009) *What Is Web 2.0*, O'Reilly Media, Inc.,. Available at: <https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=2> (Accessed: 3 April 2020).

OECD (2020) 'Making Migration and Integration Policies Future Ready Making Migration and Integration Policies Future Ready Ministerial and Forum on Migration'. Available at: <https://www.oecd.org/migration/mig/migration-strategic-foresight.pdf>.

Palmer, C. C. (2001) 'Ethical hacking', *IBM Systems Journal*, 40(3), σ. 769–780. doi: 10.1147/sj.403.0769.

Paper, W., Lakhani, K. R. and Wolf, R. G. (2003) 'Why Hackers Do What They Do: Understanding Motivation Effort in Free/Open Source Software Projects', *Social Science Research*, (September). Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=443040.

Pariser, E. (2011) *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*. USA: Penguin Group.

Pearson, M. (2013) 'Press freedom, social media and the citizen', *Pacific Journalism Review*, 19(2), σ. 215–227. doi: 10.24135/pjr.v19i2.226.

Pernot-Leplay, E. (2020) 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?', *Penn State Journal of Law & International Affairs*, 8(1), p. 49.

Ponna, S. (2020) 'Online sexual blackmail sextortion', (December).

Prime minister's department broke the law delaying FOI request, watchdog finds (2020). Available at: <https://www.theguardian.com/australia-news/2020/feb/27/prime-ministers-department-broke-the-law-delaying-foi-request-watchdog-finds> (Accessed: 27 February 2020).

Protecting children from radicalisation (2020). Available at: <https://www.nspcc.org.uk/keeping-children-safe/reporting-abuse/dedicated-helplines/protecting-children-from-radicalisation/> (Accessed: 22 May 2020).

Reyes, C. (2011) 'WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive', *Melbourne Journal of International Law*, 12(1), σ. 141–176.

Roger, D. (2018) *Law, liberty and the pursuit of terrorism*. The University of Michigan Press. Available at: <http://dx.doi.org/10.1016/j.cirp.2016.06.001><http://dx.doi.org/10.1016/j.powtec.2016.12.055><https://doi.org/10.1016/j.ijfatigue.2019.02.006><https://doi.org/10.1016/j.matlet.2019.04.024><https://doi.org/10.1016/j.matlet.2019.127252><http://dx.doi.org/10.1016/j.ijfatigue.2019.02.006>

Ronen, Dov, Robin, Law, S. S. A. (2021) 'Benin', *Britannica*. britannica. Available at: <https://www.britannica.com/place/Benin>.

Sáez-Martín, A., López-Hernandez, A. M. and Caba-Perez, C. (2017) 'Access to public information: a scientometric study of legal versus voluntary transparency in the public sector', *Scientometrics*, 113(3), σ. 1697–1720. doi: 10.1007/s11192-017-2541-5.

Sameer Hinduja (2016) *Sextortion*, <https://cyberbullying.org>. Available at: <https://cyberbullying.org/sextortion> (Accessed: 16 October 2020).

Schudson, M. (2018) 'Troubling Transparency', *Troubling Transparency*. doi: 10.7312/poze18498.

Sebastian Morris (2005) 'Electronic copy available at: <http://ssrn.com/abstract=2545489> Electronic copy available at ', *Grou*, 23529(2), pp. 1–45.

Serrat, O. (2017) 'Knowledge Solutions: Tools, Methods, and Approaches to Drive

Organizational Performance’, *Knowledge Solutions: Tools, Methods, and Approaches to Drive Organizational Performance*, σ. 1–1140. doi: 10.1007/978-981-10-0983-9.

Shanker, S. G. (2019) *Artificial Intelligence At The Cross-roads, Questions In Artificial Intelligence*. ITALY. doi: 10.2760/705074.

Signs of radicalisation (2020). Available at: <https://educateagainsthate.com/signs-of-radicalisation/> (Accessed: 22 May 2020).

Spyratos, Spyridon, Yildiz, D. *et al.* (2019) ‘Using Twitter data for demographic research’, *Demographic Research*, 37(1), σ. 1477–1514. doi: 10.4054/DemRes.2017.37.46.

States, United Commission, S. and exchange (2015) *Facebook annual report report pursuant to section 13 or 15(d) of the securities exchange act of 1934 for the fiscal year ended December 31, 2018, Washington, D.C. 20549*. Available at: <https://www.sec.gov/Archives/edgar/data/1326801/000132680115000032/fb-9302015x10q.htm> (Accessed: 1 June 2020).

The Constitution Unit (2011) *Zimbabwe International Focus, THE CONSTITUTION UNIT*. Available at: <https://www.ucl.ac.uk/constitution-unit/research/research-archive/foi-archive/international-focus/zimbabwe> (Accessed: 5 February 2020).

The Global Compact for Safe, O. and R. M. (2020) ‘The Global Compact for Safe, Orderly and Regular Migration (GCM)’, <https://www.iom.int/global-compact-migration>. Available at: <https://www.iom.int/global-compact-migration>.

Thomas, L. and Hoofnagle, C. J. (2011) *Exploring Information Sharing through California’s ‘Shine the Light’ Law, SSRN Electronic Journal*. doi: 10.2139/ssrn.1448365.

Thorn (2017) *Sextortion*.

Toby McIntosh (2014) “‘Paraguay is 100th Nation to Pass FOI Law, but Struggle for Openness Goes on.’”, <https://www.theguardian.com/>. Available at: <https://www.theguardian.com/public-leaders-network/2014/sep/19/paraguay-freedom-information-law-transparency>.

Trip, S. *et al.* (2019) ‘Psychological mechanisms involved in radicalization and extremism. A rational emotive behavioral conceptualization’, *Frontiers in Psychology*, 10(MAR). doi: 10.3389/fpsyg.2019.00437.

Union, E. (2009) *Data protection on line privacy*. Available at: <https://europa.eu/>

(Accessed: 5 May 2020).

VerLoren van Themaat, W. and Reuder, B. (2018) ‘Charter of Fundamental Rights of the European Union’, *European Competition Law*, σ. 713–714. doi: 10.4337/9781786435477.00032.

Villa, M. and Magri, P. (2020) *The future of migration to Europe*, Ispi.

Washington Post (2020) *China is exporting its digital authoritarianism*, *Washington post*. Available at: https://www.washingtonpost.com/opinions/china-is-exporting-its-digital-authoritarianism/2020/08/05/f14df896-d047-11ea-8c55-61e7fa5e82ab_story.html (Accessed: 20 September 2020).

Widiawati, N. (2020) ‘Global radicalism: the phenomenon of local Islamic radicalism in the structure of global radicalism’, 6(2), σ. 164–180. doi: http://dx.doi.org/10.30983/islam_realitas.v6i2.3423.

Wu, H. (2020) *In land of big data, China sets individual privacy rights*, *REUTERS*. Available at: <https://www.reuters.com/article/us-china-parliament-lawmaking-privacy-idUSKBN2320EF> (Accessed: 20 September 2020).

Yakovleva, S. and Irion, K. (2020) ‘Pitching trade against privacy: Reconciling EU governance of personal data flows with external trade’, *International Data Privacy Law*, 10(3), σ. 201–221. doi: 10.1093/idpl/ipaa003.

Zimbabwe, G. (2020) ‘Zimbabwe Act’.

Zimmer, M. (2010) “‘But the data is already public’: On the ethics of research in Facebook”, *Ethics and Information Technology*, 12(4), σ. 313–325. doi: 10.1007/s10676-010-9227-5.

Zittrain, J. and Edelman, B. (2003) ‘Internet filtering in China’, *IEEE Internet Computing*, 7(2), σ. 70–75. doi: 10.1109/MIC.2003.1189191.

Ανασταστας, Ε. (2018a) *Πες ‘όχι’ στον σεξουαλικό εξαναγκασμό – Προστατεύστε τα παιδιά σας !!!* Available at: <http://safer-internet.gr/> (Accessed: 2 May 2020).

Ανασταστας, Ε. (2018b) *Συνελήφθη 25χρονος που έκλεινε ραντεβού σε ανήλικες με ψεύτικο προφίλ στο Facebook*, *saferinternet.gr*. Available at: <https://www.safer-internet.gr/25xronos-ekleine-rantevou-sto-facebook-se-anilik-es-me-pseutiko-profil/>.

Δραγώνα, Θ. (2015) ‘Επιστήμη και Κοινωνία: Επιθεώρηση Πολιτικής και Ηθικής

Θεωρίας’, *Επιστήμη και Κοινωνία:Επιθεώρηση Πολιτικής και Ηθικής Θεωρίας*, σ. 17–39. Available at: <https://doi.org/10.12681/sas.642>.

Επίσημος ιστότοπος της Ευρωπαϊκής Ένωσης (2020) *Διαφάνεια και ΕΕ*. Available at: <https://ec.europa.eu/transparencyregister/public/homePage.do> (Accessed: 27 May 2020).

Ευρωπαϊκό Κοινοβούλιο (2016) ‘EUR-Lex - 32016R0679 - EL - EUR-Lex’, *Επίσημη Εφημερίδα Της Ευρωπαϊκής Ένωσης*, 2014, σ. 88. doi: 10.1104/pp.16.01100.

Εφημερίδα της Ευρωπαϊκής Ένωσης (2007) *Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης*. Available at: <https://fra.europa.eu/el/eu-charter/article/11-eleytheria-ekfrasis-kai-pliroforisis#TabNational>.

Η Εναρκτήρια ομιλία του CEO της Samsung Electronics στη CES 2015 (2014). Available at: <https://techingreek.com/i-enarktiria-omilia-tou-ceo-tis-samsung-electronics-stices-2015/> (Accessed: 17 September 2020).

Ιγγλεζιάκης, Ι. (2018) *ΙΓΓΛΕΖΑΚΗΣ: ΔΙΚΑΙΟ ΠΛΗΡΟΦΟΡΙΚΗΣ*. ΣΑΚΚΟΥΛΑΣ Α.Ε.

Ιστότοπος Ευρωπαϊκής Ένωσης (2019) *Biometrics and the Schengen Information System – Fostering identification capabilities*. Available at: <https://ec.europa.eu/jrc/en/news/biometrics-and-schengen-information-system-fostering-identification-capabilities> (Accessed: 7 July 2020).

Κανελλοπούλου-Μπότη, Μ. (2012) ‘Κοινωνικά δίκτυα και προσωπικότητα-II’, *ΔiMME*, 2, σ. 196–199.

Κελάλη, Π. (2018) ‘«Προστασία των προσωπικών δεδομένων των παιδιών στην κοινωνία της πληροφορίας», Παιδί και Πληροφορία Αναζητήσεις ιστορίας, δικαίου, δεοντολογίας και πολιτισμού’, in, σ. 78. doi: <https://events.ihrc.gr/infokid2017/>.

Λιαλιούτη, Ζ. *et al.* (2017) ‘Η ξеноφοβία στην Ελλάδα ως ερευνητικό πρόβλημα: Εννοιολογικά και μεθοδολογικά ζητήματα.’, 3712.

Μήτρου, Λ. (2017) *Ο Γενικός Κανονισμός για την προστασία δεδομένων*.

N. 2225/1994 και τροποποιήσεις (2016) *ΥΠΟΥΡΓΕΙΟ ΔΙΚΑΙΟΣΥΝΗΣ*. Available at: <http://www.opengov.gr/ministryofjustice/?p=6323> (Accessed: 29 July 2020).

Νόμος που κυρώνει τη συμβαση για τα δικαιωματα του παιδιου (1990) *Φ.Ε.Κ.* 192/2.12.92.

Ομάδα Εργασίας του άρθρου 29 για την προστασία των δεδομένων (2014) 'Ομάδα Εργασίας του άρθ.29 για την προστασία των δεδομένων προσωπικού χαρακτήρα 0829/14'.

Παναγοπούλου-Κουτνατζή, Φ. (2010) *Περί της ελευθερίας των ιστολογίων (blogs), Οι νέες τεχνο- λογίες ως εθνική, ευρωπαϊκή και διεθνής πρόκληση στην ελευθερία διαδόσεως των ιδεών*. θήνα-Θεσσαλονίκη: Εκδόσεις Σάκ- κουλα.

Παναγοπούλου-Κουτνατζή, Φ. (2013) 'Κοινωνικά δίκτυα και προσωπικότητα', *NOMIKH BIBLIOΘΗΚΗ ΑΕΒΕΒΙΒΛΙΟΘΗΚΗ ΑΕΒΕ*, 2, σ. 186 επ.

Παναγοπούλου-Κουτνατζή, Φ. (2017) *Ο Γενικός Κανονισμός για την προστασία δεδομένων 679/2016/ΕΕ*. ΣΑΚΚΟΥΛΑΣ Α.Ε.

Παπαδημητρίου, Δ. (2017) 'Ριζοσπαστισμός. Η έννοια', *Επιστήμη και Κοινωνία:Επιθεώρηση Πολιτικής και Ηθικής Θεωρίας*, 35(Ριζοσπαστισμός. Η έννοια.), σ. 9–33. Available at: <https://doi.org/10.12681/sas.10605>.

Στεφανου, Σ. (2020) 'Sextortion scam: Η ΕΛ.ΑΣ. προειδοποιεί για νέα απάτη', *CNN Ελλάδαςellada*. Available at: <https://www.cnn.gr/ellada/story/231487/sextortion-scam-h-el-as-proeidopoiei-gia-ne-a-pati>.

Τσαλικη, Α. (2013) 'Παιδια Και Διαδικτυο Στην Ελλαδα', σ. 1-106.

Τυπογραφείο, Ε. (2019) *Συνταγμα της Ελλάδος*.

ΙΣΤΟΣΕΛΙΔΕΣ

<https://www.nationsonline.org/oneworld/benin.htm>
<https://www.journalofdemocracy.org/wp-content/uploads/2012/01/MichenerMap-22-2.pdf>
<https://www.osibaltimore.org/>
<https://www.data.gov/>
<https://data.gov.uk/>
<https://www.dpa.gr/>
<https://www.synigoros.gr/>
<http://www.capurro.de/africa.html>
<http://blogs.dlapiper.com/>
<https://www.gdprgreece.com/article/5/gdpr>
<https://opensource.com/resources/open-government>
<https://opi.gr/index.php>
<https://ec.europa.eu/eurostat/statistics->
<https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0224134#sec005>
<https://www.abc.net.au/news/2020-03-05/turkey-says-greek-forces-killed-migrants-trying-to-cross-border/12026950>
<http://righttoinformation.info/>
https://www.efsyn.gr/stiles/apopseis/52749_rizospastikopoiisi-kai-extremismos
<https://inimareng.ee/en/open-to-the-world/tracking-trans-nationalism-with-mobile-telephone-data/>
https://migrationdataportal.org/?i=stock_abs_&t=2019
https://ec.europa.eu/knowledge4policy/migration-demography_en
<https://gmdac.iom.int/>
https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/about-ran/ran-pol_en
<https://www.truthfinder.com/public-records/>
<https://www.clarip.com/data-privacy/do-not-sell-my-personal-information/>
<http://www.wuzhenwic.org/>
<https://www.eff.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall>
<https://freedomhouse.org>

<http://www.0-18.gr/paidikiprostasia/paidikiprostasia>
<https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>
<https://rapidapi.com/blog/top-facial-recognition-apis/>
<https://www.britannica.com/place/Zimbabwe>
<https://www.fisc.uscourts.gov/>
<https://www.e-verify.gov>
<https://www.iom.int/migration-management>
<https://www.nfoic.org/coalitions/state-foi-resources/california-foia-laws>