

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

CAMBRIDGE ANALYTICA – FACEBOOK: A STRIKING SCANDAL ON SOCIAL MEDIA MANIPULATION AND THE NEED TO APPLY THE NEW EUROPEAN GDPR.



321/2013024 ΒΑΦΕΙΑΔΑΚΗ ΚΟΡΙΝΑ - ΣΠΥΡΙΔΟΥΛΑ

321/2013064 ΚΑΛΟΜΟΙΡΗ ΒΙΡΓΙΝΙΑ

ΕΠΙΒΛΕΠΟΥΣΑ: ΜΗΤΡΟΥ ΕΥΑΓΓΕΛΙΑ

ΣΑΜΟΣ, ΙΟΥΝΙΟΣ 2019



ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. ΕΙΣΑΓΩΓΗ	2
1.ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ	4
1.1 Περιγραφή και Ορισμοί Όρων Προσωπικών Δεδομένων	4
1.2 Νομοθεσία	12
1.2.1 Ευρωπαϊκή Νομοθεσία (GDPR - General Data Protection Regulation).....	12
1.2.2 Αμερικάνικη Νομοθεσία.....	24
1.2.3 Privacy Shield EU–US (Ασφάλεια Απορρήτου)	28
1.3 Πεδίο Εφαρμογής	30
1.4 Εταιρείες που Συλλέγουν και Διαχειρίζονται Προσωπικά Δεδομένα	32
2. CAMBRIDGE ANALYTIKA	37
2.1 Περιγραφή Εταιρείας.....	37
2.2 Απολογισμός Παραχθέντος Έργου της Cambridge Analytica	43
2.3 Περιγραφή Σκανδάλου	45
2.4 Ανάλυση Σκανδάλου Σχετικά με τη Τεχνική της Ψυχομετρίας.....	48
3. ΑΝΑΛΥΣΗ ΣΚΑΝΔΑΛΟΥ	57
3.1 Τεχνολογίες του Facebook που Εξυπηρέτησαν την Υποκλοπή	58
3.2 Τρόποι Εκμετάλλευσης Τεχνολογιών	63
3.3 Αποκάλυψη Σκανδάλου	67
3.4 Χειραγώγηση των Χρηστών	69
4. ΔΥΣΜΕΝΗΣ ΑΝΤΙΚΤΥΠΟΙ ΤΟΥ ΣΚΑΝΔΑΛΟΥ	73
4.1 Αντίκτυποι σε διάφορους τομείς της κοινωνίας	74
4.1.1 Κοινωνικός Αντίκτυπος.....	74
4.1.2 Οικονομικός Αντίκτυπος	78
4.1.3 Πολιτικός Αντίκτυπος.....	82
4.1.4 Τεχνολογικός Αντίκτυπος.....	87
4.2 Εφαρμογή Γενικού Κανονισμού Προστασίας Δεδομένων σε τομείς της κοινωνίας	89
4.2.1 Οικονομικός Τομέας.....	90
4.2.2 Τεχνολογικός Τομέας	91
4.2.3 Πολιτικός Τομέας	93
5. ΣΥΜΠΕΡΑΣΜΑΤΑ	95
6. ΒΙΒΛΙΟΓΡΑΦΙΑ	98

Εισαγωγή

Σήμερα ζούμε την τέταρτη Βιομηχανική επανάσταση που χαρακτηρίζεται ως «Εποχή της Πληροφορίας», με επιτεύγματα στη ρομποτική, τη νανοτεχνολογία, τη γενετική, τα αυτοδηγούμενα οχήματα, την τεχνική νοημοσύνη και τις Τεχνολογίες της Πληροφορίας/Επικοινωνίας. Οι παραπάνω επιτυχίες, έχουν οδηγήσει σε ριζικές κοινωνικές αλλαγές τα τελευταία χρόνια, όπου η κοινωνία της πληροφορίας θα πρέπει να είναι μια κοινωνία της γνώσης και όλοι θα πρέπει να συμμετέχουν ισότιμα.

Ο χαρακτηρισμός «εποχή της πληροφορίας» οφείλεται στο ότι σήμερα υπάρχει η δυνατότητα στους ανθρώπους να ανταλλάσσουν και να μεταφέρουν πληροφορίες ελεύθερα και να έχουν άμεση πρόσβαση σε γνώσεις που θα ήταν δύσκολο ή αδύνατο να βρεθούν στο παρελθόν. Τα σύγχρονα τεχνολογικά μέσα παρέχουν την δυνατότητα της γρήγορης και εύκολης αποθήκευσης, της εύκολης χρήσης και επεξεργασίας της πληροφορίας, ενώ παράλληλα το διαδίκτυο, αποτελώντας ένα παγκόσμιο ιστό πληροφοριών, έχει διεισδύσει σε σχεδόν όλους τους τομείς της ανθρώπινης δραστηριότητας συνεισφέροντας πολλά στην εξέλιξη τους. Η έννοια αυτή συνδέεται με την έννοια της **ψηφιακής εποχής** και μεταφέρει την αλλαγή από την παραδοσιακή βιομηχανία σε μια οικονομία που βασίζεται στο χειρισμό των πληροφοριών. Η περίοδος αυτή θεωρείται ότι ξεκίνησε γύρω στα τέλη του δεύτερου μισού του 20ού αιώνα μ.Χ., χωρίς να υπάρχει επίσημη ημερομηνία έναρξης. Ωστόσο, η επεξεργασία, η πρόσβαση, η φορητότητα της πληροφορίας δεν πρέπει να γίνεται ανεξέλεγκτα αλλά σύννομα, εξασφαλίζοντας τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, διότι υπάρχει κίνδυνος εμπορευματοποίησης και όχι μόνο, των προσωπικών δεδομένων από ιδιωτικούς φορείς εν αγνοία των υποκειμένων. Ειδικότερα, τα προσωπικά δεδομένα του ατόμου, δηλαδή οι πληροφορίες σχετικά με την προσωπικότητα και την ιδιωτική του ζωή, δεν πρέπει να δημοσιοποιούνται ή να κρατούνται σε βάσεις δεδομένων χωρίς την συγκατάθεση του, ιδίως αν πρόκειται για ευαίσθητα προσωπικά δεδομένα, με εξαίρεση τις περιπτώσεις που αναφέρει το δίκαιο (GDPR).

Τα τελευταία χρόνια πολιτικά κόμματα και επιχειρήσεις καμπάνιας χρησιμοποιούν όλο και περισσότερο προσωπικές πληροφορίες και εξελιγμένες τεχνικές ανάλυσης δεδομένων προκειμένου να στοχεύσουν τους ψηφοφόρους. Τα μοντέλα συμπεριφοράς που χρησιμοποιούνται ευρέως στα μέσα κοινωνικής δικτύωσης και στον εμπορικό τομέα έχουν υιοθετηθεί στην πολιτική εκστρατεία. Για να διατηρηθεί η εμπιστοσύνη των εκλογέων και η

ακεραιότητα των εκλογών, όλοι οι εμπλεκόμενοι με την πολιτική εκστρατεία πρέπει να χρησιμοποιούν τις τεχνικές ανάλυσης προσωπικών δεδομένων με τρόπους που είναι διαφανείς, κατανοητοί από τους ανθρώπους, με τη συγκατάθεση τους και σύννομους. Η έλλειψη διαφάνειας, συγκατάθεσης και νόμιμης επεξεργασίας προσωπικών πληροφοριών δημιούργησε το σκάνδαλο Cambridge Analytica που αποτελεί και το θέμα της παρούσας διπλωματικής.

Η Βρετανική εταιρεία Cambridge Analytica που έχει έδρα στο Λονδίνο, εκμαίευε μέσω φαινομενικά «αθώων» πνευματικών παιχνιδιών με ερωτήσεις (κουίζ) προσωπικά δεδομένα χρηστών αλλά και των διαδικτυακών φίλων τους. Κατάφερε να συγκεντρώσει στοιχεία από 50 εκατομμύρια προφίλ χρηστών στις ΗΠΑ και στη συνέχεια βάσει των ψυχογραφημάτων τους, τους σφυρηλάτησε με πολιτικές διαφημίσεις που τελικά επηρέαζαν την κρίση τους και τις επιλογές τους υπέρ συγκεκριμένου υποψηφίου.

Η παρούσα εργασία που χωρίζεται σε 4 κεφάλαια. Παρουσιάζει το σκάνδαλο Cambridge Analytica, με σκοπό την διερεύνηση του σκανδάλου και τον δυσμενή αντίκτυπο στην Οικονομία, την Πολιτική, την Κοινωνία, και την Τεχνολογία και την εξαγωγή συμπερασμάτων.

Το πρώτο κεφάλαιο, τιτλοφορείται "ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ" κι ως σκοπό έχει να εισάγει τον αναγνώστη στην έννοια του όρου των ευαίσθητων προσωπικών δεδομένων και τον κατάλογο με τους ορισμούς που καθορίζουν το Γενικό Κανονισμό Προσωπικών Δεδομένων (GDPR). Στην συνέχεια, αναλύεται συνοπτικά ο κανονισμός (GDPR) και το πεδίο εφαρμογής του. Επιπλέον, αναφέρεται η Αμερικανική νομοθεσία, εντοπίζεται η διαφορετικότητα τους και καταγράφεται η συμφωνία μεταξύ Ευρώπης και Αμερικής σχετικά με τα προσωπικά δεδομένα.

Στο δεύτερο κεφάλαιο, που ονομάζεται "CAMBRIDGE ANALYTICA", γίνεται περιγραφή της εταιρείας και του έργου που παράγει, ενώ ακολουθεί η σύντομη περιγραφή και ανάλυση του σκανδάλου.

Στο τρίτο κεφάλαιο "ΑΝΑΛΥΣΗ ΣΚΑΝΔΑΛΟΥ" αναλύεται το σκάνδαλο και τεχνολογικά, ενώ το τελευταίο κεφάλαιο της εργασίας τιτλοφορείται "ΔΥΣΜΕΝΗΣ ΑΝΤΙΚΤΥΠΟΙ ΤΟΥ ΣΚΑΝΔΑΛΟΥ" και επιχειρεί μια αναλυτική εξέταση τόσο των κινδύνων όσο και του δυσμενή αντικτύπου στην Οικονομία, Πολιτική, Κοινωνία και Τεχνολογία. Τέλος παρουσιάζονται τα Συμπεράσματα της Διπλωματικής.

Κεφάλαιο 1

ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

1.1 Περιγραφή και Ορισμοί Όρων που αφορούν τα Προσωπικά Δεδομένα

Η διάκριση μεταξύ δημόσιας και ιδιωτικής ζωής ανάγεται στην αρχαία ελληνική φιλοσοφία «...απόσταση , χώρος και απομόνωση από τη δημόσια ζωή ...», (Αριστοτέλης «Ηθικά Νικομάχεια»). Στη φιλελεύθερη παράδοση, «η αξίωση της ιδιωτικότητας δεν εμφανίζεται ως η εκπλήρωση μιας "φυσικής ανάγκης" όλων των ατόμων αλλά ως η κατάκτηση ενός προνομίου από μία κοινωνική ομάδα» / «*To refugium είναι αγαθό που μπορούν να διασφαλίσουν όσοι διαθέτουν ισχύ, χρήματα και προνόμια*» (J.Locke και John Stuart Mill). Στη Γαλλική Επανάσταση ο Saint-Just διακήρυξε ότι η ελευθερία των ανθρώπων βρίσκεται στην ιδιωτική τους ζωή, «*Fragments sur les institutions republicaines*», δηλώνοντας κατ' ουσία ότι η κοινωνία που θεωρεί την αυτονομία των ατόμων θεμελιώδη κανονιστική αρχή πρέπει να διακρίνει σαφώς μεταξύ δημόσιας και ιδιωτικής ζωής και να προστατεύει την τελευταία (Μήτρου, 2018).

Η προστασία της ιδιωτικής ζωής και της ελεύθερης ανάπτυξης της προσωπικότητας αποτελούν πρωταρχική επιδίωξη κάθε δημοκρατικής κοινωνίας. Η ανάπτυξη νέων τεχνολογιών και η πρόοδος της πληροφορικής καθώς και η ανάγκη της ηλεκτρονικής οργάνωσης των κρατών, έχουν σαν συνέπεια την αυξημένη ζήτηση προσωπικών πληροφοριών από τον ιδιωτικό και τον δημόσιο τομέα. Η ανεξέλεγκτη καταχώρηση και επεξεργασία των προσωπικών δεδομένων σε συνδυασμό με το διαδίκτυο μπορεί να δημιουργήσει προβλήματα στην ιδιωτική ζωή του πολίτη. Για την προστασία του ατόμου στην κοινωνία της πληροφορίας δεν αρκούν οι παραδοσιακές ρυθμίσεις αλλά χρειάζεται ειδική αντιμετώπιση με νέους νόμους.

Η εξέλιξη της σχετικής νομοθεσίας με τα προσωπικά και ιστορικά δεδομένα έχει ως εξής:

<p>Δεκαετία 1970:</p>	<ul style="list-style-type: none"> - Εισαγωγή νομοθεσίας στη Γερμανία, Αυστρία, Γαλλία και σκανδιναβικές χώρες.
<p>Δεκαετία 1980:</p>	<ul style="list-style-type: none"> - Η “διεθνοποίηση” των κανονιστικών απαιτήσεων και αρχών - Σύμβαση 108 Συμβουλίου της Ευρώπης: αυτοματοποιημένη επεξεργασία - Κατευθυντήριες Αρχές ΟΟΣΑ: μη δεσμευτική ισχύς, αλλά σημείο αναφοράς οδήγησε και τους νομοθέτες άλλων χωρών να υιοθετήσουν νομοθεσία.
<p>Δεκαετία 1990:</p>	<ul style="list-style-type: none"> - Υιοθέτηση Οδηγίας 95/46/EK, - Ενιαίες ροές πληροφοριών και ενιαίες απαιτήσεις - Επίδραση στην κανονιστική εξέλιξη διεθνώς
<p>Δεκαετία 2000:</p>	<ul style="list-style-type: none"> - Προστασία προσωπικών δεδομένων ως “κοινοτικό κεκτημένο” και η “συνταγματοποίηση της προστασίας” - Η προστασία προσωπικών δεδομένων αναγνωρίζεται ως διακριτό δικαίωμα στον Χάρτη των Θεμελιωδών Δικαιωμάτων και Ελευθεριών (άρθρο 8) - Δεσμευτική ισχύς με τη Συνθήκη της Λισαβόνας
<p>Δεκαετία 2010:</p>	<ul style="list-style-type: none"> - Πρόταση Κανονισμού/Πρόταση Οδηγίας ως αντίδραση στην αλλαγή του τεχνολογικού περιβάλλοντος 2018 - Γενικός Κανονισμός Προστασίας Δεδομένων ΕΕ (GDPR).

Οι ραγδαίες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση δημιούργησαν νέες προκλήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα. Η κλίμακα της συλλογής και της ανταλλαγής δεδομένων προσωπικού χαρακτήρα αυξήθηκε σημαντικά. Η τεχνολογία επιτρέπει τόσο σε ιδιωτικές επιχειρήσεις, όσο και σε δημόσιες αρχές, να κάνουν χρήση δεδομένων προσωπικού χαρακτήρα σε πρωτοφανή κλίμακα για την επιδίωξη των δραστηριοτήτων τους. Τα φυσικά πρόσωπα ολοένα και περισσότερο δημοσιοποιούν προσωπικές πληροφορίες και τις καθιστούν διαθέσιμες σε παγκόσμιο επίπεδο. Η τεχνολογία έχει αλλάξει τόσο την οικονομία όσο και την κοινωνική ζωή και θα πρέπει να διευκολύνει περαιτέρω την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης και τη διαβίβαση σε τρίτες χώρες και διεθνείς οργανισμούς, διασφαλίζοντας παράλληλα υψηλό επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα.

Οι εξελίξεις αυτές απαιτούν ένα ισχυρό και πιο συνεκτικό πλαίσιο προστασίας των δεδομένων στην Ένωση, υποστηριζόμενο από αυστηρή εφαρμογή της νομοθεσίας, δεδομένου ότι είναι σημαντικό να δημιουργηθεί η αναγκαία εμπιστοσύνη που θα επιτρέψει στην ψηφιακή οικονομία να αναπτυχθεί στο σύνολο της εσωτερικής αγοράς. Τα φυσικά πρόσωπα θα πρέπει να έχουν τον έλεγχο των δικών τους δεδομένων προσωπικού χαρακτήρα. Θα πρέπει να ενισχυθούν η ασφάλεια δικαίου και η πρακτική ασφάλεια για τα φυσικά πρόσωπα, τους οικονομικούς παράγοντες και τις δημόσιες αρχές.

Με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ – GDPR) 2016/679, που τέθηκε σε εφαρμογή στις 25 Μαΐου το 2018, καθιερώθηκε νομικό πλαίσιο για την προστασία προσωπικών δεδομένων των κρατών της Ευρωπαϊκής Ένωσης. Με αυτόν καθορίζονται οι υποχρεώσεις των Υπευθύνων επεξεργασίας, θεσπίζονται κανόνες που αφορούν στην προστασία φυσικών προσώπων ως προς την επεξεργασία δεδομένων προσωπικού χαρακτήρα και προστατεύει θεμελιώδη δικαιώματα φυσικών προσώπων, ειδικότερα στην προστασία δεδομένων προσωπικού χαρακτήρα.

Για την καλύτερη κατανόηση των ζητημάτων που τίθενται θεωρούμε χρήσιμο να παραθέσουμε τους ορισμούς που περιλαμβάνει ο Γενικός Κανονισμός Προστασίας Δεδομένων:

«Δεδομένα Προσωπικού Χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας,

σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

«Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα (ευαίσθητα δεδομένα)»: κάθε πληροφορία που αφορά στη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν στην υγεία ή δεδομένων που αφορούν στη σεξουαλική ζωή φυσικού προσώπου ή στον γενετήσιο προσανατολισμό προσωπικού χαρακτήρα.

«Επεξεργασία»: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

«Περιορισμός της Επεξεργασίας»: η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον.

«Κατάρτιση Προφίλ»: οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου.

«Ανωνυμοποίηση»: η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων.

«Ψευδωνυμοποίηση»: η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των

δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

«Αρχείο Δεδομένων»: κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση.

«Υπεύθυνος Επεξεργασίας»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα: όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

«Από κοινού υπεύθυνοι επεξεργασίας»: δύο ή περισσότεροι υπεύθυνοι επεξεργασίας, οι οποίοι καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας.

«Εκτελών την Επεξεργασία»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

«Αποδέκτης»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι.

«Τρίτος»: οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα.

«Συγκατάθεση» του υποκειμένου των δεδομένων: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρη επίγνωση, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

«Κίνδυνος»: η υπόθεση εργασίας που περιγράφει ένα συμβάν και τις επιπτώσεις του, που έχουν εκτιμηθεί με όρους σοβαρότητας και πιθανότητας επέλευσης. Ως διαχείριση κινδύνου ορίζεται το σύνολο των συντονισμένων δραστηριοτήτων για την καθοδήγηση και τον έλεγχο ενός οργανισμού ως προς τον κίνδυνο.

«Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα»: η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

«Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα (ευαίσθητα δεδομένα)»: κάθε πληροφορία που αφορά στη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν στην υγεία ή δεδομένων που αφορούν στη σεξουαλική ζωή φυσικού προσώπου ή στον γενετήσιο προσανατολισμό προσωπικού χαρακτήρα.

«Γενετικά Δεδομένα»: τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου.

«Βιομετρικά Δεδομένα»: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεδεμένη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δάκτυλο-σκοπικά δεδομένα.

«Δεδομένα που αφορούν την Υγεία»: δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανόμενης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του.

«Κύρια Εγκατάσταση»:

α) όταν πρόκειται για υπεύθυνο επεξεργασίας με εγκατάσταση σε περισσότερα του ενός

κράτη μέλη, ο τόπος της κεντρικής του διοίκησης στην Ένωση, εκτός εάν οι αποφάσεις όσον αφορά τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα λαμβάνονται σε άλλη εγκατάσταση του υπευθύνου επεξεργασίας στην Ένωση και η εγκατάσταση αυτή έχει την εξουσία εφαρμογής των αποφάσεων αυτών, οπότε ως κύρια εγκατάσταση θεωρείται η εγκατάσταση στην οποία έλαβε τις αποφάσεις αυτές,

β) όταν πρόκειται για εκτελούντα την επεξεργασία με εγκατάσταση σε περισσότερα του ενός κράτη μέλη, ο τόπος της κεντρικής του διοίκησης στην Ένωση ή, εάν ο εκτελών την επεξεργασία δεν έχει κεντρική διοίκηση στην Ένωση, η εγκατάσταση του εκτελούντος την επεξεργασία στην Ένωση στην οποία εκτελούνται οι κύριες δραστηριότητες επεξεργασίας στο πλαίσιο των δραστηριοτήτων εγκατάστασης του εκτελούντος την επεξεργασία, στον βαθμό που ο εκτελών την επεξεργασία υπόκειται σε ειδικές υποχρέωσης.

«Εκπρόσωπος»: φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ένωση, το οποίο ορίζεται εγγράφως από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία βάση του άρθρου 27 και εκπροσωπεί τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ως προς τις αντίστοιχες υποχρεώσεις τους.

«Επιχείρηση»: φυσικό ή νομικό πρόσωπο που ασκεί οικονομική δραστηριότητα, ανεξάρτητα από τη νομική του μορφή, περιλαμβανομένων των προσωπικών εταιρειών ή των ενώσεων που ασκούν τακτικά οικονομική δραστηριότητα.

«Ομίλος Επιχειρήσεων»: μια ελέγχουσα επιχείρηση και οι ελεγχόμενες από αυτήν επιχειρήσεις.

«Δεσμευτικοί Εταιρικοί Κανόνες»: οι πολιτικές προστασίας δεδομένων προσωπικού χαρακτήρα τις οποίες ακολουθεί ένας υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία εγκατεστημένος στο έδαφος κράτους μέλους για διαβίβαση ή δέσμη διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία σε μία ή περισσότερες τρίτες χώρες εντός ομίλου επιχειρήσεων, ή ομίλου εταιρειών που ασκεί κοινή οικονομική δραστηριότητα.

«Εποπτική Αρχή»: η ανεξάρτητη δημόσια αρχή που συγκροτείται από κράτος-μέλος της Ένωσης και εποπτεύει τη σωστή εφαρμογή της νομοθεσίας για την προστασία δεδομένων προσωπικού χαρακτήρα.

«Ενδιαφερόμενη Εποπτική Αρχή»: εποπτική αρχή την οποία αφορά η επεξεργασία δεδομένων προσωπικού χαρακτήρα, διότι:

- α) ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι εγκατεστημένος στο έδαφος του κράτους μέλους της εν λόγω εποπτικής αρχής,
- β) τα υποκείμενα των δεδομένων που διαμένουν στο κράτος μέλος της εν λόγω εποπτικής αρχής επηρεάζονται ή ενδέχεται να επηρεαστούν ουσιωδώς από την επεξεργασία ή
- γ) έχει υποβληθεί καταγγελία στην εν λόγω εποπτική αρχή.

«Διασυνοριακή Επεξεργασία»:

- α) η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων διάφορων εγκαταστάσεων σε περισσότερα του ενός κράτη μέλη υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση όπου ο υπεύθυνος επεξεργασίας ή ο εκτελών επεξεργασία είναι εγκατεστημένος σε περισσότερα του ενός κράτη μέλη ή
- β) η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων μίας μόνης εγκατάστασης υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση αλλά που επηρεάζει ή ενδέχεται να επηρεάσει ουσιωδώς υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη μέλη.

«Σχετική και Αιτιολογημένη Ένσταση»: ένσταση σε ένα σχέδιο απόφασης ως προς την ύπαρξη παράβασης του GDPR κανονισμού, ή ως προς τη συμφωνία με τον GDPR κανονισμό της προβλεπόμενης ενέργειας σε σχέση με τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, η οποία καταδεικνύει σαφώς τη σημασία των κινδύνων που εγκυμονεί το σχέδιο απόφασης όσον αφορά τα θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και, κατά περίπτωση, την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης.

«Υπηρεσία της Κοινωνίας των Πληροφοριών»: υπηρεσία κατά την έννοια του άρθρου 1 παράγραφος 1 στοιχείο β) της οδηγίας (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*).

«Διεθνής Οργανισμός»: οργανισμός και οι υπαγόμενοι σε αυτόν φορείς που διέπονται από το δημόσιο διεθνές δίκαιο ή οποιοσδήποτε άλλος φορέας που έχει ιδρυθεί δυνάμει ή επί τη βάση συμφωνίας μεταξύ δύο ή περισσότερων χωρών.

«Κανονισμοί»: είναι δεσμευτικές νομοθετικές πράξεις, με την εφαρμογή τους σε όλες τις χώρες της Ευρωπαϊκής Ένωσης να είναι υποχρεωτική.

«Οδηγίες»: είναι νομοθετικές πράξεις που ορίζουν έναν στόχο τον οποίο πρέπει να επιτύχουν όλες οι χώρες της ΕΕ, εναπόκειται ωστόσο σε κάθε χώρα να θεσπίσει τους δικούς της νόμους για την επίτευξη των στόχων αυτών.

1.2 Νομοθεσία περί Προσωπικών Δεδομένων

1.2.1 Ευρωπαϊκή Νομοθεσία (GDPR - General Data Protection Regulation)

Η ευρωπαϊκή οδηγία για την προστασία των δεδομένων (οδηγία 95/46/EK) , η οποία σχεδιάστηκε το 1990 και εγκρίθηκε το 1995, θεωρείται βασικός πυλώνας του δικαίου σχετικά με την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής (Μήτρου,2017). Ωστόσο, παρά την γενική αποδοχή και αποτελεσματικότητα της Οδηγίας 95/46/EK, οι νέες δυνατότητες μεταφοράς πληροφοριών παγκοσμίως μέσω του διαδικτύου, δημιούργησαν την ανάγκη θέσπισης ενός νέου εξελιγμένου γενικού κανονισμού.

Ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) ισχύει από τις 25 Μαΐου 2018 σε όλα τα Κράτη-Μέλη της Ευρωπαϊκής Ένωσης, αντικαθιστώντας την Οδηγία 95/46/EK. Στη θέσπιση του νέου κανονισμού, οδήγησε η ανάγκη για ένα αυστηρότερο θεσμικό πλαίσιο που αφορά στην επεξεργασία των προσωπικών δεδομένων και κατ' επέκταση στην προστασίας τους. Παρ' όλα αυτά, ο νέος Κανονισμός δεν παρεκκλίνει ουσιωδώς από τις γενικές αρχές του προηγούμενου πλαισίου προστασίας των προσωπικών δεδομένων.

Οι καινοτόμες νομικές ρυθμίσεις του GDPR καθορίζουν τις υποχρεώσεις του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία, οι οποίοι είναι εγκατεστημένοι στην Ευρωπαϊκή Ένωση. Ωστόσο, στις ίδιες νομικές ρυθμίσεις υπόκεινται και οι υπεύθυνοι επεξεργασίας ή/και οι εκτελούντες επεξεργασία που είναι εγκατεστημένοι εκτός Ευρωπαϊκής Ένωσης εφόσον δραστηριοποιούνται α) σε παροχή αγαθών ή υπηρεσιών σε πρόσωπα εγκατεστημένα στην ΕΕ ή β) αφορούν την παρακολούθηση της συμπεριφοράς των εν λόγω προσώπων στον βαθμό που η συμπεριφορά τους λαμβάνει χώρα εντός της Ένωσης (άρθρο 3 παρ. 2).

Ο GDPR θεσπίζει και βασίζεται ταυτόχρονα στις κάτωθι καινοτόμες νομικές ρυθμίσεις:

α) στην θεμελίωση της επεξεργασίας σε νόμιμη βάση (άρθρα 6-10)

- β) στην τήρηση των αρχών επεξεργασίας (άρθρο 5)
- γ) στον σεβασμό των δικαιωμάτων των φυσικών προσώπων (άρθρα 12-23)
- δ) στην τήρηση των προσθέτων υποχρεώσεων που επιβάλλει ο ΓΚΠΔ (όπως η εκτίμηση αντικτύπου, η τήρηση αρχείων επεξεργασίας κ.α.) – (άρθρα 24-43).

Νόμιμες Βάσεις Επεξεργασίας

Η επεξεργασία καθίσταται σύννομη και συνταγματικά αποδεκτή, εφόσον αφενός εδράζεται σε βάσεις επεξεργασίας όπως αποτυπώνονται στο άρθρο 6 του GDPR και αφετέρου τηρεί τις αρχές στο σύνολό τους.

Οι προϋποθέσεις για μια νόμιμη επεξεργασία των προσωπικών δεδομένων (άρθρο 6 GDPR) είναι οι εξής:

- α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,*
- β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,*
- γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,*
- δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,*
- ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,*
- στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που*

επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί. (GDPR,2018)

Παρ' ότι ο κανονισμός θεσπίζει απαγόρευση της επεξεργασίας των ευαίσθητων προσωπικών δεδομένων κάμπτεται στις ακόλουθες περιπτώσεις όπου:

- i. το φυσικό πρόσωπο παράσχει ρητή συγκατάθεση για την επεξεργασία,
- ii. η επεξεργασία εκτελείται στα πλαίσια υποχρεώσεων/δικαιωμάτων του φυσικού προσώπου σε θέματα εργατικού δικαίου, δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας προκειμένου να εξασφαλιστούν ζωτικά συμφέροντα του φυσικού προσώπου. Η επεξεργασία πρέπει να πραγματοποιείται στα πλαίσια των νόμιμων δραστηριοτήτων του ιδρύματος, οργάνωσης κ.ο.κ.,
- iii. η επεξεργασία αφορά δεδομένα τα οποία έχουν δημοσιοποιηθεί από το φυσικό πρόσωπο,
- iv. η επεξεργασία είναι απαραίτητη για την υποστήριξη νομικών αξιώσεων,
- v. η επεξεργασία είναι απαραίτητη για ζητήματα δημόσιου συμφέροντος και δημόσιας υγείας,
- vi. η επεξεργασία είναι απαραίτητη για ιατρικούς σκοπούς,
- vii. η επεξεργασία είναι απαραίτητη για αρχειοθέτηση σε τομείς επιστημονικής ή ιστορικής ερευνάς ή στατιστικούς σκοπούς εφόσον εξυπηρετεί δημόσιο συμφέρον.

Ειδική μνεία απαιτείται για την συγκατάθεση του φυσικού προσώπου για τη επεξεργασία προσωπικών δεδομένων, η οποία πρέπει να παρέχεται με σαφή θετική ενέργεια του φυσικού προσώπου και με πλήρη επίγνωση της συμφωνίας υπέρ της επεξεργασίας των δεδομένων που το αφορούν. Η συγκατάθεση μπορεί να γίνει γραπτά, προφορικά ή με ηλεκτρονικά μέσα. Οποτεδήποτε μπορεί να ανακληθεί η συγκατάθεση του υποκειμένου χωρίς ειδική αιτιολογία με την προϋπόθεση ότι δεν θίγεται η νομιμότητα της μέχρι τότε επεξεργασίας.

Αρχές Επεξεργασίας

Σημαντικό ρολό διαδραματίζουν στον Κανονισμό οι αρχές (αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας, αρχή του σκοπού, αρχή της ελαχιστοποίησης, αρχή της ακρίβειας, αρχή της χρονικά περιορισμένης διατήρησης των δεδομένων, αρχή της ασφάλειας, αρχή της λογοδοσίας), που πρέπει να διέπουν την επεξεργασία προσωπικών δεδομένων οι οποίες διατυπώνονται στο άρθρο 5 του GDPR. Σε κάθε επεξεργασία πρέπει να διασφαλίζεται

από τον υπεύθυνο η σύννομη, αντικειμενική και διαφανή επεξεργασία δεδομένων σε σχέση με το υποκείμενο. Κάθε επεξεργασία προσωπικών δεδομένων θα πρέπει να βασίζεται σε μια από τις προβλεπόμενες νόμιμες βάσεις του Κανονισμού και το φυσικό πρόσωπο να είναι πλήρως ενημερωμένο για κάθε επεξεργασία προσωπικών του δεδομένων.

Σύμφωνα με την αρχή του σκοπού, η επεξεργασία πρέπει να είναι σαφής, νόμιμη και γνωστοποιημένη στο υποκείμενο των δεδομένων. Θα πρέπει να καθορίζονται οι δυνατότητες επέμβασης και συλλογής, περιορίζοντας ποιοτικά την εμβέλεια της επεξεργασίας και προσδιορίζοντας τη διάρκειά της (Λαμπρινουδάκης, Μήτρου, Γκρίτζαλης & Κατσίκας, 2009). Ειδικότερα, η αρχή «περιορισμού του σκοπού» καθορίζει την συλλογή των δεδομένων για καθορισμένους, ρητούς και νόμιμους σκοπούς. Λόγω της συγκεκριμένης αρχής, τα δεδομένα δεν επιτρέπεται να υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς (άρθρο 5 παρ. 1β).

Ο Κανονισμός για την αρχή της ελαχιστοποίησης απαιτεί να *«είναι [τα προσωπικά δεδομένα] κατάλληλα, συναφή και [να] περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία»* (GDPR,2018). Ο υπεύθυνος περιορίζεται στην επεξεργασία δεδομένων που παρουσιάζουν άμεση συνάφεια στον συγκεκριμένο σκοπό που επιδιώκεται με την επεξεργασία.

Η αρχή της ακρίβειας του GDPR υποχρεώνει τα δεδομένα να είναι ακριβή και να επικαιροποιούνται. Υποχρεώνει δε, σε διαγραφή ή σε διόρθωση δεδομένων τα ανακριβή δεδομένα που αποκλίνουν από τους σκοπούς της επεξεργασίας.

Όσον αφορά την αρχή της χρονικά περιορισμένης διατήρησης των δεδομένων, ο Κανονισμός επαναλαμβάνει την αρχή του «περιορισμού της περιόδου αποθήκευσης» προσδιορίζοντας ως νόμιμο χρονικό όριο διατήρησης των προσωπικών δεδομένων το διάστημα που απαιτείται για την επίτευξη των σκοπών (άρθρο 5 παρ. 1 ε)(ΕΔΔΑ,2008). Ως εξαίρεση της αρχής είναι οι επιστημονικοί, ιστορικοί, στατιστικοί και δημοσίου συμφέροντος σκοποί.

Η αρχή της ασφάλειας ως προς την ακεραιότητα και την εμπιστευτικότητα, παρατίθενται στο άρθρο 5 παράγραφος 1 στ («αρχές επεξεργασίας») και στο άρθρο 32 όπου παρατίθεται κατάλογος μέτρων ασφαλείας, όπως η ψευδωνυμοποίηση και η κρυπτογράφηση αλλά και διαδικασίες που συνιστούν πολιτική ασφαλείας.

Η ριζική αλλαγή που υπέστη ο Κανονισμός, είναι η εισαγωγή της αρχής της Λογοδοσίας (Accountability Principle), η οποία συνίσταται στο σχεδιασμό και εφαρμογή μέτρων και

πολιτικών βάσει του Κανονισμού. Ταυτόχρονα, θα πρέπει να αποδεικνύουν τη συμμόρφωση τους ενώπιον δικαστηρίων και εποπτικών αρχών όπως τεκμαίρεται από το άρθρο 24 παράγραφος 1 του Κανονισμού που διατυπώνει ως στοιχείο «ευθύνης» (*responsibility*) του υπεύθυνου επεξεργασίας την υποχρέωση να «εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον [παρόντα] κανονισμό».

Δικαιώματα των Υποκειμένων των Δεδομένων

Στο τρίτο κεφάλαιο του GDPR, ρυθμίζονται τα βασικά δικαιώματα των υποκειμένων των δεδομένων. Ο υπεύθυνος επεξεργασίας οφείλει να τηρεί ένα πλαίσιο γενικών αρχών και διαδικαστικών όρων προκειμένου να ασκηθούν αποτελεσματικά τα δικαιώματα των υποκειμένων. Οι σχετικές ρυθμίσεις για την άσκηση των δικαιωμάτων του υποκειμένου αναφέρονται στα άρθρα από 12 έως 22 του Κανονισμού. Πιο συγκεκριμένα υπογραμμίζονται, το δικαίωμα στην ενημέρωση στο άρθρο 12, το δικαίωμα στην πρόσβαση στο άρθρο 15, το δικαίωμα στην διόρθωση στο άρθρο 16, το δικαίωμα στην διαγραφή στο άρθρο 17, το δικαίωμα στον περιορισμό επεξεργασίας στο άρθρο 18, το δικαίωμα στην φορητότητα στο άρθρο 20, το δικαίωμα αντίρρησης στο άρθρο 21, το δικαίωμα εναντίωσης στην αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ στο άρθρο 22 και τέλος η δυνατότητα περιορισμού δικαιωμάτων από τον εθνικό νομοθέτη στο άρθρο 23. Το υποκείμενο των δεδομένων έχει δικαίωμα να ενημερώνεται για τα προσωπικά του δεδομένα με σαφή, κατανοητό και διαφανή τρόπο, μέσω εγγράφου ή ηλεκτρονικού τρόπου ή ακόμα και προφορικού εφόσον είναι αποδεδειγμένη η ταυτότητά του.

Στην περίπτωση που τα προσωπικά δεδομένα συλλέχθηκαν από το ίδιο το υποκείμενο, ο υπεύθυνος επεξεργασίας παρέχει σε αυτό τις παρακάτω πληροφορίες (άρθρο 13 του GDPR):

- α) την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας,
- β) τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση,
- γ) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία,

- δ) εάν η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο στ), τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο,
- ε) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν,
- στ) κατά περίπτωση, την πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή την απουσία απόφασης επάρκειας της Επιτροπής ή, όταν πρόκειται για τις διαβιβάσεις αναφέρονται στο άρθρο 46 ή 47 ή στο άρθρο 49 παράγραφος 1 δεύτερο εδάφιο, αναφορά στις ενδεδειγμένες ή κατάλληλες εγγυήσεις και τα μέσα για να αποκτηθεί αντίγραφο τους ή στο πού διατέθηκαν,
- ζ) το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,
- η) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορούν το υποκείμενο των δεδομένων ή δικαιώματος ανάταξης στην επεξεργασία, καθώς και δικαιώματος στη \ φορητότητα των δεδομένων,
- θ) όταν η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο α) ή στο άρθρο 9 παράγραφος 2 στοιχείο α), την ύπαρξη του δικαιώματος να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε, χωρίς να θίγει η νομιμότητα τη επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της,
- ι) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,
- κ) κατά πόσο η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική ή συμβατική υποχρέωση ή απαίτηση για τη σύναψη σύμβασης, καθώς και κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ποιες ενδεχόμενες συνέπειες θα είχε η μη παροχή των δεδομένων αυτών (GDPR,2018).

Όταν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεχθεί από το υποκείμενο των δεδομένων (άρθρο 14 GDPR), ο υπεύθυνος επεξεργασίας υποχρεούται εκτός από τις ανωτέρω πληροφορίες να ενημερώσει το υποκείμενο σχετικά με την πηγή των πληροφοριών και την

προσβασιμότητα της πηγής από το κοινό. Η παροχή πληροφοριών από το αίτημα του υποκειμένου δεν πρέπει να υπερβαίνει τον ένα μήνα.

Οι περιπτώσεις που δεν εφαρμόζει, ο υπεύθυνος επεξεργασίας, τα παραπάνω (άρθρο 14 παρ.5) είναι:

- α) Όταν το υποκείμενο των δεδομένων διαθέτει ήδη τις πληροφορίες.
- β) Όταν η παροχή τέτοιων πληροφοριών αποδεικνύεται αδύνατη ή θα συνεπαγόταν δυσανάλογη προσπάθεια.
- γ) Όταν η απόκτηση ή κοινολόγηση προβλέπεται ρητώς από το ενωσιακό δίκαιο ή το εθνικό δίκαιο του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, το οποίο παρέχει τα κατάλληλα μέτρα για την προστασία των εννόμων συμφερόντων του υποκειμένου των δεδομένων.
- δ) Όταν τα δεδομένα προσωπικού χαρακτήρα πρέπει να παραμείνουν εμπιστευτικά δυνάμει υποχρέωσης επαγγελματικού απορρήτου (GDPR,2018).

Το δικαίωμα της πρόσβασης καταλαμβάνει κομβική θέση στο σύστημα των δικαιωμάτων καθώς εξασφαλίζει την δυνατότητα ενός προσώπου να ζητά επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία και, εάν συμβαίνει αυτό, την πρόσβαση στα δεδομένα προσωπικού χαρακτήρα και σε πληροφορίες σχετικά με τους σκοπούς της επεξεργασίας, τους αποδέκτες κ.α. Ο υπεύθυνος επεξεργασίας παρέχει αντίγραφο των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Για επιπλέον αντίγραφα που ενδέχεται να ζητηθούν από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας μπορεί να επιβάλει την καταβολή εύλογου τέλους για διοικητικά έξοδα. Επίσης, ανεξάρτητα του τρόπου που υποβάλλει το αίτημα το υποκείμενο, η ενημέρωση παρέχεται σε ηλεκτρονική μορφή.

Στο δικαίωμα της διόρθωσής (άρθρο 16 του GDPR), το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας, χωρίς αδικαιολόγητη καθυστέρηση, τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Έχοντας υπόψιν τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλিপών δεδομένων προσωπικού χαρακτήρα μεταξύ άλλων, μέσω συμπληρωματικής δήλωσης.

Το δικαίωμα διαγραφής (άρθρο 17) που φέρει και τον παράτιτλο «δικαίωμα στην λήθη», υποχρεώνει τον υπεύθυνο επεξεργασίας να διαγράψει τα δεδομένα εφόσον:

- α) στερούνται νόμιμης βάσης (ανάκληση συγκατάθεσης, παράνομη επεξεργασία, υπέρβαση αναγκαίου για τον σκοπό χρόνου τήρησης), ή*
- β) η διαγραφή επιβάλλεται εκ του νόμου, ή*
- γ) ασκείται λυσιτελώς το δικαίωμα εναντίωσης στην επεξεργασία ή*
- δ) πρόκειται για δεδομένα που είχαν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών σε παιδί (άρθρο 8).*

Στο δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18), το υποκείμενο των δεδομένων δικαιούται να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό των δεδομένων που τυγχάνουν επεξεργασίας όταν:

- α) η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα,*
- β) η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους,*
- γ) ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων,*
- δ) το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερισχύουν έναντι των λόγων του υποκειμένου των δεδομένων.*

Το δικαίωμα στην φορητότητα (άρθρο 20) συνίσταται σε δύο βασικά δικαιώματα:

- στο δικαίωμα του υποκειμένου να λαμβάνει δεδομένα που έχει χορηγήσει στον υπεύθυνο επεξεργασίας και

- στο δικαίωμα να διαβιβάζει δεδομένα χωρίς να αποτρέπεται σε αυτό από τον υπεύθυνο επεξεργασίας.

Με το δικαίωμα φορητότητας δίνεται η δυνατότητα στην ευχερή «μετακίνηση» δεδομένων από πάροχο σε πάροχο, κυρίως στα ψηφιακά κοινωνικά δίκτυα. Ο Κανονισμός οριοθετεί το δικαίωμα της φορητότητας και δεν επιτρέπει να επηρεάζει τα δικαιώματα και τις ελευθερίες τρίτων, όπως πνευματικά δικαιώματα ή εταιρικά απόρρητα.

Το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, η οποία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο ε) ή στ), περιλαμβανομένης της κατάρτισης προφίλ βάσει των εν λόγω διατάξεων. Ο υπεύθυνος επεξεργασίας δεν υποβάλλει πλέον τα δεδομένα προσωπικού χαρακτήρα σε επεξεργασία, εκτός εάν ο υπεύθυνος επεξεργασίας καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία οι οποίοι υπερσχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων (GDPR, 2018).

Το δικαίωμα της αντίρρησης είναι απόλυτο στην περίπτωση επεξεργασίας για σκοπούς marketing. Εάν δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν για την εν λόγω εμπορική προώθηση, περιλαμβανομένης της κατάρτισης προφίλ, εάν σχετίζεται με αυτήν την απευθείας εμπορική προώθηση. Όταν τα υποκείμενα των δεδομένων αντιτίθενται στην επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, τα δεδομένα προσωπικού χαρακτήρα δεν υποβάλλονται πλέον σε επεξεργασία για τους σκοπούς αυτούς.

Σύμφωνα με το άρθρο 22 του GDPR, το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο. Ωστόσο, ο Κανονισμός αποδέχεται υπό την αίρεση εγγυήσεων (κατάλληλων μέτρων) και την αυτοματοποιημένη λήψη ατομικής απόφασης και της κατάρτισης προφίλ, εάν η επεξεργασία θεμελιώνεται στην ρητή συγκατάθεση του υποκειμένου ή στην επιδίωξη δημόσιου συμφέροντος.

Η εθνική νομοθεσία των κρατών μελών μπορεί να περιορίσει την εφαρμογή των δικαιωμάτων του Κανονισμού στον βαθμό που αυτοί σέβονται τα θεμελιώδη δικαιώματα και

τις ελευθερίες των ατόμων (άρθρο 23). Για να είναι αποδεκτοί οι περιορισμοί των δικαιωμάτων, θα πρέπει να αποτελεί αναγκαίο και αναλογικό μέτρο για την διασφάλιση:

α) της ασφάλειας του κράτους,

β) της εθνικής άμυνας,

γ) της δημόσιας ασφάλειας,

δ) της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανόμενης της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της πρόληψης αυτών,

ε) άλλων σημαντικών στόχων γενικού δημόσιου συμφέροντος της Ένωσης ή κράτους μέλους, ιδίως σημαντικού οικονομικού ή χρηματοοικονομικού συμφέροντος της Ένωσης ή κράτους μέλους, συμπεριλαμβανομένων των νομισματικών, δημοσιονομικών και φορολογικών θεμάτων, της δημόσιας υγείας και της κοινωνικής ασφάλισης,

στ) της προστασίας της ανεξαρτησίας της δικαιοσύνης και των δικαστικών διαδικασιών,

ζ) της πρόληψης, της διερεύνησης, της ανίχνευσης και της δίωξης παραβάσεων δεοντολογίας σε νομοθετικά κατοχυρωμένα επαγγέλματα,

η) της παρακολούθησης, της επιθεώρησης ή της κανονιστικής λειτουργίας που συνδέεται, έστω περιστασιακά, με την άσκηση δημόσιας εξουσίας στις περιπτώσεις που αναφέρονται στα στοιχεία α) έως ε) και ζ),

θ) της προστασίας του υποκειμένου των δεδομένων ή των δικαιωμάτων και των ελευθεριών τρίτων,

ι) της εκτέλεσης αστικών αξιώσεων.

Με την ενίσχυση των δικαιωμάτων του GDPR επιδιώκεται η θωράκιση του υποκειμένου και η ανάκτηση ελέγχου επί των δεδομένων. Ο ενωσιακός νομοθέτης επιχειρεί να ενδυναμώσει την θέση των φυσικών προσώπων ως προς την προάσπιση των δικαιωμάτων τους. Επιπλέον, πρέπει να υπάρχει πρόσβαση των υποκειμένων σε διοικητικές και δικαστικές διαδικασίες προκειμένου να διορθωθούν πρακτικές επεξεργασίες και να επανορθωθούν βλάβες που έχουν τυχόν υποστεί. Κάθε υποκείμενο των δεδομένων έχει το δικαίωμα να υποβάλει καταγγελία σε

εποπτική αρχή, ιδίως στο κράτος μέλος στο οποίο έχει τη συνήθη διαμονή του ή τον τόπο εργασίας του ή τον τόπο της εικαζόμενης παράβασης, εάν το υποκείμενο των δεδομένων θεωρεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορά παραβαίνει τον GDPR. Η εποπτική αρχή, στην οποία έχει υποβληθεί καταγγελία, ενημερώνει τον καταγγέλλοντα για την πρόοδο και για την έκβαση της καταγγελίας, καθώς και για τη δυνατότητα άσκησης δικαστικής προσφυγής σύμφωνα με το άρθρο 78.

Αντίστοιχη είναι η προσέγγιση και ως προς τη δικαστική προστασία των υποκειμένων των δεδομένων. Τα φυσικά πρόσωπα μπορούν να στραφούν δικαστικά τόσο κατά του υπευθύνου επεξεργασίας όσο και κατά του εκτελούντος, επιλέγοντας είτε τον τόπο εγκατάστασης του υπευθύνου ή του εκτελούντος είτε τον τόπο της δικής του συνήθους διαμονής (άρθρο 79 παρ.2). Επίσης, ο GDPR προβλέπει (άρθρο 80) το δικαίωμα του φυσικού προσώπου να αναθέτει σε οργάνωση ή ένωση ή σε μη κερδοσκοπικό φορέα να καταθέτει την καταγγελία για λογαριασμό του προκειμένου να ασκήσει τα δικαιώματα ενώπιον δικαστηρίου και να αιτηθεί αποζημίωσης εξ ονόματός του εφόσον προβλέπεται από την νομοθεσία του κράτους μέλους.

Εποπτική Αρχή

Κάθε εποπτική αρχή στο έδαφός της παρακολουθεί και επιβάλλει την εφαρμογή του GDPR, προωθεί την ευαισθητοποίηση του κοινού και την κατανόηση των κανόνων, συμβουλεύει σύμφωνα με το δίκαιο του κράτους μέλους, ενώ προωθεί την ευαισθητοποίηση των υπεύθυνων επεξεργασίας και των εκτελούντων την επεξεργασία. Κατόπιν αιτήματος, παρέχει πληροφορίες στα υποκείμενα των δεδομένων όσον αφορά την άσκηση των δικαιωμάτων τους, χειρίζεται τις καταγγελίες που υποβάλλονται και διενεργεί έρευνες σχετικά με την εφαρμογή του GDPR. Τέλος, αναπτύσσει συμβουλευτικό ρόλο έναντι της νομοθετικής εξουσίας και της διοίκησης (άρθρο 57 παρ.1). Η ανεξάρτητη αρχή σχετικά με την διασυνοριακή ροή επιτρέπει συμβατικές ρήτρες και εγκρίνει δεσμευτικούς εταιρικούς κανόνες προκειμένου να προστατεύσει τα δικαιώματα των προσώπων όταν τα δεδομένα τους διαβιβάζονται σε τρίτες χώρες.

Καθοριστική είναι η λειτουργία της ανεξάρτητης αρχής σχετικά με τα εργαλεία της συμμόρφωσης και της λογοδοσίας. Η ανεξάρτητη αρχή, υιοθετεί και τηρεί αυστηρά μέτρα στην ασφαλεία και στην διαδικασία γνωστοποίησης παραβίασης δεδομένων (άρθρα 32-33). Κρίσιμος είναι και ο ρόλος της σε σχέση με τους κώδικες δεοντολογίας (άρθρο 40) και την θέσπιση μηχανισμών πιστοποίησης (άρθρο 42). Αξιοσημείωτη είναι και η κανονιστική

αποτύπωση των εξουσιών, στις οποίες συγκαταλέγονται οι εξουσίες διερεύνησης αλλά και αδειοδοτικές και συμβουλευτικές εξουσίες (άρθρο 58 παρ.3). Σημαντικές είναι επίσης οι διορθωτικές εξουσίες της ανεξάρτητης αρχής, οι εξουσίες που σχετίζονται με την επιβολή κυρώσεων και την παραπομπή παραβάσεων των διατάξεων του Κανονισμού στις δικαστικές αρχές, καθώς και το δικαίωμα να συμμετέχουν σε νομικές διαδικασίες. Ο ενωσιακός νομοθέτης επιτάσσει να ασκούνται οι εξουσίες των εποπτικών αρχών σύμφωνα με το δίκαιο, αμερόληπτα, δίκαια και σε εύλογο χρονικό διάστημα.

Κυρώσεις

Τα κράτη μέλη θεσπίζουν τους κανόνες σχετικά με τις άλλες κυρώσεις που επιβάλλονται για παραβάσεις του παρόντος κανονισμού, ιδίως για τις παραβάσεις που δεν αποτελούν αντικείμενο διοικητικών προστίμων δυνάμει του άρθρου 83, και λαμβάνουν όλα τα αναγκαία μέτρα για να διασφαλιστεί ότι εφαρμόζονται. Οι εν λόγω κυρώσεις είναι αποτελεσματικές, αναλογικές και αποτρεπτικές (άρθρο 84). (GDPR,2018)

Τα διοικητικά πρόστιμα αποτελούν το ισχυρότερο κυρωτικό εργαλείο του GDPR. Οι ρυθμίσεις του άρθρου 83 καθορίζουν το ύψος των προστίμων και το πεδίο των παραβάσεων για τις οποίες επιβάλλονται. Ο GDPR επισύρει διοικητικά πρόστιμα α) έως δέκα εκατομμύρια ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους και β) πρόστιμα έως είκοσι εκατομμύρια ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους. Επιβάλλεται το υψηλότερο πρόστιμο σε περίπτωση παρεμπόδισης της άσκησης των ελεγκτικών εξουσιών της εποπτικής αρχής ή και μη συμμόρφωσης προς τις εντολές της. Ο ενωσιακός νομοθέτης όρισε το ανώτατο ύψος των προστίμων αλλά μερίμνησε ώστε «η επιβολή διοικητικών προστίμων να είναι για κάθε μεμονωμένη περίπτωση αποτελεσματική, αναλογική και αποτρεπτική» (άρθρο 83 παρ.1), επιδιώκοντας μία προληπτική - παραδειγματική λειτουργία της επιβολής των κυρώσεων.

Στον προσδιορισμό του ύψους του προστίμου βασικοί παράγοντες είναι η ύπαρξη δόλου ή αμέλειας, ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία (βάσει των άρθρων 25 και 32), η προσπάθεια μετριασμού των επιπτώσεων της παράβασης, προηγούμενα πρόστιμα αλλά και ο βαθμός συνεργασίας και συμμόρφωσης με την εποπτική αρχή. Σε συνάρτηση με την αρχή της λογοδοσίας, ο ενωσιακός νομοθέτης εντάσσει στα κριτήρια την τήρηση εγκεκριμένων κωδικών δεοντολογίας (άρθρο 40) ή εγκεκριμένων

μηχανισμών πιστοποίησης (άρθρο 42). Η κύρωση θα πρέπει να είναι τέτοιας τάξεως ώστε να μην είναι οικονομικά συμφέρουσα η παρανομία. Ο GDPR καλεί την εποπτική αρχή να *«λαμβάνει υπόψη το γενικό επίπεδο εισοδημάτων στο κράτος μέλος, καθώς και την οικονομική κατάσταση του προσώπου, όταν εξετάζει το ενδεδειγμένο ποσό του προστίμου»*. Ο Κανονισμός αφήνει στη διακριτική ευχέρεια του κράτους μέλους να καθορίζει τους κανόνες για το εάν και σε ποιο βαθμό τα διοικητικά πρόστιμα μπορεί να επιβάλλονται σε δημόσιες αρχές και δημόσιους φορείς.

1.2.2 Αμερικανική Νομοθεσία περί Προσωπικών Δεδομένων

Στις ΗΠΑ, δεν υπάρχει ενιαίος, περιεκτικός ομοσπονδιακός νόμος που να ρυθμίζει τη συλλογή και χρήση προσωπικών δεδομένων. Ωστόσο, κάθε όρος του Κογκρέσου φέρνει προτάσεις για την τυποποίηση των νόμων σε ομοσπονδιακό επίπεδο. Αντ' αυτού, οι ΗΠΑ έχουν ένα συνονθύλευμα ομοσπονδιακών και κρατικών νόμων και κανονισμών που μπορεί μερικές φορές να επικαλύπτονται, να συμπλέκονται και να αντιβαίνουν ο ένας στον άλλο. Επιπλέον, υπάρχουν πολλές κατευθυντήριες γραμμές που αναπτύσσονται από κυβερνητικούς οργανισμούς και βιομηχανικές ομάδες που δεν έχουν ισχύ νόμου, αλλά αποτελούν μέρος κατευθυντήριων γραμμών και πλαισίων αυτορρύθμισης που θεωρούνται «βέλτιστες πρακτικές». Αυτά τα πλαίσια αυτορρύθμισης έχουν στοιχεία λογοδοσίας και επιβολής, τα οποία χρησιμοποιούνται ολοένα και περισσότερο ως μέσο επιβολής από τις ρυθμιστικές αρχές.

Υπάρχει ήδη μια σειρά από ομοσπονδιακούς νόμους σχετικούς με την προστασία της ιδιωτικής ζωής που ρυθμίζουν τη συλλογή και τη χρήση προσωπικών δεδομένων. Ορισμένοι ισχύουν για συγκεκριμένες κατηγορίες πληροφοριών, όπως οικονομικές ή υγειονομικές πληροφορίες ή ηλεκτρονικές επικοινωνίες. Άλλοι ισχύουν για δραστηριότητες που χρησιμοποιούν προσωπικές πληροφορίες, όπως τηλεμπορία και εμπορικό ηλεκτρονικό ταχυδρομείο. Επιπλέον, υπάρχουν ευρείς νόμοι για την προστασία των καταναλωτών οι οποίοι δεν ταυτίζονται με τους νόμους περί προστασίας της ιδιωτικής ζωής, αλλά έχουν χρησιμοποιηθεί για την απαγόρευση των αθέμιτων ή παραπλανητικών πρακτικών που αφορούν στη γνωστοποίηση και στις διαδικασίες ασφαλείας για την προστασία προσωπικών πληροφοριών.

Μερικοί από τους πιο σημαντικούς ομοσπονδιακούς νόμους περί ιδιωτικότητας περιλαμβάνουν, χωρίς περιορισμό, τα ακόλουθα:

- Ο νόμος της Federal Trade Commission (15 U.S.C. §§41-58) (FTC Act) είναι ένας ομοσπονδιακός νόμος για την προστασία των καταναλωτών που απαγορεύει τις αθέμιτες ή παραπλανητικές πρακτικές και έχει εφαρμοστεί στις πολιτικές προστασίας προσωπικών δεδομένων σε απευθείας σύνδεση στο διαδίκτυο (online) και εκτός σύνδεσης (offline). Η FTC, έχει ασκήσει πολλές ενέργειες επιβολής ενάντια σε εταιρείες που δεν συμμορφώνονται με τις δημοσιευμένες πολιτικές απορρήτου και για μη εξουσιοδοτημένη αποκάλυψη προσωπικών δεδομένων. Η FTC είναι επίσης ο κύριος υπεύθυνος για την εφαρμογή του νόμου για την προστασία της ιδιωτικής ζωής των παιδιών στο Διαδίκτυο (COPPA) (15 U.S.C. §§6501-6506), η οποία ισχύει για την ηλεκτρονική συλλογή πληροφοριών από παιδιά και τις Αυτορρυθμιζόμενες Αρχές για τη Συμπεριφορική Διαφήμιση.
- Ο νόμος περί εκσυγχρονισμού των χρηματοπιστωτικών υπηρεσιών (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827) ρυθμίζει τη συλλογή, τη χρήση και τη γνωστοποίηση οικονομικών πληροφοριών. Μπορεί να εφαρμοστεί ευρέως σε χρηματοπιστωτικά ιδρύματα όπως τράπεζες, εταιρείες κινητών αξιών, ασφαλιστικές εταιρείες και σε άλλες επιχειρήσεις που παρέχουν χρηματοπιστωτικές υπηρεσίες και προϊόντα. Η GLB περιορίζει τη γνωστοποίηση μη προσωπικών πληροφοριών και σε ορισμένες περιπτώσεις απαιτεί από τα χρηματοπιστωτικά ιδρύματα να ενημερώνουν για τις πρακτικές προστασίας προσωπικών δεδομένων τους και δίνει την ευκαιρία στα άτομα, στα οποία αναφέρονται τα δεδομένα, να επιλέξουν να μην μοιράζονται τις πληροφορίες τους. Επιπλέον, υπάρχουν διάφοροι Κανόνες Προστασίας Προσωπικών Δεδομένων που δημοσιεύονται από τις εθνικές τραπεζικές υπηρεσίες, ο Κανονισμός Διασφαλίσεων, Κανόνες Απόρριψης και Κανόνες Κόκκινων Σημαιών που έχουν εκδοθεί από την FTC και αφορούν στην προστασία και διάθεση οικονομικών στοιχείων.
- Ο Νόμος περί Φορητότητας και Υπευθυνότητας Ασφάλισης Υγείας (HIPAA) (42 U.S.C. § 1301 και επόμενα) ρυθμίζει ιατρικές πληροφορίες. Μπορεί να εφαρμοστεί στους παρόχους υγειονομικής περίθαλψης, επεξεργαστές δεδομένων, φαρμακεία και άλλες οντότητες που έρχονται σε επαφή με ιατρικές πληροφορίες. Τα πρότυπα για την

προστασία προσωπικών δεδομένων των ατομικά αναγνωρίσιμων πληροφοριών για την υγεία (HIPAA Privacy Rule) (45 C.F.R. Μέρη 160 και 164) ισχύουν για τη συλλογή και τη χρήση προστατευμένων πληροφοριών υγείας (PHI). Τα πρότυπα ασφαλείας για την προστασία των πληροφοριών ηλεκτρονικής προστατευμένης υγείας (HIPAA Security Rule) (45 C.F.R. 160 και 164) παρέχουν πρότυπα για την προστασία των ιατρικών δεδομένων. Τα Πρότυπα Ηλεκτρονικών Συναλλαγών (Κώδικας Συναλλαγών HIPAA) (45 C.F.R. 160 και 162) ισχύουν για την ηλεκτρονική διαβίβαση ιατρικών δεδομένων. Οι παραπάνω κανόνες της HIPAA αναθεωρήθηκαν στις αρχές του 2013 βάσει του "Omnibus Rule" της HIPAA.

- Το άρθρο Omnibus της HIPAA αναθεώρησε επίσης τον κανόνα κοινοποίησης παραβίασης ασφαλείας (45 C.F.R. Part 164), ο οποίος απαιτεί από τις καλυπτόμενες οντότητες να ενημερώσουν για παραβίαση προστατευόμενων πληροφοριών για την υγεία. Σύμφωνα με τον αναθεωρημένο κανόνα, μια καλυπτόμενη οντότητα θα πρέπει να παρέχει ειδοποίηση απόκτησης, πρόσβασης, χρήσης ή αποκάλυψης του PHI κατά τρόπο μη επιτρεπτό από τον Κανόνα περί Προστασίας Προσωπικών Δεδομένων, εκτός εάν η καλυπτόμενη οντότητα ή επιχειρηματικός συνεργάτης αποδείξει ότι υπάρχει μικρή πιθανότητα η προστατευόμενη υγεία και οι πληροφορίες να διακυβευτούν.

Τα περισσότερα κράτη των Ηνωμένων Πολιτειών έχουν θεσπίσει κάποια μορφή νομοθεσίας για την προστασία της ιδιωτικής ζωής. Ωστόσο, η Καλιφόρνια πρωτοστατεί στον χώρο της ιδιωτικής ζωής, έχοντας θεσπίσει πολλαπλούς νόμους περί ιδιωτικότητας, μερικοί από τους οποίους έχουν εκτεταμένες επιπτώσεις σε εθνικό επίπεδο.

Η Καλιφόρνια ήταν το πρώτο κράτος που θέσπισε νόμο κοινοποίησης παραβίασης της ασφάλειας (Πολιτικός Κώδικας της Καλιφόρνιας §1798.82). Ο νόμος απαιτεί από οποιοδήποτε πρόσωπο ή επιχείρηση που κατέχει ή διαθέτει ηλεκτρονικά δεδομένα που περιλαμβάνουν προσωπικά στοιχεία, να αποκαλύψει τυχόν παραβίαση της ασφάλειας του συστήματος σε όλους τους κατοίκους της Καλιφόρνιας των οποίων τα μη κρυπτογραφημένα προσωπικά στοιχεία αποκτήθηκαν από μη εξουσιοδοτημένο πρόσωπο. Οι περισσότεροι από τους νόμους έγκαιρης κοινοποίησης παραβίασης της ασφάλειας της χώρας αντικατόπτριζαν τον νόμο της Καλιφόρνιας και τείνουν να είναι αντιδραστικοί, δηλαδή καθόρισαν τις απαιτήσεις για την αντιμετώπιση μιας παραβίασης της ασφάλειας. Πιο πρόσφατα, αρκετοί νόμοι των κρατών

έχουν θεσπίσει κανονιστικούς και προληπτικούς νόμους, δηλαδή οι νόμοι αυτοί είναι πιο αυστηροί και στην πραγματικότητα δημιουργούν απαιτήσεις για την αποφυγή παραβίασης της ασφάλειας. Το καλύτερο παράδειγμα προληπτικού νόμου είναι ο Κανονισμός της Μασαχουσέτης (201 CMR 17.00), ο οποίος προβλέπει έναν εκτεταμένο κατάλογο τεχνικών, φυσικών και διοικητικών πρωτοκόλλων ασφαλείας που αποσκοπούν στην προστασία των προσωπικών πληροφοριών που πρέπει να εφαρμόζουν οι εταιρείες στην αρχιτεκτονική τους ασφαλείας και να περιγράφουν σε ένα ολοκληρωμένο γραπτό πρόγραμμα την αρχιτεκτονική ασφαλείας των πληροφοριών.

Από τις 28 Μαρτίου 2018 και τα 50 κράτη, καθώς και η περιφέρεια της Κολούμπια, το Πουέρτο Ρίκο και οι αμερικανικές Παρθένοι Νήσοι έχουν θεσπίσει νόμους που απαιτούν την κοινοποίηση παραβιάσεων ασφαλείας που αφορούν στα προσωπικά δεδομένα. Οι νέοι νόμοι και οι προτεινόμενες τροποποιήσεις αυξάνονται διαρκώς, οι τεχνολογικές απειλές αλλάζουν, καθώς και η πρόοδος προς την ομοιόμορφη ομοσπονδιακή νομοθεσία. Για παράδειγμα, η Καλιφόρνια παρακολουθεί την εφαρμογή ποικίλων νόμων περί απορρήτου δεδομένων και όπου χρειάζεται τροποποιεί του νόμους που θέσπισε το 2015, όπως:

- Το νόμο περί προστασίας της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες της Καλιφόρνια (S.B. 178), ο οποίος περιορίζει σημαντικά την ικανότητα των κυβερνητικών αρχών να αναζητούν πληροφορίες ηλεκτρονικών επικοινωνιών για σκοπούς επιβολής του νόμου.
- Το νόμο περί κοινοποίησης παραβιάσεων της ασφάλειας (S.B. 570), ο οποίος τροποποιεί το απαιτούμενο περιεχόμενο των ανακοινώσεων παραβίασης της ασφάλειας, απαιτώντας οι ειδοποιήσεις να εμφανίζουν σαφώς και εμφανώς ορισμένες συγκεκριμένες επικεφαλίδες.
- Το νόμο A.B. 964 ο οποίος ορίζει τον όρο «κρυπτογραφημένο» για τους σκοπούς του νόμου της Καλιφόρνιας για την κοινοποίηση παραβιάσεων ως «άχρηστο, μη αναγνωρίσιμο ή ανεξήγητο σε μη εξουσιοδοτημένο πρόσωπο μέσω τεχνολογίας ασφαλείας ή μεθοδολογίας γενικά αποδεκτής στον τομέα της ασφάλειας πληροφοριών». Ο συγκεκριμένος νόμος τέθηκε σε ισχύ την 1η Ιανουαρίου 2016.
- Το νόμος A.B. 1541, ο οποίος τροποποιεί τον ορισμό των «προσωπικών πληροφοριών» στο καταστατικό του κράτους για την προστασία της ιδιωτικής ζωής, ώστε να περιλαμβάνει το όνομα χρήστη ή τη διεύθυνση ηλεκτρονικού ταχυδρομείου σε

συνδυασμό με το κωδικό πρόσβασης ή την ερώτηση ασφαλείας και την απάντηση για πρόσβαση σε λογαριασμό στο διαδίκτυο, καθώς και πληροφορίες ασφάλισης υγείας.

Τον Ιούλιο του 2018, η Καλιφόρνια πέρασε τον πιο σαρωτικό όλων των νόμων περί απορρήτου στις ΗΠΑ, τον California Privacy Act για το 2018 (που ισχύει από την 1η Ιανουαρίου 2020). Ο νόμος παρέχει στους πολίτες πολλά νέα δικαιώματα, συμπεριλαμβανομένου του δικαιώματος:

- Της απαίτησης της διαγραφής των προσωπικών δεδομένων οποιουδήποτε φυσικού προσώπου.
- Της γνωστοποίησης πληροφοριών σχετικά με τον τρόπο συλλογής και κοινής χρήσης πληροφοριών.
- Της απαγόρευσης πώλησης των δεδομένων από οποιαδήποτε εταιρεία.

Υπάρχει επίσης ένα ιδιωτικό δικαίωμα δράσης για τα άτομα να καταδιώκουν τους παραβάτες, γεγονός που πιθανώς να οδηγήσει σε αξιόλογες αγωγές κατηγορίας στην Καλιφόρνια. Πρόκειται για περίπλοκο νόμο ο οποίος εξακολουθεί να υπόκειται σε ενδεχόμενες αναθεωρήσεις πριν από την ημερομηνία εφαρμογής του 2020. (*Ieuan Jolly, Loeb & Loeb, 2018*)

1.2.3 Privacy Shield EU–US (Ασφάλεια Απορρήτου) Μνημόνιο Συνεργασίας μεταξύ Αμερικής και Ευρώπης περί Προσωπικών Δεδομένων

Το Privacy Shield είναι ένα πλαίσιο Ασφαλείας Προστασίας Προσωπικών Δεδομένων που σχεδιάστηκε από το Υπουργείο Εμπορίου των ΗΠΑ και από την Ευρωπαϊκή Επιτροπή για να ρυθμίσει τις διατλαντικές ανταλλαγές προσωπικών δεδομένων για εμπορικούς σκοπούς μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών. Ο σκοπός της συμφωνίας είναι να δοθεί η δυνατότητα σε εταιρείες εγκατεστημένες στις ΗΠΑ, οι οποίες κρίνονται ότι προσφέρουν ένα επαρκές επίπεδο προστασίας προσωπικών δεδομένων, να μεταφέρουν δεδομένα από την Ένωση στις ΗΠΑ. Η ανταλλαγή θα πραγματοποιείται σύμφωνα με τους νόμους της ΕΕ για την προστασία της ιδιωτικής ζωής που αποσκοπούν στην προστασία των πολιτών της Ευρωπαϊκής Ένωσης. Η συμφωνία Privacy Shield μεταξύ ΕΕ και ΗΠΑ είναι

διάδοχος της συμφωνίας-πλαισίου Safe Harbour η οποία υπογράφηκε το 2000, ακυρώθηκε όμως μετά την απόφαση του ΔΕΕ τον Οκτώβριο του 2015, καθώς κρίθηκε ότι δεν ήταν αρκετά αυστηρή αναφορικά με το επίπεδο προστασίας των προσωπικών δεδομένων των πολιτών της ΕΕ. Η Ευρωπαϊκή Επιτροπή αντέδρασε τότε αμέσως ξεκινώντας διαπραγματεύσεις για μια νέα συμφωνία Privacy Shield προκειμένου να εγγυηθεί «επαρκές» επίπεδο προστασίας των προσωπικών δεδομένων που μεταφέρονται και αποθηκεύονται σε εταιρείες στις ΗΠΑ. Το νέο ισχύον πλαίσιο για τις μεταφορές δεδομένων μεταξύ ΕΕ και ΗΠΑ υιοθετήθηκε τον Ιούλιο του 2016(Privacy Shield Framework,2016).

Με την εφαρμογή της συμφωνίας διαπιστώθηκε ότι υπήρχαν τρωτά σημεία που οδήγησαν στην μη τήρηση της. Η διαπίστωση αυτή αφορούσε στο σκάνδαλο παραβίασης προσωπικών δεδομένων «Facebook-Cambridge Analytica», δεδομένου ότι και οι δύο εταιρείες είναι πιστοποιημένες στο πλαίσιο της συμφωνίας Privacy Shield. Οι ευρωβουλευτές που μετέχουν στη σύνθεση της ως άνω Επιτροπής του ΕΚ, τονίζουν την ανάγκη για καλύτερη εποπτεία της συμφωνίας. Έτσι, με ψήφισμά που εγκρίθηκε την Τρίτη 12 Ιουλίου 2018, οι ευρωβουλευτές ζητούν από τις ΗΠΑ να συμμορφωθούν το αργότερο έως την 1η Σεπτεμβρίου όσον αφορά στην συμφωνία Privacy Shield για την μεταφορά δεδομένων. Το εν λόγω ψήφισμα, μεταξύ άλλων, καταλήγει στα εξής:

- Η συμφωνία για την μεταφορά προσωπικών δεδομένων μεταξύ ΕΕ και ΗΠΑ δεν παρέχει υψηλό επίπεδο ασφαλείας.
- Οι ευρωβουλευτές προτείνουν την αναστολή της εφαρμογής της συμφωνίας σε περίπτωση που οι ΗΠΑ δε συμμορφωθούν πλήρως το αργότερο μέχρι την 1η Σεπτεμβρίου.
- Η υπόθεση παραβίασης προσωπικών δεδομένων «Facebook-Cambridge Analytica» κατέδειξε ότι υπάρχει περιορισμένη προστασία από πλευράς ΗΠΑ.

Ειδικότερα, η Επιτροπή Πολιτικών Ελευθεριών, Δικαιοσύνης και Εσωτερικών Υποθέσεων του Ευρωπαϊκού Κοινοβουλίου (ΕΚ) προτείνει στην Ευρωπαϊκή Επιτροπή να αναστείλει τη συμφωνία Privacy Shield μεταξύ ΕΕ-ΗΠΑ καθώς δεν υπάρχει ικανοποιητικό επίπεδο προστασίας δεδομένων για τους πολίτες της Ένωσης. Η συμφωνία θα ανασταλεί στην περίπτωση που οι Ηνωμένες Πολιτείες δε συμμορφωθούν με αυτή μέχρι την 1η Σεπτεμβρίου 2018, βάση των δηλώσεων των ευρωβουλευτών. Επιπλέον οι ευρωβουλευτές πρόσθεσαν ότι η συμφωνία θα πρέπει να συνεχίσει να βρίσκεται σε κατάσταση αναστολής μέχρι οι αμερικανικές αρχές να συμμορφωθούν πλήρως με τα όσα έχουν οριστεί. Ταυτόχρονα ζητούν

απο τις αμερικανικές αρχές να δρουν χωρίς καμία καθυστέρηση σε παρόμοιες περιπτώσεις παραβιάσεων και εάν αυτό είναι απαραίτητο, να αφαιρούνται από τη λίστα της Privacy Shield, οι εταιρείες που έχουν χρησιμοποιήσει παράνομα προσωπικά δεδομένα. Προσθέτουν δε, ότι οι ενωσιακές αρχές θα πρέπει επίσης να ερευνούν ανάλογες περιπτώσεις και αν κρίνεται απαραίτητο να προβαίνουν απευθείας σε αναστολή ή απαγόρευση μεταφορών δεδομένων στο πλαίσιο της συμφωνίας Privacy Shield. Οι ευρωβουλευτές εκφράζουν την ανησυχία τους σχετικά με το νόμο των ΗΠΑ «περί αποσαφήνισης της νόμιμης χρήσης δεδομένων στο εξωτερικό» (CLOUD Act). Ο νόμος αυτός δίνει την δυνατότητα, στις ΗΠΑ και σε αλλοδαπές αστυνομικές αρχές, να έχουν πρόσβαση εκτός των συνόρων σε προσωπικά δεδομένα. Επισημαίνουν ότι ο συγκεκριμένος νόμος θα μπορούσε να έχει σοβαρό αντίκτυπο στην ΕΕ και να προβεί σε σύγκρουση με το ενωσιακό νομοθετικό πλαίσιο για την προστασία προσωπικών δεδομένων(Καννέλος, 2018).

1.3 Πεδίο Εφαρμογής του GDPR

Τα προσωπικά δεδομένα προστατεύονται ήδη τόσο από ευρωπαϊκές οδηγίες όσο και από το δίκαιο του κράτους. Ο νέος κανονισμός εισάγει ένα αυστηρότερο ενιαίο πλαίσιο, ενισχύει τα δικαιώματα των υποκειμένων και τις υποχρεώσεις των διαχειριστών δεδομένων ενώ διευρύνει και το πεδίο εφαρμογής του. Ο παρόν Κανονισμός θα πρέπει να εφαρμόζεται σε όλα τα θέματα που αφορούν στην προστασία θεμελιωδών δικαιωμάτων και ελευθεριών, ειδικότερα το δικαίωμά στην προστασία δεδομένων προσωπικού χαρακτήρα.

Αφορά α) όλες τις εταιρείες και όλους τους δημόσιους φορείς που επεξεργάζονται προσωπικά δεδομένα Ευρωπαίων πολιτών, είτε συναλλασσόμενων είτε εργαζομένων, ανεξαρτήτως του πού έχουν την εγκατάστασή τους, β) τους υπευθύνους επεξεργασίας και εκτελούντες αυτήν για λογαριασμό των υπευθύνων και γ) δεδομένα που τηρούνται σε φυσική και ηλεκτρονική μορφή.

Πιο συγκεκριμένα:

- i. Ο Κανονισμός ουσιαστικά εφαρμόζεται, εν όλω ή εν μέρη, σε αυτοματοποιημένη ή μη, επεξεργασία δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης. Δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από φυσικό

πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας. Ως τέτοια δραστηριότητα νοείται εκείνη που αναφέρεται στο ιδιωτικό πεδίο δράσης ενός προσώπου ή μιας οικογένειας, δηλαδή εκείνη που δεν εμπίπτει στην επαγγελματική ή και εμπορική δραστηριότητα και δεν έχει ως σκοπό ή ως αποτέλεσμα τη συστηματική διαβίβαση ή τη διάδοση δεδομένων σε τρίτους (Υπουργείο Δικαιοσύνης, 2018).

- ii. Ο παρών κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης.
- iii. Ο παρών κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με:
 - α) την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή
 - β) την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης.
- iv. Ο παρών κανονισμός εφαρμόζεται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ένωση, αλλά σε τόπο όπου εφαρμόζεται το δίκαιο κράτους μέλους δυνάμει του δημόσιου διεθνούς δικαίου.

Το κριτήριο της εδαφικότητας εξακολουθεί να ισχύει στον GDPR δίνοντας προτεραιότητα στον χρήστη (στον οποίο αναφέρονται τα δεδομένα) ως το βασικό σημείο αναφοράς. Η παρακολούθηση της συμπεριφοράς των φυσικών προσώπων στα οποία αναφέρονται τα δεδομένα αποτελεί επαρκή λόγο για την εφαρμογή του ευρωπαϊκού δικαίου. Ωστόσο, οι δραστηριότητες και οι πληροφορίες στο διαδίκτυο δεν είναι, ή τουλάχιστον δεν ήταν, εύκολο να εντοπισθούν και οι διευθύνσεις IP ενδέχεται να μην είναι γεωγραφικά σταθερές (Μήτρου, 2017).

Ανεξάρτητα από τον τόπο εγκατάστασης, στο GDPR αναφέρεται ότι ακόμη και οι υπεύθυνοι επεξεργασίας και επεξεργαστές εκτός ΕΕ, θα υπόκεινται στο μέλλον στις διατάξεις και στις απαιτήσεις της νομοθεσίας της ΕΕ, αν εκτελούν δραστηριότητες που είναι σχετικές

με υπηρεσίες ή προσφορές αγαθών στα υποκείμενα των δεδομένων της Ένωσης ή την παρακολούθηση της συμπεριφοράς των προσώπων στα οποία αναφέρονται τα δεδομένα, στο μέτρο που η συμπεριφορά τους λαμβάνει χώρα εντός της Ένωσης(αιτιολογική σκέψη 24).

1.4 Εταιρείες που συλλέγουν και διαχειρίζονται Προσωπικά δεδομένα

Σε μια εποχή που το ίντερνετ έχει εδραιωθεί στην καθημερινότητα όλων των ανθρώπων πολλά εκατομμύρια δεδομένων δημιουργούνται ανά δευτερόλεπτο. Ο όγκος των δεδομένων αυτών, αποθηκεύεται σε διάφορες ψηφιακές αποθήκες που βρίσκονται σε όλο τον κόσμο. Οι ψηφιακές αποθήκες ανήκουν σε εταιρείες που συλλέγουν τα δεδομένα και τα διαχειρίζονται, αναλόγως την επεξεργασία που θέλουν να πραγματοποιήσουν κάθε φορά. Μερικές από αυτές τις εταιρείες είναι η Google, η Microsoft, το Facebook, το Amazon κλπ. Η κάθε μια εταιρεία διαχειρίζεται διαφορετικά τα δεδομένα που της έχουν δοθεί απλόχερα από τους χρήστες.

Τα τελευταία χρόνια έχουν ιδρυθεί καινοτόμες εταιρείες διαχείρισης προσωπικών δεδομένων με σκοπό πολιτικές και εμπορικές καμπάνιες. Αυτές οι εταιρείες συλλέγουν από διάφορες πηγές προσωπικά δεδομένα, τα επεξεργάζονται η κάθε μια ανάλογα με την πολιτική της και στην συνέχεια δημιουργούν διαφημίσεις, στοχευμένα σποτάκια για την τηλεόραση και τα social media, στέλνουν προσωπικά μηνύματα στο υποψήφιο κοινό τους κλπ. Τέτοιου είδους εταιρεία είναι η Cambridge Analytica. Παρόμοιες εταιρείες που δραστηριοποιούνται στον ίδιο χώρο είναι η Global Strategy Group, η GMMB, η Precision Strategies, η FP1 Strategies, η BrabenderCox και η SCL Group.



Η *Global Strategy Group* είναι μια πολιτική συμβουλευτική εταιρεία η οποία διαθέτει έξι γραφεία σε όλες τις Ηνωμένες Πολιτείες της Αμερικής. Τα γραφεία βρίσκονται στη Νέα Υόρκη, στην Ουάσιγκτον, στο Χέρτφορντ(Hertford), στο Σιάτλ(Seattle), στο Ντένβερ(Denver) και στο Σικάγο. Η GSG ειδικεύεται στην έρευνα και τις ιδέες, στις στρατηγικές επικοινωνίες και στη ψηφιακή στρατηγική. Σαν εταιρεία έχει συνεργαστεί με εθνικούς πολιτικούς ηγέτες, με το περιοδικό Fortune για τον ετήσιο κατάλογο Fortune 100, με ενώσεις και με μη κερδοσκοπικούς οργανισμούς(Kenton,2019). Μερικές από τις δουλειές που έχει πραγματοποιήσει είναι η νίκη της στο δημοκρατικό

δημοψήφισμα, η αποδοτική έρευνα για την αντιπολίτευση της εκάστοτε κυβέρνησης και η διαδικτυακή διαφήμιση της Super PAC.



Η *GMMB* είναι μία εξίσου πολιτική συμβουλευτική εταιρεία η οποία διαθέτει γραφεία στο Σιάτλ (Seattle) και στην Ουάσιγκτον. Συγκεκριμένα, στην Ουάσιγκτον έχει εδραιωθεί ως η κορυφαία εταιρεία σε ολόκληρο το έθνος.

Παρέχει μια ποικιλία υπηρεσιών για τους πελάτες της. Οι υπηρεσίες που διαθέτει είναι ανάπτυξη στρατηγικής, διαφήμιση, ψηφιακή εμπλοκή, γραφικός σχεδιασμός, οικοδόμηση συνασπισμού και καλές σχέσεις με τα μέσα ενημέρωσης. Ουσιαστικά η εταιρεία ειδικεύεται στην χρήση προηγμένων και καινοτόμων τεχνικών, στην δημιουργία διαφημίσεων, στην ψηφιακή αναλυτική, στην στόχευση και στην οργάνωση πολυμέσων. Έχει κερδίσει 10 βραβεία το 2017, στα ετήσια βραβεία και συνέδρια της AAPC. Η AAPC είναι μια επαγγελματική ένωση για άτομα που εργάζονται σε συγκεκριμένους τομείς διοίκησης εντός των επιχειρήσεων υγείας στις Ηνωμένες Πολιτείες, δηλαδή είναι ένας από τους πολλούς παρόχους που προσφέρουν υπηρεσίες όπως πιστοποίηση και εκπαίδευση σε ιατρικούς κωδικοποιητές, ιατρικούς ελεγκτές, διαχειριστές συμμόρφωσης και διαχειριστές πρακτικής. Ένα δείγμα της δουλειάς της είναι η ολοκληρωμένη εκστρατεία που της ανέθεσε η Pramila Jayaraj βασισμένη σε έρευνα. Η αρχική δημοσκόπηση έδειξε ότι η Pramila ήταν αρκετά πίσω από τον αντίπαλό της. Η ακούραστη δουλειά και η έξυπνη εκστρατεία που διοργάνωσε η GMMB οδήγησε στην νίκη της Pramila με περισσότερες από 40% ψήφους. Μετά από αυτή την επιτυχημένη δουλειά ανέλαβε και άλλου τέτοιου είδους αναθέσεις.



Η *Precision Strategies* είναι μια συμβουλευτική εταιρεία που βρίσκεται στην Ουάσιγκτον. Ειδικεύεται στο στρατηγικό σχεδιασμό, στις τεχνικές μάρκετινγκ, στην δημιουργία μηνυμάτων, στα ψηφιακά προγράμματα και στις μετρήσεις βάσει δεδομένων. Έχει κερδίσει το βραβείο της υπηρεσίας Digital PR το 2016 της Holmes Report. Το Digital PR είναι ένα στρατηγικό online marketing που χρησιμοποιούν οι επιχειρήσεις για να κάνουν περισσότερο αισθητή την παρουσία τους στο διαδίκτυο (Marchant, 2018). Το βραβείο αναφέρεται συγκεκριμένα σε τρεις εκστρατείες της Precision και συγκεκριμένα στην εκστρατεία υπέρ του Συνασπισμού της Δημόσιας Ασφάλειας, στην εκστρατεία υπέρ της Βιβλιοθήκης John F. Kennedy και στην προεκλογική εκστρατεία του LPC. Πιο συγκεκριμένα, το 2015 το LPC (Liberty Party of Canada) προσέλαβε την Precision Strategies για μια εκστρατεία δεδομένων και ψηφιακών τακτικών μηνυμάτων για να πείσει τους Καναδούς να ψηφίσουν τον Justin Trudeau. Η εταιρεία άρχισε να εργάζεται μήνες πριν από τις εκλογές για να χτίσει την απαραίτητη υποδομή ώστε να διεξαχθεί μια εκστρατεία που βασίζεται σε δεδομένα. Η εκστρατεία είχε χτυπήσει πάνω από 5 εκατομμύρια πόρτες, έκανε προσωπικές επαφές με τους ψηφοφόρους, συζήτησε τις ανησυχίες τους, καθώς και το όραμα του υποψηφίου. Στόχευε τόσο τους διαδικτυακούς όσο και τους εκτός σύνδεσης ψηφοφόρους, που ήταν η μεγαλύτερη προσπάθεια συμμετοχής στην καναδική ιστορία. Το κόμμα κέρδισε μια απροσδόκητη νίκη στις εκλογές, εξασφαλίζοντας το 40% των ψήφων σε εθνικό επίπεδο. Εκτός από αυτή την δουλειά, στο παρελθόν η εταιρεία είχε αναλάβει και την εκστρατεία του Ομπάμα και άλλων παρόμοιων σημαντικών προσώπων.



Η *FPI Strategies* είναι και αυτή μια συμβουλευτική εταιρεία που εδρεύει στην Ουάσιγκτον. Ειδικεύεται στην διαφήμιση, στη ψηφιακή δέσμευση, στην ανάπτυξη μηνυμάτων, στην διαχείριση κρίσεων, στις δημόσιες σχέσεις (PR) και στις σχέσεις με τα μέσα ενημέρωσης. Έχει κερδίσει το AAPC 2017 Gold Pollie για το Best in Show. Εκτός από αυτό το βραβείο, η FPI, έχει κερδίσει πολλά άλλα βραβεία για τις καλύτερες μεθόδους προώθησης μέσω διαδικτύου. Μια από τις μεγαλύτερες δουλειές που

έχει αναλάβει η εταιρεία είναι η πολιτική καμπάνια του Rob Portman, η οποία συνδύαζε την ανάπτυξη στρατηγικής ανταλλαγής μηνυμάτων και διαφημιστικής καμπάνιας. Ο στόχος ήταν η παρουσίαση του αυξημένου ποσοστού προτίμησης των ψηφοφόρων προς τον γερουσιαστή Rob Portman, έναντι του μικρού ποσοστού υπέρ του Ted Strickland. Ο Portman στήριζε τις ανεξάρτητες γυναίκες και την δημιουργία λύσεων σοβαρών ζητημάτων για την κοινωνία, όπως είναι το ζήτημα των ναρκωτικών και το ζήτημα της Κίνας. Οι τηλεοπτικές εκστρατείες ξεκίνησαν το 2016, εστιάζοντάς στο σχέδιο του υποψηφίου για τη σφυρηλάτηση λύσεων της εξάρτησης των πολιτών του από την ηρωίνη και την υπερβολική δόση. Η πρώτη τηλεοπτική διαφήμιση που προβλήθηκε στο κοινό ονομαζόταν "Holly" και παρουσίαζε μια συναισθηματική μαρτυρία μιας μάνας που έχασε την κόρη της από υπερβολική δόση ναρκωτικών ουσιών. Η διαφήμιση έγινε πολύ δημοφιλής και κέρδισε την υποστήριξη πολλών ψηφοφόρων. Πριν από αυτή την διαφήμιση η FP1 είχε απελευθερώσει στο διαδίκτυο μια σειρά με βίντεο που καθόρισαν την εκστρατεία του Portman και τόνισαν τους στόχους του. Τα βίντεο σε μικρό χρονικό διάστημα κέρδισαν την προσοχή των MME στο Οχάιο. Τα πιο δημοφιλή βίντεο ήταν το "Abyss" και το "Ohio Lost Jobs" τα οποία ήταν υπεύθυνα για την καταστροφή της εκστρατείας του Strickland. Όλα τα παραπάνω είχαν ως συνέπεια την επανεκλογή του γερουσιαστή Rob Portman με μεγάλη διαφορά από τον επόμενο υποψήφιο.



Η *BrabenderCox* είναι μια δημοκρατική πολιτική συμβουλευτική εταιρεία και έχει γραφεία στο Πίτσμπουργκ (Pittsburgh), στην Πενσυλβανία (Pennsylvania), στην Ουάσιγκτον και στο Χάρισμπουργκ (Harrisburg) της Πενσυλβανίας. Ειδικεύεται στο αντιπαραγωγικό μάρκετινγκ, στη πολιτική διαφήμιση και στις δημόσιες σχέσεις. Είναι μία από τις πιο δημιουργικές επιχειρήσεις στην Αμερική, έχοντας κερδίσει εκατοντάδες βραβεία για εργασία τόσο στην παραδοσιακή διαφήμιση όσο και στον ψηφιακό χώρο. Η πελατεία της αποτελείται από Προέδρους, Διοικητές, Γερουσιαστές, Επαγγελματίες Αθλητικούς Δικαιούχους, Εταιρείες Fortune 500, Gaming Resorts, Οργανισμούς Υγείας και Μη Κερδοσκοπικούς Οργανισμούς. Ο Todd Young προσέλαβε την BrabenderCox για να κερδίσει μια έδρα της Γερουσίας στην Ιντιάνα. Η

σκέψη της επιχείρησης για αυτή την εκστρατεία ήταν να δημιουργήσει μια σειρά δημοσιευμάτων που έλεγαν για την μέχρι τότε ιστορία του Young και την μέχρι τότε ιστορία του αντιπάλου του που θα εξαργίωνε τους πολίτες προς τον αντίπαλο του και ταυτόχρονα θα έφερνε θετικά αποτελέσματα στον ίδιο. Μέσω αυτής της σκέψης, η επιχείρηση έστειλε στοχευμένα μηνύματα σε συγκεκριμένες ομάδες κοινού, ικανά να φέρουν τα επιθυμητά αποτελέσματα σε υψηλό βαθμό. Με αυτά τα μηνύματα κατάφερε να έχει την υποστήριξη στρατιωτικών βετεράνων και ψηφοφόρων εθνικής ασφαλείας με κατάληξη να κερδίσει τις εκλογές. Ουσιαστικά ο Young επωφελήθηκε από την υιοθέτηση των μεθόδων που ακολούθησε η BrabenderCox αφού μπόρεσε να κατακτήσει την θέση που ζητούσε.

Οι πολιτικές συμβουλευτικές εταιρείες πρέπει να προσφέρουν ένα ευρύ φάσμα υπηρεσιών και εμπειρογνωμοσύνης. Τέτοιου είδους εταιρείες ενσωματώνουν την καινοτομία και τη μελλοντική σκέψη, κατανοούν τις σύγχρονες πολιτικές τάσεις, τη δημοσιογραφία, τα μέσα ενημέρωσης, τη διαφήμιση, τις δημόσιες σχέσεις και τη διαχείριση κρίσεων.

Κεφάλαιο 2

CAMBRIDGE ANALYTICA

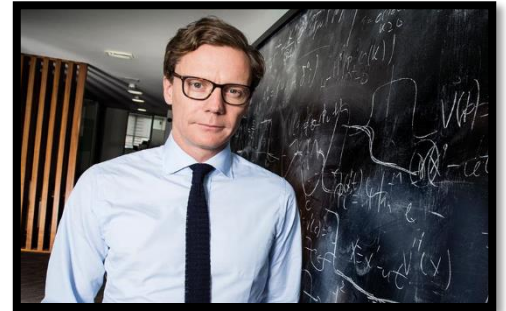
2.1 Περιγραφή Εταιρείας



Η **Cambridge Analytica Ltd (CA)** είναι μια πολιτική συμβουλευτική εταιρεία με έδρα της την Βρετανία, που ασχολείται με τον συνδυασμό της προγνωστικής ανάλυσης, τις επιστήμες συμπεριφοράς και την τεχνολογία διαφημίσεων με στόχο τα δεδομένα και σκοπό την επιρροή της συμπεριφοράς των καταναλωτών μέσω μιας μοναδικής προσέγγισης για εμπορικές ή πολιτικές εκστρατείες. Το λογότυπο της είναι ένας εγκέφαλος που αποτελείται από κόμβους του διαδικτύου, σαν χάρτης. Ξεκίνησε το 2013 ως παρακλάδι του Ομίλου SCL. Τελικά, η Cambridge Analytica έκλεισε τις δραστηριότητές της το 2018, λόγω της εμπλοκής της σε ένα μεγάλο σκάνδαλο, παρόλο που συνέχισαν να υπάρχουν συναφείς επιχειρήσεις.

Η SCL Group (Strategic Communication Laboratories) ήταν μία ιδιωτική, εξίσου Βρετανική εταιρεία, η οποία δραστηριοποιήθηκε στον χώρο των στρατηγικών και πολιτικών εκστρατειών (Bloomberg, 2019). Πιο συγκεκριμένα, πραγματοποιούσε εξαγωγή και ανάλυση δεδομένων από το ακροατήριό της. Βάσει αυτών των αποτελεσμάτων μπορούσε να επηρεάσει συγκεκριμένες ομάδες κοινού ώστε να τροποποιήσει τη συμπεριφορά τους σύμφωνα με το στόχο του πελάτη της. Η εταιρεία περιγράφει τον εαυτό της ως μια παγκόσμια υπηρεσία διαχείρισης εκλογών. Η SCL που εδρεύει στο Λονδίνο ιδρύθηκε από τον Nigel Oakes, ο οποίος είναι και ο διευθύνων σύμβουλος (CEO) της (Wikispeaks, 2018). Έγινε γνωστή για την υποτιθέμενη εμπλοκή της στις εκστρατείες στρατιωτικής παραπληροφόρησης, για την διαχείριση των κοινωνικών μέσων και τη στοχοθέτηση των ψηφοφόρων. Το 2005, η SCL απέδειξε την ικανότητά της σε δραστηριότητες επιρροής με σκοπό να βοηθήσει στην ενορχήστρωση μιας εξελιγμένης εκστρατείας για την μαζική εξαπάτηση ενός πολυάριθμου κοινού, όπως είναι το κοινό του Λονδίνου. Σύμφωνα με την ιστοσελίδα της, έχει συμμετάσχει σε περισσότερες από 25 διεθνείς πολιτικές και εκλογικές εκστρατείες από το 1994. Η συμμετοχή της SCL στον πολιτικό κόσμο βρισκόταν κυρίως στον αναπτυσσόμενο κόσμο όπου χρησιμοποιήθηκε από τους στρατιωτικούς και τους πολιτικούς για να μελετήσει και να χειραγωγήσει την κοινή γνώμη και την πολιτική βούληση. Μερικά δείγματα του έργου της

είναι η επιρροή των εκλογών στην Ιταλία, τη Λετονία, την Ουκρανία, την Αλγερία, τη Ρουμανία, τη Νότια Αφρική, τη Νιγηρία, την Κένυα, τον Μαυρίκιο, την Ινδία, την Ινδονησία, τις Φιλιππίνες, του Αγίου Βικεντίου και των Γρεναδίνων, του Αγίου Χριστόφορου, του Νέβις, του Τρινιδάδ και του Τομπάγκο. Παρόλο που η εταιρεία αρχικά συμμετείχε στις εκλογές στο Ηνωμένο Βασίλειο, έπαψε να το κάνει μετά το 1997, διότι οι υπάλληλοι δεν παρουσίαζαν τον ίδιο ζήλο όπως με τα σχέδια τους στο εξωτερικό. Τέλος, η SCL υποστήριξε ότι η μεθοδολογία της έχει εγκριθεί από οργανισμούς της κυβέρνησης του Ηνωμένου Βασιλείου και της ομοσπονδιακής κυβέρνησης των Ηνωμένων Πολιτειών.



Alexander Nix

Η αρχική σκέψη της δημιουργίας της Cambridge Analytica, έγινε το 2013 από τον Alexander Nix και έναν, μέχρι τότε, υπάλληλο της θυγατρικής εταιρείας SCL, τον Christopher Wylie. Οι δύο συνεργάτες προκειμένου να πείσουν ένα εκατομμυριούχο επενδυτή να χρηματοδοτήσει την ιδέα τους, δημιούργησαν μία εικονική εταιρεία, όπου τα γραφεία της βρίσκονταν στο Cambridge. Αυτή η εταιρεία ασχολούταν υποτιθέμενα με πανεπιστημιακές έρευνες, με βιτρίνα μία ψεύτικη ιστοσελίδα. Όταν ο επενδυτής, Steve Bannon, θέλησε να επισκεφτεί τα γραφεία της εταιρείας, που είχε σκοπό να επενδύσει τα χρήματά του, οι δυο προαναφερθέντες συνεργάτες μετέφεραν ένα μέρος του προσωπικού από τα κεντρικά γραφεία της μητρικής εταιρείας στα γραφεία της εικονικής με σκοπό την επίτευξη της επένδυσης. Η πραγματική ίδρυση της Cambridge Analytica πραγματοποιήθηκε τον Ιανουάριο του 2015 με έδρα το Westferry Circus, στο Λονδίνο. Ιδρυτές της ήταν οι συντηρητικοί επιχειρηματίες Steve Bannon και Robert Mercer (Δημοπούλου, 2018). Ο Steve Bannon αποχώρησε από τις συμμετοχές του στην εταιρεία τον Απρίλιο του 2017, όπως απαιτεί ο ρόλος του στρατηγικού αναλυτή του Λευκού Οίκου. Η επιχείρηση διατηρούσε γραφεία στο Λονδίνο, στη Νέα Υόρκη και στην Ουάσιγκτον, με διευθύνων σύμβουλο τον Alexander James Ashburner Nix (ο οποίος διορίστηκε επίσης τον Ιανουάριο του 2015). Ο Alexander Nix είναι επίσης διευθυντής σε εννέα παρόμοιες εταιρείες που μοιράζονται τις ίδιες έδρες στο Λονδίνο και τις ίδιες τεχνολογίες, συμπεριλαμβανομένων των τεχνολογιών Firecrest, Emerdata και έξι εταιρειών του Ομίλου SCL.

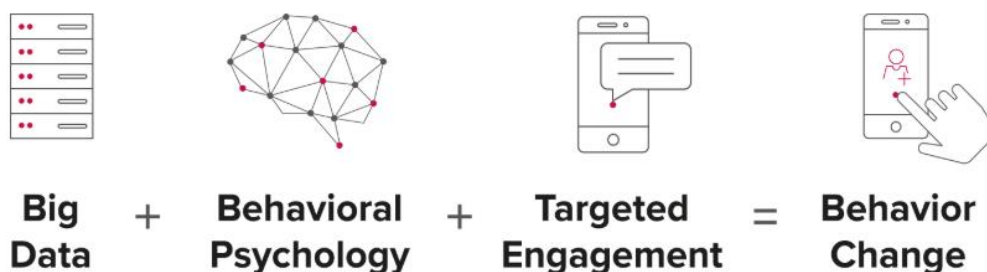
Η Cambridge Analytica είναι μια μη παραταξιακή οργάνωση χωρίς συγκεκριμένο πολιτικό προσανατολισμό. Το δίκτυο πελατών της περιλαμβάνει κυβερνήσεις και ΜΚΟ, μεγάλες και μικρές εμπορικές οντότητες και πολιτικούς πελάτες σε όλο το ιδεολογικό φάσμα. Λόγω του όγκου των πελατών της έχει χωριστεί σε δύο κατηγορίες, η πρώτη κατηγορία είναι η CA

Commercial και η δεύτερη είναι η CA Political. Και στις δύο αυτές κατηγορίες, έχει ως γνώμονα τα δεδομένα που έχει στην κατοχή της για το κοινό στο οποίο πρέπει να απευθυνθεί. Πιο συγκεκριμένα, οι πληροφορίες που βασίζονται σε δεδομένα, δίνουν τα εργαλεία που χρειάζεται για να δημιουργηθεί ένα γεμάτο διαφημιστικό τοπίο και ο πελάτης να μπορέσει μέσω αυτής της διαφήμισης, να μιλήσει απευθείας σε μεμονωμένους πελάτες του. Έτσι, παράγεται μια διαφήμιση που επηρεάζει αποτελεσματικά την αλλαγή συμπεριφοράς. Οι υπηρεσίες που χρησιμοποιούνται για την επίτευξη του τελικού αποτελέσματος είναι η έρευνα αγοράς, η ενσωμάτωση δεδομένων, η κατάτμηση κοινού, η στοχοθετημένη διαφήμιση και η εκτίμηση απόδοσης της καμπάνιας(Cambridge Analytica, 2015).

Μέθοδοι Ανάλυσης Δεδομένων

Οι μέθοδοι ανάλυσης δεδομένων της CA βασίζονται σε μεγάλο βαθμό στο ακαδημαϊκό έργο του Michal Kosinski. Το 2008, ο Michal Kosinski συμμετείχε στο Κέντρο Ψυχομετρίας του Πανεπιστημίου του Cambridge, όπου στη συνέχεια ανέπτυξε με τους συναδέλφους του ένα σύστημα δημιουργίας προφίλ που χρησιμοποιεί γενικού τύπου ηλεκτρονικά δεδομένα. Η άντληση αυτών των δεδομένων γίνεται από το Facebook και τα smartphones. Με αυτό το σύστημα απέδειξε ότι το ισχυρότερο εργαλείο επιρροής είναι η ατομική ψυχολογική στόχευση. Με βάση την παραπάνω διαπίστωση, η CA συνέλλεγε στοιχεία για τους ψηφοφόρους χρησιμοποιώντας πηγές όπως είναι η δημογραφία, η συμπεριφορά των καταναλωτών, η δραστηριότητα στο διαδίκτυο και άλλες δημόσιες και ιδιωτικές πηγές. Μια άλλη πηγή πληροφοριών ήταν η εφαρμογή για κινητά "Cruz Crew" που παρακολουθούσε τις φυσικές κινήσεις και τις επαφές του χρήστη, ενώ σύμφωνα με το Associated Press, εισέβαλε σε περισσότερα προσωπικά δεδομένα σε σχέση με τις προηγούμενες εφαρμογές της προεκλογικής καμπάνιας. Τον Οκτώβριο του 2016 ο Alexander Nix, διευθύνων σύμβουλος της Cambridge Analytica, δήλωσε ότι *“Στις Ηνωμένες Πολιτείες έχουμε περίπου τέσσερις ή πέντε χιλιάδες στοιχεία δεδομένων για κάθε άτομο. Έτσι μοντελοποιήσαμε την προσωπικότητα κάθε ενήλικα στις Ηνωμένες Πολιτείες, δηλαδή περίπου 230 εκατομμύρια ανθρώπων”*. Σε μία άλλη δήλωση, η εταιρεία ισχυρίστηκε ότι χρησιμοποιεί τεχνικές βελτίωσης δεδομένων και τεχνικές κατακερματισμού ακροαματικότητας που παρέχουν ψυχολογική ανάλυση για μια βαθύτερη γνώση του κοινού-στόχου. Με αυτό τον τρόπο, μπορεί να προβλέψει τις ανάγκες του κοινού και πώς αυτές οι ανάγκες μπορούν να αλλάξουν με την πάροδο του χρόνου. Καταλήγοντας στις υπηρεσίες που εξυπηρετούν τις ανάγκες αυτές, φροντίζει να τις διαμορφώσει βάσει των συμφερόντων που θα εξυπηρετηθούν τόσο στην πολιτική σκηνή όσο

και στον επιχειρηματικό κόσμο, παρέχοντας καλύτερη και πιο ευέλικτη εικόνα για το βασικό τους ακροατήριο.



Σχήμα 2.1: Τα τρία στοιχεία που δημιουργούν μια στοχευμένη διαφήμιση.

Η CA απέκτησε μεγάλο μέρος των στοιχείων της σχετικά με την προσωπικότητά σε έρευνες που διεξήγαγε σε συνεχή βάση. Για κάθε πολιτικό πελάτη, η επιχείρηση περιορίζει τα τμήματα ψηφοφόρων σε 32 διαφορετικούς τύπους προσωπικότητας που ταιριάζει σε κάθε ενήλικα. Κάθε τύπος προσωπικότητας έχει διαφορετικό τον τόνο της γλώσσας που χρησιμοποιείται στα μηνύματα διαφημίσεων ή στα σενάρια επικοινωνίας ψηφοφόρων. Επιπλέον, χρησιμοποιούνται στοιχεία για τον προσδιορισμό των θέσεων των ψηφοφόρων σε συγκεκριμένα θέματα. Τα στοιχεία αυτά ενημερώνονται με μηνιαίες έρευνες, οι οποίες ρωτούν για τις πολιτικές προτιμήσεις και πώς οι άνθρωποι χρησιμοποιούν τις πληροφορίες που παίρνουν για τη λήψη των αποφάσεών τους. Καλύπτει επίσης τα θέματα των καταναλωτών σχετικά με τα διάφορα εμπορικά σήματα και τα προτιμώμενα προϊόντα, δημιουργώντας μια εικόνα του τρόπου με τον οποίο κάποιος καταλήγει στον τρόπο ψηφοφορίας.

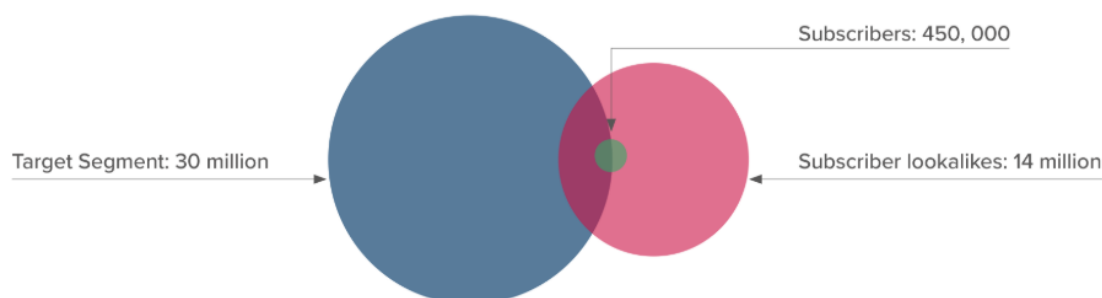
Για να κατανοήσουμε στην πράξη πως δουλεύει η εν λόγω εταιρεία θα αναφέρουμε ένα σενάριο ενός πελάτη. Ο πελάτης που θα μελετήσουμε είναι ένας σεβαστός παγκόσμιος εκδότης περιοδικού, που ανέθεσε ένα έργο στην CA για να κατανοήσει καλύτερα τους σημερινούς συνδρομητές του καθώς και το κοινό-στόχο του στις Ηνωμένες Πολιτείες.

Το αρχικό έργο είχε τέσσερις καθορισμένους στόχους:

1. Τον προσδιορισμό της αγοράς στην οποία υπάρχει ήδη απήχηση, καθώς και τον προσδιορισμό καινούριας ομάδας ατόμων που θα μπορούσαν να αποτελέσουν τη νέα αγορά.
2. Την κατανόηση του κοινωνικού, πολιτικού και γεωγραφικού προφίλ της κάθε ομάδας.
3. Τη σύγκριση και την αντιπαραβολή των δύο ομάδων.
4. Την παροχή οδηγιών προσέγγισης της μέχρι τώρα αγοράς με κριτήριο το ψυχολογικό της προφίλ.

Το κοινό στο οποίο απευθυνόταν ο εκδότης μέχρι εκείνη τη στιγμή, είχε διαμορφωθεί από μια εταιρία που ανέλαβε τον προσδιορισμό του. Ωστόσο, διαπιστώθηκε ότι το κοινό στο οποίο απευθυνόταν η εταιρία του εκδότη, δεν έφερε τα χαρακτηριστικά τα οποία θα βοηθούσαν στην αύξηση των πωλήσεων, κινώντας το απαιτούμενο ενδιαφέρον. Το αξιοσημείωτο είναι ότι από τους 450.000 συνδρομητές της εταιρίας, μόνο οι 85.000 έδειχναν ενδιαφέρον και ανταποκρίνονταν στις πωλήσεις του περιοδικού. Επιπλέον, υπήρχε δυνατότητα «ανοίγματος» στην αγορά των Ηνωμένων Πολιτειών, κάτι που δεν είχε προταθεί μέχρι εκείνη τη στιγμή.

Το νέο κοινό που προτάθηκε μετά την ανάλυση της Cambridge Analytica άγγιζε τα 30 εκατομμύρια. Τα 5 εκατομμύρια από το κοινό, έδειχνε ήδη ενδιαφέρον για παρόμοιες εταιρίες, επομένως ήταν πολύ εύκολο να αποτελέσουν κομμάτι της νέας αγοράς. Αν μόνο το 10% του κοινού αυτού ανταποκρινόταν θετικά στο περιοδικό, η υπάρχουσα βάση δεδομένων με τα στοιχεία των συνδρομητών, θα αυξανόταν κατά 85%.



Σχήμα 2.2: Είδη κοινού που απευθυνόταν η εταιρία του εκδότη.

Η επόμενη ανάλυση ήταν λεπτομερέστερη και επικεντρώθηκε στο επιθυμητό κοινό και στο κοινό που «ακολουθούσε» παρόμοιες, ανταγωνιστικές εταιρίες. Υπήρχαν αρκετές διαφορές στα κοινωνικά, γεωγραφικά, δημογραφικά και πολιτικά χαρακτηριστικά συγκριτικά με τα υπάρχοντα. Στο σχήμα 2.2., φαίνονται τα τρία είδη του κοινού στο οποίο μπορούσε να απευθυνθεί η εταιρία του εκδότη. Με μπλε, είναι το επιθυμητό κοινό, με κόκκινο το κοινό που «ακολουθούσε» ανταγωνιστές και με πράσινο το κοινό στο οποίο θεωρητικά αποτελούσε το έως τώρα κοινό του περιοδικού. Μετά την ανάλυση των δεδομένων από την Analytica, η αγορά στην οποία μπορούσε η εταιρία να κινηθεί φαίνεται στο σχήμα 2.3.



Σχήμα 2.3: Γεωγραφικός προσδιορισμός του νέου κοινού.

Για την παροχή οδηγιών προσέγγισης της αγοράς με κριτήριο το ψυχολογικό της προφίλ, οι εμπειρογνώμονες επικοινωνίας της Cambridge Analytica πρότειναν μηνύματα και διαφημίσεις του εκδοτικού οίκου, που ξεκινούσαν με ένα αρνητικό αρχικό ερέθισμα ακολουθούμενο από μια καθησυχαστική λύση. Ο τόνος θα έπρεπε να είναι αναλυτικός, λεπτομερής, άμεσος και συγκεκριμένος. Εν συνέχεια, οι λέξεις που θα έπρεπε να περιλαμβάνονται στο κείμενο θα έπρεπε να είναι αισθητές, όπως «εμπιστοσύνη», «προετοιμασία», «απόφαση» και «σταθερότητα». Στη συνέχεια, αναπτύχθηκε παράδειγμα αντιγράφου για να καταδείξει πως θα έπρεπε να μοιάζει το τελικό διαφημιστικό σε πολλά ψηφιακά μέσα. Αποτέλεσμα ήταν η αύξηση του κοινού του περιοδικού, με σταθερά και επιτυχημένα βήματα, καθώς και η κατανόηση των χαρακτηριστικών του. Η συνέχεια της εταιρίας είχε ανοδική πορεία (Cambridge Analytica, 2015).

2.2 Απολογισμός παραχθέντος έργου της Cambridge Analytica

Η επιτυχία της επιχείρησης βασίστηκε στα εργαλεία που παρέχει στους πελάτες της για την αναφορά και την διαχείριση της καμπάνιας τους. Αυτά τα εργαλεία δίνουν την δυνατότητα στον διαχειριστή τους, να αποκτήσει την πλήρη και την σαφή εικόνα της απόδοσης της καμπάνιας σε πραγματικό χρόνο. Τα διαθέσιμα προϊόντα της CA είναι το LiveSpend, το CA Blockchain και το SelecTV.

The logo for LiveSpend, featuring the word "LiveSpend" in a blue, sans-serif font.

Το LiveSpend είναι ένα πρόγραμμα- πλατφόρμα-ταμπλό που αναφέρεται σε διαφημίσεις, αναλύει τα δεδομένα απο όλες τις πλατφόρμες σε μια ενιαία προβολή, ενώ ταυτόχρονα βελτιστοποιεί τη σύνδεση μεταξύ των τάσεων μάρκετινγκ και των επιχειρηματικών αποτελεσμάτων.

The logo for CA Blockchain, featuring a stylized "CA" in blue followed by the word "Blockchain" in a grey, sans-serif font.

Το CA Blockchain παρέχει μια πλατφόρμα, η οποία επηρεάζει το κοινό με βάση τα θέλω και τις ανάγκες του, βοηθώντας στην οικοδόμηση της ισχυρότερης σχέσης του κοινού με τον πελάτη-διαχειριστή.

The logo for SelecTV+, featuring the word "SelecTV" in a blue, sans-serif font with a plus sign to the right.

Το εργαλείο SelecTV διαθέτει διευθυνσιοδοτούμενες(στοχευμένες) λύσεις για την τοποθέτηση διαφημίσεων, συνδυάζοντας την ανάλυση δεδομένων της συμπεριφοράς του κοινού και της τεχνογνωσίας που υπάρχει ως την τρέχουσα στιγμή.

Γενικότερα, η Analytica είναι συμβατή με πολλές πλατφόρμες για την καλύτερη δυνατή αποστολή μηνυμάτων σε τηλεοράσεις, σε φορητούς και επιτραπέζιους υπολογιστές, σε κινητά και σε άλλες συσκευές. Η αποστολή των μηνυμάτων, συνήθως πραγματοποιείται μέσω του Facebook, του Twitter και άλλων κοινωνικών μέσων δικτύωσης με την μορφή βίντεο ή στατικής διαφήμισης.

Ο απολογισμός του παραχθέντος έργου της είναι οι αναθέσεις που έχει ολοκληρώσει στην συνολική πορεία της. Η επιχείρηση από την πρώτη μέρα λειτουργίας της εισέβαλε στον τομέα της πολύ δυναμικά, αφού συμμετείχε σε 44 πολιτικούς αγώνες στις ΗΠΑ. Στην πραγματικότητα, η SCL συνέστησε στην Cambridge Analytica να συμμετάσχει στην εκλογική διαδικασία στις Ηνωμένες Πολιτείες. Εξαιτίας της προαναφερθείσας παρακίνησης, η Analytica πήρε την απόφαση να εισέλθει στην αμερικάνικη εκλογή συμμετέχοντας σε 44 εκλογές του Κογκρέσου των ΗΠΑ και της Γερουσίας των ΗΠΑ, στις ενδιάμεσες εκλογές του 2014. Για να μπορέσει να είναι αποδοτική στις δουλειές που ανέλαβε, την ίδια χρονιά αγόρασε η μητρική της εταιρεία, η SCL, ένα σύνολο δεδομένων που βασίστηκαν σε αυτά οι πρώτες δραστηριότητες της Cambridge Analytica. Τα δεδομένα πάρθηκαν από μια εταιρεία με την επωνυμία Global Science Research που ίδρυσε ο Aleksandr Kogan, ψυχολόγος στο Cambridge. Την επόμενη χρονιά ακριβώς, δηλαδή το 2015, πραγματοποίησε υπηρεσίες ανάλυσης δεδομένων για την προεδρική εκστρατεία ως σύμβουλος για τους Ρεπουμπλικάνους Ben Carson και Ted Cruz. Το 2016, η Cambridge Analytica εργάστηκε για την προεδρική εκστρατεία του Donald Trump, καθώς και για την καμπάνια υπέρ του Brexit, αφού ολοκληρώθηκαν οι αμερικανικές εκλογές. Ωστόσο, οι δουλειές που αναλάμβανε δεν περιορίστηκαν μόνο στις Ηνωμένες Πολιτείες της Αμερικής και στην Βρετανία, αφού ανέλαβε τις εκλογές της Κένυας το 2013 και το 2017. Στην Κένυα βέβαια, οι διαφημίσεις της δεν στόχευαν τόσο το facebook, για τον λόγο ότι στην Αφρική δεν είναι τόσο πολύ διαδεδομένα τα μέσα κοινωνικής δικτύωσης. Το 2018, ανέλαβε επίσης τις γενικές εκλογές του Μεξικού και για το Θεσμικό Επαναστατικό κόμμα(Cambridge Analytica, 2015).

Όλα τα παραπάνω στοιχεία μας δείχνουν ότι η εν λόγω εταιρεία, είχε μία σταθερή και ανοδική πορεία στον χώρο που ειδικευόταν. Όμως, η ξαφνική δημοσίευση ενός σκανδάλου της σταμάτησε απότομα την άνοδο αυτή. Ήταν μεγάλο πλήγμα για την φήμη της αυτή η δημοσίευση και την οδήγησε στο κλείσιμό της χωρίς δεύτερη σκέψη. Σύμφωνα με την ανακοίνωσή της, η εταιρεία κατέθεσε αίτηση πτώχευσης στο Ηνωμένο Βασίλειο και ήταν έτοιμη να ξεκινήσει διαδικασίες πτώχευσης και στις ΗΠΑ. Αυτή η επιλογή έγινε διότι οι πελάτες της δεν θα την εμπιστεύονταν το ίδιο και υπήρχαν πολλές κυρώσεις για την ανάμιξή της στο σκάνδαλο(CNN Greece, 2018). Εκπρόσωποι της εταιρείας κατέθεσαν αίτηση υπαγωγής στο άρθρο 7, για εθελοντική χρεοκοπία, την Πέμπτη 16 Μαΐου 2018, σε δικαστήριο της Νέας Υόρκης. Σύμφωνα με το Reuters, τα περιουσιακά στοιχεία της Cambridge Analytica LLC εκτιμώνται σε 100.000-500.000 δολάρια, ενώ οι υποχρεώσεις της κυμαίνονται μεταξύ 1-

10 εκατ. δολαρίων. Η Cambridge Analytica και η μητρική της SCL Elections Ltd είχαν προαναγγείλει στις αρχές Μάϊου την πτώχευση εξαιτίας ραγδαίας πτώσης στον κύκλο εργασιών τους (Bloomberg, 2018). *«Η πολιορκία από την κάλυψη των μέσων ενημέρωσης έδωσε ουσιαστικά όλους τους πελάτες και προμηθευτές της εταιρείας. Κατά συνέπεια, αποφασίστηκε ότι δεν είναι πλέον βιώσιμη η συνέχιση της επιχειρηματικής δραστηριότητας, που άφησε την Cambridge Analytica χωρίς καμία ρεαλιστική εναλλακτική να τεθεί η εταιρεία υπό διαχείριση»*, είχαν αναφέρει σε ανακοίνωσή τους.

Οι κατηγορίες για κατάχρηση των δεδομένων 87 εκατομμυρίων χρηστών του Facebook τα οποία η Cambridge Analytica χρησιμοποίησε για να αναπτύξει τεχνικές υποστήριξης του Donald Trump κατά την προεκλογική εκστρατεία του 2016, έπληξαν τις μετοχές του Facebook, προκαλώντας πολυάριθμες επίσημες έρευνες από τις αμερικανικές αρχές. (Bloomberg, 2018).

2.3 Περιγραφή Σκανδάλου

Τα τελευταία χρόνια το Διαδίκτυο χαρακτηρίζεται ως ένα ισχυρό μέσο πληροφόρησης και επικοινωνίας που χρησιμοποιείται καθημερινά από ένα μεγάλο ποσοστό χρηστών. Εκτός από την “εξυπηρέτηση” που παρέχει στους χρήστες του, ταυτόχρονα μετασχηματίζεται σε ένα εύφορο έδαφος για τη συλλογή προσωπικών δεδομένων. Πολλοί ιστότοποι, online επιχειρήσεις και πάροχοι υπηρεσιών διαδικτύου που προσφέρουν προϊόντα, υπηρεσίες και πληροφορίες, συλλέγουν, επεξεργάζονται και αποθηκεύουν τεράστια ποσά πληροφοριών σχετικά με τους καταναλωτές, είτε γνωστοποιώντας ότι τα δεδομένα τους συλλέγονται είτε οδηγούν στη συναίνεση της συλλογής αυτής. Αυτό έχει ως αποτέλεσμα οι χρήστες να χάνουν τον έλεγχο των δεδομένων τους και τη χρήση τους, καθώς καθίστανται ανιχνεύσιμα. Ο συνδυασμός όλων αυτών των πληροφοριών παρέχει ένα ισχυρό εργαλείο για την ακριβή κατατομή των χρηστών (Μήτρου, 2017). Η χρήση των προσωπικών δεδομένων έχει μετατραπεί σε έναν παράγοντα που χρησιμοποιείται για την επιρροή της κοινής γνώμης σε θέματα εκλογικών αναμετρήσεων, marketing και συμπεριφοράς.

Τον Μάρτιο του 2018 έγινε γνωστό πως η Cambridge Analytica βοήθησε στην προεκλογική εκστρατεία δύο Ρεπουμπλικάνων υποψηφίων, αναλύοντας προσωπικά δεδομένα χιλιάδων Αμερικανών πολιτών. Στην συνέχεια, γνωστοποιήθηκε ότι όλα τα δεδομένα προήλθαν από τον ιστότοπο κοινωνικής δικτύωσης του Facebook, γεγονός που έδωσε στο σκάνδαλο μεγάλες

διαστάσεις(Πανοπούλου, 2018). Η χρήση των προσωπικών δεδομένων είναι μια καινοτόμα ιδέα για τον κλάδο της πολιτικής και των εκλογικών αναμετρήσεων. Η πρώτη φορά που χρησιμοποιήθηκαν δεδομένα ως πολιτικό εργαλείο ήταν το 2012 στην προεκλογική εκστρατεία του Barack Obama. Έκτοτε έχουν χρησιμοποιηθεί και σε επόμενες εκλογικές αναμετρήσεις.

Οι εφημερίδες “The Guardian” και “The New York Times”, στις 17 Μάρτιου 2018 έφεραν στο φως της δημοσιότητας άρθρα που ανέφεραν ότι περίπου 50 εκατομμύρια προφίλ χρηστών του Facebook έχουν υποκλαπεί και χρησιμοποιηθεί από την Cambridge Analytica. Σε επόμενα δημοσιεύματα διαπιστώθηκε ότι ο αριθμός των χρηστών που επηρεάστηκαν τελικώς, αυξήθηκε σε 87 εκατομμύρια χρήστες(Meredith, 2018). Η πρόσβαση σε προσωπικές πληροφορίες εκατομμυρίων πολιτών είχε ως στόχο τη συλλογή τους και στην συνέχεια τη χρήση τους για την καθοδήγηση αυτών των ατόμων προς μια συγκεκριμένη επιλογή. Στοιχεία όπως τα πολιτικά και θρησκευτικά πιστεύω, το μορφωτικό επίπεδο, ο σεξουαλικός προσανατολισμός, ακόμα και τα “likes” που έχει πατήσει ένας χρήστης, όπως και κάποιες συζητήσεις με τρίτα πρόσωπα στο Messenger, συλλέχθηκαν και αναλύθηκαν από ομάδα ειδικών, με σκοπό την δημιουργία προφίλ για τους υποψήφιους και κατ’ επέκταση, «ατομικές προεκλογικές εκστρατείες». Η χρήση του διαδικτύου δίνει την δυνατότητα στους σχεδιαστές των εκστρατειών να μπορούν μέσω αυτού να εξατομικεύουν τις πολιτικές διαφημίσεις ανάλογα με το ποια θέση υποστηρίζει ο κάθε ένας χρήστης (Privacy International).

Το 2010 το Facebook εγκαινίασε μια νέα πλατφόρμα, την Open Graph, που επέτρεπε την είσοδο σε τρίτες εφαρμογές. Όταν ένας χρήστης ήθελε να χρησιμοποιήσει μία τέτοιου είδους εφαρμογή στο Facebook, αυτή του ζητούσε πρόσβαση σε πολλά προσωπικά δεδομένα του, συμπεριλαμβάνοντας τις συνομιλίες με τους φίλους τους. Μετά από τρία χρόνια, δηλαδή το 2013, δημιουργήθηκε μία εφαρμογή με το όνομα “Thisisyourdigitallife” από τον ερευνητή του Πανεπιστημίου Cambridge, Aleksandr Kogan και την εταιρία του σε συνεργασία με την εταιρία Cambridge Analytica. Η εφαρμογή καταγινόταν με ερωτήσεις που απαντούσε ο κάθε χρήστης ξεχωριστά, με σκοπό την δημιουργία ψυχολογικού προφίλ. Περίπου 300.000 χρήστες συμμετείχαν στην έρευνα μέσω της εφαρμογής “Thisisyourdigitallife” και οι συμμετέχοντες πληρώθηκαν λιγότερο από 5\$ για την παροχή των προσωπικών τους στοιχείων. Τα δεδομένα που συλλέχθηκαν δεν διαγράφηκαν όπως θα έπρεπε σύμφωνα με τους νέους κανόνες που είχε εντάξει το Facebook (Meredith,2018).

Η εμπλοκή με τις αμερικανικές εκλογές του 2016 ξεκίνησε με αρχικό πρωταγωνιστή τον Ρεπουμπλικάνο υποψήφιο Ted Cruz, ο οποίος προσέλαβε την εταιρία Cambridge Analytica ώστε να του παρέχει ψυχολογικά προφίλ ψηφοφόρων που θα τον βοηθούσαν να αποκτήσει πλεονέκτημα έναντι του ετέρου υποψηφίου, Donald Trump. Το Facebook υποστηρίζει πως εκείνη την περίοδο προσπάθησε να σταματήσει την εφαρμογή του Kogan και να διαγράψει όλα τα δεδομένα που είχαν συγκεντρωθεί. Ωστόσο, λίγο καιρό αργότερα η Cambridge Analytica θα συνεργαζόταν με τον Donald Trump, και θα φρόντιζε να βελτιώσει την εκστρατεία του μετέπειτα Προέδρου της Αμερικής με πληθώρα διαφημίσεων στο Facebook (Meredith, 2018). Ως manager της εκστρατείας του Trump διορίστηκε ο Steven Bannon γεγονός που δεν ήταν τυχαίο, αφού ο Bannon ήταν πρώην αντιπρόεδρος της Cambridge Analytica. Ακόμα, είναι σημαντικό να αναφερθεί πως η οικογένεια Mercer, η οποία θεωρείται από τους σημαντικότερους Ρεπουμπλικάνους δωρητές στο κόμμα, είναι στενά συνδεδεμένη με την εταιρία Cambridge Analytica (Cadwalladr & Graham-Harrison, 2018).

Ο Γενικός Διευθυντής και δημιουργός του Facebook, Mark Zuckerberg, κατέθεσε στην επιτροπή των Γερουσιαστών λίγες εβδομάδες μετά την αποκάλυψη του σκανδάλου. Το Facebook είχε ήδη πληγεί αρκετά σε οικονομικό επίπεδο, λόγω της πτώσης τις τιμές των μετοχών του στο χρηματιστήριο. Η εταιρεία υπέστη ζημιά άνω των 50 δισεκατομμυρίων δολαρίων της αξίας της σε μία μόνο ημέρα. Επιπλέον και σε κοινωνικό επίπεδο υπέστη μεγάλη ζημιά, αφού πολλοί χρήστες αποφάσισαν να περιφρονήσουν το συγκεκριμένο κοινωνικό μέσο. Η κριτική μετά το τέλος της κατάθεσης του Zuckerberg ήταν θετική και όλοι συμφώνησαν πως εκπροσώπησε πολύ καλά τον τεχνολογικό κλάδο. Παράλληλα, είχε ως αποτέλεσμα την άνοδο της τιμής των μετοχών του Facebook στο χρηματιστήριο. Βασικά θέματα που έλαβαν χώρα κατά την διάρκεια της κατάθεσης ήταν η δυνατότητα ενός δικτύου σαν το Facebook να μπορεί να αυτοελέγχεται, ώστε να μην επαναληφθούν παρόμοια συμβάντα με αυτό του σκανδάλου. Επίσης, υπογραμμίστηκε η αδυναμία του Facebook να αποτρέψει την παρεμβολή διαφημίσεων με σκοπό τον πολιτικό προσηλυτισμό των χρηστών. Η σχετική ελευθερία που έχει δοθεί στα μέσα κοινωνικής δικτύωσης είχε ανησυχήσει τους γερουσιαστές, οι οποίοι πίστευαν ότι ίσως πρέπει να υπάρξει η κατάλληλη νομοθεσία. Ακόμα, συζητήθηκε αν στο Facebook γνώριζαν από νωρίτερα για την χρήση των προσωπικών δεδομένων από την Cambridge Analytica, και για ποιο λόγο δεν ενημέρωσαν νωρίτερα τα 87 εκατομμύρια χρηστών των οποίων οι πληροφορίες είχαν χρησιμοποιηθεί. Σχετικά με το τελευταίο ζήτημα, ο Zuckerberg δήλωσε ότι ήταν λάθος να μην ενημερώσουν τους χρήστες, ωστόσο δεν παραδέχτηκε αν ηθελημένα οι

χρήστες στερήθηκαν αυτής της ενημέρωσης. Τέλος, δήλωσε ότι η πλατφόρμα θα διορθώσει ό,τι χρειάζεται ώστε να μην προκύψει κάτι αντίστοιχο στο μέλλον(Roose & Kang, 2018).

2.4 Ανάλυση Σκανδάλου σχετικά με τη τεχνική της ψυχομετρίας

Το σκάνδαλο που οδήγησε στο κλείσιμο της Cambridge Analytica βασίζεται στη λάθος διαχείριση της προεκλογικής καμπάνιας του Donald Trump στις ΗΠΑ. Με βάση τα άρθρα που δημοσιεύτηκαν, η επιχείρηση κατηγορήθηκε για χορηγούμενες δημοσιεύσεις-διαφημίσεις στο Facebook που μπορούσαν να βλέπουν μόνο χρήστες με συγκεκριμένα προφίλ. Μέσω συγκεκριμένων ψυχομετρικών μεθόδων και τεχνικών διαχείρισης δεδομένων, η επιχείρηση διαμόρφωνε **μοντέλα προφίλ συμπεριφοράς**, τα οποία χωρίζονταν σε κατηγορίες και στην συνέχεια ταυτίζονταν με τα προφίλ των χρηστών. Αφού πραγματοποιούνταν αυτή η ταύτιση ανάλογα με τα χαρακτηριστικά της εκάστοτε κατηγορίας, δημιουργούνταν οι αντίστοιχες στοχευμένες διαφημίσεις με στόχο τον προσηλυτισμό των χρηστών. Στην συνέχεια, αποστέλλονταν μαζικά στοχευμένα μηνύματα ανάλογα με την κατηγορία που βρισκόταν ο κάθε χρήστης. Το κοινό χαρακτηριστικό που είχαν όλοι οι χρήστες ήταν ότι ήταν ψηφοφόροι στις Ηνωμένες Πολιτείες.

Μέχρι τώρα δεν έχει αναφερθεί κάτι μεμπτό ώστε να εξηγεί τον λόγο που έβαλε λουκέτο μια επιτυχημένη και αξιοζήλευτη εταιρία, όπως είναι η Cambridge Analytica. Το ερώτημα που γεννήθηκε είναι με ποιόν τρόπο βρήκε και συνέλεξε τα δεδομένα, ώστε να δημιουργήσει μοντέλα προφίλ συμπεριφοράς. Η βασική κατηγορία που της προσάπτεται, είναι ότι παραβίασε την ιδιωτικότητα των προσωπικών δεδομένων μερικών χρηστών του Facebook. Με ποιόν τρόπο όμως παραβίασε την ιδιωτικότητα των προσωπικών δεδομένων; Η Cambridge Analytica χρειάστηκε την βοήθεια της Global Science Research (GSR), η οποία έστησε ένα κουίζ με ονομασία *«thisisyourdigitallife»* και το διαφήμιζε ως κοινωνικό πείραμα που το χρησιμοποιούν ψυχολόγοι. Με αυτό το «υποτιθέμενο» κουίζ, πήρε τα προσωπικά δεδομένα από περίπου 270.000 χρήστες που ασχολήθηκαν με την εφαρμογή. Δυστυχώς, δεν πήρε μόνο τα προσωπικά δεδομένα των χρηστών που επέλεξαν να ασχοληθούν με το κουίζ, αλλά μπόρεσε και είχε πρόσβαση και στα προσωπικά δεδομένα των φίλων τους. Ο συνολικός αριθμός των ατόμων που υποκλάπηκαν τα προσωπικά τους στοιχεία, είναι 50 εκατομμύρια χρήστες(Οικονόμου, 2018).

Τα ερωτήματα είναι πολλά γύρω από αυτό το σκάνδαλο που έχει ταράξει την εμπιστοσύνη του απλού κόσμου με τα μέσα κοινωνικής δικτύωσης. Πόσο έμπιστα είναι για τους χρήστες τους; Μπορούν ευκολά να παραβιαστούν από τρίτους για προσωπικό όφελος; Τι συμπεράσματα μπορούν να διεξαχθούν για την προσωπικότητά του εκάστοτε χρήστη, με βάση τις προτιμήσεις και τις δημοσιεύσεις του στα μέσα κοινωνικής δικτύωσης; Για να μπορέσουμε να απαντήσουμε σε αυτά τα ερωτήματα πρέπει να γνωρίζουμε όλα τα γεγονότα που συνέβησαν πριν αλλά και μετά την εμπλοκή της Analytica σε ένα τέτοιο μεγάλο σκάνδαλο, καθώς και με ποιόν τρόπο εμπλέκεται.

Ο Michal Kosinski, είναι ένας 34χρονος ερευνητής και κορυφαίος ειδικός στην ψυχομετρία. Η ψυχομετρία είναι ένας υποκλάδος της ψυχολογίας που σχετίζεται με τα δεδομένα. Ο Kosinski κάνει τακτικά διαλέξεις σχετικά με τους κινδύνους των Big Data. Με τον όρο Big Data, στην ουσία εννοούμε όλα τα δεδομένα που συλλέγονται από τις κινήσεις του κάθε χρήστη, τόσο διαδικτυακά όσο και έκτος δικτύου. Αυτά τα δεδομένα είναι τα λεγόμενα ψηφιακά ίχνη. Η συλλογή των δεδομένων δίνεται από κάθε αγορά που κάνει ο χρήστης με τις κάρτες του, κάθε αναζήτηση στο Google, κάθε κίνηση που γίνεται στην κινητή συσκευή καθώς βρίσκεται στην τσέπη του χρήστη, κάθε δημοσίευση ή like που έχει πραγματοποιήσει ο χρήστης. Όλα αυτά αποθηκεύονται σε μια μεγάλη βάση δεδομένων. Για μεγάλο χρονικό διάστημα δεν υπήρχε λόγος χρησιμοποίησης αυτών των δεδομένων, μέχρι που γεννήθηκε η ιδέα, ότι μπορεί με βάση αυτά τα δεδομένα να χαρακτηριστεί η προσωπικότητα του κάθε χρήστη. Με ποιόν τρόπο όμως θα χρησιμοποιούσαμε όλα αυτά τα δεδομένα ώστε να υπάρχει δυνατότητα σωστών αποτελεσμάτων;

Τη δεκαετία του 1980, δύο ομάδες ψυχολόγων ανέπτυξαν ένα μοντέλο που προσπαθούσε να αξιολογήσει τα ανθρώπινα όντα με βάση πέντε χαρακτηριστικά της προσωπικότητας, γνωστά ως «**Big Five**». Αυτά τα χαρακτηριστικά είναι:

1. *Ανοιχτή αντίληψη*, δηλαδή πόσο δεκτικό μπορεί να είναι ένα άτομο σε νέες εμπειρίες,
2. *Συνειδητότητα*, δηλαδή πόσο τελειομανής είναι ένας άνθρωπος,
3. *Εξωστρέφεια*, δηλαδή πόσο κοινωνικό μπορεί να είναι ένα άτομο,
4. *Συγκαταβατικότητα*, δηλαδή πόσο διακριτικό και συνεργάσιμο μπορεί να είναι ένα άτομο,
5. *Νευρωτισμός*, δηλαδή πόσο εύκολα μπορεί να θυμώσει.

Με βάση τις μετρήσεις των παραπάνω χαρακτηριστικών, μπορούμε να κάνουμε μια σχετικά ακριβή εκτίμηση του είδους του ατόμου που έχουμε μπροστά μας. Πιο συγκεκριμένα,

μας δίνεται η δυνατότητα να γνωρίζουμε τις ανάγκες του, τους φόβους του και την πιθανότερη συμπεριφορά του. Τα «Big Five», είναι ουσιαστικά η πρότυπη τεχνική της ψυχομετρίας. Για πολύ καιρό όμως, το πρόβλημα με αυτήν την προσέγγιση ήταν η συλλογή των δεδομένων. Μία λύση σε αυτό το πρόβλημα ήταν να συμπληρωθεί ένα περίπλοκο, αλλά και ιδιαίτερος προσωπικό ερωτηματολόγιο. Όπως είναι προφανές, η λύση δεν ήταν και πολύ αποδοτική ώσπου ήρθε το Ίντερνετ και στην συνέχεια δημιουργήθηκε το Facebook(Grassegger & Krogerus, 2017).



Το 2008, ο Michal Kosinski φοιτούσε στην Βαρσοβία ώσπου τον δέχθηκαν στο Πανεπιστήμιο του Cambridge για να ξεκινήσει το διδακτορικό του στο Κέντρο Ψυχομετρίας. Το τμήμα που τον δέχτηκε είναι ένα από τα πιο παλιά ιδρύματα του είδους του στον κόσμο. Στην διάρκεια της φοίτησής του, γνωρίστηκε και στην συνέχεια συνεργάστηκε με έναν συμφοιτητή του που ονομαζόταν David Stillwell. Ο Stillwell, που σήμερα είναι καθηγητής στο Judge Business School του Πανεπιστημίου του Cambridge, είχε φτιάξει μια μικρή εφαρμογή στο Facebook. Η εφαρμογή λεγόταν «My Personality» και επέτρεπε στους χρήστες να συμπληρώνουν διάφορα ψυχομετρικά ερωτηματολόγια, συμπεριλαμβανομένων ψυχολογικών ερωτήσεων από το ερωτηματολόγιο προσωπικότητας Big Five. Μερικές ερωτήσεις που περιείχε η εφαρμογή ήταν «Πόσο εύκολα πανικοβάλλομαι;», «Πόσο συχνά κοντράρομαι με του άλλους» κλπ. Αφού ολοκλήρωναν το ερωτηματολόγιο, οι χρήστες λάμβαναν ένα «προφίλ προσωπικότητας» το οποίο μπορούσαν να το μοιραστούν με του φίλους τους στο Facebook. Εκτός από του φίλους τους όμως, το μοιράζονταν και με τους ερευνητές.



Michal Kosinski

Στην αρχή, ο Kosinski, πίστευε ότι δεν θα επιθυμούσαν να συμπληρώσουν το ερωτηματολόγιο πολλοί, πάρα μόνο οι φίλοι του από το κολέγιο. Δεν πέρασε πολύς καιρός μέχρι να διαψευσθεί, αφού εκατομμύρια άνθρωποι επιθυμούσαν να συμπληρώσουν το ερωτηματολόγιο. Έτσι, σιγά σιγά οι δύο υποψήφιοι διδάκτορες είχαν στην κατοχή τους το μεγαλύτερο σύνολο δεδομένων που συνδυάζει ψυχομετρικά αποτελέσματα με προφίλ του Facebook, που είχε συλλεχθεί μέχρι τότε. Αναλόγως τις απαντήσεις των ερωτηθέντων, η ομάδα των ψυχολόγων μπόρεσε να υπολογίσει τις προσωπικές Big Five αξίες των συμμετεχόντων. Έπειτα, συνέκριναν τα αποτελέσματα με όλα τα είδη των δεδομένων που βρίσκονταν διασκορπισμένα στο διαδίκτυο. Τα δεδομένα που τους ενδιέφεραν πιο πολύ ήταν τι «άρεσε» σε κάθε χρήστη με βάση τα like του, τι δημοσίευαν οι χρήστες στο Facebook ώστε να το δουν οι φίλοι τους, τι μοιράζονταν με τους φίλους τους, τι φύλο και τι ηλικία ήταν ο κάθε χρήστης, καθώς και ο τόπος κατοικίας του. Με αυτή την σύγκριση, κατάφεραν να ενώσουν τέλεια ή να συσχετίσουν τους χρήστες μέσω των κινήσεων τους στο προφίλ με τις προσωπικότητες των Big Five.

Μετά την ταύτιση προσωπικοτήτων, ήταν πλέον εύκολο να διεξαχθούν αξιόπιστα συμπεράσματα για την προσωπικότητα του καθενός από απλές κινήσεις στο διαδίκτυο. Μερικά παραδείγματα των συμπερασμάτων που είχαν εξαχθεί είναι ότι ένας από τους καλύτερους δείκτες για την ετεροφυλοφιλία ήταν η προτίμηση στο άκουσμα του συγκροτήματος Wu-Tang Clan. Οι ακόλουθοι της Lady Gaga ήταν πιθανότατα εξωστρεφείς, ενώ εκείνοι που προτιμούσαν τη φιλοσοφία έτειναν να είναι εσωστρεφείς. Από την άλλη, ποσό έγκυρη είναι μια μεμονωμένη ενέργεια του χρήστη, ώστε να καταλήξει στην εξαγωγή κάποιων συγκεκριμένων συμπερασμάτων; Φυσικά και από μόνη της δεν είναι έγκυρη καμία ενέργεια, όμως ο συνδυασμός από εκατοντάδες ή ακόμη και χιλιάδες μεμονωμένων δεδομένων μπορεί να γίνει μια ακριβής πρόβλεψη για την προσωπικότητα του καθενός. Το 2012, ο Kosinski μαζί με την ομάδα του απέδειξαν ότι με βάση έναν μέσο όρο 68 likes στο Facebook από έναν χρήστη, ήταν πιθανό να προβλέψει το χρώμα του δέρματός του, με ακρίβεια 95%, τον σεξουαλικό προσανατολισμό του, με ακρίβεια 88% και τη σχέση του με το Δημοκρατικό ή το Ρεπουμπλικανικό Κόμμα, με ακρίβεια 85%. Προφανώς δεν ήταν και τα μόνα συμπεράσματα που μπορούσαν να προβλεφθούν από αυτά τα 68 likes. Η νοημοσύνη, οι θρησκευτικές πεποιθήσεις, καθώς επίσης η χρήση αλκοόλ, τσιγάρου και ναρκωτικών ήταν μερικά από αυτά

που θα μπορούσαν να προσδιοριστούν. Το αξιοσημείωτο είναι ότι από αυτά τα δεδομένα, ήταν δυνατό να εξαχθεί το συμπέρασμα εάν κάποιου οι γονείς είχαν χωρίσει. Η ομάδα των ψυχολόγων δεν επαναπαύτηκε στα ως τότε αποτελέσματα και συνέχισε την σκληρή δουλειά, ώσπου έφτασε στο σημείο να μπορεί να αξιολογήσει ένα άτομο καλύτερα από τον μέσο συνάδελφο του στην δουλειά, μόνο και μόνο από τα like του στο Facebook. Δεν σταμάτησε ούτε σε αυτό το σημείο, συνεχίζοντας την αδιάκοπη δουλειά και επεξεργασία των δεδομένων. Τα τελικά συμπεράσματα που εξάχθηκαν ήταν ότι 70 like ήταν αρκετά να ξεπεράσουν αυτά που γνώριζαν οι φίλοι του ατόμου για το ίδιο το άτομο, 150 like ήταν ικανά να ξεπεράσουν αυτά που γνώριζαν οι γονείς του και 300 like αυτά που γνώριζε ο σύντροφός του. Αν παίρναμε σαν γνώμονα περισσότερα like, μπορούσαν να ξεπεράσουν ακόμα και αυτά που πίστευε το ίδιο το άτομο για τον εαυτό του.

Ο Kosinski, ενθουσιασμένος από τα ευρήματα που είχε ανακαλύψει θεώρησε σωστή την επιλογή να τα δημοσιεύσει. Οι διαχειριστές όμως του Facebook, δεν είχαν τον ίδιο ενθουσιασμό με τον νεαρό ερευνητή, γι' αυτό και του έστειλαν απειλή μήνυσης. Το γεγονός ότι δεν ενθουσιάστηκαν με τα ευρήματά, δεν τους εμπόδισε να του προτείνουν θέση εργασίας στην εταιρεία τους, από την στιγμή που εκτίμησαν ότι είχε πολλές δυνατότητες. Ταυτόχρονα, ο όμιλος του Facebook μετέτρεψε σε ιδιωτικά τα like ως προεπιλογή. Πριν από αυτό το εγχείρημα, η προεπιλεγμένη ρύθμιση ήταν ότι οποιοσδήποτε θα μπορούσε να δει τα like του κάθε χρήστη. Η νέα ρύθμιση δεν επηρέαζε καθόλου την συλλογή δεδομένων, αφού η εφαρμογή του Kosinski ζητούσε την συγκατάθεση των χρηστών για να μπορέσει να συλλέξει τα δεδομένα. Αυτός είναι ο λόγος που πολλές εφαρμογές και κουίζ απαιτούν πρόσβαση στα προσωπικά δεδομένα ως προϋπόθεση για να κάνεις το τεστ προσωπικότητας.

Τα like ωστόσο, δεν είναι ο μοναδικός δείκτης που μπορεί να αποδώσει τις Big Five αξίες. Ο αριθμός των φωτογραφιών προφίλ που έχει ένα άτομο στο Facebook ή ο αριθμός των επαφών που έχει, είναι ένας ικανοποιητικός δείκτης της εξωστρέφειας του. Επιπλέον, δεν είναι απαραίτητο να είναι στο διαδίκτυο ένα άτομο για να δείξει στοιχεία του χαρακτήρα του. Για παράδειγμα, ο αισθητήρας κίνησης στο κινητό δείχνει πόσο γρήγορα κινείται ο κάτοχός του και πόσο μακριά ταξιδεύει. Ένα τέτοιο δείγμα σχετίζεται με την συναισθηματική αστάθεια του κάθε ατόμου. Με βάση όλα τα παραπάνω, ο Kosinski κατέληξε ότι το smartphone είναι ένα τεράστιο ψυχολογικό ερωτηματολόγιο το οποίο συμπληρώνουμε συνεχώς, τόσο συνειδητά όσο και ασυνείδητα. Δυστυχώς, η χρήση των δεδομένων δεν αρκείται μόνο για την δημιουργία ψυχολογικών προφίλ, αλλά και για την αναζήτηση συγκεκριμένων προφίλ. Η χρησιμότητα της

αναζήτησης συγκεκριμένων προφίλ γίνεται για την ευκολότερη χειραγώγηση του κοινού. Ουσιαστικά, αυτό που ο Kosinski είχε εφεύρει ήταν ένα είδος μηχανής αναζήτησης ανθρώπων.

Στις αρχές του 2014, προσέγγισε τον Kosinski ένας νεαρός βοηθός καθηγητή στο Τμήμα Ψυχολογίας που ονομαζόταν Aleksandr Kogan. Τον ενημέρωσε ότι έκανε έρευνα για λογαριασμό μιας εταιρείας που ενδιαφερόταν για τη μέθοδο του και ήθελε να έχει πρόσβαση στη βάση δεδομένων της εφαρμογής My Personality. Ο Kogan δεν αποκάλυψε τον λόγο για τον οποίο η εταιρεία ήθελε τα δεδομένα. Η εταιρεία που εκπροσωπούσε ο Kogan ήταν η SCL. Στην αρχή, ο Kosinski και η ομάδα του σκέφτηκαν αυτή την προσφορά, καθώς σήμαινε πάρα πολλά χρήματα για το ινστιτούτο, αλλά στη συνέχεια δίστασε. Αποφάσισε λοιπόν, να κάνει μια έρευνα για την εταιρεία και τον άνθρωπο που του ζήτησε τόσο πολύτιμα αρχεία. Στην ερευνά του, ανακάλυψε ότι ο Aleksandr Kogan είχε ιδρύσει μυστικά μια εταιρεία που συνεργαζόταν με την SCL. Σύμφωνα με ρεπορτάζ του Δεκεμβρίου του 2015, στην εφημερίδα «*The Guardian*» και τα εσωτερικά έγγραφα της εταιρείας που δόθηκαν στο περιοδικό «*Das Magazin*», προκύπτει ότι η SCL έμαθε για τη μέθοδο του Kosinski από τον Kogan (Δημοπούλου, 2018). Ο Kosinski υποπτευόταν ότι η εταιρεία του Kogan ίσως είχε χρησιμοποιήσει τα like του Facebook με βάση το εργαλείο μέτρησης των Big Five, προκειμένου να το πουλήσει σε αυτήν την επιχείρηση που επηρεάζει τις εκλογές. Αμέσως, πήρε την απόφαση να σπάσει το συμβόλαιο με τον Kogan και πληροφόρησε τον διευθυντή του ινστιτούτου, πυροδοτώντας μια περίπλοκη σύγκρουση μέσα στο πανεπιστήμιο. Το ινστιτούτο ανησυχούσε για τη φήμη του και αμέσως έληξε τη συνεργασία. Έτσι, ο Aleksandr Kogan μετακόμισε στη Σιγκαπούρη, παντρεύτηκε και άλλαξε το όνομά του σε Dr. Spectre. Ο Michal Kosinski τελείωσε το διδακτορικό του και του προσέφεραν δουλειά στο Stanford καταλήγοντας να μετακομίσει στις ΗΠΑ.

Μέχρι εκείνη την εποχή, όλες οι εταιρείες που αναλάμβαναν τις προεκλογικές καμπάνιες πολιτικών αρχηγών βασίζονταν σε δημογραφικά στοιχεία. Η Cambridge Analytica όμως, από την αρχή της καριέρας της χρησιμοποίησε την ψυχομετρία. Βέβαια, για να το καταφέρει όλο αυτό βασίστηκε στα στοιχεία που αγόρασε η θυγατρική της εταιρία από την εταιρεία του Aleksandr Kogan. Σύμφωνα με τον Nix, η επιτυχία του μάρκετινγκ της Cambridge Analytica βασίζεται σε έναν συνδυασμό τριών στοιχείων. Το πρώτο στοιχείο είναι η χρήση του μοντέλου OCEAN, αυτό το μοντέλο είναι η επιστήμη της συμπεριφοράς ενός ατόμου με βάση τα πρότυπα Big Five. Το δεύτερο στοιχείο είναι η ανάλυση των Big Data και το τρίτο η στοχευμένη διαφήμιση. Μια στοχευμένη διαφήμιση, είναι στην ουσία μια προσωποποιημένη διαφήμιση, που εναρμονίζεται όσο το δυνατόν καλύτερα με την προσωπικότητα ενός

μεμονωμένου καταναλωτή. Ο Nix μας εξηγεί τον τρόπο που δουλεύει η εταιρεία του. Αρχικά, η Analytica αγοράζει προσωπικά δεδομένα από διαφορετικές πηγές όπως τα υποθηκοφυλακεία, τα δεδομένα αυτοκινήτων, τα δεδομένα για ψώνια, τις κάρτες bonus, τις συνδρομές σε λέσχες, τα περιοδικά που επιλέγουν να διαβάσουν οι καταναλωτές, σε ποιες εκκλησίες πηγαίνουν κλπ. Για να μπορέσει να βρει όλα αυτά τα δεδομένα, έρχεται σε επαφή με μεσίτες δεδομένων, όπως είναι οι Ascision και Experian στις ΗΠΑ και αγοράζει από αυτές τα δεδομένα που χρειάζεται εκείνη την στιγμή. Έτσι, συγκεντρώνει τα δεδομένα που θέλει, τα συνδυάζει με τους εκλογικούς καταλόγους του Ρεπουμπλικανικού Κόμματος και με τα δεδομένα που βρίσκονται στο διαδίκτυο και με αυτό τον τρόπο προβλέπει ένα προφίλ προσωπικότητας Big Five. Τα ψηφιακά ίχνη που χρησιμοποιεί σε αρχικό στάδιο, μετατρέπονται ξαφνικά σε πραγματικούς ανθρώπους με φόβους, ανάγκες, ενδιαφέροντα και διευθύνσεις κατοικίας.



Την χρονιά του 2016, η Analytica είχε προσληφθεί από τον Donald Trump για την προεκλογική του καμπάνια στο δημοψήφισμα των Ηνωμένων Πολιτειών της Αμερικής. Αμέσως, η επιχείρηση κινητοποιήθηκε για την υπεράσπιση του πελάτη της και την εξάλειψη των υπολοίπων πολιτικών αρχηγών. Πώς όμως οι ψηφοφόροι των αντίπαλων του Trump θα άλλαζαν εν τέλει την επιλογή τους; Την ημέρα που έγινε η τρίτη προεδρική συνάντηση μεταξύ του Trump και της Clinton, η ομάδα του Trump δοκίμασε 175.000 διαφορετικές παραλλαγές για τα επιχειρήματά του, προκειμένου να βρουν τις σωστές εκδοχές μέσω του Facebook. Τα μηνύματα διέφεραν μόνο σε μικροσκοπικές λεπτομέρειες, προκειμένου να εστιάσουν τους αποδέκτες κατά τον βέλτιστο ψυχολογικό τρόπο. Οι λεπτομέρειες που τροποποιήθηκαν είναι διαφορετικοί τίτλοι, χρώματα, λεζάντες, διαφορετικές φωτογραφίες ή βίντεο. Ένα παράδειγμα μια τέτοιας διαφήμισης είναι στην περιοχή της Μικρής Αϊτής του Μαϊάμι. Η καμπάνια του

Trump παρείχε στους κατοίκους ειδήσεις για την αποτυχία του Ιδρύματος Clinton μετά τον σεισμό στην Αϊτή, προκειμένου να τους αποτρέψει να ψηφίσουν υπέρ της Hilary Clinton. Ο στόχος αυτού του διαφημιστικού είναι να επηρεάσει την γνώμη των εν δυνάμει ψηφοφόρων της Clinton. Οι εν δυνάμει ψηφοφόροι είναι αμφιταλαντευόμενοι Αριστεροί, Αφροαμερικάνοι και γυναίκες νεαρής ηλικίας. Άλλο είναι παράδειγμα, είναι κάποιες στοχευμένες – χορηγούμενες αναρτήσεις στο Facebook, που μπορούσαν να τις δουν μόνο χρήστες με συγκεκριμένα προφίλ. Σε αυτή την περίπτωση μπορούσαν να τις δουν μόνο Αφροαμερικάνοι. Οι συγκεκριμένες διαφημίσεις έδειχναν ότι η Hilary Clinton αναφέρεται στους έγχρωμους άνδρες ως αρπακτικά. Όλη αυτή η επίθεση δεν ήταν τόσο αντιληπτή από τον λαό της Αμερικής διότι γινόταν μέσω διαλλακτικών διαφημίσεων στην τηλεόραση και περισσότερο στα social media ή την ψηφιακή τηλεόραση. Γι' αυτό τον λόγο, η ομάδα που είχε αναλάβει την καμπάνια της Clinton πίστευε ότι ηγούνταν του αγώνα, βάσει των δημογραφικών προβλέψεων. Αποδείχτηκε ότι έκαναν μεγάλο λάθος στις προγνώσεις τους και ότι στην καθημερινότητα του ανθρώπου έχει εισχωρήσει ένας νέος ψηφιακός τρόπος διαφήμισης που είναι αποδοτικότερος σε σχέση με τον παραδοσιακό.

Για την επίτευξη όμως της εκλογής του Trump, πάρθηκαν πιο ριζοσπαστικά μέτρα. Τον Ιούλιο του 2016, οι ψηφοθήρες του Trump ήταν εφοδιασμένοι με μια εφαρμογή με την οποία μπορούσαν να προσδιορίσουν τις πολιτικές απόψεις και τους τύπους της προσωπικότητας των ενοίκων ενός σπιτιού. Έτσι, χτύπησαν τις πόρτες των σπιτιών μόνο όσων η εφαρμογή τους αξιολόγησε ως δεκτικούς στα μηνύματά τους. Οι ψηφοθήρες ήταν προετοιμασμένοι με κατευθυντήριες γραμμές, για συζητήσεις ανάλογες με τον τύπο της προσωπικότητας του ενοίκου του σπιτιού. Μετά την συνάντησή τους με τους ενοίκους, οι ίδιοι οι ψηφοθήρες εμπλούτιζαν την εφαρμογή με τις αντιδράσεις του κάθε ενοίκου. Αυτά τα πρόσθετα δεδομένα έμπαιναν στους πίνακες της καμπάνιας του Trump. Με όλα τα παραπάνω δεδομένα, η Cambridge Analytica χώρισε τον αμερικανικό λαό σε 32 τύπους προσωπικότητας και εστίασε σε 17 πολιτείες. Όπως ακριβώς είχε προβλέψει ο Kosinski, ότι κάποιες προτιμήσεις των ατόμων παραπέμπουν σε κάποια χαρακτηριστικά του, η εταιρεία ανακάλυψε ότι η προτίμηση των ατόμων για φτιαγμένα αυτοκίνητα στις ΗΠΑ, ήταν μια σοβαρή ένδειξη ενός εν δυνάμει ψηφοφόρου του Trump. Μεταξύ άλλων, τα συμπεράσματα των αποτελεσμάτων των δεδομένων έδειξαν στον Trump ποια μηνύματα λειτουργούσαν καλύτερα και σε ποια περιοχή. Η απόφαση να εστιάσει στο Michigan και το Wisconsin τις τελευταίες εβδομάδες της εκστρατείας του, ελήφθη βάσει της ανάλυσης των δεδομένων. Ουσιαστικά, ο υποψήφιος έγινε το όργανο για την υλοποίηση ενός μοντέλου Big Data(Grassegger & Krogerus, 2017).

Συμπερασματικά, η Cambridge Analytica, είναι μια πολύ ικανή εταιρεία που ξέρει πως να χειρίζεται κατάλληλα την γνώμη του απλού κοινού, φέρνοντας επιθυμητά αποτελέσματα στον εκάστοτε πελάτη της. Οι μέθοδοι όμως που χρησιμοποιεί είναι νομικά σωστές ή μήπως όχι; Αυτό το ερώτημα έχει απασχολήσει τον τελευταίο καιρό τον τύπο. Όλα ξεκίνησαν τον Μάρτιο του 2018, από μία δημόσια δήλωση ενός πρώην υπαλλήλου της, του Christopher Wylie, για υποκλοπή δεδομένων από την εφαρμογή του Facebook. Ο Christopher Wylie δεν ήταν ένας απλός υπάλληλος, αλλά ήταν διευθυντής στον τομέα της έρευνας της επιχείρησης. Οι δηλώσεις του δεν παρέμειναν εκεί, αφού του ζητήθηκε να αποκαλύψει ό,τι γνώριζε σχετικά με την εταιρία και την υπόθεση υποκλοπής. Στην δήλωσή του ανέφερε ότι η Analytica εξήγαγε προσωπικές πληροφορίες περίπου 50 εκατομμυρίων ανθρώπων στις ΗΠΑ το 2014. Επιπλέον, ανέφερε περισσότερες λεπτομέρειες για τις πρακτικές που ακολούθησε η εταιρία για τη χειραγώγηση του κόσμου μέσω του Facebook. Ο ακριβής τρόπος με τον οποίο υποκλάπηκαν τα δεδομένα και πώς αυτά χρησιμοποιήθηκαν στην συνέχεια, φαίνεται αναλυτικότερα στο επόμενο κεφάλαιο. Μετά από αυτές τις δηλώσεις ένας εκπρόσωπος της Cambridge Analytica είπε ότι *«Η Cambridge Analytica δεν χρησιμοποιεί δεδομένα από το Facebook. Δεν είχε κάνει καμία συμφωνία με τον Michal Kosinski. Δεν έχει αναθέσει την έρευνα σε άλλους. Δεν χρησιμοποιεί την ίδια μεθοδολογία. Τα ψυχογραφικά στοιχεία χρησιμοποιήθηκαν ελάχιστα. Η Cambridge Analytica δεν συμμετείχε σε προσπάθειες να αποθαρρύνει οποιονδήποτε Αμερικανό να πάει να ψηφίσει στις προεδρικές εκλογές. Οι προσπάθειές της ήταν αποκλειστικά προς την κατεύθυνση να αυξήσει τον αριθμό των ψηφοφόρων στις εκλογές»* (Grassegger & Krogerus, 2017).

ΚΕΦΑΛΑΙΟ 3

ΑΝΑΛΥΣΗ ΣΚΑΝΔΑΛΟΥ

Στο κεφάλαιο αυτό, θα μελετήσουμε και θα αναλύσουμε τον τρόπο με τον οποίο έγινε η υποκλοπή των δεδομένων. Πώς ακριβώς έγινε; Ποια χρονική περίοδο; Πώς αναλύθηκαν τα στοιχεία που συλλέχθηκαν; Γνώριζαν οι χρήστες τον σκοπό της χρήσης των δεδομένων τους; Είχαν γνώση του ζητήματος όταν έδιναν τη συγκατάθεση τους στην ελεύθερη πρόσβαση στο προφίλ τους, από τις υπηρεσίες της Cambridge Analytica; Η υπόθεση αυτή γέννησε ερωτηματικά, ενώ κάθε εμπλεκόμενος στην υπόθεση αυτή έχει τη δική του οπτική γωνία και τη δική του γραμμή υπεράσπισης.

Όλα ξεκίνησαν από ένα «αθώο» τεστ προσωπικότητας στο Facebook. Πιο περιεκτικό από τα συνηθισμένα τεστ με τίτλους όπως «Ποια θα είναι η τυχερή σας ημέρα του έτους;» ή «Τι χρώμα έχει η αύρα του σκύλου σας;», το τεστ αυτό συντάχθηκε από το Πανεπιστήμιο του Cambridge, κάτι το οποίο του έδινε αυτομάτως άλλη βαρύτητα. Παρ' όλ' αυτά, η επεξεργασία των αποτελεσμάτων δεν ήταν τελικά όσο νόμιμη έμοιαζε αρχικά.

Ο ακαδημαϊκός που ασχολήθηκε με την επεξεργασία των αποτελεσμάτων, ήταν ο Aleksandr Kogan. Ο ακαδημαϊκός αυτός συνέλεξε τα δεδομένα με την πρόθεση να τα πουλήσει στην Cambridge Analytica, προκειμένου να δημιουργηθούν στοχευμένες διαφημίσεις στο διαδίκτυο. Όταν λοιπόν οι χρήστες ολοκλήρωσαν το τεστ προσωπικότητας, συμφώνησαν ότι ο ακαδημαϊκός Kogan θα μπορούσε να χρησιμοποιήσει τα αποτελέσματα του τεστ. Επιπροσθέτως, συμφώνησαν στην ελεύθερη πρόσβαση στο προφίλ τους, συμπεριλαμβανομένων των κινήσεων τους (likes) και των φίλων τους.

Με την εγκεκριμένη πρόσβαση σε προφίλ περίπου 270.000 χρηστών που έκαναν το τεστ, ο Kogan, κατάφερε να συλλέξει πληροφορίες, δεδομένα και πληροφορίες για παραπάνω από 50 εκατομμύρια φίλους των χρηστών που ολοκλήρωσαν το τεστ. Η Cambridge Analytica λοιπόν, ανέλυσε τα δεδομένα που είχαν συλλεχθεί με σκοπό τη δημιουργία «Ψυχογραφικών Προφίλ» των χρηστών βασιζόμενη στη διαχυτικότητα των χρηστών, τη συνειδητή πλοήγηση, την εξωστρέφεια και τη γενικότερη συμπεριφορά στο Facebook. Με άλλα λόγια, το Project λειτούργησε ως εξής: Τα αποτελέσματα του τεστ έδωσαν τα προφίλ των χρηστών. Από τα προφίλ αυτά, καταχωρήθηκαν για κάθε χρήστη διαφορετικά, οι κινήσεις του στο Facebook, οι σελίδες που ακολουθούσε και τα «likes» που υπήρχαν μέχρι εκείνη τη στιγμή. Η ίδια τακτική

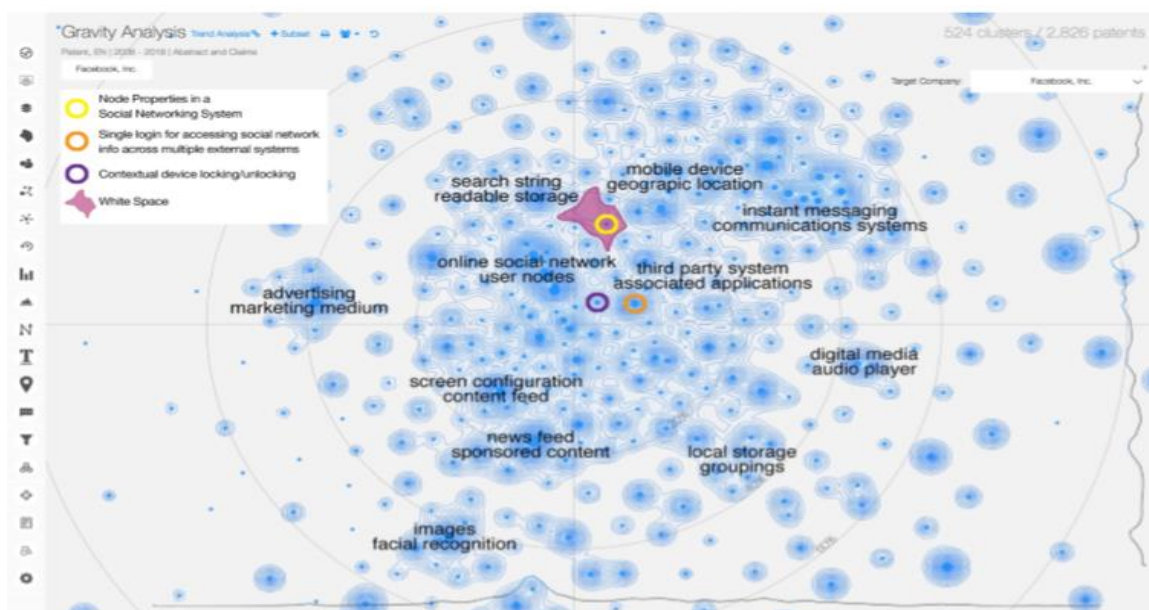
εφαρμόστηκε και στα προφίλ των επιπλέον 50 εκατομμυρίων χρηστών που ανακαλύφθηκαν μέσω των προφίλ των αρχικών χρηστών που έκαναν το τεστ (Justin Cudmore & James True, 2018).

3.1 Τεχνολογίες του Facebook που εξυπηρέτησαν την υποκλοπή

Η ολοκλήρωση της στοχευμένης αυτής διαδικασίας, είναι αποτέλεσμα ορισμένων παραγόντων και δυνατοτήτων. Πιο συγκεκριμένα, το Facebook διαθέτει διάφορες τεχνολογίες για τη διευκόλυνση ενεργειών σε άλλες εφαρμογές. Μία από τις πιο γνωστές τεχνολογίες, είναι το επονομαζόμενο «Facebook Login». Η τεχνολογία αυτή επιτρέπει στο χρήστη να χρησιμοποιεί τον λογαριασμό του Facebook που διαθέτει, προκειμένου να εγγραφεί σε άλλες ιστοσελίδες και εφαρμογές, χωρίς όμως να δημιουργήσει νέο λογαριασμό για τις ανάγκες της εκάστοτε εφαρμογής. Οι χρήστες προτιμούν λοιπόν, τη χρήση της συγκεκριμένης δυνατότητας, καθώς δεν χρειάζεται να απομνημονεύουν διαφορετικά στοιχεία πρόσβασης κάθε φορά.

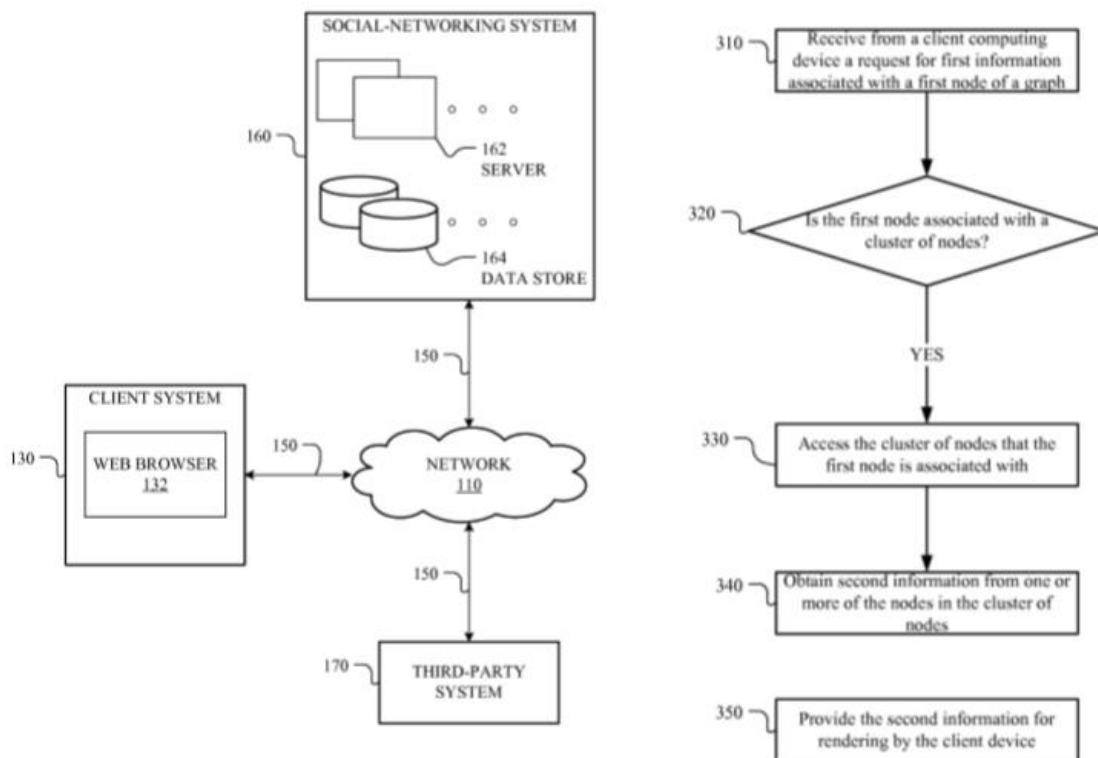
Παρά το γεγονός ότι οι περισσότεροι χρήστες εκμεταλλεύονται την τεχνολογία αυτή, λίγοι γνωρίζουν ότι δίνουν αβίαστα τη συγκατάθεση τους στη χρήση πληροφοριών του προφίλ τους, όπως δεδομένα γεωεντοπισμού, στοιχεία ηλεκτρονικού ταχυδρομείου ή ακόμη και λίστες με τους «φίλους» που διαθέτει ο καθένας. Κάτι ανάλογο, λοιπόν, χρησιμοποιήθηκε και στην περίπτωση μελέτης που εξετάζεται στην εργασία αυτή.

Η αντίστοιχη τεχνολογία που χρησιμοποιήθηκε για την ανάκτηση των απαραίτητων δεδομένων για την υποτιθέμενη «Πανεπιστημιακή Έρευνα», είναι αυτή της ελεύθερης πρόσβασης τρίτων στο προφίλ του κάθε χρήστη. Έχουν όμως γνωστοποιηθεί από το Facebook οι τεχνολογίες αυτές; Στο παρακάτω σχήμα φαίνονται όλες οι τεχνολογίες του Facebook.



Σχήμα 3.1: Τεχνολογίες του Facebook.

Μπορούμε να παρατηρήσουμε υψηλή πυκνότητα γύρω από τις διαφημίσεις, τα ψηφιακά μέσα, την αναγνώριση προσώπου, τον γεωεντοπισμό καθώς και τη συλλογή δεδομένων από τρίτους. Στο παραπάνω σχήμα φαίνεται μια περιοχή με την ονομασία «White Space». Όταν σε ένα σχεδιάγραμμα τεχνολογιών υπάρχει μία περιοχή που χαρακτηρίζεται με τον όρο αυτό, σημαίνει ότι δεν υπάρχει αρκετή γνώση για την ολοκλήρωση της ανάπτυξης των τεχνολογιών που την αποτελούν. Στην περιοχή αυτή βρίσκεται η τεχνολογία «**NODE PROPERTIES IN A SOCIAL-NETWORKING SYSTEM.**» με αριθμό 20150113060 (FACEBOOK: A BREACH IN THE WALL. A TECHNOLOGICAL APPROACH TO THE FACEBOOK CAMBRIDGE ANALYTICA SCANDAL, 2018).

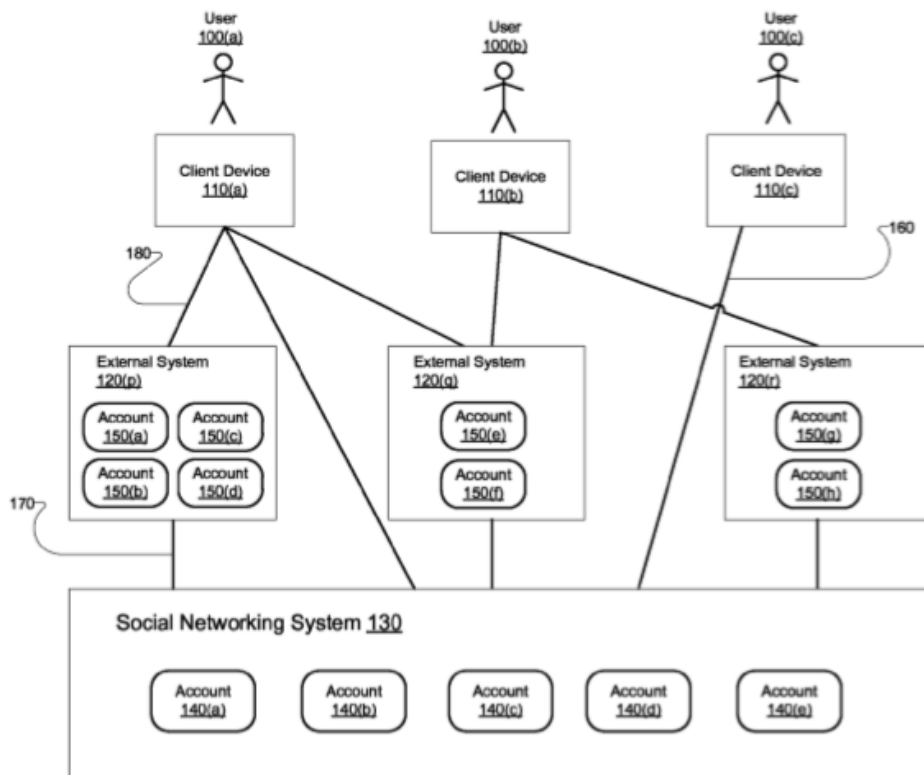


Σχήμα 3.2: Τεχνολογία σύνδεσης χρήστη στον ιστό

Σύμφωνα με την τεχνολογία αυτή, μία ή περισσότερες συσκευές διακομιστών (servers), θα λαμβάνουν από μία ή περισσότερες συσκευές χρηστών ένα αίτημα σύνδεσης. Για τη μεταφορά της οποιασδήποτε πληροφορίας, είναι απαραίτητη η σύνδεση της συσκευής του χρήστη με έναν αρχικό κόμβο ο οποίος θα τον συνδέσει τελικά στον ιστό. Ο αρχικός κόμβος συνδέεται σε ένα σύμπλεγμα κόμβων για την ανάκτηση πληροφοριών. Στο ίδιο σύμπλεγμα συνδέονται παραπάνω από ένας διακομιστές και συσκευές χρηστών. Με τον τρόπο αυτό ένα λειτουργικό σύστημα «τρίτων», μπορεί να συνδεθεί σε απομακρυσμένους διακομιστές που συνδέονται με το σύμπλεγμα των κόμβων που μελετάμε και να ανακτήσουν έτσι πληροφορίες για παραπάνω από μία συσκευές χρηστών.

Έτσι, κατανοήσαμε την τεχνολογία πίσω από την ελεύθερη πρόσβαση τρίτων στο προφίλ ενός χρήστη. Το ερώτημα όμως που γεννάται, είναι το εξής: Γιατί η εφαρμογή «Εισόδου» του Facebook επέτρεψε την εκμετάλλευση των στοιχείων των χρηστών από κάποια άλλη εφαρμογή πλην του ίδιου του Facebook; Την ερώτηση αυτή, έρχεται να απαντήσει μια άλλη τεχνολογία που χρησιμοποιείται, με αριθμό 9306927 και ονομασία «**SINGLE LOGIN PROCEDURE FOR ACCESSING SOCIAL NETWORK INFORMATION ACROSS MULTIPLE EXTRENAL SYSTEMS**», η δράση της οποίας φαίνεται στο παρακάτω

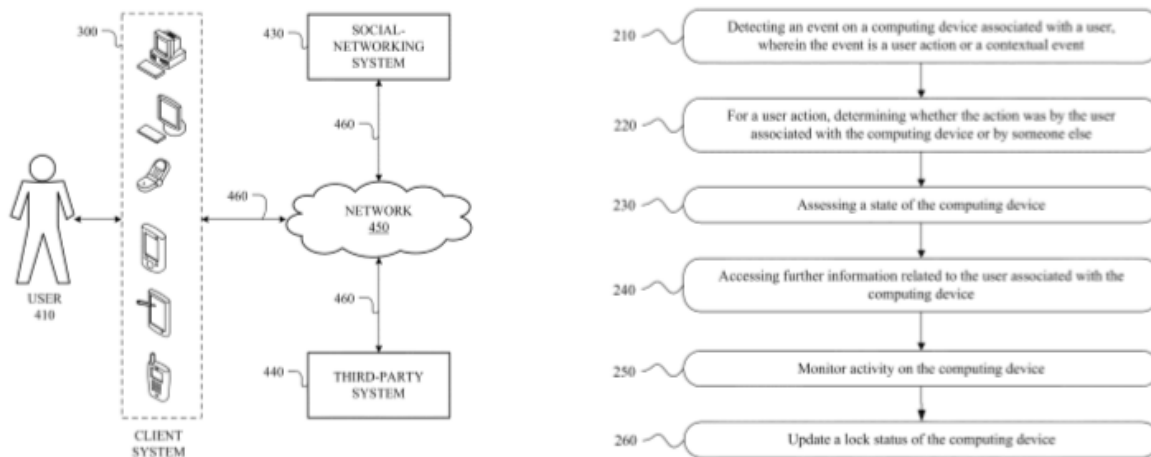
διάγραμμα (FACEBOOK: A BREACH IN THE WALL. A TECHNOLOGICAL APPROACH TO THE FACEBOOK CAMBRIDGE ANALYTICA SCANDAL, 2018).



Σχήμα 3.3: Προσπάθεια τρίτων συστημάτων να ανακτήσουν πληροφορίες

Σύμφωνα με την τεχνολογία αυτή, ένα οποιοδήποτε εξωτερικό σύστημα το οποίο δεν μπορεί να φέρει και να διατηρήσει πληροφορίες προσωπικού χαρακτήρα για τους χρήστες του, προσπαθεί να αποκομίσει δεδομένα με οποιονδήποτε τρόπο. Λόγω του γεγονότος ότι οι πληροφορίες αυτές είναι εξαιρετικά σημαντικές για τέτοια συστήματα, διάφορες παραποιήσεις της τεχνολογίας αυτής επιτρέπουν στα συστήματα αυτά να έχουν πρόσβαση σε πληροφορίες κοινωνικού ενδιαφέροντος. Η εκμετάλλευση των πληροφοριών των χρηστών, κρύβονται πίσω από το πλεονέκτημα της διατήρησης της αυθεντικοποίησης σε διαφορετικά συστήματα που παρέχεται στους χρήστες.

Η τεχνολογία «**CONTEXTUAL DEVICE LOCKING/UNLOCKING**», που έχει πρωταγωνιστικό ρόλο στο Facebook, είναι μία τεχνολογία που θα έπρεπε να έχει αποτρέψει την υποκλοπή στοιχείων των χρηστών.



Σχήμα 3.4: Τεχνολογία εντοπισμού και αποτροπής υποκλοπής στοιχείων

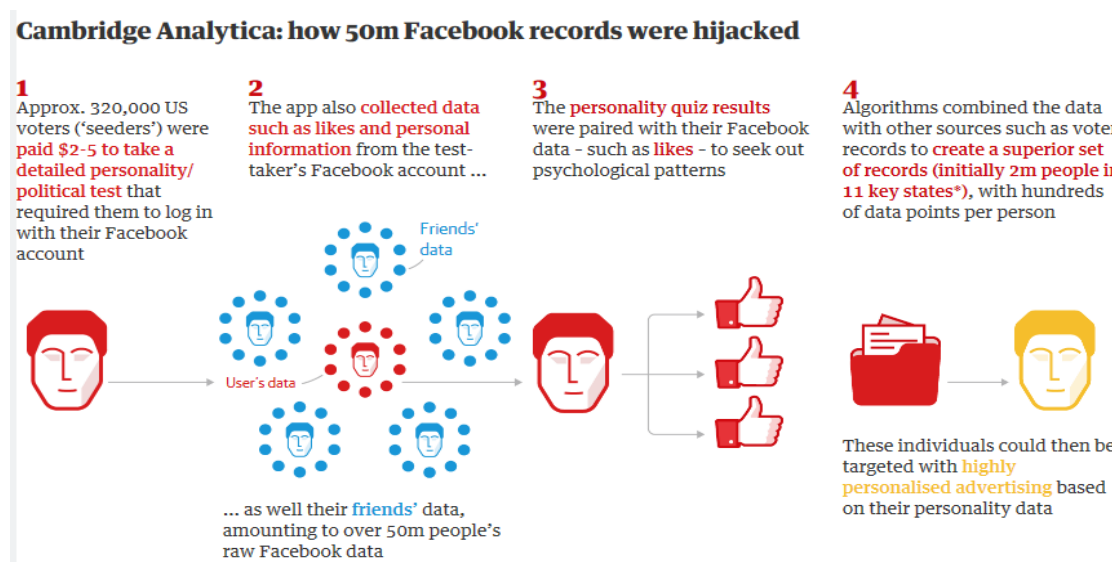
Σύμφωνα με την τεχνολογία αυτή, όταν παρατηρηθεί μια ασυνήθιστη συμπεριφορά στη συσκευή του χρήστη, όπως για παράδειγμα η προσπάθεια τρίτων να υποκλέψουν δεδομένα χρησιμοποιώντας την εφαρμογή του Facebook σε αυτή την περίπτωση, θα πρέπει να εμποδίζεται (FACEBOOK: A BREACH IN THE WALL. A TECHNOLOGICAL APPROACH TO THE FACEBOOK CAMBRIDGE ANALYTICA SCANDAL, 2018). Ο χρήστης εισέρχεται στον ιστό και έρχεται αντιμέτωπος με συστήματα τρίτων που επεξεργάζονται τους ίδιους κόμβους. Τα εξωτερικά συστήματα προσπαθούν να αποσπάσουν πληροφορίες για τον κάθε χρήστη. Η παραπάνω τεχνολογία θα πρέπει να εμποδίζει τα συστήματα τρίτων προστατεύοντας τους χρήστες της εφαρμογής που τη διαθέτουν.

Πώς όμως χρησιμοποιήθηκαν οι τεχνολογίες αυτές; Όταν βρίσκονται στο παρασκήνιο, σε μια εποχή που τα social media είναι τρόπος ζωής, κανείς δεν ενδιαφέρεται για τον τρόπο λειτουργίας τους, παρά μόνο για τη δυνατότητα χρήσης τους.

3.2 Τρόποι εκμετάλλευσης των τεχνολογιών

Βασιζόμενος στις παραπάνω τεχνολογίες, ο Kogan κατάφερε να δημιουργήσει την εφαρμογή προσωπικότητας στην οποία ο χρήστης θα είχε πρόσβαση μόνο χρησιμοποιώντας τον λογαριασμό που διαθέτει στο Facebook. Όταν οι χρήστες ενημερώθηκαν ότι το τεστ προσωπικότητας που θα ολοκλήρωναν θα βοηθούσε την ακαδημαϊκή έρευνα του Πανεπιστημίου του Cambridge, δεν δίστασαν να βοηθήσουν. Για να δελεαστούν οι χρήστες και να συμμετέχουν στο τεστ αυτό, η εφαρμογή θα πλήρωνε κάθε συμμετέχοντα λιγότερο από 5 δολάρια. Όταν λοιπόν κάποιος ξεκινούσε κάνοντας login μέσω Facebook, αυτόματα ο Kogan αποκτούσε πρόσβαση στα προσωπικά δεδομένα των χρηστών, συμπεριλαμβανομένων των γενεθλίων, των γεωγραφικών συντεταγμένων και κυρίως των «likes».

Όταν τελικά συλλέχθηκαν τα δεδομένα, η εταιρία του Kogan, συνδύασε τα αποτελέσματα του τεστ προσωπικότητας με τα δεδομένα που συλλέχθηκαν κρυφά από το προφίλ του εκάστοτε χρήστη προκειμένου να δημιουργηθεί ένα σχεδιάγραμμα ψυχολογίας για τον κάθε χρήστη. Το σχεδιάγραμμα αυτό, συσχετίστηκε με τις λίστες των εγγεγραμμένων ψηφοφόρων και παραδόθηκε στην Cambridge Analytica. Η Analytica, επεξεργάστηκε τα δεδομένα αυτά κυρίως κατά τη διάρκεια της προεκλογικής περιόδου του Trump (Aiswarya Ramachandran, 2018).



Εικόνα 3.1: Τρόπος συλλογής δεδομένων από το Facebook

Πώς ακριβώς όμως συλλέχθηκαν τα δεδομένα; Το Facebook, αποθηκεύει όλα τα στοιχεία και τις κινήσεις των χρηστών σε βάσεις δεδομένων. Οι πληροφορίες που αποθηκεύονται

αφορούν κυρίως σε φωτογραφίες που μοιράζονται οι χρήστες με τους φίλους τους, τα γκρουπ επικοινωνίας στα οποία βρίσκονται καθώς και τα προσωπικά μηνύματα. Εάν κάποιος χρήστης αποφασίσει να δημοσιεύσει κι άλλες πληροφορίες όπως τον προσωπικό του αριθμό τηλεφώνου, την προσωπική του διεύθυνση ή το ηλεκτρονικό του ταχυδρομείο, το Facebook δεν παραλείπει την αποθήκευση και αυτών των στοιχείων (Carole Cadwalladr and Emma Graham-Harrison, 2018).

Τα παραπάνω στοιχεία, αποτέλεσαν τη βασική πηγή του Kogan για την ολοκλήρωση των προφίλ των χρηστών και τελικά την παράδοση τους στην Analytica. Συγκεκριμένα ο Kogan εκμεταλλεύτηκε τα αποθηκευμένα στοιχεία από:

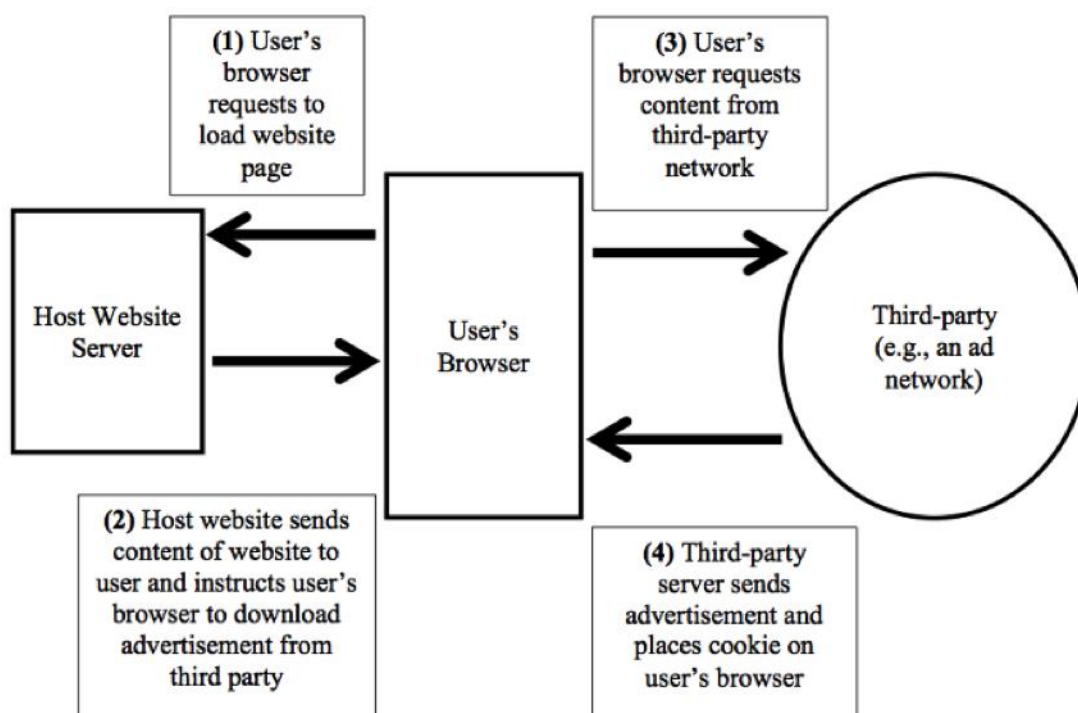
- Το κουμπί «Like». Το κουμπί αυτό, το χρησιμοποιούν οι χρήστες προκειμένου να μοιραστούν αυτόματα περιεχόμενο από σελίδες της εφαρμογής οι οποίες θα εμφανιστούν στους φίλους τους.
- Το κουμπί «Share». Επιτρέπει στους χρήστες να κοινοποιήσουν εσκεμμένα περιεχόμενο σελίδων στους φίλους τους.
- Το κουμπί αποστολής προσωπικών μηνυμάτων. Οι χρήστες κοινοποιούν περιεχόμενο σελίδων σε φίλους τους μέσω προσωπικών μηνυμάτων.
- Τη «Διαμορφωμένη κοινοποίηση». Οι χρήστες κοινοποιούν το επιθυμητό περιεχόμενο μόνο σε συγκεκριμένα άτομα.
- Το κουμπί «Follow». Επιτρέπει στους χρήστες να εγγραφούν σε άλλες δημόσιες ενημερώσεις.

Όλες οι κινήσεις των χρηστών έδωσαν στον Kogan το ακριβές προφίλ τους όταν εκείνοι ολοκλήρωσαν το τεστ και απέστειλαν τα αποτελέσματα. Το περιεχόμενο των δεδομένων αφορούσε σε ευαίσθητες πληροφορίες σχετικά με το σεξουαλικό προσανατολισμό, τη φυλή, το φύλο ακόμη και τη νοημοσύνη του εκάστοτε χρήστη (Hannah Ersdal, Sølvi Svendby Skjærstad, 2016).

Πώς όμως αποκρυπτογραφήθηκαν τα προφίλ αυτά; Είναι πολύ απλό. Έστω ότι σε έναν χρήστη αρέσει η Hello Kitty. Είναι άμεσα εμφανή η ευαισθησία του αλλά και η έλλειψη νευρικότητας. Έστω ότι κάποιος άλλος ακολουθεί τη Lady Gaga. Είναι αμέσως κατανοητή η εξωστρέφεια του αλλά και ίσως μία κρυμμένη εκκεντρικότητα. Ακολούθησαν λοιπόν οι ανάλογες διαφημίσεις που στόχευαν στα άτομα βάση του προφίλ τους. Αν κάποιος είχε αξιολογηθεί ως νευρωτικός για παράδειγμα, οι διαφημίσεις «φρόντιζαν» την απεικόνιση μιας εισβολής σε ένα σπίτι.

Μετά τη συλλογή όλων αυτών των πληροφοριών, η Cambridge Analytica κατάφερε να δημιουργήσει αλγορίθμους που θα μπορούσαν να προβλέψουν την πολιτική τοποθέτηση των χρηστών που δεν εγκατέστησαν την εφαρμογή του Kogan. Δημιούργησε λοιπόν διαφημίσεις πολιτικού περιεχομένου, καμπάνιες και απέστειλε μηνύματα σε κάθε χρήστη ανάλογα με τις προτιμήσεις του. Με τον τρόπο αυτό, κατηγοριοποιήθηκαν οι πολίτες των Ηνωμένων Πολιτειών της Αμερικής και ομαδοποιήθηκαν προκειμένου να τους κοινοποιούνται οι επιθυμητές πληροφορίες.

Οι διαφημίσεις που εμφανίστηκαν σε κάθε χρήστη προσαρμόστηκαν ουσιαστικά στο προφίλ του καθενός, την καταλληλότερη χρονική στιγμή. Πιο συγκεκριμένα, παρακάτω παρουσιάζεται ακριβώς ο τρόπος με τον οποίο εμφανίστηκαν διαφημίσεις και καμπάνιες μεθοδευμένα στους ψηφοφόρους.



Σχήμα 3.5: Τεχνολογία εμφάνισης στοχευμένων διαφημίσεων από τρίτα συστήματα

Πρώτο βήμα είναι το αίτημα του χρήστη σε ιστοσελίδα ή εφαρμογή της επιλογής του. Η εφαρμογή χρησιμοποιεί έναν SSP (Storage Service Provider) διακομιστή, προκειμένου να αποθηκεύσει τα δεδομένα του χρήστη ασφαλώς και γρήγορα. Στη συνέχεια, η εταιρία που παρέχει το Server, χρησιμοποιεί το εργαλείο «Ad Exchange», με σκοπό να διαφημιστεί και σε άλλες εφαρμογές ή ιστοσελίδες, ενώ παράλληλα το εργαλείο αυτό, βασίζεται στην

προηγούμενη συμπεριφορά των χρηστών μέσω cookies. Έτσι «φροντίζει» να εμφανιστεί το επιθυμητό περιεχόμενο στον εκάστοτε χρήστη. Τη δυνατότητα αυτή εκμεταλλεύτηκε η Cambridge Analytica, η οποία φρόντισε μετά τον προσδιορισμό των χρηστών, να εμφανίσει διαφημίσεις με στοχευμένο περιεχόμενο. Η πρόσβαση που είχε καταχωρηθεί μετά την ολοκλήρωση του τεστ, επέτρεψε στην Analytica και την αποστολή προσωπικών μηνυμάτων πολιτικού περιεχομένου (FACEBOOK: A BREACH IN THE WALL. A TECHNOLOGICAL APPROACH TO THE FACEBOOK CAMBRIDGE ANALYTICA SCANDAL, 2018).

Ως δεύτερο βήμα, ακολούθησε, η παρακολούθηση των κινήσεων των χρηστών και κατά πόσο δείχνουν ενδιαφέρον για το περιεχόμενο που τους εμφανίζεται, με βάση το ψυχολογικό τους προφίλ. Αν δεν υπήρχε ανταπόκριση, το περιεχόμενο άλλαζε μέχρις ότου παρουσιαστεί ένα σχετικά υψηλό ποσοστό εκδήλωσης ενδιαφέροντος.

Όλη αυτή η διαδικασία στοίχισε εκατομμύρια δολάρια, καθώς χρηματοδοτήθηκε μεγάλο κομμάτι του ιστού προκειμένου να εμφανίζονται οι απαιτούμενες διαφημίσεις. Ήταν τόσο εξειδικευμένο και λεπτομερές το περιεχόμενο που κοινοποιήθηκε, που ήταν σχεδόν αδύνατο να αποτύχει το σκοπό του. Οι διαφημίσεις κατανεμήθηκαν στον ιστό, βάσει γεωγραφικών περιοχών και σε πολύ κεντρικές ιστοσελίδες με έντονη και βασική επισκεψιμότητα. Ο ιστός είχε επηρεαστεί τόσο πολύ, που ανεξαρτήτως του λόγου που ο χρήστης ξεκινούσε μία σύνδεση, ερχόταν «αντιμέτωπος» με διαφημίσεις και fake news που τον οδηγούσαν μοιραία στην ανάγνωση τους. Οι κεντρικές σελίδες γέμιζαν, τα cookies έδιναν τροφή, ο πυρετός των εκλογών ήταν υψηλός και οι χρήστες είχαν ήδη μπει στην κούρσα της εκλογής του σημερινού προέδρου των Ηνωμένων Πολιτειών.

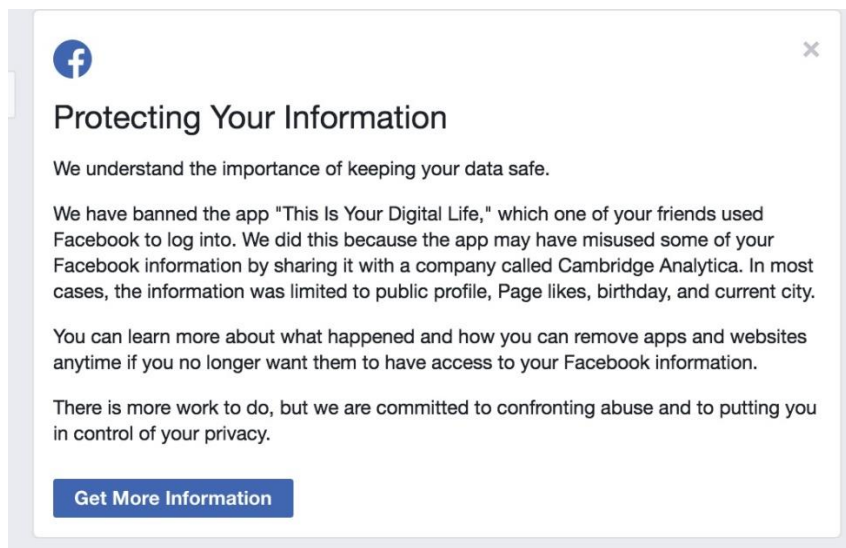
Είναι σαφές, ότι η προβλεψιμότητα ατομικών χαρακτηριστικών, με τη χρήση ψηφιακών αρχείων συμπεριφοράς, οδηγεί με μαθηματική ακρίβεια σε αρνητικές συνέπειες. Το αξιοσημείωτο, είναι ότι μπορούσε μέχρι πρότινος να εφαρμοστεί ο τρόπος αυτός υποκλοπής σε οποιονδήποτε χρήστη, χωρίς τη συγκατάθεση του.

3.3 Αποκάλυψη σκανδάλου

Το Δεκέμβριο του 2016 και καθώς η Carole Cadwalladr, μια δημοσιογράφος της εφημερίδας «The Guardian», μελετούσε τον τρόπο διεξαγωγής των προεδρικών εκλογών των Ηνωμένων Πολιτειών, ήρθε αντιμέτωπη με την εταιρία στατιστικών αναλύσεων Cambridge Analytica. Η εταιρία αυτή, παρά την ακαδημαϊκής της ταυτότητα κίνησε το ενδιαφέρον καθώς παρουσίασε ορισμένα μυστικοπαθή χαρακτηριστικά. Ο προβληματισμός της Carole, την οδήγησε σε μία μεγαλύτερη έρευνα σχετικά με την εταιρία αυτή, η οποία θα αποκάλυπτε το ρόλο του δισεκατομμυριούχου Robert Mercer στις εκλογές των ΗΠΑ. Ο συγκεκριμένος, ακολούθησε τη στρατηγική της χρηματοδότησης των διαφόρων μέσων κοινωνικής δικτύωσης για την ενίσχυση της πολιτικής καμπάνιας του Trump, συνδέοντας τον εν μέρει και με το Brexit (Carole Cadwalladr and Emma Graham-Harrison, 2018).

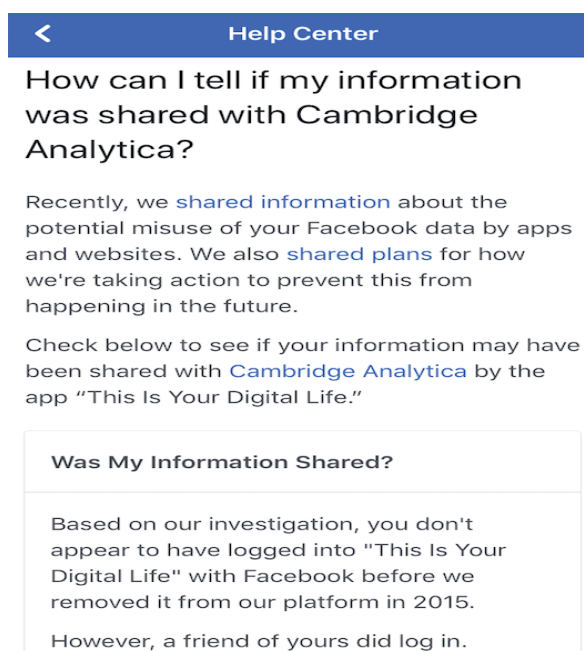
Όταν η δημοσιογράφος βρήκε τις πρώτες ενδείξεις ότι η Analytica μπορεί και να έχει χρησιμοποιήσει μεθόδους επεξεργασίας δεδομένων που παραβιάζουν τους νόμους περί προστασίας των προσωπικών δεδομένων, ξεκίνησε την έρευνα. Μετά την ολοκλήρωση του άρθρου της που τόνιζε εμμέσως τις υποψίες, η Εκλογική Επιτροπή της Βρετανίας ξεκίνησε πυρετώδεις έρευνες για τον τρόπο διεξαγωγής των αποτελεσμάτων του δημοψηφίσματος για το Brexit. Όταν η δημοσιογράφος ερευνούσε ορισμένες λεπτομέρειες σχετικά με τις συνέπειες του νόμου περί χρηματοδοτούμενων αποτελεσμάτων και χειραγώγησης, δεχόταν ανώνυμες ηλεκτρονικές επιθέσεις και επαγγελματικές επιθέσεις, ενισχύοντας τις υποψίες της. Η καμπάνια Leave.EU δημοσίευσε ένα βίντεο κατηγορώντας τη δημοσιογράφο, ενώ αρμόδιο τμήμα της πρεσβείας της Ρωσίας απέστειλε παράπονα στην εφημερίδα «Observer», στην οποία η εν λόγω δημοσιογράφος επρόκειτο να εργαστεί. Πιο συγκεκριμένα, η όλη έρευνα της δημοσιογράφου χαρακτηρίστηκε ως το καλύτερο παράδειγμα κακής δημοσιογραφίας και παραπληροφόρησης. Η επιμονή των άρθρων της όμως, έδωσε τη βεβαιότητα ότι η υπόθεση έχριζε μελέτης και έρευνας. Η έρευνα έφτασε σε μεγάλο επίπεδο και οι μάσκες άρχισαν σιγά σιγά να πέφτουν. Πολλοί πρώην εργαζόμενοι, ακαδημαϊκοί και δικηγόροι εξέφρασαν τη λύπη τους για την τακτική της δημοκρατίας που ακολούθησε και υποστήριξε η Cambridge Analytica στο βωμό του οικονομικού κέρδους.

Μετά την αποκάλυψη του σκανδάλου, το Facebook φρόντισε να ενημερώσει τόσο τους χρήστες που «έτρεξαν» την εφαρμογή, όσο και τους φίλους αυτών σχετικά με τον τρόπο προστασίας και ανάκτησης των προσωπικών τους δεδομένων.



Εικόνα 3.2: Ενημέρωση χρηστών για την απαγόρευση της εφαρμογής «ThisIsYourDigitalLife»

Όσοι χρήστες ενημερώθηκαν άμεσα για την απαγόρευση της εφαρμογής του Kogan, φρόντισαν να ενημερωθούν για την προστασία των δεδομένων τους. Υποστηρίχθηκε, ότι τα δεδομένα τα οποία συνέλεξε η εφαρμογή, ήταν κυρίως πληροφορίες σχετικά με τις δημόσιες, εν γνώσει του χρήστη, κοινοποιήσεις, τις σελίδες ενδιαφέροντος (Page likes), τα γενέθλια και την τοποθεσία. Στην πραγματικότητα ήταν πολλά παραπάνω. Εάν κάποιος χρήστης ήθελε να μάθει αν τα στοιχεία του ήταν ανάμεσα στα συγκεντρωμένα από την αντίστοιχη εφαρμογή, μπορούσε απλά να ανατρέξει στην αντίστοιχη ρύθμιση που του παρείχε το Facebook τη δεδομένη στιγμή.



Εικόνα 3.3: Μήνυμα ενημέρωσης υποκλοπής δεδομένων των χρηστών

Το μήνυμα που λάμβαναν ήταν αυτό που εμφανίζεται στην εικόνα 3.3, το οποίο τους ενημέρωνε ότι παρά το γεγονός ότι οι ίδιοι δεν είχαν χρησιμοποιήσει την εφαρμογή «This Is Your Digital Life», τα δεδομένα τους ίσως είχαν υποκλαπεί, αφού κάποιος φίλος την είχε χρησιμοποιήσει.

Όταν το σκάνδαλο βγήκε στην επιφάνεια, ένας από τους υπαλλήλους που δέχτηκε να μιλήσει ήταν ο Chris Wylie. Τόνισε ότι η Cambridge Analytica ήταν μία εξαιρετική εταιρία ψυχομετρικής ανάλυσης. Είχε τα εφόδια και σε συνεργασία με αρμόδιους καθηγητές, κατάφερε να δημιουργήσει τα προφίλ των χρηστών σε πολύ μικρό χρονικό διάστημα. Υποστήριξε, ότι προκειμένου να προβάλλουν και τον ακαδημαϊκό σκοπό της έρευνας, συνεργάστηκαν με τους καθηγητές, κυρίως όμως για κάλυψη.

3.4 Χειραγώγηση των χρηστών

Το σκάνδαλο της Cambridge Analytica, ήταν μία από τις πολλές περιπτώσεις της online καθοδήγησης και χειραγώγησης των χρηστών. Έγινε τόσο κατανοητή η ευκολία της εκμετάλλευσης των τεχνολογιών που μπορούν να ανακτήσουν πληροφορίες και προσωπικά δεδομένα, βάζοντας υποψίες στους χρήστες, χωρίς όμως οι ίδιοι να σταματούν ή να περιορίσουν την καθημερινή τους πλοήγηση στον ιστό. Το σκάνδαλο, παρουσιάζει το μεγάλο ποσοστό πιθανοτήτων χρήσης διαδικτυακών αλγορίθμων για την επεξεργασία δεδομένων με απώτερο σκοπό την πρόβλεψη και την επιρροή της συμπεριφοράς των χρηστών.

Η ευθύνη καταλογίζεται σε μεγάλο βαθμό και στους χρήστες. Έχει αποδειχθεί από έρευνες, ότι το μεγαλύτερο ποσοστό των χρηστών αποδέχεται τους όρους χρήσης (ToS – Terms of Service) και τις πολιτικές απορρήτου (PP – Privacy Policies) δίχως να διαβάσει και να μελετήσει σε τί δίνει τη συγκατάθεση του. Πολλοί αναλυτές, έχουν υποστηρίξει ότι ο σκοπός των όρων χρήσης είναι ο περιορισμός της εξαπάτησης και τις αλόγιστης εκμετάλλευσης των δεδομένων. Τονίζεται επίσης, ότι θα έπρεπε να παρέχονται οι πολιτικές απορρήτου ως γνώμονας ελέγχου των πληροφοριών που λαμβάνουν οι χρήστες και να δίνεται η ευκαιρία κατάργησης της συγκατάθεσης όπου κρίνεται απαραίτητο.

Όταν κάποιος ανοίξει τις πολιτικές απορρήτου που ακολουθεί το Facebook, λαμβάνει ουσιαστικά οδηγίες για τον τρόπο χρήσης και προώθησης των δεδομένων του. Οι οδηγίες είναι γραμμένες με τέτοιο τρόπο, που ο χρήστης αντιλαμβάνεται ότι πρέπει να είναι συνετός με τον

τρόπο και την άνεση κοινοποίησης των δεδομένων, αφήνοντας όμως μια αίσθηση απόλυτης ευθύνης σε περίπτωση άνομης χρήσης ή επεξεργασίας. Ως βασικό σκοπό χρήσης των δεδομένων, το Facebook, παρουσιάζει την ανάγκη βελτίωσης των προϊόντων και των υπηρεσιών που παρέχει, προκειμένου να καταστήσει την περιήγηση και την χρήση της εφαρμογής ως μια εύκολη και εύχρηστη διαδικασία. Παρ' όλ' αυτά, μετά το ξέσπασμα του σκανδάλου, αναφέρεται εντόνως στους όρους χρήσης, η προσπάθεια της ομάδας του Facebook, για περιορισμό της πρόσβασης των προγραμματιστών στα δεδομένα των χρηστών, για να αποτραπούν ενδεχόμενες καταχρήσεις αυτών των δεδομένων.

Κοινοποίηση σε τρίτους συνεργάτες

Η συνεργασία μας με τρίτους, οι οποίοι μας βοηθούν στην παροχή και βελτίωση των Προϊόντων μας ή χρησιμοποιούν τα Εργαλεία του Facebook Business για να αναπτύξουν τις επιχειρήσεις τους, μας δίνει τη δυνατότητα να διαχειριζόμαστε τις εταιρείες μας και να παρέχουμε δωρεάν υπηρεσίες σε πρόσωπα σε όλο τον κόσμο. Δεν πουλάμε και δε θα πουλήσουμε ποτέ σε κανέναν καμία από τις πληροφορίες σας. Επιβάλλουμε επίσης αυστηρούς περιορισμούς στον τρόπο με τον οποίο οι συνεργάτες μας μπορούν να χρησιμοποιούν και να κοινοποιούν τα δεδομένα που παρέχουμε. Παρακάτω ακολουθούν οι κατηγορίες των τρίτων συνεργατών στους οποίους κοινοποιούμε πληροφορίες:

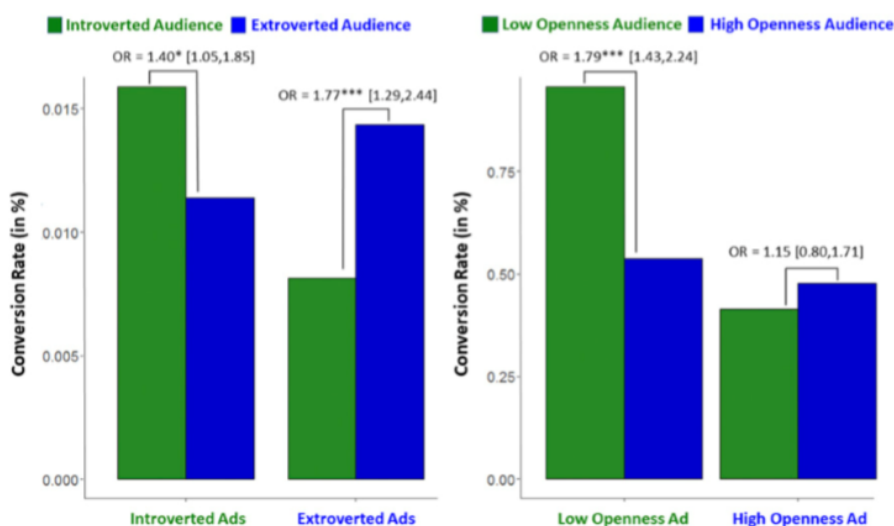
Εικόνα 3.4: Όροι και πολιτικές απορρήτου μετά την αποκάλυψη του σκανδάλου

Η παραπάνω εικόνα (3.4.), αποτελεί δείγμα των όρων και της πολιτικής απορρήτου που χρησιμοποιεί σήμερα το Facebook προκειμένου να προστατευθεί από τυχόν επαναλήψεις παρόμοιων καταχρήσεων των δεδομένων των χρηστών.

Με βάση τα παραπάνω, οι πολιτικές απορρήτου του Facebook φάνηκαν να ευνοούν στο παρασκήνιο την Cambridge Analytica καθώς φαίνεται να μη διευκρινίζει απόλυτα τους όρους περί κοινοποίησης πληροφοριών του προφίλ σε συστήματα τρίτων. Επιπλέον, επιτρέπονται έμμεσα διαδικτυακές δραστηριότητες που κατά κύριο λόγο επιδιώκουν τη μείωση του ορθολογισμού των χρηστών, είτε με τη μορφή διαφημίσεων, είτε μέσω fake news. Με τον τρόπο αυτό, όχι μόνο δεν μειώνεται η εξαπάτηση των χρηστών, αλλά ενισχύεται η προπαγάνδα και η παραπληροφόρηση. Θεωρητικά, θα έπρεπε οι μηχανισμοί του Facebook όπως οι πίνακες πρόσβασης δεδομένων να μπορούν να εντοπίζουν κινήσεις υποκλοπής από εξωτερικά συστήματα και να ανταποκρίνονται σε οποιοδήποτε απροσδόκητο γεγονός.

Από μία πιο γενική οπτική, μπορούμε να συμπεράνουμε ότι οι παραπάνω κινήσεις δεν έγιναν τυχαία. Η επιρροή χρηστών με βάση τα ψυχογραφικά τους χαρακτηριστικά, είναι ένας τρόπος κατεύθυνσης και χειραγώγησης του κοινού, που προήλθε από μακροχρόνιες έρευνες. Όλες κατέληξαν στο συμπέρασμα ότι τα ψυχογραφικά προφίλ μπορούν να διαμορφωθούν έπειτα από την παρατήρηση της ψηφιακής συμπεριφοράς. Με τη δημιουργία περιοχών συζήτησεων στον ιστό συχνά και επαναλαμβανόμενα, ένα μεγάλο ποσοστό των χρηστών επηρεάζεται και τείνει να καταλήγει και να συμφωνεί με τον δημιουργό της συζήτησης και την άποψη που αυτός πρεσβεύει. Το επίτευγμα αυτό είναι ισχυρό, αν κάποιος σκεφτεί ότι κατά κύριο λόγο ο σκοπός της επιρροής των χρηστών είναι για την ικανοποίηση συμφερόντων. Ωστόσο, είναι γεγονός ότι είναι αναμφίβολο κατά πόσο και σε ποιο βαθμό τα αποτελέσματα των ερευνών των εργαστηρίων μπορούν να γενικευθούν στην εφαρμογή της ψυχολογικής πειθούς στην πραγματική ζωή. Αυτό συμβαίνει καθώς το δείγμα των συμμετεχόντων που διεξήγαγαν τα ερωτηματολόγια για την έρευνα, ήταν σχετικά μικρό. Για το λόγο αυτό παρατηρήθηκε πιο έντονα η αντίδραση των χρηστών στον ιστό με απλές, καθημερινές και αυτόβουλες ενέργειες στο χώρο του διαδικτύου.

Η περίπτωση της Analytica και του Facebook δεν είναι η μόνη που εκμεταλλεύτηκε τις παραπάνω παρατηρήσεις. Σε δύο έρευνες εργαστηρίου για τον προσδιορισμό του ποσοστού των ατόμων που επηρεάζονται ψυχολογικά στον ιστό, μπορούμε να παρατηρήσουμε ότι τα νούμερα είναι σχετικά υψηλά.



Σχήμα 3.6: Επιρροή του κοινού με γνώμονα της εσωστρέφεια

Στο σχήμα 3.6 μπορούμε να παρατηρήσουμε την επιρροή του κοινού, έχοντας σαν γνώμονα την εσωστρέφεια. Με πράσινο παρατηρείται η επιρροή των εσωστρεφή ατόμων με παρωπιδική συμπεριφορά, σε ένα περιεχόμενο που τους αφορά ενώ με μπλε των εξωστρεφή. Όλα τα αποτελέσματα βασίσθηκαν στα «κλικ» των χρηστών, συμπεραίνοντας τη ψυχολογική συμπεριφορά, με αποτέλεσμα οι πολιτικές παρατάξεις με μεγάλες προσδοκίες να μπορούν να κάνουν τη δουλειά τους απλά και μόνο με μερικά εκατομμύρια.

Η ανάγκη χειραγώγησης των ψηφοφόρων με απώτερο σκοπό τη διεξαγωγή κατευθυνόμενων και προκαθορισμένων εκλογών, αλλά κυρίως αποφάσεων που έχουν σημαντική βαρύτητα, είναι μία διαχρονική διαδικασία. Αποτελεί μία ακόμη μορφή εκμετάλλευσης, αυτή τη φορά στον τομέα των πληροφοριών. Όλες οι μορφές εκμετάλλευσης της ανθρώπινης φύσης έχουν τον ίδιο σκοπό: την επιθυμία της επιβολής στη βούληση και στην κρίση προς όφελος τρίτων. Η ηλεκτρονική προπαγάνδα γίνεται πλέον με τέτοιο τρόπο που είναι ταυτόχρονα αποτελεσματική και απαρατήρητη (Susan T. Fiske, 2017).

ΚΕΦΑΛΑΙΟ 4

ΔΥΣΜΕΝΗΣ ΑΝΤΙΚΤΥΠΟΙ ΤΟΥ ΣΚΑΝΔΑΛΟΥ

Το σκάνδαλο της Cambridge Analytica συγκλόνισε την παγκόσμια κοινή γνώμη και προκάλεσε μεγάλο προβληματισμό σχετικά με την προστασία των προσωπικών δεδομένων. Η καθημερινή περιήγηση των χρηστών στον ιστό, αλλά κυρίως στο Facebook, θα έπρεπε από εδώ και πέρα να αποτελεί μία πλήρως συνειδητοποιημένη κίνηση από την πλευρά τους. Τίποτα δεν μπορούσε να θεωρηθεί ασφαλές, όταν ένας κολοσσός διαδικτυακής επικοινωνίας που υπόσχεται εχεμύθεια ανάμεσα στις ανταλλαγές ψηφιακών μηνυμάτων, κλονίζεται με ένα σκάνδαλο υψίστης σημασίας για την παγκόσμια πορεία και εξέλιξη.

Στο κεφάλαιο αυτό, θα αναλύσουμε τους δυσμενείς αντικτύπους του σκανδάλου, εξετάζοντας το ζήτημα από όλες τις πτυχές της κοινωνίας. Θα μελετήσουμε την κοινωνική αντίδραση, την επίδραση στην οικονομία, την πολιτική σκηνή μετά την αποκάλυψη, καθώς και τις τεχνολογικές κινήσεις που ακολούθησαν, τόσο για την αποφυγή επανάληψης παρόμοιου περιστατικού όσο και για την αποκατάσταση της διαδικτυακής προστασίας που τελικά δεν μπορούσε να θεωρηθεί δεδομένη.



4.1 Αντίκτυποι σε διάφορους τομείς της κοινωνίας

4.1.1 Κοινωνικός Αντίκτυπος

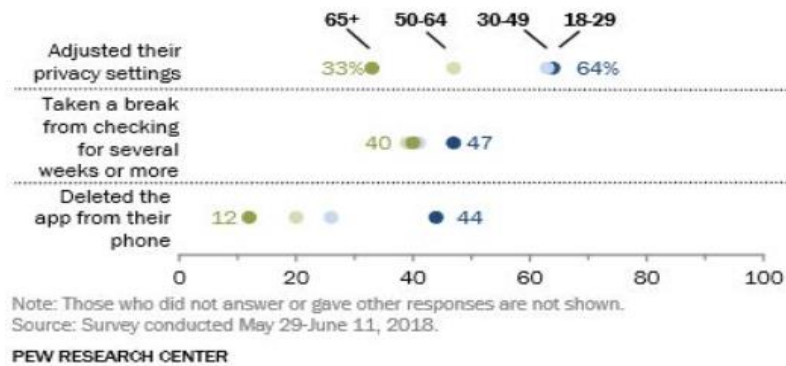
Η αρχική αντίδραση του κοινού ήταν η αναμενόμενη. Οργή, εκνευρισμός, απαξίωση και αμφισβήτηση των κοινωνικών μέσων και του ιστού γενικότερα, ακόμη και τάσεις για ονομαστικές μηνύσεις στην εταιρία του Mark Zuckerberg. Οι νομικές κινήσεις αποτελούσαν τη μοναδική σκέψη, έπειτα από το αίσθημα της προσβολής της κρίσης του κάθε χρήστη. Πολλά άτομα δεν μπορούσαν να δεχτούν ότι εξαπατήθηκαν και αποτέλεσαν βασικό κομμάτι της αλυσίδας της εκλογής του προέδρου των Ηνωμένων Πολιτειών. Η σκέψη ότι συνέστησαν τις μαριονέτες μίας ολόκληρης πολιτικής εκστρατείας έθιγε την υπόληψη και την αντίληψη τους. Πολλοί από αυτούς διέγραψαν την εφαρμογή από την κινητή τους συσκευή και κατάργησαν τον προσωπικό τους λογαριασμό, νομίζοντας ότι με τον τρόπο αυτό τα δεδομένα τους είναι πλέον ασφαλή. Τελικά, αποδείχθηκε ότι όλη αυτή η αντίδραση αποτελούσε το βασικότερο μέρος της οργής του κοινού κυρίως απέναντι στον ίδιο τους τον εαυτό, καθώς δεν διάβασαν τους όρους χρήσης και τις πολιτικές απορρήτου όταν τους δόθηκε η δυνατότητα. Έτσι «παγιδεύτηκαν» εν γνώση και εν αγνοία τους.

Μία πρώτη κοινωνική έρευνα, έδειξε ότι οι άνθρωποι νεότερης ηλικίας αντέδρασαν πιο έντονα από ότι μεγαλύτερα άτομα. Αυτό βασίστηκε στο γεγονός ότι τα νεότερα άτομα μπορούσαν να καταλάβουν με ευκολία τους αλγορίθμους συλλογής και επεξεργασίας δεδομένων. Σύμφωνα με την έρευνα που πραγματοποίησε η Pew Research Center, μετά την αποκάλυψη του σκανδάλου, οι κινήσεις των χρηστών ήταν οι εξής: είτε αναδιαμόρφωναν τις ρυθμίσεις της συσκευής και των εφαρμογών που περιείχε περί της πρόσβασης στη συσκευή και της προστασίας και επεξεργασίας των δεδομένων, είτε αποστασιοποιήθηκαν κάποιο διάστημα από τα social media και τον ιστό, είτε διέγραψαν εντελώς τις όποιες εφαρμογές κοινωνικής δικτύωσης.

Τελικά, το 54% των χρηστών άλλαξε τις ρυθμίσεις περί απορρήτου, το 42% απείχε από τα social media για ένα μεγάλο χρονικό διάστημα ενώ το 26% διέγραψε όλες τις εφαρμογές κοινωνικής δικτύωσης από τις συσκευές τους. Τα παραπάνω ποσοστά παρατηρήθηκαν σε νεαρές ηλικίες συγκριτικά με μεγαλύτερα άτομα. Πιο συγκεκριμένα, το 44% των ατόμων που ηλικιακά κυμαίνονται από τα 18 έως τα 29 έτη, διέγραψαν την εφαρμογή ενώ μία τέτοια κίνηση παρατηρήθηκε από το ποσοστό της τάξεως του 14% των ατόμων που ηλικιακά κυμαίνονται από την ηλικία των 65 και άνω.

Younger Facebook users much more likely than older users to have recently adjusted their privacy settings, deleted Facebook app from their phone

% of U.S. adults who use Facebook, in each age group, who say they have done the following in the last 12 months ...

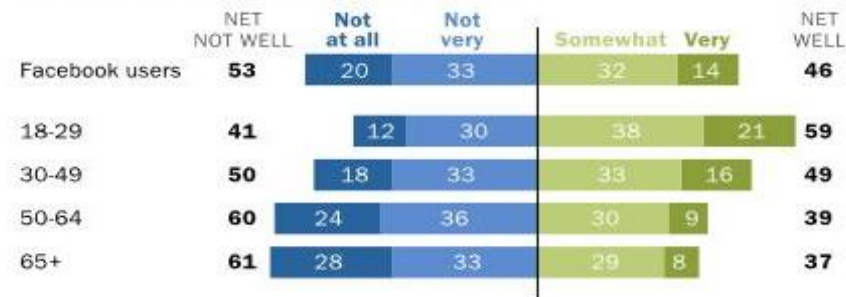


Σχήμα 4.1: Αντίδραση των χρηστών με γνώμονα την ηλικία

Στο σχήμα 4.1, βλέπουμε τις τρεις παραπάνω περιπτώσεις με βάση τα αποτελέσματα της έρευνας Pew Research Center για τους διάφορους χρήστες του Facebook.

Majority of older Facebook users do not understand why certain posts are included in their news feed

% of Facebook users who say they understand ___ well why certain posts are included in their news feed and others are not



Σχήμα 4.2: Ηλικιακό ποσοστό ατόμων που γνωρίζουν το λόγο ύπαρξης διαφημίσεων

Στο σχήμα 4.2, παρατηρούμε ότι οι χρήστες του Facebook μεγαλύτερης ηλικίας δεν καταλαβαίνουν το λόγο και τον τρόπο με τον οποίο εμφανίζονταν διαφημίσεις με στοχευμένο περιεχόμενο στο προφίλ τους.

Από την άλλη, οι ιδιοκτήτες μεγάλων εταιριών θορυβήθηκαν στον ελάχιστο βαθμό μετά το ξέσπασμα του σκανδάλου. Οι ιδιοκτήτες έδειξαν ότι δεν ενδιαφέρονται για τη «διαρροή» των

δεδομένων, καθώς το Facebook αποτελεί την τελευταία πλατφόρμα στην οποία θα βασίζονταν προκειμένου να προωθήσουν τα προϊόντα τους. Παρά το γεγονός ότι μετά την αποκάλυψη του σκανδάλου, πολλοί χρήστες διέγραψαν σελίδες και σταμάτησαν να «ακολουθούν» τις διάφορες επιχειρήσεις που εκμεταλλεύονταν το Facebook, η απήχηση τους στον κόσμο δεν επηρεάστηκε σχεδόν καθόλου. Αυτό συνέβη για τους εξής λόγους:

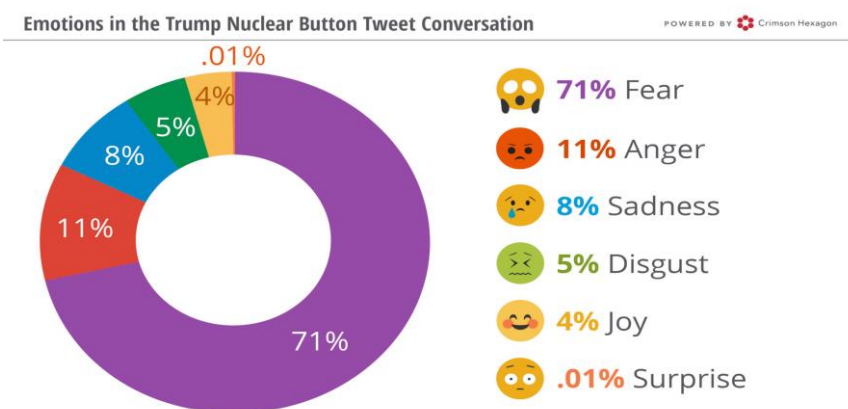
- **Η κοινοποίηση του περιεχομένου των επιχειρήσεων είναι αποκλειστικά για ενίσχυση της προώθησης των προϊόντων και μόνο.** Δίνεται η ευκαιρία δωρεάν προώθησης των προϊόντων και των υπηρεσιών της κάθε επιχείρησης μέσω Facebook, ως μια εναλλακτική μορφή διαφήμισης. Δεν κοινοποιείται ουσιαστικά κάποιο προσωπικό δεδομένο των «ακολουθών» τους, ενώ δεν υπάρχει συμμετοχή σε έρευνες και σε παιχνίδια της εφαρμογής, καθώς ο ρόλος του προφίλ είναι διαφορετικός.
- **Παρά το μέγεθος του σκανδάλου της Cambridge Analytica, οι χρήστες δυσκολεύτηκαν σε μεγάλο βαθμό να εγκαταλείψουν το Facebook.** Πολλοί χρήστες αποφάσισαν να διαγράψουν το προφίλ τους, με αρχική σκέψη να «τιμωρήσουν» έτσι τον κολοσσό των social media. Η σκέψη αυτή έπεσε στο κενό, ενώ ακόμη και να ολοκληρωνόταν, δεν θα αποτελούσε καν ποσοστό με βαρύτητα μπροστά στα 2 δις χρηστών. Ακόμη και μετά την απομάκρυνση ορισμένων χρηστών, η διαφήμιση μιας εταιρίας είχε ήδη ολοκληρώσει το σκοπό της γνωριμίας μαζί τους.

Αρκετά ήταν τα άτομα που υποστήριζαν ότι η αποκάλυψη του σκανδάλου ήταν απλώς ένα από τα χιλιάδες υποκινούμενα. Τόνισαν επίσης, ότι οι αναλυτές της Cambridge Analytica εκμεταλλεύτηκαν, προς όφελος της εταιρίας στην οποία δούλευαν και με τον καλύτερο δυνατό τρόπο τα δεδομένα που δίνουμε καθημερινά απλόχερα και δωρεάν. Άτομα κυρίως νεαρής ηλικίας, υπογράμμισαν ότι είναι αδύνατον σε μια εποχή που το ίντερνετ έχει εδραιωθεί στην καθημερινότητα μας, να μην υπάρχει η υποψία περί συλλογής και επεξεργασίας των προσωπικών δεδομένων. Διαπιστώθηκε λοιπόν, ότι ίσως οι χρήστες θα έπρεπε να είναι παραπάνω προσεκτικοί και να διαβάζουν πιο συγκεντρωμένα τους όρους χρήσης και τις πολιτικές απορρήτου πριν πατήσουν το κουμπί της αποδοχής. Καμία εταιρία δεν θα διατηρήσει τόσο ασφαλή τα δεδομένα των χρηστών της όταν δεν επωφελείται οικονομικά με κάποιον τρόπο από αυτούς (David Cohen, 2018). Αντίθετα, η κοινοποίηση ορισμένων πληροφοριών ή ακόμη πιο εύκολα η «ανοιχτή πόρτα» σε συστήματα τρίτων, υπόσχεται εύκολα και γρήγορα δισεκατομμύρια στους λογαριασμούς των στελεχών. Είναι θέμα «επιβίωσης».

Η εύκολη λύση μετά το ξέσπασμα του σκανδάλου, ήταν η κατηγορία του Facebook για τη διάδοση των πληροφοριών προσωπικού χαρακτήρα των χρηστών. Όταν όμως ο Zuckerberg,

απευθύνθηκε στο Κογκρέσο, φρόντισε να αποδείξει ότι σε καμία βάση δεδομένων και σε κανένα σημείο του συστήματος δεν παρατηρήθηκε υποκλοπή ή παραβίαση. Κάτι τέτοιο λοιπόν, σε συνδυασμό με την προθυμία του δημιουργού του Facebook να διορθώσει τυχόν λάθη, άλλαξε άμεσα και εμφανώς την κοινή γνώμη. Ο Zuckerberg φρόντισε να διαχειριστεί τόσο καλά το ζήτημα, δείχνοντας μεταμέλεια, που γρήγορα ο κόσμος ξέχασε την οργή απέναντί του και στράφηκε στο αποτέλεσμα της «διαρροής» των δεδομένων.

Μετά την εκλογή του σημερινού προέδρου των Ηνωμένων Πολιτειών, οι αντιδράσεις του κόσμου ήταν ποικίλες. Το μεγαλύτερο ποσοστό του πληθυσμού των Ηνωμένων Πολιτειών, δεν μπορούσε να δεχτεί ότι οι συμπολίτες τους δεν βολιδοσκόπησαν σωστά την κατάσταση. Εξέλεξαν για πρόεδρο έναν άνθρωπο με οπισθοδρομικές, για την εποχή, αντιλήψεις προκαλώντας απογοήτευση. Η αποκάλυψη του σκανδάλου άλλαξε τα δεδομένα. Το αίσθημα οργής ήταν πλέον ξεκάθαρο. Ένας άνθρωπος που πλήρωσε προκειμένου να εξαπατηθεί μία ολόκληρη κοινωνία για να αισθανθεί την άνεση της «καρέκλας» ήταν ικανός για τα πάντα. Χαρακτηριστικά ήταν τα μηνύματα στο Twitter, που υποστήριζαν ότι μετά την προεδρία μίας γυναίκας και ενός έγχρωμου προέδρου, η Αμερική ξεπέρασε τον εαυτό της και έπρεπε να επιστρέψει στον παρωπιδισμό της.



Σχήμα 4.3: Αντιδράσεις μετά την εκλογή του Trump στο Twitter

Ο κόσμος δεν ήξερε πώς να αντιδράσει και πού να αποδώσει τις ευθύνες. Η πλειοψηφία γνώριζε ότι η εκλογή ενός τέτοιου ατόμου θα μπορούσε να χαρακτηριστεί καταστροφική. Η Cambridge Analytica βρέθηκε στο επίκεντρο των συζητήσεων, αλλά δεν δέχθηκε την επίθεση που δέχθηκε το Facebook. Θεωρήθηκε το μοναδικό υπαίτιο για την πρόσβαση του Kogan στα δεδομένα των ψηφοφόρων και μισήθηκε από πολλούς γι' αυτό.

Αποτέλεσμα των παραπάνω, ήταν η ανάγκη καθησυχασμού των πελατών, διάφορων εταιρικών κολοσσών από τους αρμόδιους. Το σκάνδαλο προκάλεσε παγκόσμια ταραχή και οι

εταιρίες ανά τον κόσμο, θέλησαν να διαβεβαιώσουν τους πελάτες τους για την ασφάλεια των προσωπικών τους δεδομένων. Εάν έχαναν την εμπιστοσύνη, οι επιπτώσεις θα ήταν τεράστιες. Ο Samir Desai, διοικητικό στέλεχος της Funding Circle, υπογραμμίζει χαρακτηριστικά ότι υπάρχει κάτι σχετικά με τη χρήση των προσωπικών δεδομένων των χρηστών που απασχολεί περισσότερο τον κόσμο από τη διαφάνεια και τη σαφήνεια. Αυτό είναι το διεθνώς κατοχυρωμένο δικαίωμα των χρηστών να γνωρίζουν και να συναινούν στον τρόπο χρήσης των προσωπικών τους πληροφοριών.

Η κοινή γνώμη άρχισε να κατευνάζεται μετά το ψήφισμα και την εδραίωση του Γενικού Κανονισμού για την Προστασία Δεδομένων. Ο κανονισμός αυτός διασφαλίζει τη χρήση των προσωπικών δεδομένων με ασφάλεια, ειλικρίνεια, διαφάνεια και σαφήνεια, καθιστώντας τη δυνατότητα αυτή ως μία μη διαπραγματευόμενη διαδικασία.

4.1.2 Οικονομικός Αντίκτυπος

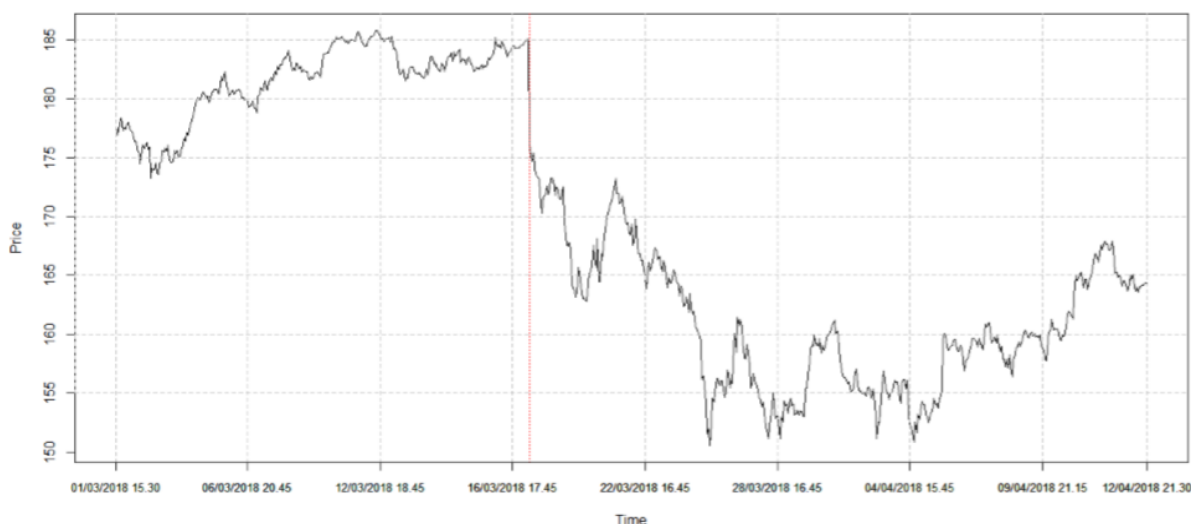
Για πολλούς μήνες, μετά την αποκάλυψη του σκανδάλου, οι υπάλληλοι της Cambridge Analytica περίμεναν μία κίνηση πολλά υποσχόμενη για τη διάσωση της εταιρίας. Ο μεγαλύτερος φόβος ήταν οι μαζικές απολύσεις καθώς πολυάριθμοι υπάλληλοι θα έμεναν άνεργοι.

Η παρατεταμένη ελπίδα διατήρησης της εταιρίας, έπεσε στο κενό, όταν μία μέρα του Μαΐου η Cambridge Analytica κήρυξε πτώχευση παρά τις προσπάθειες εβδομάδων να αφήσει πίσω το αμφιλεγόμενο παρελθόν της. Η Analytica, ήταν ήδη έτοιμη να συγχωνευτεί με μία νέα εταιρία με την επωνυμία Emerdata, μιας και υπήρξε η φήμη ότι ο CEO της Analytica, Alexander Nix εξαγόραζε υπαλλήλους σεξουαλικής απασχόλησης, με σκοπό να παγιδεύσει πολιτικούς αντιπάλους των πελατών της Cambridge Analytica. Οι υπάλληλοι που κοινοποίησαν τις κινήσεις του Nix, φρόντισαν να διατηρήσουν την ανωνυμία τους, καθώς υπήρχε ο φόβος της ανεργίας έπειτα από αυτό.

Στις 2 Μαΐου και χωρίς προειδοποίηση ο υπάλληλος της Cambridge Analytica, Julian Wheatland, ανακοίνωσε σε περίπου 40 στελέχη της εταιρίας στα γραφεία της Νέας Υόρκης, ότι η μητρική εταιρία SCL δεν υπήρχε πια. Η Analytica κήρυξε πτώχευση την ίδια ακριβώς στιγμή, ενώ οι υπάλληλοι και των δύο εταιριών θα έπρεπε να έχουν αδειάσει τα γραφεία τους μέχρι τις 12:30 εκείνο το μεσημέρι. Το meeting των στελεχών για την ενημέρωση σχετικά με την πορεία της εταιρίας είχε αναβληθεί ήδη δώδεκα φορές και εκείνη η μέρα έμελλε να είναι

η μοιραία. Όταν τα στελέχη συγκεντρώθηκαν, ενημερώθηκαν μόνο για την απόφαση της πτώχευσης ενώ για οποιαδήποτε απορία θα έπρεπε να απευθυνθούν στο διευθυντή του ανθρωπίνου δυναμικού.

Σε μία γενικότερη εικόνα, οι οικονομικές επιπτώσεις του σκανδάλου είχε πτυχές κυρίως στην πλευρά της Analytica και του Facebook, ενώ όχι τόσο σε επιχειρήσεις που εκμεταλλεύονταν την δωρεάν διαφήμιση. Ένα μεγάλο κομμάτι της παγκόσμιας οικονομίας βασίζεται σε ηλεκτρονικές ανταλλαγές υπηρεσιών τύπου B2B (Business to Business). Οι επιχειρήσεις λοιπόν που φρόντιζαν να προωθήσουν τις υπηρεσίες και τα προϊόντα τους μέσω Facebook, δεν φάνηκε να αντιμετωπίζουν κάποια οικονομική επίπτωση λόγω του σκανδάλου. Μάλιστα, η οποιαδήποτε οικονομική μετάπτωση, φάνηκε να βασίζεται σε λόγους καθαρά ανεξάρτητους του σκανδάλου. Μελετώντας λοιπόν την κύρια εταιρία που μπορούμε να πούμε ότι υπέστη τη μεγαλύτερη ζημιά, καταλήγουμε στο παρακάτω διάγραμμα που παρουσιάζει την πτώση της τιμής της μετοχής του Facebook σε διάφορα χρονικά διαστήματα.



Σχήμα 4.4: Πτώση της τιμής της μετοχής του Facebook μετά την αποκάλυψη του σκανδάλου

Η αποκάλυψη της υπόθεσης της Cambridge Analytica, βγήκε στην επιφάνεια στις 16 Μαρτίου 2018 και ώρα 3:13 μ.μ.. Στο σχήμα φαίνεται ξεκάθαρα η κατάρρευση των μετοχών μέσα σε διάστημα λίγων ωρών. Παράλληλα, παρατηρήθηκε μία διαφοροποίηση στον καταγεγραμμένο τρόπο χρήσης του Facebook, γεγονός που επηρέασε και ορισμένες εταιρίες. Η διαφοροποίηση αυτή, μπορεί να επηρεάσει τις χρηματοοικονομικές επενδύσεις των εταιριών που βασίζονται στο Facebook. Η πτώση της τιμής αυτής, στοίχισε 70 δισεκατομμύρια σε διάστημα 11 ημερών, ενώ μόνο ο δημιουργός του Facebook, στον οποίο ανήκει το 28,2% της

εταιρίας, έχασε το ποσό των 20 δισεκατομμυρίων. Σε διάστημα μίας νύχτας το Facebook έχασε περίπου 35 δισεκατομμύρια δολάρια.



Σχήμα 4.5: Πτώση των εκατομμυρίων του Facebook σε διάστημα 11 ημερών

Την Πέμπτη 26 Ιουλίου, το Facebook είδε την τιμή της μετοχής του να πέφτει κατακόρυφα. Η «συντριβή» αυτή, είναι αποτέλεσμα της κατάρρευσης των εν λόγω μετοχών στο χρηματιστήριο της Νέας Υόρκης, κατά 18%. Το αποτέλεσμα αυτό προήλθε μετά την είδηση της απεργάφης τριών εκατομμυρίων χρηστών, μόνο στην Ευρώπη, μετά την αποκάλυψη των γεγονότων που «καίνε» την Analytica. Οι επενδυτές είχαν ήδη ενημερωθεί για την επικείμενη πτώση, καθώς μια τέτοιου είδους αντίδραση των χρηστών ήταν η αναμενόμενη. Ο CFO του Facebook, David Wehner, δήλωσε ότι η εταιρία θα ακολουθήσει τους νέους κανονισμούς του Γενικού Κανονισμού Προστασίας των Προσωπικών Δεδομένων, δίνοντας περισσότερες δυνατότητες στους χρήστες στην επιλογή και τον τρόπο διαχείρισης και διάθεσης των προσωπικών τους δεδομένων.

Μετά την απολογία του Mark Zuckerberg στο Κογκρέσο, η μετοχή του Facebook αυξήθηκε στις αρχές του Απριλίου. Ακολούθησε μία πτώση της τιμής που παρέμεινε σταθερή για ορισμένες μέρες, ενώ μετά αυξήθηκε ραγδαία.



Σχήμα 4.6: Σχεδιάγραμμα τιμής της μετοχής πριν και μετά την απολογία του Mark Zuckerberg

Παρά το γεγονός ότι πολλοί χρήστες διέγραφαν τους λογαριασμούς τους, οι επενδυτές των οποίων οι διαφημίσεις προωθούνταν μέσω Facebook γοητεύτηκαν από την απολογία του Zuckerberg. Αποτέλεσμα αυτού, ήταν τα θετικά αποτελέσματα κέρδους που άρχισαν να ανεβάζουν την τιμή της μετοχής.

Το σκάνδαλο δεν περιορίστηκε μόνο στα νούμερα που επέφερε η πτώση της μετοχής του Facebook. Ο οικονομικός τομέας ήρθε αντιμέτωπος με διάφορα και έντονα ερωτήματα περί ασφάλειας προσωπικών δεδομένων. Πιο συγκεκριμένα, η βιομηχανία των τραπεζών «κάθισε» στο ειδώλιο, μιας και οι καταθέτες φοβήθηκαν για τα δεδομένα των λογαριασμών τους. Η βασική απήγηση του σκανδάλου αφορούσε στο Open Banking. Το Open Banking αποτελεί μία online υπηρεσία που επιτρέπει στους πελάτες των τραπεζών να έχουν πρόσβαση στα δεδομένα των λογαριασμών τους μέσω ιστού. Επιπλέον, δίνει τη δυνατότητα επένδυσης σε νέα προϊόντα και υπηρεσίες με σκοπό την ενίσχυση των μικροεπιχειρηματιών προτείνοντας βασικούς τρόπους.

Οι τράπεζες ήρθαν αντιμέτωπες με το Γενικό Κανονισμό για την Προστασία Δεδομένων και ελέγχθηκε εξονυχιστικά ο τρόπος χρήσης των δεδομένων των πελατών τους. Πολλοί ήταν αυτοί που απέσυραν τις καταθέσεις τους και προτίμησαν να διαχειρίζονται οι ίδιοι τα χρήματά τους, με αποτέλεσμα τη μείωση εκατομμυρίων από τις τράπεζες. Ο κόσμος αρνήθηκε έντονα τη διαχείριση των χρημάτων του μέσω του ιστού, μιας και υποστηρίχθηκε ότι το 63% δεν γνώριζε τα δικαιώματά του σχετικά με την επεξεργασία και διαχείριση των δεδομένων τους

από αρμόδιους ή και τρίτους. Τα καλά νέα για τις τράπεζες είναι ότι σε μία γενικότερη εικόνα, βρίσκονται σε μία ισχυρή θέση ως αξιόπιστος κάτοχος προσωπικών δεδομένων. Στην εποχή της ψηφιακής χρηματοδότησης και παρά την ένταση του σκανδάλου, μπορούν να αποτελέσουν τους πραγματικούς ηγέτες στις επερχόμενες εποχές δίνοντας στους πελάτες μεγαλύτερη προβολή, επιλογή και έλεγχο των προσωπικών τους δεδομένων.

4.1.3 Πολιτικός Αντίκτυπος

Όταν η αλήθεια αποκαλύφθηκε, οι κυβερνήσεις έπρεπε να λάβουν απαντήσεις, μιας και υποστήριξαν άγνοια περί του θέματος, ενώ η δικαιοσύνη έπρεπε να αναλάβει άμεση δράση. Η Cambridge Analytica σύντομα θα δήλωνε πτώχευση, επομένως δεν θα ήταν αυτή που θα καθόταν στο ειδώλιο. Αντίθετα, ο δημιουργός του Facebook, Mark Zuckerberg, ήταν ο μόνος που ήρθε αντιμέτωπος με τις βαριές κατηγορίες περί παραβίασης ανθρωπίνων, προσωπικών και απορρήτων πνευματικών δικαιωμάτων.

Το κογκρέσο υποστήριξε ότι η εταιρία του Zuckerberg δεν έκανε ό,τι ήταν απαραίτητο για να αποτρέψει την υποκλοπή αυτή, παρά το γεγονός της παρουσίασης της ως ιδεολογικής και φερέγγυας. Στην γραπτή απολογία του, ο Zuckerberg, τόνισε το εξής:

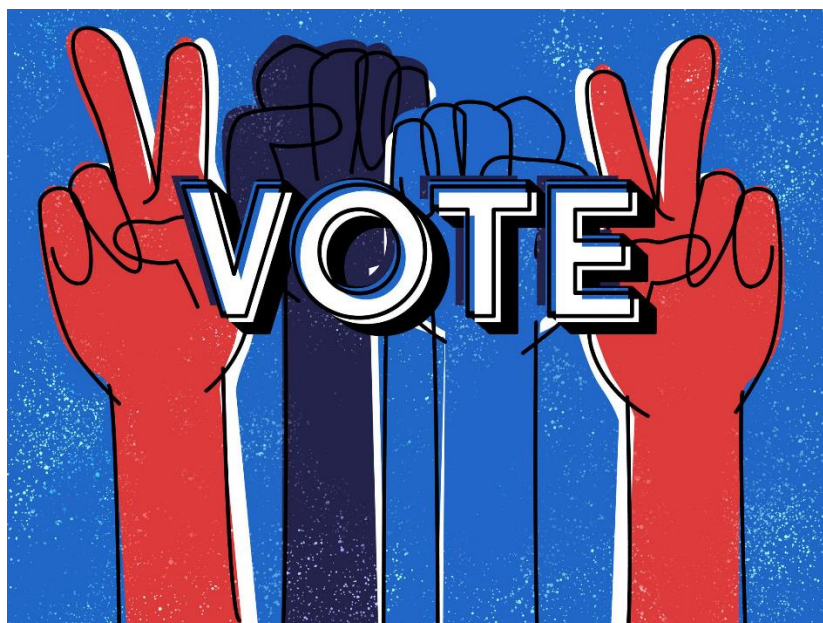
«Το Facebook αποτελεί μία εταιρία με σημαντικό ιδεολογικό χαρακτήρα. Για χρόνια, επικεντρώνεται στα πλεονεκτήματα που προέρχονται από την ανθρώπινη επικοινωνία και αλληλεπίδραση μέσω του ιστού. Όσο η οικογένεια της εταιρίας αυτής μεγάλωνε ανά τον κόσμο, ο κόσμος αποκτούσε ένα σημαντικό εργαλείο επικοινωνίας με τους ανθρώπους που αγαπά, είχε τη δυνατότητα της έκφρασης λόγου χωρίς λογοκρισία, ενώ εκμεταλλεόταν το εργαλείο αυτό για την προώθηση των επιχειρήσεών του. Περίπου 70 εκατομμύρια μικρές επιχειρήσεις κατάφεραν να αναπτυχθούν μέσω του Facebook και να θεωρούνται σήμερα επιχειρηματικοί κολοσσοί.

Παρ' όλ' αυτά, είναι ξεκάθαρο ότι η επιχείρηση δεν έκανε τις απαραίτητες ενέργειες προκειμένου να αποτρέψει την εκμετάλλευση των εργαλείων αυτών για κακό σκοπό. Η πρόταση αυτή αναφέρεται σε όλα τα fake news, τις κατευθυνόμενες εκλογές και την παραβίαση των κανόνων περί πνευματικών δικαιωμάτων. Δεν έγινε κατανοητό, στον υπέρτατο βαθμό, το επίπεδο ευθύνης που φέρει η εταιρία. Αυτό αποτέλεσε το μεγαλύτερο λάθος που μπορούσε να

γίνει και είναι δικό μου. Εγώ δημιούργησα το Facebook, εγώ το συντήρησα και εγώ είμαι ο μόνος υπεύθυνος.»

Επιπλέον, εξήγησε ακριβώς τί έγινε με την Cambridge Analytica. Τόνισε ότι τα δεδομένα μοιράστηκαν μέσω του Πανεπιστημίου του Cambridge, από το quiz των προσωπικοτήτων. Το Facebook δεν είχε καμία ιδέα για την ανταλλαγή των δεδομένων. Οι δημοσιογράφοι ήταν αυτοί που αποκάλυψαν το σκάνδαλο και ενημέρωσαν ότι ο Kogan ήταν αυτός που κοινοποίησε τα δεδομένα που συνέλεξε από την εφαρμογή με την Analytica. Η κίνηση αυτή είναι αντίθετη με τις πολιτικές της εταιρίας του Facebook. Δεν υποστηρίζεται η δημοσιοποίηση δεδομένων χωρίς τη συγκατάθεση των χρηστών, κάτι το οποίο οδήγησε στην άμεση κατηγοριοποίηση του Kogan και της Cambridge Analytica, ενώ υπογραμμίστηκε ότι τα δεδομένα διαγράφηκαν, κάτι το οποίο τελικά δεν επιβεβαιώθηκε. Το Facebook σταμάτησε να παρέχει τις υπηρεσίες του στο Πανεπιστήμιο του Cambridge, όπως και στην ίδια την Analytica.

Όταν η Cambridge Analytica ήρθε αντιμέτωπη με το κογκρέσο, υποστήριξε ότι ουδέποτε χρησιμοποίησε τα δεδομένα από το Facebook ή οποιοδήποτε άλλο προσωπικό δεδομένο για την διαμόρφωση αποτελεσμάτων ή την επιρροή των εκλογών στις Ηνωμένες Πολιτείες της Αμερικής. Ουδέποτε η εκλογή του προέδρου Trump δεν προέκυψε από τις ενέργειες της εταιρίας, ενώ τα αποτελέσματα που δημοσιεύθηκαν έδειχναν μόνο τις τάσεις περί ψηφοφορίας των χρηστών. Στη συζήτηση τοποθετήθηκε η επιτροπος αρμόδια για θέματα Δικαιοσύνης Καταναλωτών και Ισότητας των Φύλων, η οποία σημείωσε ότι η υπόθεση Facebook-Cambridge Analytica αποτέλεσε αφύπνιση για τη διεθνή κοινότητα και ότι ο ψηφιακός κόσμος μπορεί να πλανηθεί και να γίνει κατάχρηση και κακόβουλη χρήση των προσωπικών δεδομένων. Έκανε λόγο για την ασφάλεια του κυβερνοχώρου που σε συνδυασμό με την παραπληροφόρηση αποτελεί σοβαρό εμπόδιο για τις ελεύθερες και δημοκρατικές εκλογές. Υποστήριξε επίσης, ότι πρέπει να ληφθούν διάφορα μέτρα μιας και οι εκλογικές περίοδοι στον ιστό είναι ιδιαίτερος επιρρεπείς σε παραπληροφόρηση και χειραγώγηση από ιδιωτικά και ξένα συμφέροντα. Οι ευρωεκλογές είναι εκτεθειμένες στην απειλή αυτή. Στη συζήτηση μετείχε ο επιτροπος για την Ένωση Ασφαλείας, ο οποίος αναφέρθηκε στις δράσεις και τα μέτρα που έχει λάβει η Επιτροπή, όπως τα μέτρα για την ενίσχυση της ανθεκτικότητας από τις κλασικές απειλές στον κυβερνοχώρο.



Το Ευρωκοινοβούλιο, μετά την πολιτική τοποθέτηση των χωρών, ξεκίνησε να αναζητά και να μελετά κι άλλες παρόμοιες περιπτώσεις όπως αυτή της Cambridge Analytica. Δεν έμεινε ικανοποιημένο από τον Mark Zuckerberg και από τις ορισμένες τροποποιήσεις στις ρυθμίσεις απορρήτου του Facebook. Έγινε λοιπόν γνωστό ότι δεν ήταν μια μεμονωμένη περίπτωση, καθώς έγιναν γνωστές και νέες παραβιάσεις δεδομένων. Επιβεβαιώθηκε λοιπόν, ότι οι νέοι κανόνες της Ευρωπαϊκής Ένωσης συνιστούν αναγκαιότητα και επισημάνθηκε και στο σχέδιο ψηφίσματος του Ευρωκοινοβουλίου. Η επιτροπή του Ευρωκοινοβουλίου, ζήτησε την επεξήγηση και την κατανόηση των αλγορίθμων που χρησιμοποιούνται σε τέτοιου είδους εφαρμογές στον ιστό, ενώ τόνισε ότι η Ευρώπη είναι καλύτερα από ποτέ εξοπλισμένη με τα εργαλεία που παρέχουν οι νέοι νόμοι που προτάθηκαν. Υπογραμμίστηκε ότι υπάρχει τακτική επαφή με τον πρόεδρο του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων και τον πρόεδρο της Αρχής Προστασίας Δεδομένων του Ηνωμένου Βασιλείου, ο οποίος είναι και ο επικεφαλής της έρευνας για το Facebook και την Cambridge Analytica.

Η συνάντηση του Ευρωκοινοβουλίου με τον δημιουργό του Facebook πραγματοποιήθηκε κεκλεισμένων των θυρών σε συνεδρίαση της συνδιάσκεψης των προέδρων, την οποία θα παρακολουθήσουν και οι επικεφαλής ευρωπαϊκών πολιτικών ομάδων. Δεν ήταν όμως λίγες οι αντιδράσεις ορισμένων αρχηγών ευρωπαϊκών πολιτικών παρατάξεων που δήλωσαν ότι δεν θέλουν να παρακολουθήσουν τη συνάντηση με τον δημιουργό του Facebook, αν αυτή τελικά πραγματοποιούνταν πίσω από κλειστές πόρτες. Θεώρησαν ότι η ακρόαση θα έπρεπε να γίνει δημοσία. Κάτι τέτοια θα ήταν η αρχή της διαφάνειας. Δεν έλλειψαν οι πολιτικές και κομματικές διαμάχες μεταξύ των συμμετεχόντων στο Ευρωκοινοβούλιο, αφού το κεντροδεξιό ευρωπαϊκό

Λαϊκό Κόμμα και η ακροδεξιά κατηγορήθηκαν ότι θέλουν να κρατήσουν τη συνάντηση κλειστή. Πηγές όμως μέσα από το κοινοβούλιο, σύμφωνα με την εφημερίδα Guardian, δήλωσαν ότι αν η συνάντηση μεταδιδόταν σε όλο τον κόσμο, δεν υπήρχε πιθανότητα ο Zuckerberg να αποδεχθεί την πρόκληση. Στη δήλωση αυτή πάτησε και η Βρετανική βουλή, η οποία ήθελε να «ανακρίνει» τον Zuckerberg και εξέλαβε την απόρριψη του αιτήματος της επίσκεψης του ως «σνομπάρισμα». Σε ψήφισμα του, το Ευρωπαϊκό Κοινοβούλιο, παρότρυνε το Facebook να επιτρέψει σε φορείς της Ευρωπαϊκής Ένωσης να διενεργήσουν πλήρη έλεγχο, για την αξιολόγηση της προστασίας και της ασφάλειας των προσωπικών δεδομένων των χρηστών. Οι ευρωβουλευτές υπογράμμισαν ότι δεν παραβιάστηκε μόνο η εμπιστοσύνη των πολιτών της Ευρωπαϊκής Ένωσης, αλλά παραβιάστηκε και το Ευρωπαϊκό Δίκαιο. Τονίστηκαν οι επικείμενες αλλαγές στην πλατφόρμα του Facebook, καθώς και η συμμόρφωση με τη νομοθεσία της Ευρώπης για την προστασία προσωπικών δεδομένων.

Μια γενικότερα εικόνα, είναι ότι οι αντιπρόσωποι των χωρών συμφώνησαν ότι η υπόθεση αποτέλεσε σοκ στον πυρήνα του δημοκρατικού πολιτεύματος και συστήματος. Τόνισαν ότι οι κανονισμοί και οι εκλογικές διεκπεραιώσεις υπάρχουν πριν ακόμη την είσοδο του ψηφιακού κόσμου στην καθημερινότητα μας. Τα χρηματικά όρια των προεκλογικών εκστρατειών, οι αυστηροί κανόνες για τον τρόπο διεξαγωγής των πολιτικών διαφημίσεων, η διαφάνεια των πολιτικών με χρηματοδότες των προεκλογικών εκστρατειών, η περίοδος αδράνειας, ο ρόλος των μέσων ενημέρωσης στην παραπληροφόρηση και όλοι οι κανόνες που αφορούν στα συμβατικά μέσα μαζικής ενημέρωσης πρέπει και θα επιβληθούν και στο διαδίκτυο. Οι επόμενες Ευρωεκλογές, και όχι μόνο, δεν θα είναι η συνήθης διαδικασία, ενώ υποστηρίχθηκε ότι το εθνικό δίκτυο εκλογών θα είναι πλέον σε θέση να αντιμετωπίζει γρήγορα πιθανές απειλές και να επιβάλλει ταχέως τους υφιστάμενους κανόνες και οικονομικές κυρώσεις.

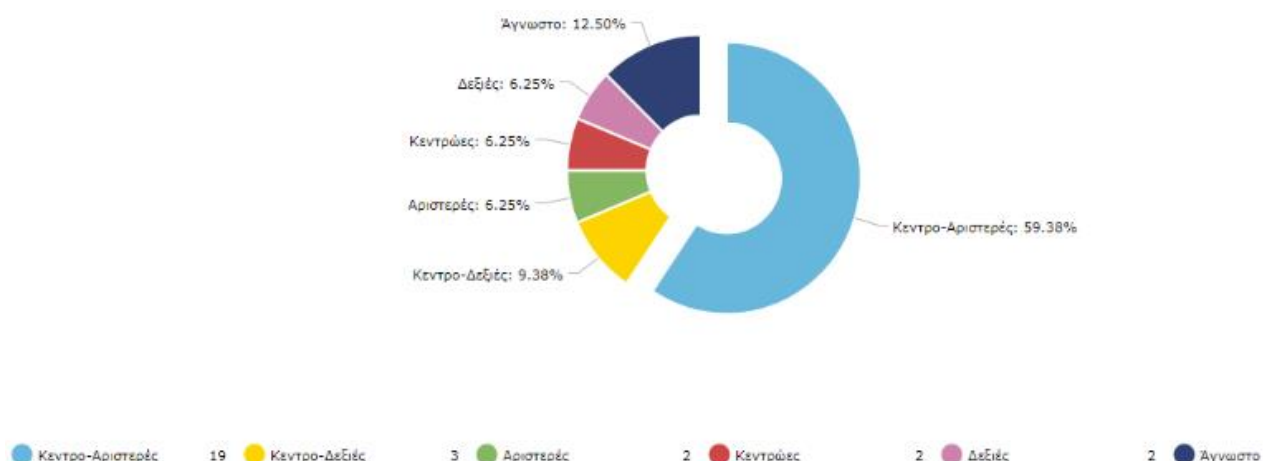
Προκειμένου να αποφευχθεί ανάμειξη σε εκλογές από τα μέσα κοινωνικής δικτύωσης, το Ευρωπαϊκό Κοινοβούλιο πρότεινε τα εξής:

- Τη διευκόλυνση της αναγνώρισης των πολιτικών διαφημιστικών μηνυμάτων στο διαδίκτυο και τις οργανώσεις που κρύβονται πίσω από αυτές.
- Την απαγόρευση της κατάρτισης προφίλ για εκλογικούς σκοπούς, συμπεριλαμβανομένης και της κατάρτισης προφίλ βάσει συμπεριφοράς στο διαδίκτυο που ενδέχεται να αποκαλύπτει πολιτικές προτιμήσεις.
- Την άμεση επισήμανση του περιεχομένου που μπορεί να διανέμεται από ρομπότ στα μέσα κοινωνικής δικτύωσης, καθώς και την επιτάχυνση της διαδικασίας της απομάκρυνσης ψεύτικων λογαριασμών.

- Τη συνεργασία με ανεξάρτητους φορείς εξακρίβωσης γεγονότων («fact crackers»), καθώς και με την ακαδημαϊκή κοινότητα για την αντιμετώπιση της παραπληροφόρησης.
- Οι έρευνες θα πρέπει να διεξάγονται από τα κράτη μέλη με την υποστήριξη της Eurojust, σε περιπτώσεις υποτιθέμενης κατάχρησης του διαδικτυακού πολιτικού χώρου από ξένες δυνάμεις.

Ζητήθηκε λοιπόν, από την Ευρωπαϊκή Επιτροπή και τις εθνικές κυβερνήσεις να ενεργήσουν για την προστασία των εκλογών και να θεσπίσουν ισχυρότερους νόμους για την προστασία της ιδιωτικής ζωής. Οι περισσότερες εταιρίες με παρόμοια περιστατικά, προσπάθησαν να διορθώσουν τα λάθη τους και να στηρίξουν την προσπάθεια να καταστούν οι εκλογές πιο δίκαιες και διαφανείς. Διαφάνεια θα πρέπει να υπάρχει και γύρω από τους αλγορίθμους επεξεργασίας των δεδομένων, ενώ οι χρήστες θα πρέπει να ανακαλύπτουν ευκολότερα περιεχόμενα, να έχουν πρόσβαση σε εναλλακτικές πηγές πληροφόρησης και να μπορούν να αναφέρουν και να τονίζουν την παραπληροφόρηση. Οι δημοκρατικοί θεσμοί και οι δημοκρατικές διαδικασίες πρέπει να προστατευτούν περισσότερο με το ψήφισμα του σχεδίου του Ευρωκοινοβουλίου.

Όταν το θέμα της Analytica πήρε μεγάλες διαστάσεις, ξεκίνησαν έρευνες σχετικά με την αντίδραση του κόσμου για το συγκεκριμένο ζήτημα, λαμβάνοντας υπόψιν το συναισθηματικό βαρόμετρο του θέματος. Σκοπός των ερευνών ήταν η προσέγγιση και η πρόβλεψη της αντίδρασης των πολιτών σχετικά με την πολιτική ηγεσία και τον κλονισμό της εμπιστοσύνης σε αυτή.



Σχήμα 4.7: Ποσοστά αντίδρασης των πολιτών με βάση τις πολιτικές τους αντιλήψεις

Με βάση το παραπάνω διάγραμμα, το μεγαλύτερο ποσοστό αντίρρησης και αμφισβήτησης της πολιτικής ηγεσίας προκύπτει από πηγές φιλικά προσκείμενες σε μια κεντροαριστερή αντίληψη των ειδήσεων. Η βασική παρατήρηση του παραπάνω διαγράμματος, είναι πως η εμβάθυνση και κάλυψη του θέματος ωφελεί απόψεις που είναι αντίθετα προσκείμενες επί της έως εκείνη τη στιγμή πολιτικής ηγεσίας.

4.1.4 Τεχνολογικός Αντίκτυπος

Μετά το σκάνδαλο, η επιστήμη της τεχνολογίας ήταν αυτή που θα ερχόταν αντιμέτωπη με τη μεγαλύτερη αντίδραση του κοινού. Ήταν αναμενόμενο να αναζητηθούν οι υπεύθυνοι για τον κλονισμό ορισμένων ηθικών αξιών του ευρύτερου κοινωνικού περιβάλλοντος. Οι κινήσεις της Cambridge Analytica μπορεί να μην αποτέλεσαν κάτι πρωτότυπο και ανήκουστο για τα δεδομένα του σημερινού κόσμου, όμως ήταν αυτές που τάραξαν τα νερά στον μεγαλύτερο ως τώρα δυνατό βαθμό.

Η AI (Artificial Intelligence) τεχνολογία, αποτελεί τον πυλώνα των καθημερινών συναλλαγών και κινήσεων μέσω ίντερνετ. Χρησιμοποιεί τεχνικές όπως την εκπαίδευση των μηχανών προκειμένου να ενισχύσει την οικονομία, τα μέσα κοινωνικής δικτύωσης καθώς και να αναπτύξει τα ανθρώπινα δικαιώματα. Τα συστήματα που χρησιμοποιούν την τεχνολογία αυτή, βασίζονται σε στατιστικές τεχνικές που μπορούν αυτόματα να αυθεντικοποιήσουν τα δοθέντα δεδομένα. Χρησιμοποιούνται κατά περιόδους εκλογικών αναμετρήσεων για να προϊδεάσουν και να ενημερώσουν τους ψηφοφόρους σχετικά με τις επικείμενες εξελίξεις. Ταυτόχρονα όμως, η AI τεχνολογία μπορεί να καταχραστεί και να χρησιμοποιηθεί για μη προβλέψιμες και εσκεμμένα βλαβερές ενέργειες. Μετά την αποκάλυψη της κατάχρησης αυτής, η τεχνολογία αυτή αμφισβητήθηκε και ο κόσμος αντιδρούσε σε καθετί συνδύαζε τα προσωπικά δεδομένα με online συναλλαγές και κινήσεις. Ο κόσμος άρχισε να αμφισβητεί ότι είναι ασφαλής και πολλές συναλλαγές, κυρίως τραπεζικές, γίνονταν με τον παραδοσιακό τρόπο. Ήταν εύκολο να κατηγορηθεί η AI τεχνολογία για το σκάνδαλο αυτό, παρά το γεγονός ότι η τεχνολογία αυτή είναι αντικειμενικά αξιόπιστη. Οι αλγόριθμοι όμως που χρησιμοποιήθηκαν για την παραποίηση, την παραπληροφόρηση και τη σύγχυση των πολιτών ήταν τελικά αυτοί που έβλαψαν ουσιαστικά τη δημοκρατία. Η ευρύτερη κοινή γνώμη κατέληγε στα εξής:

- Η τεχνολογία ΑΙ θα έπρεπε να αναπτύσσεται και να χρησιμοποιείται για το κοινό καλό και προς όφελος της ανθρωπότητας.
- Θα πρέπει να βασίζεται στις αρχές της διαφάνειας και της δικαιοσύνης.
- Δεν θα πρέπει να χρησιμοποιείται για την παραποίηση των προσωπικών δεδομένων του ατόμου ή της οικογένειας αυτού ή ακόμη και της ίδιας της κοινωνίας.
- Η αυτόνομη δυνατότητα της βλάβης, της καταστροφής ή της αμφισβήτησης του ανθρώπου δεν πρέπει να χρησιμοποιείται στην τεχνολογία αυτή.
- Όλοι οι πολίτες θα πρέπει να έχουν το δικαίωμα να εκπαιδεύονται προκειμένου να αποφεύγεται η συναισθηματική και οικονομική εκμετάλλευση που μπορεί να επιδιώκεται από τρίτους μέσω της τεχνολογίας αυτής.

Ήταν πλέον ξεκάθαρο ότι η τεχνολογία αυτή μπορούσε να χρησιμοποιηθεί ξανά, αυτή τη φορά για την ενίσχυση της φωνής του κοινού και την καταγγελία περιστατικών παραπληροφόρησης ή προσπάθειας επιρροής. Η χρήση των τεχνικών της τεχνολογίας αυτής σε πολιτικές καμπάνιες δεν θα εξαλειφθεί. Είναι όμως εφικτό να χρησιμοποιηθεί ηθικά και σωστά, προκειμένου να διασφαλιστεί η διαφάνεια και η ενίσχυση της δημοκρατίας.

Λίγες εβδομάδες πριν το ξέσπασμα του σκανδάλου της Analytica, ο δημιουργός του ιστού Tim Berners-Lee, τόνισε σε μία ομιλία του την ανάγκη της προβλεψιμότητας των κινδύνων που ελλοχεύονται για την αποφυγή της επιστράτευσης των τεχνολογιών για παράνομους σκοπούς. Πιο συγκεκριμένα, υποστήριξε ότι τα τελευταία χρόνια, είναι πολλές οι θεωρίες συνωμοσίας που αμφισβητούν τις πλατφόρμες των μέσων κοινωνικής δικτύωσης. Πολλοί λογαριασμοί σε Facebook και Twitter υποκλέπτουν τις κοινωνικές αντιδράσεις, χειραγωγούν και κατευθύνουν τους χρήστες για τη διεκπεραίωση εκλογών, ενώ χρησιμοποιούν παράνομα τα προσωπικά δεδομένα των χρηστών. Υπογράμμισε ότι οι νομοθέτες οφείλουν να μελετούν τις υπάρχουσες πλατφόρμες για να προβλέψουν και να προστατεύσουν όπου αυτό είναι εφικτό, μιας και εκεί βρίσκονται όλες οι απαντήσεις.

Δεν ήταν όμως μόνο η ΑΙ που υπέστη την αμφισβήτηση της εγκυρότητάς της. Τα Big Data ήρθαν επίσης αντιμέτωπα με την κοινή γνώμη. Όταν ο κόσμος ξεκίνησε να εμπιστεύεται την διαδικασία συλλογής και αποθήκευσης δεδομένων μέσω διαδικτύου, συμφωνούσε με την προϋπόθεση της υπόσχεσης στο χρήστη, ότι τα δεδομένα που θα συλλέγονται ουδέποτε θα μπορούν να φωτογραφίσουν πρόσωπα. Δεν θα γινόταν ταυτοποίηση του χρήστη του οποίου τα δεδομένα συλλέχθηκαν, μιας και δεν ήταν ουσιαστικά αυτός ο σκοπός. Με την ανάλυση των Big Data, οι εταιρίες κατάφεραν να συλλέξουν δεδομένα, με σκοπό την αναζήτηση και τη

δημιουργία νέων ευκαιριών. Η τεχνολογία αυτή, κατάφερε να μειώσει το κόστος αποθήκευσης δεδομένων και της αναζήτησης πληροφοριών όταν αυτό ήταν απαραίτητο, ενώ οι αποφάσεις ήταν γρηγορότερες αφού οι πληροφορίες μπορούσαν να αναλυθούν αμέσως.

Η υπόσχεση δεν τηρήθηκε ποτέ. Όχι μόνο οι βάσεις δεδομένων διατηρούν στοιχεία και πληροφορίες για οποιονδήποτε, αλλά οι πληροφορίες είναι τόσο ξεκάθαρες που η ταυτοποίηση του ατόμου είναι θέμα δευτερολέπτων. Ο κόσμος λοιπόν αντέδρασε, φοβούμενος ότι μετά το σκάνδαλο τα προσωπικά δεδομένα θα μπορούσαν να χρησιμοποιηθούν και για άλλες κατευθυνόμενες ενέργειες σε βάρος της ανθρώπινης φύσης.

4.2 Εφαρμογή Γενικού Κανονισμού Προστασίας Δεδομένων σε τομείς της κοινωνίας

Στα τέλη Μαΐου του 2018, τέθηκε σε ισχύ το πιο εκτεταμένο καθεστώς προστασίας δεδομένων και προστασίας της ιδιωτικής ζωής που παρατηρήθηκε ποτέ. Παρά το γεγονός ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) είναι ένας ευρωπαϊκός νόμος, θα έχει παγκόσμιο αντίκτυπο. Είναι πιθανό και αναμενόμενο να υπάρχουν κάποιες απρόβλεπτες συνέπειες, τόσο στον τεχνολογικό και πολιτικό κόσμο, όσο και στην κοινωνική ανταπόκριση και τα οικονομικά επακόλουθα.



Κάθε εταιρία που έχει έναν ευρωπαϊκό πελάτη, ανεξάρτητα από την έδρα της, είναι υποχρεωμένη να υπακούει στο Γενικό Κανονισμό Προστασίας Δεδομένων. Εάν μία εταιρία

διαθέτει ιστότοπο που δίνει τη δυνατότητα συναλλαγής με τη χρήση ευρωπαϊκών νομισμάτων ή διαθέτει πληροφορίες σε ευρωπαϊκή γλώσσα, μπορεί να θεωρηθεί ότι προσφέρει αγαθά και υπηρεσίες σε πολίτη της Ευρώπης και ως αποτέλεσμα οφείλει να ακολουθεί τον παραπάνω κανονισμό.

Μετά την αποκάλυψη του σκανδάλου, η θεσμοθέτηση του κανονισμού ήταν άκρως απαραίτητη. Ο GDPR αποτελεί αποτέλεσμα της άμεσης κινητοποίησης και δραστηριοποίησης των αρμόδιων φορέων, προκειμένου να αποκατασταθεί να διορθωθεί ο τρόπος χρήσης του ιστού στην καθημερινότητα. Η απόρριψη του Internet μετά την Cambridge Analytica, θα είχε τρομερές επιπτώσεις σε πολλούς τομείς, με τον οικονομικό να κατέχει τον πρωταγωνιστικό ρόλο, μιας και τα ποσά που θα χάνονταν από τις καθημερινές συναλλαγές θα ήταν αστρονομικά. Η θέσπιση του κανονισμού θα επιφέρει συνέπειες με άκρως σημαντικό χαρακτήρα, σε παγκόσμια κλίμακα λόγω της εμβέλειας του. Στο κεφάλαιο αυτό, θα παρουσιαστούν συμπερασματικά τα αναμενόμενα αποτελέσματα της τήρησης του κανονισμού, στους τομείς που παρουσιάστηκαν στο κεφάλαιο 4 και υπέστησαν πλήγμα λόγω του σκανδάλου. Είναι γνωστό ότι έγιναν πολλές τροποποιήσεις στις πολιτικές και στις ταυτότητες υπηρεσιών, ενώ πλέον η στοχοποίηση και η ανάλυση του κοινού με βάση τις επιλογές και τα χαρακτηριστικά τους δεν θα αποτελεί εύκολη υπόθεση.

4.2.1 Οικονομικός Τομέας

Οποιαδήποτε μη συμμόρφωση μιας εταιρίας ή οργανισμού ή ακόμη και χώρας με το GDPR, θα μπορούσε να οδηγήσει σε πρόστιμα ύψους 20 εκατομμυρίων ευρώ ή 4% της παγκόσμιας οικονομίας (που αφορά σε συναλλαγές), με γνώμονα το μεγαλύτερο. Για οποιονδήποτε οικονομικό κολοσσό, το οικονομικό πλήγμα θα μπορούσε να ανέλθει σε δισεκατομμύρια δολάρια. Σύμφωνα με μία πρώτη έρευνα της Consult Hyperion, ειδικό σε ηλεκτρονικές χρηματοοικονομικές συναλλαγές, προβλέπεται ότι τα ευρωπαϊκά χρηματοπιστωτικά ιδρύματα θα αντιμετωπίσουν πρόστιμα συνολικού ύψους 4,7 δισεκατομμυρίων ευρώ, τα τρία πρώτα χρόνια μετά την έναρξη ισχύος του GDPR. Ο Anthony Lee, συνεργάτης και δικηγόρος μίας από τις μεγαλύτερες εταιρίες τηλεπικοινωνιών στο Λονδίνο δήλωσε ότι επιβλήθηκε πρόστιμο ύψους 400.000 λιρών για την αποτυχία αποφυγής παραβίασης των προσωπικών δεδομένων των πελατών της το 2015, όμως σύμφωνα με το νέο καθεστώς τα πρόστιμα θα μπορούσαν να είναι πολλαπλάσια.

Στην περίπτωση που μία επιχείρηση ή ένας οργανισμός δεν μπορεί να αποδείξει ότι η καλή προστασία των δεδομένων αποτελεί τον ακρογωνιαίο λίθο της επιχειρηματικής πολιτικής, υπάρχει μεγάλο ενδεχόμενο έκθεσης σε μέτρα επιβολής που μπορούν να βλάψουν τόσο τη δημόσια φήμη όσο και το τραπεζικό ισοζύγιο. Τα προηγούμενα χρόνια, κάθε επιχείρηση ήταν σε θέση να υιοθετήσει το δικό της πρωτόκολλο σε περίπτωση παραβίασης των δεδομένων. Τώρα, ο GDPR ορίζει ότι οι υπεύθυνοι προστασίας δεδομένων είναι υποχρεωμένοι να αναφέρουν τυχόν παραβίαση προσωπικών δεδομένων εντός 72 ωρών. Η κοινοποίηση της παραβίασης πρέπει να περιλαμβάνει λεπτομέρειες σχετικά με τη φύση και τον τρόπο παραβίασης, καθώς και τον κατά προσέγγιση αριθμό των προσώπων που επηρεάζονται. Η κοινοποίηση της παραβίασης και το στάδιο αποκατάστασης πρέπει να αποστέλλονται στον επηρεασμένο πελάτη χωρίς την παραμικρή καθυστέρηση. Η ευθύνη σε περίπτωση παραβίασης είναι σημαντική και οι οικονομικές κυρώσεις καθορίζονται με γνώμονα τα παραπάνω οικονομικά κριτήρια.

Σύμφωνα με το CNN, το κόστος συμμόρφωσης με το νέο κανονισμό έχει ήδη αναγκάσει επιχειρήσεις να περιορίσουν την χωρική τους εμβέλεια ή ακόμη και να κλείσουν εξ ολοκλήρου. Η Ευρωπαϊκή Ένωση είναι η δεύτερη μεγαλύτερη οικονομία στον κόσμο, μία οικονομία στην οποία οι επιχειρήσεις με ψηφιακή παρουσία δεν μπορούν παρά να αλληλοεπιδρούν. Το GDPR έχει σαρωτικές απαιτήσεις. Πολλές αμερικάνικες εταιρίες έχουν επιβαρυνθεί εκατομμύρια προκειμένου να συμμορφωθούν, ενώ σε ορισμένες περιπτώσεις αυτό δεν ήταν αρκετό για να αποφευχθεί η κατάθεση αγωγών.

Μεγάλο ανασχηματισμό και επανεξέταση θα υποστούν οι πολιτικές των τραπεζών ανά τον κόσμο. Η αποδοχή του κανονισμού ήταν αναμενόμενη, ωστόσο το έργο των τραπεζών θα είναι δύσκολο τα επόμενα χρόνια, καθώς οι πελάτες θα έχουν τη δυνατότητα να έχουν απόλυτη πρόσβαση στα δεδομένα τους και δυνατότητα απόσυρσης αυτών.

4.2.2 Τεχνολογικός Τομέας

Η εφαρμογή του κανονισμού αναμένεται να έχει σημαντικό αντίκτυπο στις τεχνολογικές πλατφόρμες και στις αρχιτεκτονικές που συλλέγουν δεδομένα, τα αποθηκεύουν και τα διαχειρίζονται. Σε πολλές από αυτές τις περιπτώσεις, θα χρειαστεί ο ανασχεδιασμός υφιστάμενων συστημάτων ή πλατφορμών προκειμένου να αποφευχθεί ο κίνδυνος της μη συμμόρφωσης ενός οργανισμού ή μιας εταιρίας στον κανονισμό.

Οι αναδυόμενες τεχνολογίες, όπως η τεχνητή νοημοσύνη και το cloud computing αποτελούν αποτελεσματικό μέσο ενίσχυσης των επιδόσεων και της παραγωγικότητας ενός οργανισμού. Η ανάπτυξη των τεχνολογιών αυτών είναι καθοριστικής σημασίας για την ενίσχυση της οικονομίας και έχουν καταστεί ένας από τους ισχυρότερους ανταγωνιστικούς παράγοντες μεταξύ των χωρών. Το αξιοσημείωτο είναι ότι οι τεχνολογίες αυτές αποδίδουν σωστά και αποτελεσματικά μέσω αλγορίθμων υψηλής ποιότητας. Οι αυστηρότεροι κανονισμοί όμως σχετικά με τη συλλογή, την ανάλυση και την μεταποίηση δεδομένων ενδέχεται να παρεμποδίσουν την ανάπτυξη και τη χρήση νέων τεχνολογιών και αναπόφευκτα να αυξήσουν το κόστος υλοποίησης των τεχνολογιών αυτών.

Η ανάπτυξη της τεχνητής νοημοσύνης (AI) θα επηρεαστεί μελλοντικά, μιας και ο Γενικός Κανονισμός Προστασίας Δεδομένων θα αυξήσει το κόστος και θα περιορίσει το πεδίο εφαρμογής. Τα άρθρα 13 και 22 του GDPR, απαιτούν την επανεξέταση και εξήγηση ορισμένων αλγορίθμων που χρησιμοποιούνται. Οι περιορισμοί αυτοί θα αυξήσουν σημαντικά το κόστος εργασίας, ενώ θα σπάσουν την εγγενή ισορροπία μεταξύ ακρίβειας και διαφάνειας. Το άρθρο 17 παρέχει στο χρήστη τη δυνατότητα υπαναχώρησης και διαγραφής των προσωπικών του δεδομένων, όταν αυτό απαιτείται, χωρίς αδικαιολόγητη καθυστέρηση, γεγονός που μπορεί να καταστρέψει τους βασικούς κανόνες που υποστηρίζουν ένα σύστημα AI. Το αποτέλεσμα που θα επέλθει, είναι η μείωση της αποτελεσματικότητας και της ακρίβειας των αλγορίθμων.



Στο cloud computing, ο GDPR δημιουργεί υποχρεώσεις και στους παρόχους υπηρεσιών cloud, οι οποίοι θα πρέπει να παρέχουν πληροφορίες σχετικά με όλες τις ενέργειες

επεξεργασίας δεδομένων και πληροφοριών των πελατών. Αυτό θα φέρει επιχειρησιακές δυσκολίες και θα αυξήσει το κόστος της υλοποίησης μιας υπηρεσίας cloud, δεδομένου ότι η αποτελεσματικότητα των υπηρεσιών αυτών προέρχεται από τη βέλτιστη κατανομή πόρων που καθορίζεται από τρέχουσες απαιτήσεις.

4.2.3 Πολιτικός Τομέας

Ο πολιτικός τομέας είναι αυτός που υπέστη τη μεγαλύτερη αμφισβήτηση μετά την αποκάλυψη του σκανδάλου της Cambridge Analytica. Η κοινή γνώμη εναντιώθηκε σε κάθε πολιτική παράταξη, σε πολλές χώρες τόσο της Ευρώπης όσο και της Αμερικής. Μετά την έκδοση του Γενικού Κανονισμού Προστασίας Δεδομένων, ο πολιτικός κόσμος δεν θα μπορούσε να είναι πλέον ο ίδιος.

Παρά το γεγονός ότι κατά τη διάρκεια εκλογικών εκστρατειών επιτρέπεται η συλλογή προσωπικών πληροφοριών, είναι άκρως απαραίτητες οι κατάλληλες διασφαλίσεις αυτών. Τα πολιτικά κόμματα θα πρέπει να κρατούν τα δεδομένα και τις πληροφορίες αυτές με ασφάλεια, δηλαδή με τη χρήση κρυπτογραφημένων μεθόδων και cloud διακομιστών για την αποθήκευση των απαραίτητων πληροφοριών. Κάθε υποψήφιος θα πρέπει να ενημερώνεται ενδελεχώς για τον τρόπο και το λόγο για τον οποίο διατίθενται οι προσωπικές τους πληροφορίες, ενώ έχει το δικαίωμα της αίτησης διαγραφής αυτών, όταν κριθεί απαραίτητο. Οι πολιτικές παρατάξεις θα πρέπει να στελεχώνονται από άτομα που έχουν λάβει την απαραίτητη εκπαίδευση και ενημέρωση σχετικά με το νέο κανονισμό και τις βέλτιστες πρακτικές όσον αφορά στην προστασία της ιδιωτικής ζωής και της συλλογής δεδομένων.



Η μη συμμόρφωση των πολιτικών παρατάξεων με την εφαρμογή του κανονισμού, θα αποφέρει πραγματική οικονομική ζημία και βλάβη της φήμης τους. Σύμφωνα με τον Peter Wilson της εφημερίδας Specialist, οι παρατάξεις πρέπει να δουν το GDPR ως ευκαιρία επικοινωνίας με το κοινό και του υποψήφιους ψηφοφόρους. Αυτό θα τους δώσει τη δυνατότητα να ανταποκριθούν καταλληλότερα στις προκλήσεις, κερδίζοντας ίσως τη χαμένη εμπιστοσύνη του κοινού.

Το πιο οδυνηρό ζήτημα που οφείλουν να αντιμετωπίσουν τα πολιτικά κόμματα είναι η ρύθμιση του πολιτικού μάρκετινγκ. Οι κανονισμοί θα εξακολουθήσουν να είναι πολύ περιορισμένοι ενώ οι νόμοι που διέπουν αυτές τις πρακτικές δεν έχουν ακόμη εναρμονιστεί. Τα κουραστικά εισερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου θα αποτελούν παρελθόν και θα αποστέλλονται μόνο στους πραγματικά ενδιαφερόμενος, εφ' όσον υπάρχει η αναμενόμενη συγκατάθεση. Οι πολιτικές παρατάξεις δεν επιτρέπεται να επιστρατεύσουν σαν μέσο το ηλεκτρονικό ταχυδρομείο προκειμένου να γνωστοποιηθούν οι προθέσεις και το πολιτικό τους όραμα. Συμπερασματικά, ο κανονισμός για τα πολιτικά κόμματα περιλαμβάνει μία αυστηρή πολιτική μάρκετινγκ που απαιτεί συγκατάθεση στις περισσότερες των περιπτώσεων. Τα κόμματα είναι υποχρεωμένα να επενδύσουν στην ασφάλεια των δεδομένων, όχι μόνο λόγω του κανονισμού, αλλά και για την αποκατάσταση της εμπιστοσύνης που κατέρρευσε μετά τη γνωστοποίηση του σκανδάλου.

Συμπεράσματα

Με την ολοκλήρωση της διπλωματικής εργασίας και έπειτα από εκτενή και ενδελεχή έρευνα, τα συμπεράσματα, όπως και τα ερωτήματα, ποικίλουν. Είναι εμφανές το γεγονός της άνευ ορίου εκμετάλλευσης των ανθρωπίνων δεδομένων και δικαιωμάτων. Τόσο η ανάγκη κέρδους όσο η ανάγκη κυριαρχίας, ή ακόμη ο συνδυασμός των παραπάνω, διαλύει τον παραμικρό ηθικό φραγμό. Η κοινωνία και τα άτομα από τα οποία αποτελείται μπορεί ευκόλως να στοχοποιηθεί, να παρακολουθηθεί και να κατευθυνθεί, για πολιτικά κίνητρα ή για λόγους δημόσιας και κρατικής ασφάλειας. Αναρίθμητες εφαρμογές παρακολούθησης στο διαδίκτυο αναλύουν δεδομένα χρηστών, όπως τα προφίλ και τις κινήσεις αυτών, καταλήγοντας στις προτιμήσεις και στις επιλογές τους προσαρμόζοντας τελικά τις πολιτικές τους και τις προσπάθειες μάρκετινγκ ειδικά προς συγκεκριμένα συμφέροντα. Έγινε κατανοητό, πως ένα άτομο είναι εύκολο να παραπλανηθεί, να χειραγωγηθεί και να καθοδηγηθεί, ακόμη και αν έχει επιθυμήσει να διαγράψει βασικά προσωπικά του στοιχεία από τον ιστό. Οι κοινωνικές συνδέσεις, τα σχόλια, τα ανταλλασσόμενα μηνύματα, οι δημόσιες τοποθετήσεις και προτιμήσεις μέσω «likes» και σχολίων, μετατρέπονται σε ορατά, μετρήσιμα και ευτελώς καθοδηγούμενα αποτελέσματα.

Λόγω της ύπαρξης πολλών και διαφορετικών κοινωνικών δικτύων, σε συνδυασμό με την ιλιγγιώδη ανάπτυξη της τεχνολογίας, το ζήτημα της ιδιωτικότητας και της προστασίας της καθίστανται ως περίπλοκα ζητήματα που πρόκειται να απασχολήσουν όλες τις κυβερνήσεις. Σε πολλές περιπτώσεις, δεν είναι εύκολο να αναγνωρίσει κανείς τους κινδύνους σχετικά με τα προσωπικά δεδομένα που ο οποιοσδήποτε χρήστης μπορεί να «ανεβάσει» στο διαδίκτυο. Ακριβώς λόγω των κινδύνων που ελλοχεύουν, κρίνεται σημαντική η ανάπτυξη ενός νομοθετικού πλαισίου, καθώς μέχρι τώρα δεν υπάρχουν σαφείς διευκρινήσεις. Θα είναι αδιαμφισβήτητα ενδιαφέρον να παρακολουθηθεί κανείς τον διάλογο επί του θέματος, όσο και τις επόμενες κινήσεις των νομοθετικών οργάνων. Παρ' όλ' αυτά, η ευθύνη της διαρροής, απώλειας και εκμετάλλευσης προσωπικών δεδομένων οφείλεται να καταλογίζεται σε μεγάλο βαθμό και στους χρήστες. Η ανάγνωση και έγκριση των όρων χρήσης και των πολιτικών απορρήτου απαιτείται να γίνεται με σύνεση και συγκέντρωση πριν την αποδοχή αυτών.

Οι επιπτώσεις του σκανδάλου σε αρκετούς τομείς της καθημερινότητας ήταν έντονες. Οι κοινωνικές αντιδράσεις ήταν μαζικές, ενώ οι κινήσεις που ακολουθήθηκαν από τον κόσμο, έδωσαν την εντύπωση παρορμητισμού και θυμού. Το κοινό δεν άργησε να καταλάβει ότι οι μετέπειτα κινητοποιήσεις ήταν μάταιες, ενώ η αποχή από οποιοδήποτε κοινωνικό μέσο θα

αποτελούσε μία έμμεση αποστασιοποίηση από την καθημερινότητα. Αργά ή γρήγορα θα γύριζαν στις καθημερινές συνήθειες, με μία υποτιθέμενη δυσαρέσκεια και επιφύλαξη, οι οποίες μοιραία θα ξεχασθούν μετά από καιρό. Το ρολόι υπενθύμισης φρόντισε να αποτελέσει ο GDPR. Μπορεί ο κανονισμός να προστατεύει τα προσωπικά δεδομένα, έχοντας μεγάλη ισχύ και εμβέλεια παγκοσμίως, αυτό όμως δεν συνεπάγεται την αδρανοποίηση και τον εφησυχασμό των πολιτών. Οφείλουμε να προσέχουμε πού και γιατί δίνουμε την συγκατάθεση μας, εάν και εφ' όσον δεν επιθυμούμε την αντιμετώπιση μας ως διαδικτυακά φερέφωνα. Από την άλλη, ο πολιτικός κόσμος και οι εθνικές κυβερνήσεις υποχρεούνται να ενεργήσουν με πλήρη αντικειμενικότητα και σεβασμό στα προσωπικά δεδομένα, ενώ η διαφάνεια θα εκτιμηθεί εάν αποτελέσει σημαντικό μέρος της ιδεολογίας της κάθε πολιτικής παράταξης.

Ανερχόμενες τεχνολογίες όπως το Cloud Computing και τα Big Data αναγκάζονται να προσαρμόσουν τους αλγορίθμους που χρησιμοποιούν στο νέο ευρωπαϊκό κανονισμό, γεγονός που υποδεικνύει αναθεώρηση βασικών πολιτικών και δεοντολογιών των εν λόγω τεχνολογιών. Η δυνατότητα υπαναχώρησης και διαγραφής των προσωπικών δεδομένων, όταν αυτό απαιτείται και χωρίς αδικαιολόγητη καθυστέρηση, καταστρέφει με γοργούς ρυθμούς βασικούς κανόνες που υποστηρίζουν ένα σύστημα τεχνολογίας Artificial Intelligence. Η μείωση της αποτελεσματικότητας και της ακρίβειας των αλγορίθμων θα μειωθεί αισθητά, όμως είναι προτιμότερη από τις κολοσσιαίες οικονομικές επιπτώσεις σε περίπτωση παραβίασης ή καταπάτησης προσωπικών δεδομένων μέσω του ιστού.

Συμπεραίνουμε ότι το νέο πλαίσιο του κανονισμού, μετά τις αλλαγές που υπέστη, σε συνδυασμό με καινοτόμα ρυθμιστικά στοιχεία, όπως η προστασία της ιδιωτικής ζωής, ή ακόμη και η κατανόηση των επιπτώσεων σε περίπτωση παραβίασης ή εκμετάλλευσης των προσωπικών δεδομένων, δίνουν αυτόματα μεγαλύτερη βαρύτητα και ισχύ στην αρμόδια νομοθεσία. Οι νέοι κανονισμοί της Ευρωπαϊκής Ένωσης είναι οι αυστηρότεροι κανονισμοί που έχουν συνταχθεί μέχρι στιγμής. Ορισμένοι ειδικοί του χώρου θεωρούν ότι οι συγκεκριμένοι κανονισμοί δείχνουν τον δρόμο για την προστασία προσωπικών δεδομένων. Το ερώτημα που μένει να απαντηθεί είναι εάν θα καταφέρουν πραγματικά να αλλάξουν το τοπίο της δαιδαλώδους και περίεργης «βιομηχανίας» συλλογής δεδομένων.

Η απάντηση δεν είναι προφανής και θα πρέπει να περάσει αρκετός καιρός για να φανούν απτά αποτελέσματα. Προς το παρόν φαίνεται μόνο η μια όψη του νομίσματος, δηλαδή ποιοι είναι οι νέοι κανονισμοί και τι πρέπει να κάνουν οι επιχειρήσεις για να προσαρμοστούν στην καινούργια πραγματικότητα. Δεν είναι γνωστό, ακόμα, πώς ακριβώς οι ευρωπαίοι ελεγκτές θα

τους εφαρμόσουν, ούτε πόσο επιθετικοί θα είναι όταν εντοπίζουν κάποια παράβαση. Το μόνο που είναι γνωστό με σιγουριά αυτή τη στιγμή είναι πως οι παραβάσεις θα κοστίζουν πολύ ακριβά στους επιχειρηματίες. Επιπλέον, ιστοσελίδες και εταιρείες θα προσπαθήσουν να μειώσουν τους συνεργάτες με τους οποίους μοιράζονται προσωπικά δεδομένα προκειμένου να περιοριστεί το κόστος. Σίγουρα, αυτό θα μπορέσει να θεωρηθεί μια μικρή «νίκη» για τις ευαίσθητες πληροφορίες των χρηστών. Όσο για τα υπόλοιπα, θα φανούν εν καιρώ.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

Κεφάλαιο 1:

Άρθρο 2 – Πεδίο Εφαρμογής, Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων, Ανακτήθηκε 20 Φεβρουαρίου, 2018 από

<http://www.opengov.gr/ministryofjustice/?p=9329>

AAPC (healthcare) – Wikipedia από [https://en.wikipedia.org/wiki/AAPC_\(healthcare\)](https://en.wikipedia.org/wiki/AAPC_(healthcare))

Γεώργιος Π. Κανέλλος, (2018), Privacy Shield: Την αναστολή της συμφωνίας ΕΕ-ΗΠΑ για τη διαβίβαση προσωπικών δεδομένων ζητάει το Ευρωκοινοβούλιο Ανακτήθηκε 13

Ιουνίου, 2018 και τελευταία τροποποίηση: 27 Ιουνίου, 2018 από

<https://www.lawspot.gr/nomika-nea/privacy-shield-tin-anastoli-tis-symfonias-ee-ipa-gia-ti-diaivivasi-prosopikon-dedomenon>

CallHub, (2018), 5 Best Political Consulting Firms, Ανακτήθηκε: 14 Μαΐου 2018 από

<https://callhub.io/best-political-consulting-firms/>

Charlie Marchant, (2018), What is Digital PR? (and How It Can Improve Your SEO), Ανακτήθηκε: 23 Φεβρουαρίου, 2018 από

<https://exposureninja.com/blog/digital-pr-business/>

Ieuan Jolly, Loeb & Loeb, (2018), “Data protection in the United States”, Ανακτήθηκε

Αύγουστο 2018 από [https://uk.practicallaw.thomsonreuters.com/6-502-](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&h)

[0467?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&h](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&h)
[hcp=1](#)

Λαμπρινουδάκης Κ., Μήτρου Λ., Γκρίτζαλης Σ. και Κάτσικας Σ., (2009), Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά

Θέματα, Ανακτήθηκε 2009

Λίλιαν Μήτρου,(2018), Η ιστορία της προστασίας προσωπικών δεδομένων

Privacy Shield Framework από <https://www.privacyshield.gov/Program-Overview>

S. and Marper v. UK, (2008), Η διάσταση της αναλογικότητας ως προς το χρόνο διατήρησης των δεδομένων αναδεικνύεται και στην απόφαση, με την οποία το ΕΔΔΑ

απεφάνθη ότι η διατήρηση των δεδομένων απαιτείται να είναι ανάλογη του σκοπού για τον οποίο έχουν συλλεγεί και χρονικά περιορισμένη (απόφαση της 4/12/2008).

WILL KENTON, (2018), Fortune 100, Ανακτήθηκε 14 Ιουνίου, 2018 απο <https://www.investopedia.com/terms/f/fortune-100.asp>

Κεφάλαιο 2:

Αγγελική Δημοπούλου, (2018), Πώς στήθηκε το μεγαλύτερο σκάνδαλο δεδομένων στο Facebook, Ανακτήθηκε 20 Μαρτίου, 2018 από <https://tvxs.gr/news/kosmos/postithike-megalo-skandalo-me-ta-dedomena-sto-facebook>

Bloomberg, (2019), Company Overview of SCL Group Limited, Ανακτήθηκε 20 Μαΐου, 2019 από <https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=72454231>

Cambridge Analytica, (2015) απο <https://cambridgeanalytica.org/>

Carole Cadwalladr and Emma Crahan-Harrison, (2018), Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, Ανακτήθηκε 17 Μαρτίου, 2018 από <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

CNN Greece, (2018), Κλείνει η Cambridge Analytica μετά το σκάνδαλο υποκλοπής δεδομένων, Ανακτήθηκε 02 Μαΐου, 2018 από <https://www.cnn.gr/news/kosmos/story/128346/kleinei-i-cambridge-analytica-meta-to-skandalo-ypoklopis-dedomenon>

Hannes Grassegger & Mikael Krogerus, (2017), Data που Ανέτρεψαν τον Κόσμο - Πώς το Facebook Οδήγησε στο Brexit και στον Trump, Ανακτήθηκε 28 Μάρτιο, 2017 απο <https://www.vice.com/gr/article/pg9zjm/ta-big-data-poy-anetrepsan-ton-kosmo-pws-to-facebook-odhghe-sto-brexit-kai-ston-trump>

Meredith, S., (2018), **Facebook-Cambridge Analytica: A timeline of the data hijacking scandal**, Ανακτήθηκε 10 Απριλίου, 2018 απο

<https://www.cNBC.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>

Murillo Javier, (2018), Cambridge Analytica, sigan la ruta del dinero, Ανακτήθηκε 9 Απριλίου, 2018 από <https://www.elfinanciero.com.mx/opinion/javier-murillo/cambridge-analytica-sigan-la-ruta-del-dinero>

Πανοπούλου Ι., (2018), Το Σκάνδαλο Της Cambridge Analytica Και Ο Mark Zuckerberg, Ανακτήθηκε 10 Μαΐου, 2018 από <https://powerpolitics.eu/%CE%B9%CF%89%CE%AC%CE%BD%CE%BD%CE%B1-%CF%80%CE%B1%CE%BD%CE%BF%CF%80%CE%BF%CF%8D%CE%BB%CE%B04-%CF%84%CE%BF-%CF%83%CE%BA%CE%AC%CE%BD%CE%B4%CE%B1%CE%BB%CE%BF-%CF%84%CE%B7%CF%82-cambridge-a/>

Point of view on Cambridge Analytica scandal από http://social-lab.eu/wp-content/uploads/2018/03/Whitepaper_FB_SL.pdf

Privacy International. (n.d.), **Data and elections**, από <https://privacyinternational.org/topics/data-and-elections>

Roose K. & Kang C., (2018), **Mark Zuckerberg testifies on Facebook before skeptical lawmakers**, Ανακτήθηκε 10 Απριλίου, 2018 από <https://www.nytimes.com/2018/04/10/us/politics/zuckerberg-facebook-senate-hearing.html?module=ArrowsNav&contentCollection=Politics&action=keypress®ion=FixedLeft&pgtype=article>

Stephanie Borg Psaila, (2018), Cambridge Analytica explained: The fact, implications and open questions, Ανακτήθηκε 24 Απρίλιο, 2018 από <https://dig.watch/trends/cambridge-analytica>

Τάσος Οικονόμου, (2018), Γιατί μας αφορά όλους το σκάνδαλο της Cambridge Analytica, Ανακτήθηκε 21 Μαρτίου, 2018 από https://www.huffingtonpost.gr/entry/yiati-mas-afora-oloes-to-skandalo-tes-cambridge-analytica_gr_5ab23378e4b0decad04586a6

Wikipedia, SCL Group από https://en.wikipedia.org/wiki/SCL_Group

Wikispooks, (2018), Strategic Communication Laboratories, Ανακτήθηκε 2018 από https://wikispooks.com/wiki/Strategic_Communication_Laboratories

Κεφάλαιο 3:

VALUENEX (2018), INC., FACEBOOK: A BREACH IN THE WALL. A TECHNOLOGICAL APPROACH TO THE FACEBOOK CAMBRIDGE ANALYTICA SCANDAL

Justin Cudmore & James True, (2018), How Cambridge Analytica (And Facebook?) Breached All The Privacy Laws, newmatilda.com. Ανακτήθηκε 29 Μαρτίου, 2018 από <https://newmatilda.com/2018/03/29/cambridge-analytica-facebook-breached-privacy-laws/>

Jim Isaak, Mina J. Hanna, (2018), THE POLICY CORNER: User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection, pp. 56-59, vol. 51. Ανακτήθηκε Αύγουστο, 2018 από <https://www.computer.org/csdl/magazine/co/2018/08/mco2018080056/13rRUxbCbmn>

Hannah Ersdal, Sølvi Svendby Skjærstad, (2016), Master of Science in Communication Technology, Department of Telematics, Norwegian University of Science and Technology, Privacy and Social Media: Do Users Really Care?. Ανακτήθηκε τον Ιούνιο, 2016 από https://brage.bibsys.no/xmlui/bitstream/handle/11250/2403229/15179_FULLTEXT.pdf?sequence=1

Carole Cadwalladr and Emma Graham-Harrison, (2018), The Guardian: How Cambridge Analytica turned Facebook ‘likes’ into a lucrative political tool. Ανακτήθηκε 17 Μαρτίου, 2018 από <https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm?fbclid=IwAR1I1hokbXuMWPoOux3tEyX7EBQhSWdJsSckujRuktHp6E8zFZbN4lndsJl>

Marcello Ienca, Effy Vayena, (2018), SCIENTIFIC AMERICAN: Cambridge Analytica and Online Manipulation. Ανακτήθηκε 30 Μαρτίου, 2018 από <https://blogs.scientificamerican.com/observations/cambridge-analytica-and-online-manipulation/>

<https://el-gr.facebook.com/about/privacy>

Susan T. Fiske, Princeton University, Princeton, NJ,(2017), Psychological targeting as an effective approach to digital mass persuasion. Ανακτήθηκε 13 Νοεμβρίου, 2017 από <https://www.pnas.org/content/pnas/114/48/12714.full.pdf>

Hal Berghel, University of Nevada, Las Vegas, (2018), Malice Domestic: The Cambridge Analytica Dystopia, Computer (Volume 51, Issue 5, Μάιος 2018), pp. 84-89. Ανακτήθηκε 24 Μαΐου, 2018 από <https://ieeexplore.ieee.org/document/8364652>

Aiswarya Ramachandran, (2018), Analyzing Medium posts to understand impact of Cambridge Analytica Scandal, Ανακτήθηκε 2 Σεπτεμβρίου, 2018 από <https://medium.com/analytics-vidhya/analyzing-medium-posts-to-understand-impact-of-cambridge-analytica-scandal-5841f46703d6>

Adam Satariano, (2018), The New York Times, What the G.D.P.R., Europe’s Tough New Data Law, Means for You. Ανακτήθηκε 6 Μαΐου, 2018 από

<https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html>

Rick Robinson, (2018), Data Privacy Vs. Data Protection, Defrag This. Ανακτήθηκε 29 Ιανουαρίου, 2018 από <https://blog.ipswitch.com/data-privacy-vs-data-protection>

Robert Cruz, (2018), Social Media and Regulation: Where Do We Go From Here?, Smarsh. Ανακτήθηκε 12 Απριλίου, 2018 από <https://www.smarsh.com/blog/social-media-regulation-go/>

Justin Jaffe, Laura Hautala, (2018), CNET, What the GDPR means for Facebook , the EU and you. Ανακτήθηκε 25 Μαΐου, 2018 από <https://www.cnet.com/how-to/what-gdpr-means-for-facebook-google-the-eu-us-and-you/>

Dana Simberkoff, (2018), CMS Wire, How Facebook's Cambridge Analytica Scandal Impacted the Intersection of Privacy and Regulation. Ανακτήθηκε 30 Αυγούστου, 2018 από <https://www.cmswire.com/information-management/how-facebooks-cambridge-analytica-scandal-impacted-the-intersection-of-privacy-and-regulation/>

Iga Kozłowska, (2018), Facebook and Data Privacy in the Age of Cambridge Analytica. Ανακτήθηκε 30 Απριλίου, 2018 από <https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/>

Penn Bullock, (2018), The New York Times, Elections, Brexit, Facebook: Your Wednesday Briefing. Ανακτήθηκε 7 Νοεμβρίου, 2018 από <https://www.nytimes.com/2018/11/07/briefing/elections-brexit-facebook.html>

Tim Adams, (2018), The Guardian: Facebook's week of shame: the Cambridge Analytica fallout. Ανακτήθηκε 24 Μαρτίου, 2018 από <https://www.theguardian.com/technology/2018/mar/24/facebook-week-of-shame-data->

[breach-observer-revelations-zuckerberg-silence](#)

Mark Scott, (2018), POLITICO, Cambridge Analytica helped ‘cheat’ Brexit vote and US election, claims whistleblower. Ανακτήθηκε 29 Μαρτίου, 2018 από <https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/>

Hillary Grigonis, (2018), Digital Trends, 9 things to know about Facebook privacy and Cambridge Analytica. Ανακτήθηκε 4 Μαΐου, 2018 από <https://www.digitaltrends.com/social-media/what-facebook-users-should-know-about-cambridge-analytica-and-privacy/>

Κεφάλαιο 4:

David Cohen, (2018), ADWEEK, Younger People Were More Likely to React to Facebook’s Cambridge Analytica Scandal. Ανακτήθηκε το Σεπτέμβριο, 2018 από <https://www.adweek.com/digital/younger-people-were-more-likely-to-react-to-facebooks-cambridge-analytica-scandal/>

Francis Dinha – CEO of OpenVPN, (2018), Entrepreneur EUROPE, The Cambridge Analytica Scandal Has People Quitting Facebook but Business Pages are Untouched. Ανακτήθηκε το Μάιο, 2018 από <https://www.entrepreneur.com/article/312126>

Lisa Ryan, (2016), THE CUT, Here’s How People Are Reacting on Social Media to Donald Trump Winning the Presidential Election. Ανακτήθηκε 9 Νοεμβρίου, 2016, από <https://www.thecut.com/2016/11/how-people-on-social-media-reacted-to-donald-trumps-win.html>

Brandy Zadrozny and Ben Collins, (2018), NEWS, Inside the final days of Cambridge Analytica: Failed rebrands, fleeing clients and Nerf basketball. Ανακτήθηκε 18 Μαΐου, 2018 από <https://www.nbcnews.com/business/business-news/inside-final-days-cambridge-analytica-failed-rebrands-fleeing-clients-nerf-n875321>

Tammy Borden, (2018), Will the Cambridge Analytica Scandal Impact How Marketers Use Facebook?. Ανακτήθηκε 27 Μαρτίου, 2018 από https://www.weidert.com/whole_brain_marketing_blog/will-the-cambridge-analytica-scandal-impact-facebook

Antonio Peruzzi, Fabiana Zollo , Walter Quattrociochi and Antonio Scala, (2018), ENTROPY, How News May Affect Markets' Complex Structure: The Case of Cambridge Analytica. Ανακτήθηκε 6 Οκτωβρίου, 2018 από https://www.researchgate.net/publication/328151590_How_News_May_Affect_Markets_%27_Complex_Structure_The_Case_of_Cambridge_Analytica

Partisan Issues, (2018), Facebook Cambridge Analytica Scandal Is a Crisis For All Online Companies. Ανακτήθηκε 28 Μαρτίου, 2018 από <https://www.partisanissues.com/2018/03/facebook-cambridge-analytica-scandal-is-a-crisis-for-all-online-companies/>

Prachi Bhardwaj, Business Insider US, (2018), BUSINESS INSIDER, Eight weeks after the Cambridge Analytica scandal, Facebook's stock price bounces back to where it was before the controversy. Ανακτήθηκε 11 Μαΐου, 2018 από <https://www.businessinsider.sg/facebooks-stock-back-up-cambridge-analytica-charts-2018-5/>

Vaughn Highfield, (2018), ALPHR, Facebook suffers £83 billion financial blow following Cambridge Analytica scandal. Ανακτήθηκε 26 Ιουλίου, 2018 από <https://www.alphr.com/facebook/1009757/facebook-suffers-83-billion-financial-blow->

[cambridge-analytica-scandal](#)

THE TOC-TIMES OF CHANGE- Το σκάνδαλο Facebook-Cambridge Analytica στο Ευρωκοινοβούλιο. Ανακτήθηκε 24 Οκτωβρίου, 2018 από

[http://www.thetoc.gr/diethni/article/to-skandalo-facebook-cambridge-analytica-sto-
eurwkoynoboulio](http://www.thetoc.gr/diethni/article/to-skandalo-facebook-cambridge-analytica-sto-
eurwkoynoboulio)

Nextdeal newroom, NEXTDEAL-ΤΕΧΝΟΛΟΓΙΑ, Facebook-Cambridge Analytica: Το Ευρωπαϊκό Κοινοβούλιο ζητά τη λήψη μέτρων προστασίας της ιδιωτικότητας των πολιτών!, Ανακτήθηκε 26 Οκτωβρίου, 2018, από

[https://www.nextdeal.gr/epikairota/tehnologia/103467/facebook-cambridge-analytica-
eyropaiko-koinovoylio-zita-ti-lipsi](https://www.nextdeal.gr/epikairota/tehnologia/103467/facebook-cambridge-analytica-
eyropaiko-koinovoylio-zita-ti-lipsi)

iGuru- FightHoax Έρευνα και Ανάλυση Cambridge Analytica- Μάρτιος 2018, Ανακτήθηκε 16 Απριλίου, 2018 από [https://iguru.gr/2018/04/16/fighthoax-cambridge-
analytica/#i-5](https://iguru.gr/2018/04/16/fighthoax-cambridge-
analytica/#i-5)

Russell Brandom, (2018), THE VERGE, Everything you need to know about GDPR. Ανακτήθηκε 25 Μαΐου, 2018 από [https://www.theverge.com/2018/3/28/17172548/gdpr-
compliance-requirements-privacy-notice](https://www.theverge.com/2018/3/28/17172548/gdpr-
compliance-requirements-privacy-notice)

Olivia Solon, (2018), The Guardian: How Europe's 'breakthrough' privacy law takes on Facebook and Google. Ανακτήθηκε 19 Απριλίου, 2018 από [https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-
data-privacy-regulation](https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-
data-privacy-regulation)

Nellie Bowles, (2018), The New York Times, After Cambridge Analytica, Privacy Experts Get to Say 'I Told You So'. Ανακτήθηκε 12 Απριλίου, 2018 από

<https://www.nytimes.com/2018/04/12/technology/privacy-researchers-facebook.html>

Julie Beck, (2018), The Atlantic, People Are Changing the Way They Use Social Media.

Ανακτήθηκε 7 Ιουνίου, 2018 από

<https://www.theatlantic.com/technology/archive/2018/06/did-cambridge-analytica-actually-change-facebook-users-behavior/562154/>