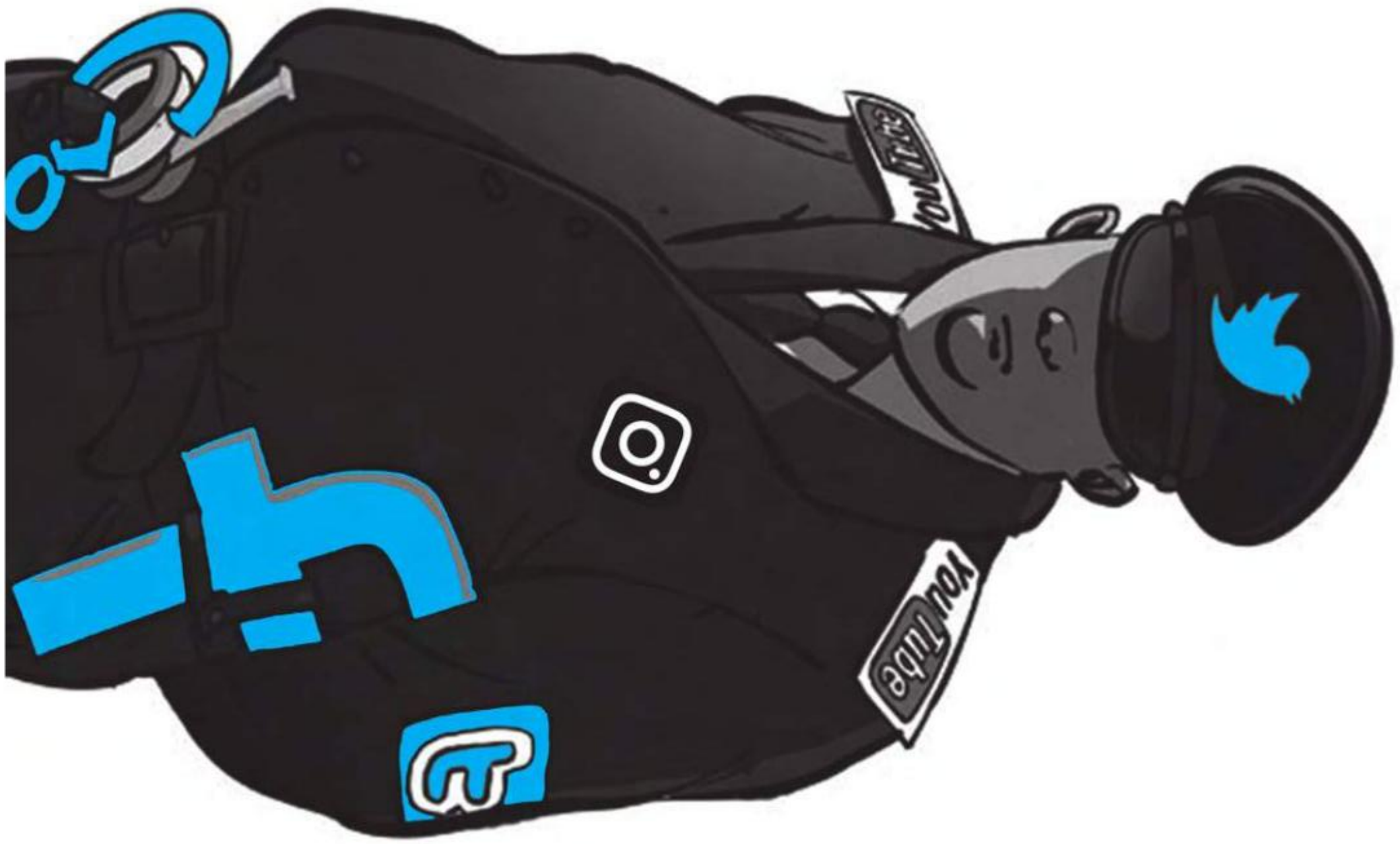
ΕΠΙΤΗΡΗΣΗ
ΚΟΙΝΩΝΙΚΟΣ ΕΛΕΓΧΟΣ
ΚΑΙ ΚΑΤΑΣΤΟΛΗ



Εισαγωγή

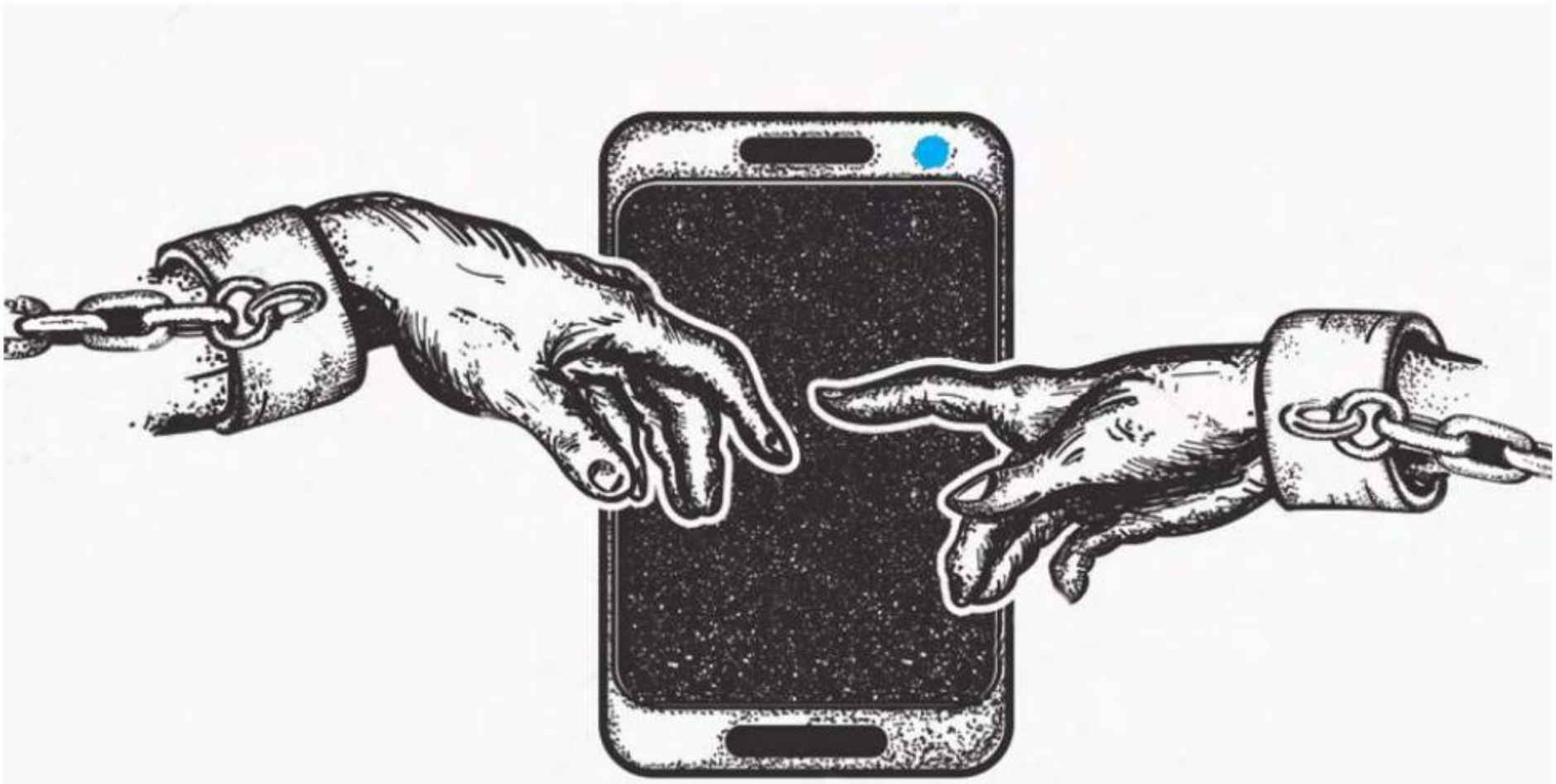
Η έκδοση αυτή είναι το αποτέλεσμα κουβέντας και ζυμώσεων με θέμα το διαδίκτυο και τις κακοτοπιές του. Ξεκίνησαμε να συζητάμε καθώς βρίσκαμε συνέχεια μπροστά μας ζητήματα που άπτονται σε αυτό. Αντί να τα εξηγούμε ατομικά, θεωρήσαμε πιο γόνιμο να τα επεξεργαστούμε και να τοποθετηθούμε συλλογικά. Εξαρχής φάνηκε ότι το θέμα είναι τεράστιο και πολυδιάστατο. Προτιμήσαμε να το σπάσουμε σε ενότητες, φιλοδοξώντας να παράξουμε και μελλοντικές εκδόσεις που θα περιλαμβάνουν διαφορετικές πτυχές.

Δεν αποσκοπούμε μόνο στο να γνωστοποιήσουμε τους προβληματισμούς μας και την κριτική πάνω στο συγκεκριμένο θέμα, αλλά κυρίως στο να ανοίξει μια συζήτηση βασισμένη στα σημεία που θέτουμε. Ώστε να μπορέσουμε εν τέλει να αντιτάξουμε κάτι ρεαλιστικό στα προβλήματα που εγείρονται και να μην αρκεστούμε σε ένα ξόρκισμα χωρίς αντιπρόταση.

Το συγκεκριμένο ζήτημα αφορά το σύνολο των ανθρώπων που συνδέονται στο διαδίκτυο. Η απεύθυνσή μας όμως είναι κυρίως σε συντρόφους και συντρόφισσες, μιας και εκεί η επιτήρηση και η καταστολή δεν είναι αφηρημένες έννοιες αλλά βίωμα.

Βρεθήκαμε γύρω από τη συλλογικότητα Cybrigade και έχοντας γνώση του διαδικτύου και των προβλημάτων του, μιλάμε κριτικά απέναντι τους.

Ιστορικό υπολογιστών διαδικτύου



Οι ηλεκτρονικοί υπολογιστές έκαναν την πρώτη μαζική εμφάνισή τους τη δεκαετία του ‘80. Από το 2000 και μετά η χρήση τους έγινε τόσο διαδεδομένη που πλέον κάποια γεννημένη μέσα σε αυτό το φάσμα εποχών, δεν μπορεί να σκεφτεί πώς η ροή της ζωής οργανωνόταν χωρίς αυτούς. Βασικό ρόλο στην μεγάλη εξάπλωσή τους σε οικιακό και προσωπικό επίπεδο έπαιξε το ίντερνετ. Το διαδίκτυο αν και προϋπήρχε ως στρατιωτικό project των Η.Π.Α. με το όνομα ARPANET, ξεκίνησε να διαδίδεται μαζικά ως αγαθό προς τους πολίτες στις αρχές της δεκαετίας του ‘90. Η αρχική στόχευσή του ήταν ο πειραματισμός με τις νέες τεχνολογίες για τις ανάγκες των μιλιταριστών. Ακόμα και σήμερα, ο έλεγχος πολύ κομβικών σημείων του διαδικτύου, είναι υπό την αιγίδα των κυβερνήσεων και κυρίως των ΗΠΑ. Η κύρια υποδομή που χρειάζεται για να λειτουργήσει το διαδίκτυο, είτε πρόκειται για δρομολογητές/μεταγωγείς, είτε για καλωδίωση οπτικών ινών, ανήκει σε μεγάλους τηλεπικοινωνιακούς παρόχους, κρατικούς και ιδιωτικούς. Η ονοματοδοσία (DNS) βρίσκεται υπό την εποπτεία ηπειρωτικών οργανισμών, που με τη σειρά τους, είναι κάτω από μια υπηρεσία του υπουργείου εμπορίου των ΗΠΑ. Το διαδίκτυο γνώρισε τη μεγάλη του άνθιση, ως δημόσια διαθέσιμο εμπορικό προϊόν με την έλευση του 21ου αιώνα.

Στην εξέλιξη του διαδικτύου και τελικά στην τεχνολογική αυτή έκρηξη συνέβαλαν καθορι-

στικά κάποιοι παράγοντες. Ένας από αυτούς ήταν η εξέλιξη των web τεχνολογιών. Στις αρχές του 2000 έγινε η στροφή σε αυτό που ονομάστηκε web 2.0. Στη ουσία το web 2.0 σηματοδοτεί την νέα εποχή του ίντερνετ, όπου πλέον οι χρήστες των ιστοσελίδων μπορούν οι ίδιοι να διαμορφώνουν το περιεχόμενο της σελίδας και να έχουν διαδραστική σχέση με αυτή. Πριν την εμφάνιση του web 2.0, μπορούσες να φτιάξεις μια προσωπική ιστοσελίδα και να διαχειρίζεσαι το περιεχόμενό της, αλλά αυτό απαιτούσε εξειδικευμένες τεχνικές γνώσεις και, εκτός αυτού, το περιεχόμενο διαμορφωνόταν μόνο από τους διαχειριστές της οι οποίοι είχαν και άμεση πρόσβαση στον κώδικά της. Στην μετά web 2.0 εποχή, η φιλοξενία ιστοσελίδων έγινε υπηρεσία, και μπορούσες να ανοίξεις ένα blog ή ένα προφίλ με μια απλή αίτηση. Χαρακτηριστικό παράδειγμα της αξιοποίησης των δυνατοτήτων του web 2.0 είναι τα social media.

Ταυτόχρονα, το κεφάλαιο αναγνώρισε στη νέα αυτή τεχνολογική τάση μια τεράστια αγορά με δυνατότητες που δε φανταζόταν μέχρι τότε. Το αγοραστικό κοινό πλέον δεν περιοριζόταν στις χώρες όπου η κάθε εταιρία είχε έδρα, αλλά εκτεινόταν σε κάθε γωνιά του πλανήτη που υπήρχε ίντερνετ. Η πρώτη online πώληση προϊόντος στην ιστορία καταγράφεται το 1994[1] και ήταν ένα CD του Sting. Ένα χρόνο μετά εμφανίζεται το Amazon, που σήμερα βρίσκεται στο νούμερο τρία των πιο πλούσιων εταιριών στον κόσμο, πίσω από την Apple και την Google[2] και ακολουθεί μια γεωμετρική αύξηση των eshops και online υπηρεσιών επί πληρωμή.

Μέσα σε αυτή τη συνθήκη οι επιχειρηματίες του διαδικτύου αρχίζουν να διαπιστώνουν πόσο επικερδής μπορεί να γίνει η συλλογή των προσωπικών δεδομένων. Οι διαφημιστές εργάζονται πυρετωδώς για να βρουν τρόπους να φτιάξουν εύστοχες και προσωποποιημένες διαφημίσεις και στη συνέχεια να τις διασπείρουν αποδοτικά στους καταναλωτές του κόσμου μέσω των υπολογιστών. Τα tracking cookies[3], η συλλογή διευθύνσεων IP, τα λογισμικά καταγραφής, εισέβαλαν στους υπολογιστές με σκοπό την σκιαγράφηση του προφίλ των χρηστών και τελικά την προβολή διαφημίσεων με τον πιο αποδοτικό τρόπο.

Η εξάπλωση smartphones και tablet, και στη συνέχεια η κυκλοφορία μιας ολόκληρης γκάμας από "έξυπνα" αντικείμενα, που μεταξύ άλλων συνδέονται και στο διαδίκτυο, όπως ιατρικά μηχανήματα, τηλεοράσεις, ταΐστρες κατοικίδιων, ψυγεία, εκτυπωτές, αυτοκίνητα ακόμα και θερμοστάτες ενυδρείων, έθεσε την πρόσβαση στο διαδίκτυο ως απαραίτητη προϋπόθεση της ύπαρξης του ατόμου μέσα σε ένα κοινωνικό περιβάλλον με νέους ρυθμούς και νέα οργάνωση της καθημερινότητας. Πλέον δεν είναι απαραίτητο να έχουμε ένα σταθερό υπολογιστή ή laptop για να αποκτήσουμε πρόσβαση στο internet. Με την χρήση των κινητών συσκευών είμαστε μονίμως συνδεδεμένοι, οπουδήποτε κι αν βρισκόμαστε.

---

1. http://time.com/money/3108995/online-shopping-history-anniversary/
2. http://fortune.com/2018/02/15/amazon-microsoft-third-most-valuable-company/
3. Για τεχνικές λεπτομέρειες, υπάρχουν τα Παράρτηματα στο τέλος της μπροσούρας

Ιστορικό επιτήρησης

Τα εργαλεία και οι μέθοδοι επιτήρησης βρίσκονταν σχεδόν πάντα σε αντιστοιχία με την τεχνογνωσία της κάθε εποχής. Η φυσική επιτήρηση υπήρξε ο πιο συνηθισμένος τρόπος ελέγχου. Περιπολίες των αρχών επιβολής του νόμου στις γειτονιές, μυστικές υπηρεσίες και πράκτορες, ή απλά ρουφιάνοι, χρησιμοποιούνται εδώ και αιώνες μέχρι σήμερα. Μέθοδοι που γενικά απαιτούν μεγάλο ανθρώπινο δυναμικό και πόρους, με τα αποτελέσματα που φέρνουν να είναι συχνά αναντίστοιχα της προσπάθειας που καταβάλλεται.

Με την μαζική χρήση του τηλεφώνου, μπήκαν στο παιχνίδι και οι τηλεφωνικές παρακολουθήσεις, με καταγραφές συνομιλιών υπόπτων και όχι μόνο. Στη δεκαετία του '60[4] ένα νεότερο και αρκετά αποτελεσματικό μέσο παρακολούθησης και καταγραφής κινήσεων εμφανίζεται, το οποίο στη δεκαετία του '90 αρχίζει να χρησιμοποιείται συστηματικά: οι κάμερες καταγραφής. Οι πρώτες μαζικές εγκαταστάσεις καμερών σε δημόσιους χώρους ξεκίνησαν με το πρόσχημα του ελέγχου της κυκλοφορίας σε κεντρικούς δρόμους των αστικών κέντρων ή της καταγραφής των συναλλαγών στα ΑΤΜ, εξοικειώνοντας τους ανθρώπους στην ιδέα της παρακολούθησης των κινήσεών τους ακόμα και όταν κάποιο φυσικό πρόσωπο δεν ήταν παρόν. Ιδιαίτερο ρόλο στην αύξηση της επιτήρησης μέσω CCTV έπαιξε η επίθεση στους δίδυμους πύργους το 2001. Σε πολύ μικρό χρονικό διάστημα μετά την επίθεση και με το πρόσχημα της πρόληψης μελλοντικών χτυπημάτων, οι κάμερες κατέλαβαν όλο και μεγαλύτερο μέρος του δημόσιου χώρου, επιβάλλοντας ή εκμαιεύοντας γρήγορα την κοινωνική νομιμοποίηση του μέσου. Ακολούθησε η εμφάνισή τους σε όλο και περισσότερους ιδιωτικούς χώρους για την "ασφάλεια των περιουσιών" των πολιτών, με αποτέλεσμα να δημιουργηθεί ένα άτυπο δίκτυο καμερών που καταγράφουν επί 24ώρου βάσεως μαγαζιά, πλατείες πεζοδρόμια και δρόμους, με υλικό εν δυνάμει άμεσα διαθέσιμο στην αστυνομία.

Οι μηχανισμοί επιτήρησης έπαιζαν πάντα πολύ σημαντικό ρόλο στην άσκηση του ελέγχου των κοινωνικών συνόλων. Ήδη με την εμφάνιση των πρώτων δομών εξουσίας, επενδύονταν πόροι και ενέργεια για την ανακάλυψη όλο και καλύτερων και ευφάνταστων τρόπων παρακολούθησης της καθημερινής ζωής των υπηκόων. Από την εκκλησία μέχρι τα εργοστάσια και την επιτήρηση της εργασίας, μέχρι τη σημερινή ψηφιακή δυστοπία, οι πρακτικές διαφέρουν τόσο

4. https://en.wikipedia.org/wiki/Closed-circuit_television#Application

στην ένταση της επιτήρησης όσο και στον βαθμό που τα υποκείμενα συμμετέχουν ενεργά ή παθητικά σε αυτήν . Στη σύγχρονη εποχή, η εμφάνιση των ψηφιακών τεχνολογιών έχει εισάγει ιδιαίτερα σημαντικές και αποτελεσματικές μεθόδους προς την κατεύθυνση της πανοπτικής λειτουργίας της επιτήρησης.

Χαρακτηριστικό παράδειγμα είναι οι κάθε είδους κάμερες γύρω μας, στους δρόμους, σε κτήρια, ακόμη και σε χώρους εργασίας για την παρακολούθηση των εργαζομένων. Η πιο ολοκληρωτική εκδοχή είναι τα "badges" στους χώρους εργασίας. Πρόκειται για συσκευές με ανοιχτά μικρόφωνα και GPS, που καταγράφουν τις διαδρομές των εργαζομένων, το χρόνο κίνησης και στάσης, τι λένε, με ποιους κλπ. Η Amazon π.χ. υποχρεώνει τους εργαζόμενους και τις εργαζόμενές της να φοράνε ένα περικάρπιο (που είναι πατέντα της ίδιας της εταιρίας), το οποίο καταγράφει κάθε στιγμή την θέση τους, πόση ώρα έκαναν διάλειμμα για τουαλέτα, αν μιλάνε με κάποιον συνάδελφό τους κτλ. Η συγκεκριμένη πατέντα επίσης, διαθέτει σύστημα δόνησης που ενεργοποιείται όταν τα χέρια του υπαλλήλου δεν πηγαίνουν προς την σωστή κατεύθυνση. Για παράδειγμα, όταν ο υπάλληλος πρέπει να πακετάρει ένα συγκεκριμένο δέμα αλλά τα χέρια του κατευθυνθούν προς κάπου αλλού, το περικάρπιο θα δονηθεί για να του επισημάνει το λάθος του[5].

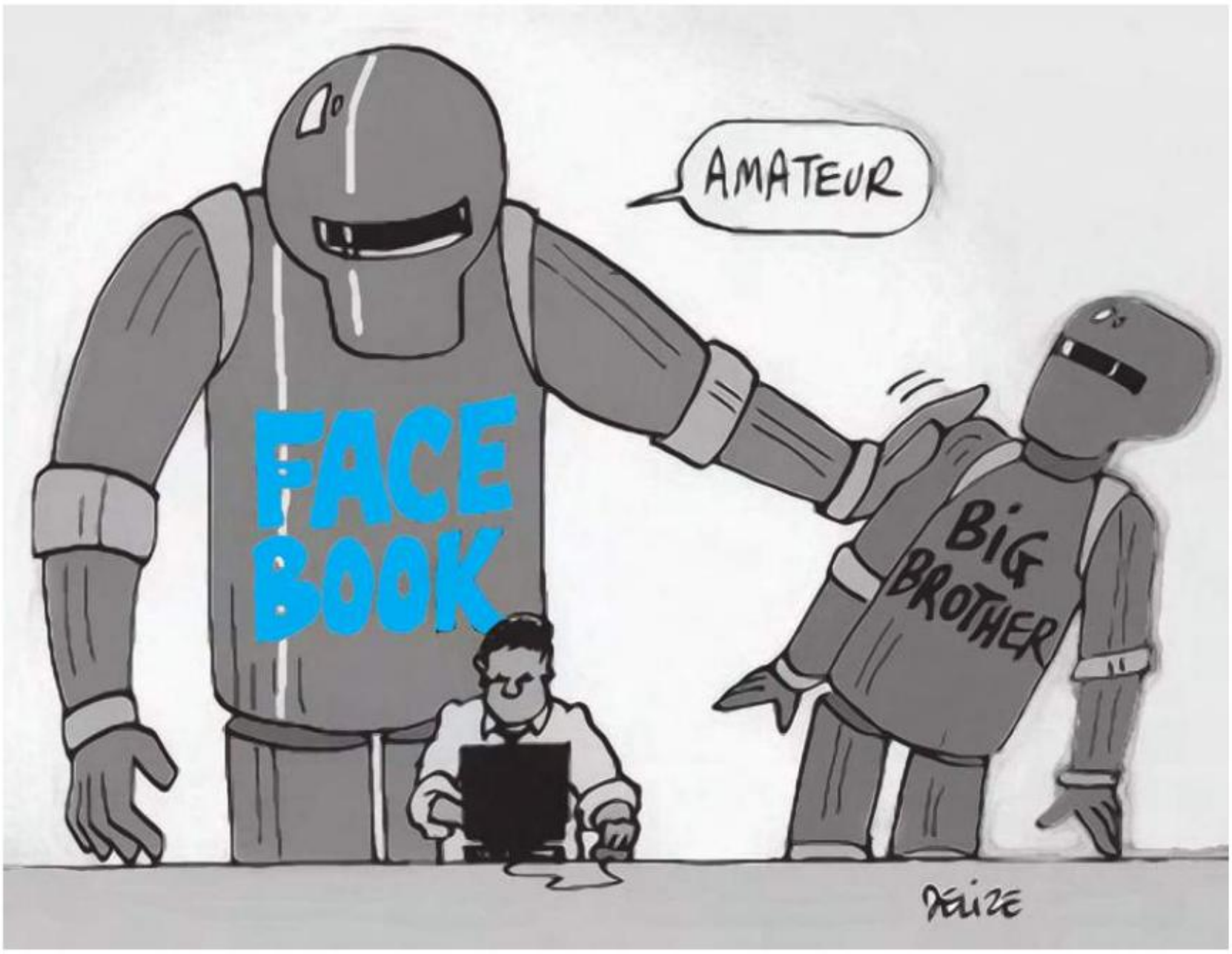
Ένα άλλο παράδειγμα που αποδεικνύει πως μια "ουδέτερη" επιστημονική τεχνολογική ανακάλυψη μπορεί να πάρει ξεκάθαρο πρόσημο στα κατάλληλα χέρια αποτελεί η χρήση ειδικών συσκευών οι οποίες φοριούνται στα κεφάλια εργαζομένων και με αποκωδικοποίηση των εγκεφαλικών κυμάτων προβλέπουν την ψυχολογική κατάσταση στην οποία ένας εργαζόμενος βρίσκεται[6]. Αν λοιπόν ξαφνικά αρχίσει κάποιος να βαριέται ή να εκνευρίζεται (με τις απάνθρωπες ίσως συνθήκες στις οποίες πολλοί και πολλές δουλεύουν), αυτόματα η μηχανή τον μεταθέτει σε κάποια άλλη θέση (είτε ως τιμωρία είτε ως πρόληψη για να μην πέσει η παραγωγικότητα ή η ποιότητα). Κι αν τα παραπάνω μας φαίνονται πολύ μακριά (γεωγραφικά) ώστε να τα λάβουμε ως σοβαρό τρομακτικό αντίλογο στο επιχείρημα περί "ουδέτερων μηχανών επεξεργασίας δεδομένων", μπορούμε να έρθουμε σε ευρωπαϊκό επίπεδο όπου πλέον σε διάφορες χώρες εφαρμόζεται "ηλεκτρονικό σκανάρισμα[7]" των μεταναστών για να απορρίπτονται αυτόματα όσοι δεν είναι στη "λίστα καλεσμένων[8]" . Κάτι παρόμοιο άλλωστε (με λιγότερους αυτοματισμούς προς το παρόν) υπάρχει και σε χώρες όπως Αγγλία / Αμερική στις οποίες η αστυνομία του αεροδρομίου μπορεί κατά την είσοδο στη χώρα να ζητήσει να δει τα δεδομένα του κινητού / υπολογιστή καθώς και λογαριασμούς social media ώστε να εγκρίνει ή να αρνηθεί την είσοδο του ταξιδιώτη στη χώρα. Με τη σύγχρονη τεχνολογία τέτοιοι "χειρισμοί" είναι πιο γρήγοροι, με λιγότερο προσωπικό και μηδαμινά αισθήματα. Στον "ουδέτερο" κόσμο των αυτοματισμών, όταν χάνεις ή σου κλέβουν το πορτοφόλι, θα πηγαίνεις με τα πόδια σπίτι γιατί η αυτόματη μπάρα εισόδου είναι συναισθηματικά (και υλικά) κουφή και παγερά αδιάφορη σε σχέση με τον οδηγό/ελεγκτή ενός ΜΜΜ.

---

5. https://www.theverge.com/2018/2/1/16958918/amazon-patents-trackable-wristband-warehouse-employees
6. https://futurism.com/china-emotional-surveillance/
7. https://yro.slashdot.org/story/18/07/03/1650232/europe-is-using-smartphone-data-as-a-weapon-to-deport-refugees
8. Χώρες όπως η Γερμανία άλλωστε στο παρελθόν έχουν ανοίξει τα σύνορά τους επιλεκτικά μόνο σε εργατικό δυναμικό που τους έλλειπε συγκεκριμένων εθνικοτήτων (π.χ Σύριοι γιατροί)

Η μαζική εξάπλωση του ίντερνετ δημιούργησε μία νέα αναγκαιότητα για τους μηχανισμούς εξουσίας και επιτήρησης. Η κίνηση στο θεωρητικά "ανεξάρτητο" και "ελεύθερο" παγκόσμιο διαδίκτυο έπρεπε να τεθεί υπό πλήρη έλεγχο και οι πληροφορίες που διακινούνται σε αυτό έπρεπε να γίνουν χρήσιμες για το χτίσιμο του προφίλ των χρηστών. Έτσι άρχισαν να δημιουργούνται κρατικές υπηρεσίες "δίωξης ηλεκτρονικού εγκλήματος". Η ιδιαιτερότητα της ψηφιακής φύσης του ίντερνετ δημιουργεί την ψευδαίσθηση πως ό,τι κάνουμε σε αυτό, αφορά μόνο εμάς και κανείς δε βλέπει ή δεν ασχολείται με τις πληροφορίες που ανταλλάσσουμε. Τα νέα αυτά σώματα επιτήρησης μπήκαν έτσι αθόρυβα στις ζωές μας, παρακολουθώντας και καταγράφοντας την κάθε μας ηλεκτρονική κίνηση.

Με την εμφάνιση των social media μπορούμε να μιλήσουμε για μια νέα εποχή στις μεθόδους επιτήρησης της καθημερινότητας από τους μηχανισμούς της κυριαρχίας. Τα social media έφεραν μια τεράστια αλλαγή: όλο και περισσότεροι άνθρωποι ξεκίνησαν να χρησιμοποιούν το ίντερνετ. Δε το χρησιμοποιούν απλά, αλλά οικειοθελώς εκθέτουν πληροφορίες για τη ζωή τους και μάλιστα συνδεδεμένοι σε 24ωρη βάση. Πριν από μερικές δεκαετίες μόνο σε (δυστοπικά) μυθιστορήματα επιστημονικής φαντασίας θα μπορούσε να αποτυπωθεί αυτός ο βαθμός έκθεσης του ατόμου και η διαφάνεια της καθημερινής ζωής.



Από τον έλεγχο της πληροφορίας στον κοινωνικό έλεγχο

Το διαδίκτυο εισήλθε στην κοινωνική ζωή πολύ απότομα και μέσα σε πολύ μικρό χρονικό διάστημα κρίθηκε απαραίτητο για πολλές πτυχές της. Από την επαγγελματική δραστηριότητα μέχρι την επικοινωνία μεταξύ οικείων προσώπων οι νέες ψηφιακές τεχνολογίες προσέφεραν νέες δυνατότητες (για παράδειγμα άμεση επικοινωνία μέσω μηνυμάτων) και οι δυνατότητες αυτές μετεξελίχθηκαν σταδιακά σε κοινωνικές ανάγκες.

Από τη δεκαετία του 90 μέχρι σήμερα, τα πρώτα βήματα στο διαδίκτυο ήταν η χρήση μιας μηχανής αναζήτησης ή/και email. Σήμερα, θεωρείται αυτονόητη η δημιουργία τουλάχιστον ενός λογαριασμού σε κάποια υπηρεσία social media. Αν και το διαδίκτυο κοντεύει τα 30 χρόνια ζωής, παραμένει αρκετά νέο και πολύπλοκο στη συνείδηση του κόσμου. Λόγω της φύσης του, δυσκολευόμαστε να έχουμε ουσιαστική γνώση για τον τρόπο λειτουργίας μιας ιστοσελίδας ή υπηρεσίας που χρησιμοποιούμε. Στον πραγματικό κόσμο, αν για παράδειγμα θέλουμε να στείλουμε ένα γράμμα θα πάμε στο ταχυδρομείο. Με την επίσκεψή μας στο ταχυδρομείο, δεν μπορούμε να γνωρίζουμε όλη τη διαδικασία και τα ενδιάμεσα στάδια που χρειάζεται ένα γράμμα για να φτάσει από εμάς στην παραλήπτρια. Παρόλ' αυτά, έχουμε μια γενική ιδέα για την διαδικασία που ακολουθείται. Στον ψηφιακό κόσμο, δεν έχουμε την παραμικρή ιδέα για το πώς λειτουργεί για παράδειγμα η αποστολή email, τι εξοπλισμός χρειάζεται, ποια είναι η δομή που επιτρέπει την αποστολή (πώς δομείται ένα email, τι είναι ο mail server, πως επικοινωνούν μεταξύ τους οι mail servers, κλπ). Για να στείλουμε ένα email δε χρειάζεται να πάμε στο ταχυδρομείο, το στέλνουμε από την άνεση του σπιτιού μας.

Τεράστιος όγκος πληροφοριών και δεδομένων που αφορούν τους χρήστες του παγκόσμιου ιστού διακινείται μέσα σε αυτό το απέραντο δίκτυο, εγείροντας αυτόματα ένα σημαντικό ζήτημα. Ποιοι μπορούν να έχουν πρόσβαση σε αυτές τις πληροφορίες και πως ακριβώς τις χρησιμοποιούν; Σε ατομικό επίπεδο θυσιάζουμε την ψηφιακή μας ανωνυμία και ιδιωτικότητα με αντάλλαγμα την ευκολία που προσφέρουν τα εταιρικά μέσα, τα οποία διατείνονται πως προσφέρουν λύσεις για να ικανοποιήσουν τις "ψηφιακές μας ανάγκες".

Όλες μας οι ενέργειες στο διαδίκτυο, οι πληροφορίες που εμείς οι ίδιοι απλόχερα εκθέτουμε δημοσιεύοντας προτιμήσεις, πολιτικές απόψεις, στοιχεία ταυτότητας, σε συνδυασμό με ερωτή-

ματα σε μηχανές αναζήτησης, πλοήγηση σε διαδραστικούς χαρτες, επιλογές μουσικής[9], όλα αυτά συνθέτουν ένα σχεδόν μοναδικό προφίλ για το άτομό μας. Ένας αλγόριθμος που αναπτύχθηκε και χρησιμοποιήθηκε σε έρευνα πανεπιστημίων και διέθετε πρόσβαση στα likes των χρηστών, παρήγαγε τα ακόλουθα εντυπωσιακά αποτελέσματα: με 10 likes ο αλγόριθμος μπορούσε να γνωρίζει για την χρήστρια περισσότερα από όσα γνωρίζει ένας συνάδελφος της, με 150 περισσότερα από τους γονείς και με 300 likes αποκτούσε καλύτερη επίγνωση της προσωπικότητάς της από ό,τι ο-η σύζυγός της[10].

Όσα δεδομένα παράγονται στον ψηφιακό κόσμο των social media καταγράφονται και αποθηκεύονται για άγνωστο σε μας χρόνο, σε ιδιωτικά μηχανήματα εταιριών και υπόκεινται σε επεξεργασία από ειδικούς αλγορίθμους. Με απλά λόγια, στον ψηφιακό κόσμο ξεχάστε το μπάτσο που συλλαμβάνει και μετά δεν θυμάται τι να πει στο δικαστήριο. Κάπου σε κάποιο σκληρό δίσκο, υπάρχουν όλες οι πληροφορίες που έχουν συλλεχθεί για μας - πράγματα που δεν θυμόμαστε καν ότι είδαμε ή κάναμε[11].

Ο άνθρωπος είναι ο "καλύτερος αισθητήρας" δεδομένων. Τη χαρακτηριστική αυτή ιδιότητα της ανθρώπινης φύσης εκμεταλλεύονται οι μηχανισμοί των ψηφιακών μέσων . Παρέχοντας το "τυράκι" της ψηφιακής επιβράβευσης από τους επίσης ψηφιακούς "φίλους", δίνουν συνεχώς νέα κίνητρα ώστε οι χρήστες να παραμένουν online και να παρέχουν περισσότερα δεδομένα για τους ίδιους και τον περίγυρό τους. Αυτό αναπόφευκτα σημαίνει ότι το άτομο προσπαθεί να προβάλλει περισσότερο τον εαυτό του, βρίσκοντας νέο υλικό είτε για αναδημοσίευση είτε για πρωταρχική δημοσίευση, ψηφιοποιώντας όλο και περισσότερες εμπειρίες, επιθυμίες και αναλύ-

9. https://www.techworld.com/picture-gallery/social-media/what-facebook-knows-about-you-3656948/
10. https://www.nytimes.com/2015/01/20/science/facebook-knows-you-better-than-anyone-else.html
11. Οι υπεύθυνες εταιρίες σε γενικές γραμμές δίνουν αόριστες απαντήσεις για αυτό το θέμα, όπως "Μετά την διαγραφή τους από τον χρήστη, τα δεδομένα κρατούνται για κάποιο διάστημα στους servers μας". https://www.cbsnews.com/news/ok-youve-deleted-facebook-but-is-your-data-still-out-there/

σεις, εκθέτοντας κάθε φορά ηθελημένα ή όχι, κομμάτια της προσωπικότητάς του.

Η ψευδαίσθηση της ιδιωτικής επικοινωνίας, μιας και συνδεόμαστε και επικοινωνούμε μέσα από τις συσκευές μας και συνήθως στο χώρο μας, τις περισσότερες φορές οδηγεί στην έκθεση πληροφοριών που μπορεί να μη χρειαζόταν ή να μην έπρεπε να δημοσιευθούν. Φαινομενικά αθώα παιχνίδια ή κουίζ, δημοσίευση προσωπικών απόψεων ή ακόμη και το ρουφιανο-tagάρισμα, που σημαίνει ταίριασμα προσώπων με ονόματα σε δημόσιες φωτογραφίες, αν και εκ πρώτης όψης ασύνδετα, στοχεύουν στην άντληση όλο και περισσότερων δεδομένων που μπορούν να αποθηκευτούν και να επεξεργαστούν όταν έρθει η κατάλληλη στιγμή. Είτε για τη διαφήμιση ενός νέου προϊόντος είτε για την παροχή πληροφοριών στους μπάτσους, όταν αυτό ζητηθεί. Έτσι, τα παραδοσιακά μοντέλα επιτήρησης τείνουν να αντικατασταθούν πλέον από την αυτοέκθεση του ατόμου, δηλαδή της εκούσιας προβολής του εαυτού μας.

Μέσα σε αυτές τις συνθήκες, υπάρχει η άποψη ότι χρησιμοποιώντας προφίλ με ψευδή στοιχεία, όπως η φωτογραφία και το ονοματεπώνυμο, επιτυγχάνεται η ψηφιακή ανωνυμία. Πρόκειται για μια ακόμη ψευδαίσθηση μιας και οι χρήστες που επιλέγουν αυτή την οδό, μπορεί να καταφέρνουν να ξεγελάσουν άλλους χρήστες της πλατφόρμας, όχι όμως και την ίδια την πλατφόρμα/εταιρία, η οποία είναι σε θέση να γνωρίζει και να συνδυάζει στοιχεία για την ταυτοποίηση του ατόμου. Μεταδεδομένα όπως η φυσική τοποθεσία από την οποία γίνεται η σύνδεση, τα άλλα προφίλ χρηστών με τα οποία υπάρχει επικοινωνία, το περιεχόμενο των μηνυμάτων που ανταλλάσσονται εντός της πλατφόρμας και άλλα πολλά, μπορούν να διασταυρωθούν και να εξάγουν ένα ακριβέστατο προσωπικό, ψυχολογικό και κοινωνικό προφίλ[12].

Εκτός όμως από τους ενεργούς χρήστες, άτομα, ομαδοποιήσεις και συλλογικότητες που επιλέγουν να μην χρησιμοποιούν τα παραπάνω μέσα, μπορεί να εκτεθούν από τα άτομα που τα χρησιμοποιούν. Αυτό μπορεί να συμβεί με αναφορές ατόμων σε posts ή tag-αρισμα φωτογραφιών στα social media, επικοινωνία μέσω email -πχ. μεταξύ espiv και gmail- που ουσιαστικά παρεμβάλλει μια εταιρία στην συνομιλία, η οποία και μπορεί να διαβάσει το περιεχόμενο των μηνυμάτων. Η διαρροή των προσωπικών δεδομένων δεν εξαρτάται μόνο από το κάθε άτομο ξεχωριστά, αλλά και από το περιβάλλον του. Όταν μιλάμε για 2 δισεκατομμύρια συνδεδεμένων σε social media, πολύ σύντομα θα μπορεί να είναι ύποπτο κάποια να μην διαθέτει προφίλ σ' αυτά - κάτι που συμβαίνει ήδη με τα κινητά τηλέφωνα. Άλλωστε, ο όρος "ghost profile" ή προφίλ-φάντασμα περιγράφει ακριβώς τα προφίλ που έχουν φτιαχτεί για άτομα που δεν συμμετέχουν σε κάποιο social media. Το ίδιο το facebook έχει παραδεχτεί πρόσφατα ότι παρακολουθεί ανθρώπους που δεν έχουν καν λογαριασμό στο μέσο[13].

Μπορούμε τελικά να ισχυριστούμε ότι πάνω στα μέσα κοινωνικής δικτύωσης χτίζονται τα νέα μέσα κοινωνικού ελέγχου.

---

12. https://www.schneier.com/blog/archives/2018/07/identifying_peo_8.html
13. https://tech.slashdot.org/story/18/04/17/2157248/facebook-admits-to-tracking-users-non-users-off-site

Το ψηφιακό χρυσωρυχείο

Τα social media έχουν συγκεντρώσει σε μεγάλο βαθμό την καθημερινή επικοινωνία, την ενημέρωση και την ψυχαγωγία. Αναπτύσσονται από τεράστιες πολυεθνικές εταιρίες, που μέσα σε λίγα χρόνια έχουν βρεθεί στην κορυφή των οικονομικών δυνάμεων παγκοσμίως, δαπανώντας τεράστια ποσά για να κάνουν τα μέσα αυτά εύκολα στη χρήση και απαραίτητα στην καθημερινότητα των ανθρώπων[14].

Η εκτεταμένη συλλογή δεδομένων σε υπηρεσίες όπως τα social media εκτείνεται πολύ περισσότερο από την απλή καταγραφή διαλόγων και κλασσικών μεταδεδομένων (π.χ. ημερομηνία/ώρα που κάποιος συνδέθηκε/αντάλλαξε κάποιο μήνυμα). Στο Facebook για παράδειγμα δεν καταγράφονται/αναλύονται μόνο οι διάλογοι ενός χρήστη αλλά καταγράφονται και πληροφορίες[15] που σε εμάς περνάνε απαρατήρητες. Πληροφορίες όπως πόση ώρα κοίταξε κάποιος ένα post ή μια διαφήμιση μέχρι να κάνει scroll στην επόμενη, πόση ώρα είχε το ποντίκι πάνω από το κουμπί like, πόσο συχνά τείνει να αποφεύγει posts διαφόρων χρηστών κλπ[16]. Αντίστοιχα τα κινητά τηλέφωνα προσπαθούν να συλλέγουν τον μέγιστο αριθμό πληροφορίας για τη ζωή ενός ανθρώπου. Ποιές εφαρμογές χρησιμοποιεί πιο συχνά, τι ώρα ξυπνάει και πάει στη δουλειά, τι διαδρομή ακολουθεί, ποια μέρη επισκέπτεται[17], τι αναζητεί στο internet. Τα κινητά φαίνεται να μπορούν να χτίσουν ένα προφίλ χιλιάδες φορές πιο αναλυτικό από αυτό που θα έχτιζε ο πιο κο-

14. https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/
15. Εδώ αξίζει μια μικρή παρένθεση για να αναφέρουμε ότι τα εταιρικά μέσα δεν έχουν δημόσιο αρχείο των αναρτήσεων/πληροριών, όπως πχ ένα site. Επομένως, είναι δύσκολο να ανατρέξεις σε παλιότερες δημοσιεύσεις (συνήθως πρέπει να κάνεις scroll μέχρι να πάθεις τενοντίτιδα). Φυσικά οι ίδιες οι πλατφόρμες έχουν πλήρη πρόσβαση σε όλα τα δεδομένα και μάλιστα σε βολική μορφή για επιπλέον επεξεργασία.
16. https://techcrunch.com/2015/06/12/facebook-now-cares-about-how-long-you-look-at-stuff-in-your-news-feed/
17. https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy

ντινός φίλος μας. Υπάρχουν εκατοντάδες διαφημιστικές -και μη- εταιρίες η οποίες μέσω διαφόρων tracking cookies ή στην περίπτωση των social media κουμπιών για like/retweet μπορούν να καταγράφουν χωρίς να το ξέρουμε ποια site επισκεπτόμαστε και πότε.

Αντιλαμβανόμαστε λοιπόν ότι υπάρχει τεράστιο ενδιαφέρον από πολλές εταιρίες για συλλογή πληροφοριών σχετικά με τις συνήθειες μας και την καθημερινότητά μας. Η πληροφορία έχει μετατραπεί σε ένα σύγχρονο ψηφιακό χρυσό, και αποτελεί την κύρια μορφή εσόδων για τις περισσότερες από τις εταιρίες που παρέχουν "δωρεάν" υπηρεσίες. Με τον ίδιο τρόπο που διάφορα καταστήματα καταγράφουν και πωλούν πληροφορίες για εμάς και τις συνήθειες μας (π.χ κάρτα μέλους super market) με αντάλλαγμα μηδαμινές εκπτώσεις, οι εταιρίες παροχής "δωρεάν" ηλεκτρονικών υπηρεσιών μετατρέπουν τον ψηφιακό χρυσό σε κανονικό χρήμα πουλώντας τεράστιο όγκο πληροφορίας σχετικά με εμάς, τις συνήθειες μας καθώς και συμπεράσματα σχετικά με αυτές. Οποιοσδήποτε έχει μια επαφή με τον χώρο της τεχνολογίας θα έχει αντιληφθεί ότι την τελευταία δεκαετία (τουλάχιστον) οι όροι data mining[18] και data analytics[19] σε διάφορα πεδία (από ηλεκτρονικές υπηρεσίες μέχρι το δίκτυο) είναι σε αυξανόμενη ζήτηση και χρησιμοποιούνται όλο και πιο συχνά.

Τα social media καθώς και άλλες δημοφιλείς διαδικτυακές υπηρεσίες συνήθως διατίθενται "δωρεάν". Εδώ διαπιστώνουμε ακόμα μια ψευδαίσθηση γύρω από το διαδίκτυο και τη δομή του. Αν γνωρίζαμε το κόστος του εξοπλισμού, της συντήρησης και της 24ωρης λειτουργίας μιας υπηρεσίας "δωρεάν" email ή μιας μηχανής αναζήτησης, ειδικά όταν παρέχονται από μια εταιρία, θα μας έκανε μεγάλη εντύπωση αυτό το δωρεάν. Αυτό που οφείλουμε να κατανοήσουμε είναι ότι οι υπηρεσίες αυτές δεν είναι δωρεάν, αλλά έχουν προπληρωθεί και με το παραπάνω με την εμπορική αξία των προσωπικών μας δεδομένων.

Περιγράφοντας ένα μικρό κομμάτι του παγόβουνου που ονομάζεται επιτήρηση και συλλογή δεδομένων στο internet, αντιλαμβανόμαστε για ποιο λόγο αυτός ο τεράστιος όγκος πληροφοριών αποτελεί χρυσάφι για πολλές εταιρίες: σε μια καπιταλιστική κοινωνία τέτοιου είδους πληροφορίες βοηθούν τις εταιρίες να δημιουργήσουν και να εξελίξουν εμπορικά προϊόντα τα οποία είναι εγγυημένο ότι θα αγοραστούν και θα καταναλωθούν. Το εμπόρευμα που προσφέρουν οι πλατφόρμες αυτές είναι τα δεδομένα που παράγουν οι χρήστες τους. Τα δεδομένα αυτά ορίζουν την αξία της κάθε μίας απ' αυτές τις εταιρίες και χρησιμοποιούνται κυρίως για να προβάλλονται εξατομικευμένες διαφημίσεις σε κάθε χρήστρια ή για να μεταπωλούνται πανάκριβα σε άλλες οντότητες, εταιρικές ή κρατικές[20]. Πάγια τακτική αυτών των εταιριών είναι η εξαγορά αντίστοιχων μικρότερων ώστε να αποκτήσουν τον έλεγχο περισσότερων δεδομένων και να μεγιστοποιήσουν την εμπορική αξία τους (για παράδειγμα η εξαγορά του WhatsApp και του Instagram από το Facebook). Αυτή η συγκεντροποίηση έχει ως αποτέλεσμα τη δημιουργία μιας τεχνολογικής αλλά και οικονομικής ολιγαρχίας.

---

18. Data mining ονομάζεται η επεξεργασία μεγάλου όγκου δεδομένων ώστε να βρεθούν μοτίβα και ανωμαλίες σε αυτά και στη συνέχεια τα δεδομένα να κατηγοριοποιηθούν αντίστοιχα

19. Data analytics ονομάζεται η ανάλυση ενός όγκου δεδομένων με σκοπό να εξαχθούν συμπεράσματα και χρήσιμες πληροφορίες. Για παράδειγμα μπορεί μια Facebook να εξάγει το συμπέρασμα ότι τις ώρες πριν το μεσημεριανό, μεγάλο ποσοστό ανθρώπων κοιτάζει το Facebook και με βάσει αυτό να σας βγάζει περισσότερες ειδοποιήσεις

20. https://www.independent.co.uk/voices/facebook-data-scandal-free-products-sheryl-sandberg-a8294006.html

Έλεγχος του διαδικτύου

λογοκρισία και καταστολή

Η διεθνής φήμη και δύναμη τέτοιων "δωρεάν" υπηρεσιών και social media σε συνδυασμό με τη μηδαμινή ελευθερία λόγου που υπάρχει σε διάφορα κράτη, ήταν οι λόγοι που αυτές οι πλατφόρμες "επικοινωνίας" αλλά και το ίδιο το internet θεωρήθηκαν από πολλούς ως τα νέα "επαναστατικά" εργαλεία για την ανατροπή κυβερνήσεων. Εργαλεία που δοκιμάστηκαν και φτάσανε πολύ γρήγορα στα όριά τους σε διάφορες εξεγέρσεις όπως για παράδειγμα στην Αίγυπτο, τη Συρία, τη Λιβύη κ.α. Εκεί, στο ξεκίνημα των εξεγέρσεων αναζητήθηκαν ασφαλείς τρόποι επικοινωνίας και οι κοινωνικές ομάδες στράφηκαν σε εφαρμογές instant messaging (π.χ WhatsApp) ή και σε πλατφόρμες social media (Facebook, Twitter) ώστε να παρακάμψουν τη λογοκρισία αλλά και την παρακολούθηση. Δυστυχώς όμως, όπως αναφέραμε και στο ιστορικό κομμάτι, το internet και οι υπολογιστές δεν είναι κάτι που ξεπήδησε από τα χαμηλά κοινωνικά στρώματα με σκοπό την απελευθέρωση του κόσμου. Η υποδομή όλων αυτών συνεχίζει να βρίσκεται έξω από τον έλεγχό μας. Και αυτό αποδείχτηκε περίτρανα όταν μέσα σε μία νύχτα (στις 27/1/2011) η κυβέρνηση της Αιγύπτου αφού αντιλήφθηκε ότι πολλοί από τους διαδηλωτές χρησιμοποιούσαν το internet και ηλεκτρονικές πλατφόρμες "επικοινωνίας" για να οργανωθούν, αποφάσισε να κλείσει κυριολεκτικά το internet στη χώρα, διαλύοντας κυριολεκτικά το επιχείρημα περί επαναστατικού internet. Κίνηση στην οποία φαίνεται να αρέσκονται αρκετά τα αυταρχικά καθεστώτα προκειμένου να ξεπεράσουν επικίνδυνες για αυτά καταστάσεις[21].

Ακόμα και σε κράτη που θεωρούνται πιο δημοκρατικά, τα social media και ο όγκος της πληροφορίας που διακινείται σε αυτά χρησιμοποιούνται από την αστυνομία και τις σχετικές υπηρεσίες με σκοπό την καταστολή, την πρόβλεψη εγκλημάτων[22] αλλά και το χτίσιμο κοινωνικών γράφων ώστε να βρεθούν πιθανές συσχετίσεις μεταξύ ατόμων[23] και γεγονότων. Συγκεκριμένα, η ανάλυση της κανονικότητας στα social media (αν δηλαδή η χρήση είναι αυτή που η αστυ-

21. https://en.wikipedia.org/wiki/Internet_censorship_in_the_Arab_Spring https://www.independent.co.uk/news/world/asia/facebook-twitter-whatsapp-turkey-erdogan-blocked-opposition-leaders-arrested-a7396831.html Στην Αραβική Άνοιξη συγκεκριμένα, μετά τον αρχικό ενθουσιασμό κυκλοφόρησε έντυπη καμπάνια που προωθούσε άλλους τρόπους επικοινωνίας και συνιστούσε τη χρήση των social media για παραπλανητικούς σκοπούς.

22. https://www.idgconnect.com/abstract/22489/how-technology-helping-law-enforcement-predict-crime

23. Το Palantir είναι ένα μόνο από τα πολλά εργαλεία αυτού του είδους: https://www.bloomberg.com/features/2018-palantir-peter-thiel/

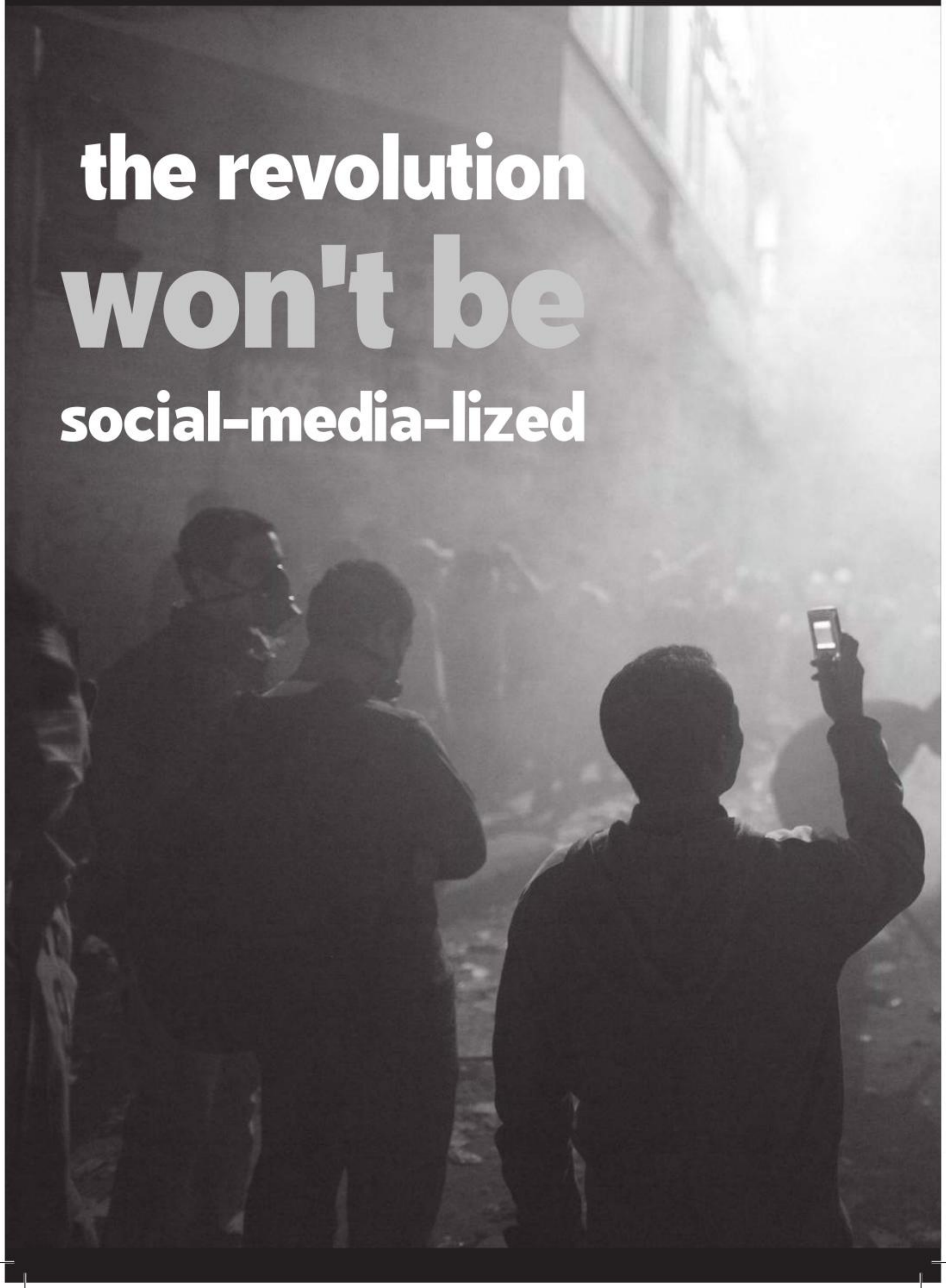
νομία/κράτος/επιχειρήσεις θεωρούν ως "φυσιολογική"/καθημερινή) αποτελεί νέο ερευνητικό πεδίο για την αστυνομία αλλά και τις διάφορες μυστικές υπηρεσίες κρατών με στόχο να προλάβουν και να καταστείλουν όσο πιο γρήγορα γίνεται πιθανές παρεκκλίσεις. Πέραν αυτών των "εξωτικών" ερευνητικών πεδίων data analytics, οι old school άρσεις απορρήτου συνομιλιών σε τέτοιες πλατφόρμες είναι ακόμα μια "βαρετή καθημερινότητα" για τις εταιρίες αυτές.

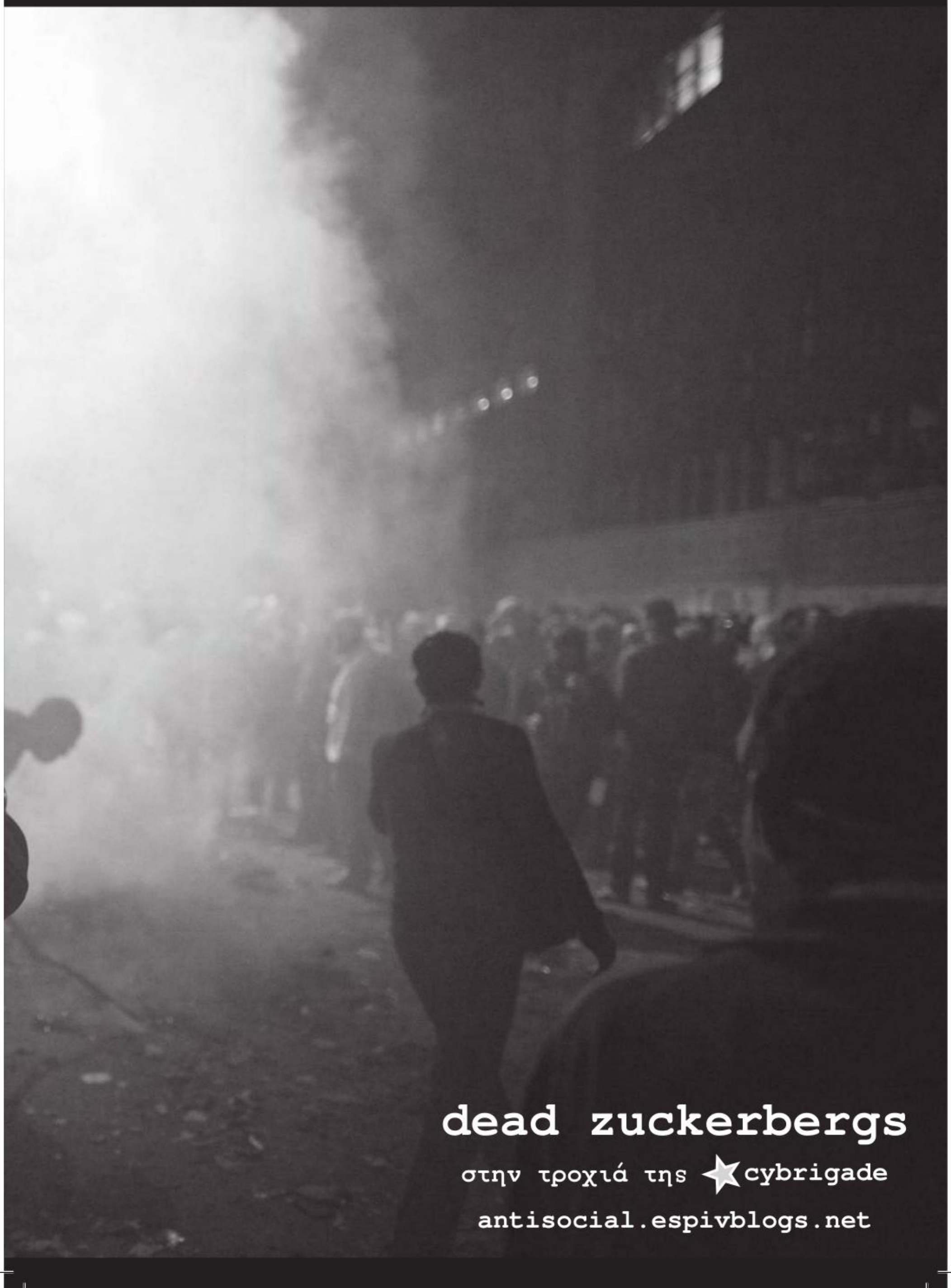
Και στις περιπτώσεις που οι εταιρίες μας ενημερώνουν ότι οι συνομιλίες μας είναι κρυπτογραφημένες, δε θα πρέπει να ξεχνάμε πως παραμένουν έξω από τον έλεγχό μας και άρα δεν μπορούμε να γνωρίζουμε αν οι εταιρίες έχουν και αυτές τα κλειδιά αποκρυπτογράφησης των συνομιλιών (για "νομικούς λόγους) ή αν κάποια μέρα χωρίς κάποια ενημέρωση αυτή η κρυπτογράφηση των συνομιλιών μας σταματήσει μετά από αίτημα των αρχών[24]. Η ευκολία με την οποία τόσο μεγάλες εταιρίες συνεργάζονται με τις αρχές θα έπρεπε να μας διαλύει οποιαδήποτε μορφή αυταπάτης. Το Facebook για παράδειγμα, έχει παραδεχτεί ότι σε μόνιμη βάση διαβάζει τις συνομιλίες[25] με σκοπό να προλάβει την τέλεση αξιόποινων πράξεων.

Κατά καιρούς το Facebook ή η Google (στο YouTube) έχει κλείσει λογαριασμούς ανθρώπων για πολιτικά ανεπίτρεπτες χρήσεις. Ας μην ξεχνάμε την "περίφημη" υπόθεση του "Γέροντα Παστίτσιου" που έκλεισε ο λογαριασμός του και συνελήφθη (αφού το Facebook έδωσε τα στοιχεία του κατόχου). Επιπλέον, κατά καιρούς έχουμε δει σε διάφορες δίκες (στο εξωτερικό αλλά και εδώ) πως τα social media και τα κινητά χρησιμοποιούνται για την εξαγωγή κοινωνικών γράφων και το χτίσιμο ενός "ιστού" γνωριμιών, ώστε να τεθούν και άλλοι άνθρωποι υπό παρακολούθηση ή ακόμα και να χρησιμοποιηθεί ως επιχείρημα εναντίον κάποιου κατηγορούμενου (έχουμε δει άλλωστε πολλάκις ότι το με ποιον συνομιλεί κάποιος μπορεί να αποτελέσει άτυπο ποινικό αδίκημα ή ενοχοποιητικό στοιχείο). Τέτοια στοιχεία για τον περίγυρό μας δίνουμε μέσα από τις εικονικές φιλίες, από το βιβλίο διευθύνσεων-επαφών, από τη συμμετοχή σε ομάδες συζητήσεων ("κλειστές" ή ανοιχτές) στα social media ή ακόμα και από τη δημόσια στήριξη ομάδων/προσώπων/απόψεων. Αυτές οι ενέργειες συμπληρώνουν αρκετά καλά το παζλ των ατομικών προφίλ.

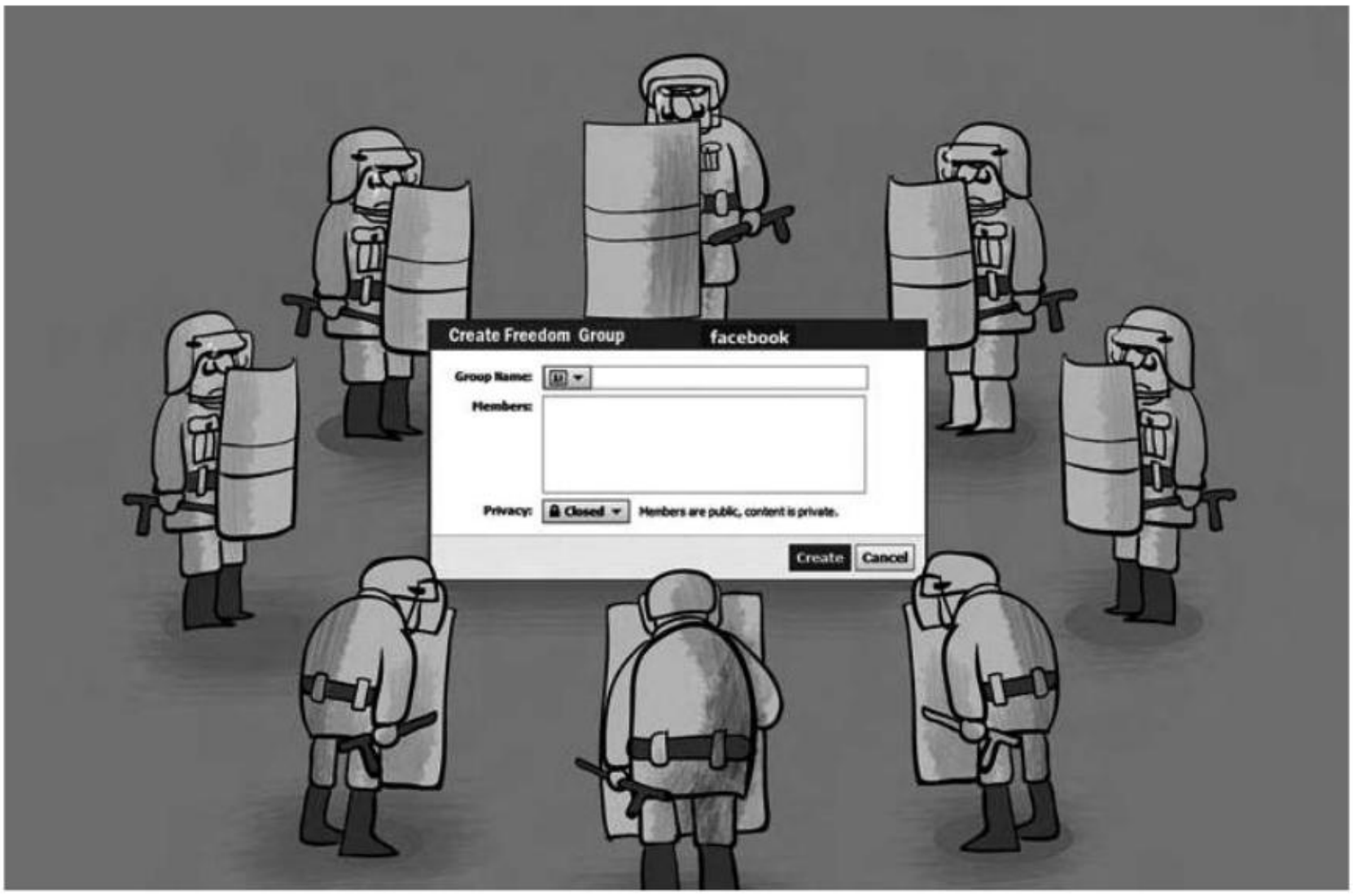
Και αν πριν κάτι χρόνια κάτι χιουμοριστικό και αθώο όπως το αστείο με το "Γέροντα Παστίτσιο" θεωρήθηκε αξιόποινο και ύποπτο, ποιος μπορεί να μας διαβεβαιώσει ότι κάτι για το οποίο συζητάμε εμείς τώρα δεν είναι εξίσου ύποπτο και άξιο καταγραφής και φακελώματος; Οι χιλιάδες άρσεις απορρήτου συνομιλιών κινητής τηλεφωνίας με πρόσχημα την τρομοκρατία[26] καθώς και οι αποκαλύψεις Snowden περί παρακολουθήσεων σε μαζικό παγκόσμιο επίπεδο απαντούν ξεκάθαρα στο παραπάνω ερώτημα. Συγκεκριμένα, με τις αποκαλύψεις του Snowden, μάθαμε για μυστικά projects μαζικής παρακολούθησης των μυστικών υπηρεσιών, όπως το Prism, που στόχευαν σε ευρύ φάσμα ψηφιακών και μη επικοινωνιών και μάλιστα σε παγκόσμια κλίμακα. Γίνονται σε καθημερινή βάση, αφορούν όλο τον πληθυσμό ανεξαιρέτως και παρακάμπτουν ακόμη και την αστική νομιμότητα (ένταλμα, εισαγγελική παραγγελία κλπ). Είναι σε αγαστή συνεργασία με παρόχους τηλεπικοινωνιών για να έχουν πρόσβαση στην υποδομή του internet αλλά και με εταιρείες παροχής υπηρεσιών όπως η Microsoft ώστε να έχουν πρόσβαση στις υπηρεσίες

24. https://tech.slashdot.org/story/18/12/06/0358200/australia-passes-anti-encryption-laws-update
25. https://www.cnet.com/news/facebook-scans-chats-and-posts-for-criminal-activity/
26. http://www.enet.gr/?i=news.el.article&id=160538


the revolution
won't be
social-media-lized


dead zuckerbergs
στην τροχιά της cybrigade
antisocial.espivblogs.net

τους. Σε μερικές περιπτώσεις, τέτοια προγράμματα αποκτούν πρόσβαση χωρίς τη συγκατάθεση των παρόχων/εταιριών, όπως έκανε το Echelon ήδη από τη δεκαετία του 60, υποκλέπτοντας δεδομένα από τους τηλεπικοινωνιακούς δορυφόρους. Υπάρχουν όμως και πολλά ακόμη που, ενίοτε, είναι και πιο στοχευμένα. Μία άλλη υπηρεσία, το Palantir, συλλέγει δεδομένα από διάφορα social media και δείχνει όλες τις διασυνδέσεις ενός ατόμου. Ίσως το πιο ανησυχητικό είναι ότι οι εταιρικές πλατφόρμες συχνά συνεργάζονται στενά με τους μπάτσους και παρέχουν απλόχερα οποιαδήποτε πληροφορία ζητηθεί. Τέτοιου είδους αιτήματα αποτελούν πολύ συχνό φαινόμενο για μεγάλες εταιρίες όπως Google, Facebook κλπ.



Φιλτράρισμα και απομόνωση της πληροφορίας

Όλα όσα είπαμε παραπάνω αποδεικνύουν ότι η εκτενής χρήση των social media αποτελεί πεδίο ενδιαφέροντος για την αστυνομία, η οποία συχνά πυκνά συνεργάζεται με τους παρόχους τέτοιων υπηρεσιών. Ταυτόχρονα, σε περίπτωση που η χρήση αυτών των μέσων είναι άλλη από την "επιτρεπτή", τα κράτη μπορούν να κλείσουν εντελώς το διακόπτη και να διακόψουν τη λειτουργία τους, όπως έγινε για παράδειγμα στην Αίγυπτο. Είδαμε ήδη όμως ότι η πληροφορία σε τόσο μεγάλο όγκο είναι ψηφιακός χρυσός καθώς πέραν του ότι μπορεί να χρησιμοποιηθεί για να παράξει νέα προϊόντα, μπορεί να χρησιμοποιηθεί για κοινωνικό έλεγχο και καταστολή. Αυτό το τελευταίο για μια εταιρία κολοσσό τύπου Facebook μεταφράζεται σε πολλαπλάσια κέρδη από την απλή πώληση προϊόντων. Γιατί αν κάτι διαφαίνεται τα τελευταία χρόνια, είναι ότι αυτές οι εταιρίες δεν ενδιαφέρονται μόνο για "ουδέτερο" εμπορικό κέρδος, αλλά αρέσκονται να λερώνουν τα χέρια τους και με πιο βρώμικα παιχνίδια που σχετίζονται με την καταστολή και τον κοινωνικό έλεγχο γενικότερα. Για το θέμα του κοινωνικού ελέγχου συγκεκριμένα, ο ιδρυτής του Facebook κατά καιρούς έχει προβεί σε δηλώσεις με τις οποίες δύσκολα μπορεί να κρύψει τα οράματά του. Οράματα που ξεκινούν από το γεγονός ότι πολύ μεγάλος όγκος καθημερινής ενημέρωσης γίνεται μέσω Facebook και άρα το ίδιο θα πρέπει να φιλτράρει με τεχνητή νοημοσύνη αυτές τις πληροφορίες ώστε να περιορίζεται ο αριθμός των fake news και φτάνουν σε υποσχέσεις για χτίσιμο κλειστών κοινοτήτων και χρήση του Facebook ως πλατφόρμα για πολιτικές καμπάνιες και εκλογές[27].

Το γεγονός ότι τα social media και ειδικά το Facebook και το Twitter χρησιμοποιούνται για καθημερινή ενημέρωση έχει ανοίξει μια μεγάλη πόρτα-ευκαιρία παραπληροφόρησης σε επιτήδειους να ανεβάζουν σωρηδόν ψεύτικες ειδήσεις. Αυτό έχει ως αποτέλεσμα μεγάλο αριθμό ψευδών ειδήσεων καθημερινά. Από ειδήσεις που μπορεί να συνέβησαν πριν 10 χρόνια και να παρουσιάζονται ως σημερινές, μέχρι ειδήσεις τελείως φανταστικές που δημοσιεύτηκαν από κάποιον και μέσω πολλαπλών share έφτασαν να θεωρούνται πραγματικά γεγονότα. Η ανάμειξη του Facebook στην καταπολέμηση αυτού του φαινομένου εκ πρώτης όψεως μπορεί να φαντάζει θετική. Στην πραγματικότητα όμως θα έπρεπε να μας προβληματίζει πως μια εταιρία σαν το

27. https://arstechnica.com/staff/2017/02/op-ed-mark-zuckerbergs-manifesto-is-a-political-trainwreck/

Facebook σκοπεύει να "φιλτράρει" κάτι τέτοιο. Ειδικά όταν έγγραφα που έχουν κατά καιρούς διαρρεύσει από το Facebook δείχνουν πως οι κανόνες του τι είναι αποδεκτό και τι όχι ευνοούν κυβερνήσεις και επιχειρήσεις κολοσσούς και περιορίζουν εθνικές μειονότητες και ακτιβιστές[28]. Το ίδιο μπορούμε να πούμε και για πλατφόρμες όπως το Twitter ή το YouTube που κατά καιρούς έχουν κλείσει λογαριασμούς ακτιβιστών. Ακόμα όμως κι όταν το Facebook δεν ασχολείται με το φιλτράρισμα ειδήσεων ή με ακτιβιστές, ο τρόπος λειτουργίας του φιλτράρει συνεχώς το τι βλέπουμε σαν περιεχόμενο καθώς και το από ποιους το βλέπουμε. Το λεγόμενο ranking system του Facebook βαθμολογεί την "προτεραιότητα" που έχει κάποιο post με βάση τις συνήθειές μας και συμπεραίνει για το αν και πόσο ψηλά πρέπει να μας το εμφανίσει. Συνεπώς ακόμα κι αν κάποιος έχει την ψευδαίσθηση ότι μπορεί να ενημερώνεται από τέτοιες πλατφόρμες, τα δεδομένα[29] δείχνουν το αντίθετο[30]. Μπορεί να υπάρχουν πραγματικά σημαντικά νέα που "φίλοι" μας να μοιράζονται, τα οποία να φιλτράρονται από το Facebook και να μη μας εμφανίζονται ποτέ ή να μας εμφανιστούν πολλές μέρες μετά. Αυτός είναι και ένας πολύ "ενδιαφέρον" τρόπος να φιμώνεις ανθρώπους σε μια πλατφόρμα που ευαγγελίζεται την επικοινωνία και το μοίρασμα ειδήσεων. Μειώνοντας σε βαθμολογία τις ειδήσεις τους -επειδή ίσως μπορεί να μη συμφωνούν με το όραμα για ένα χαρούμενο Facebook χωρίς εντάσεις, μπορεί η πλατφόρμα να εξαφανίσει φωνές "δημοκρατικά" χωρίς να τους στερήσει την πρόσβαση. Η χρησιμότητα του ελέγχου αυτού του ψηφιακού χρυσού όμως δεν αρκείται στο απλό φιλτράρισμα των ειδήσεων που φτάνουν στα μάτια μας. Οι αλγόριθμοι αυτών των πλατφορμών όπως είπαμε και παραπάνω ελέγχουν ανά πάσα στιγμή το πόση ώρα διαβάζουμε μια είδηση ενώ την ίδια στιγμή προσπαθούν να συμπεράνουν το αν μας αρέσει. Με βάση αυτά τα συμπεράσματα (και άλλα πολλά) λειτουργούν αυτοί οι "ουδέτεροι" αλγόριθμοι φιλτραρίσματος τους οποίους δυστυχώς πολλοί αγνοούν όταν επιχειρηματολογούν υπέρ της χρήσης social media με το επιχείρημα ότι "οποιοσδήποτε μπορεί να γίνει πομπός μιας είδησης". Φυσικά μπορεί, αρκεί να πληρεί κάποια "κριτήρια"... Αυτή η πολιτική φιλτραρίσματος πληροφοριών πέραν της "διακριτικής" καταστολής που επιβάλει, προσπαθεί να μας κρατήσει "χαρούμενους χρήστες" ώστε να συνεχίσουμε να χρησιμοποιούμε την πλατφόρμα. Δεν πάνε πολλά χρόνια άλλωστε που ένα άλλο έγγραφο σχετικά με το πως το Facebook και ο τρόπος και η σειρά με την οποία εμφανίζει ειδήσεις μπορεί να ελέγξει και να διαμορφώσει τα συναισθήματα των χρηστών βγήκε στην επιφάνεια[31].

---

28. https://arstechnica.com/tech-policy/2017/06/facebooks-opaque-censorship-policy-means-some-attacks-are-ok-others-arent/
29. http://www.niemanlab.org/2017/12/how-much-news-makes-it-into-peoples-facebook-feeds-our-experiment-suggests-not-much/
30. https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles
31. https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds

Τεχνολογία διαμόρφωσης απόψεων

Αν λοιπόν εταιρίες σαν το Facebook μπορούν (και το κάνουν) να μαντέψουν και να διαμορφώσουν τη διάθεση μας, αυτό σημαίνει πως μπορούν ίσως να επηρεάσουν και τον τρόπο που σκεφτόμαστε; Μια μηχανή που μπορεί να συμπεράνει (επειδή εμείς το προσφέρουμε) σχεδόν τα πάντα για εμάς και μπορεί να ανακαλύψει καλύτερα από εμάς και να διαμορφώσει τα συναισθήματά μας, τι άλλο μπορεί να κάνει άραγε; Από ότι φαίνεται μπορεί να αλλάξει μέχρι και τον τρόπο που σκεφτόμαστε εξαπατώντας μας σταδιακά με σκοπό να μας μεταπείσει για διάφορες απόψεις μας. Το σκάνδαλο Facebook-Cambridge Analytica[32] είναι ίσως η πιο μεγάλη απόδειξη του γιατί αυτός ο τεράστιος όγκος πληροφοριών που μαζεύουν πλατφόρμες σαν τα social media είναι αληθινός χρυσός για τον μαζικό κοινωνικό έλεγχο. Συγκεκριμένα με αφορμή ένα κουίζ από τα χιλιάδες που κυκλοφορούν στο Facebook, από το 2014 η εταιρία Cambridge Analytica απέκτησε πρόσβαση στις προτιμήσεις 87 εκατομμυρίων χρηστών και των φίλων τους (μέσω ενός bug). Αυτός ο όγκος πληροφορίας χρησιμοποιήθηκε στην κατασκευή και κατάταξη των χρηστών σε ψυχολογικά προφίλ και στην αξιολόγηση των πολιτικών τους πεποιθήσεων. Στη συνέχεια μέσω χρήσης στοχευμένων διαφημίσεων, ψεύτικων προφίλ και ειδήσεων η εταιρία προσέφερε τις υπηρεσίες στις σε διάφορα πολιτικά γραφεία με σκοπό τη χειραγώγηση του κοινού. Οι μέχρι τώρα πληροφορίες κάνουν λόγο για χρήση στις καμπάνιες για την εκλογή του Trump, το δημοψήφισμα του Brexit και τις Μεξικανικές εκλογές. Όλα αυτά δεν θα έπρεπε να μας εκπλήσσουν. Υπάρχει ολόκληρος επιστημονικός κλάδος που μελετά το λεγόμενο Persuasive Technology το πως δηλαδή η τεχνολογία μπορεί να χρησιμοποιηθεί για να διαμορφώσει αντιλήψεις και συνειδήσεις. "Ευαγγελιστές" αυτού του κλάδου έχουν εμπλακεί σε πολλές εφαρμογές αυτού του επιστημονικού πεδίου πάνω στη χρήση των κινητών τηλεφώνων και το πως μπορούν να μας εθίσουν στη χρήση τους αλλά και να αλλάξουν τον τρόπο με τον οποίο ζούμε καθημερινά[33].

32. https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far

33. Ένα πολύ απλό "παβλοφιανό" παράδειγμα της εφαρμογής του Persuasive Technology είναι τα διάφορα "δώρα" που μπορεί να κερδίζει κανείς όταν καθημερινά κάνει log in σε κάποια εφαρμογή. Αυτή η τακτική δίνει τη συνήθεια της επιβράβευσης μέσω της οποίας ο χρήστης "εκπαιδεύεται" με αυτόν τον τρόπο στο να χρησιμοποιεί όλο και πιο συχνά την εφαρμογή. Ένα άλλο παράδειγμα είναι ότι μεγάλες εταιρίες κάνουν αποτρεπτικά δύσκολες και με πολλά βήματα (κλικ επιβεβαίωσης), επιλογές που οφείλουν να παρέχουν όπως διαγραφή λογαριασμού κ.α. όπως παρουσιαζεται εδώ: https://gizmodo.com/facebook-google-and-microsoft-use-design-to-trick-you-1827168534

Αυτό που πρέπει να κρατήσουμε εδώ, είναι ότι πλέον υπάρχουν ξεκάθαρες αποδείξεις ότι η τεχνολογία και τα social media δεν είναι απλά ουδέτερες υπηρεσίες που φτιαχτήκαν για το καλό της ανθρωπότητας αλλά εργαλεία που χρησιμοποιούνται καθημερινά για να καταστείλουν οποιονδήποτε μπορεί να σκέφτεται "επικίνδυνα" και ταυτόχρονα να ασκήσουν αόρατο κοινωνικό έλεγχο με συγκεκριμένα πολιτικά και κερδοσκοπικά οφέλη.

Κίνα: η κοινωνική μηχανική ως "παιχνίδι" επιβράβευσης-τιμωρίας

Κι αν το παράδειγμα με το σκάνδαλο της Cambridge Analytica δε φαίνεται αρκετά τρομακτικό, το Social Credit System[34] που σκοπεύει η κυβέρνηση της Κίνας να εφαρμόσει ολοκληρωτικά και υποχρεωτικά για όλους κάπου στο 2020 θα μπορούσε εύκολα να γίνει best seller δυστοπικό μυθιστόρημα. Το σύστημα αυτό λειτουργεί μέσω του ολοκληρωτικού ελέγχου από την κυβέρνηση των εταιριών που φτιάχνουν τις πιο διάσημες ηλεκτρονικές υπηρεσίες στην Κίνα. Τέτοιες υπηρεσίες είναι η πλατφόρμα ηλεκτρονικών αγορών, η πλατφόρμα instant messaging και social media καθώς τα πιο γνωστά ηλεκτρονικά παιχνίδια σε συνδυασμό με το γεγονός ότι όλη η υποδομή του internet στην Κίνα φιλτράρεται από την κυβέρνηση. Θα αποτελεί ένα σύστημα αξιολόγησης με πόντους όλων των κατοίκων της Κίνας, με βάση το οποίο θα επιβραβεύεται (έξτρα πόντοι) ή θα τιμωρείται (μείωση πόντων) κάποιος αναλόγως το πόσο καλά φαίνεται να τηρεί το κοινωνικό προφίλ που η κινέζικη κυβέρνηση θέλει να επιβάλει. Αν για παράδειγμα κάποιος παίζει συχνά ηλεκτρονικά παιχνίδια αυτό σημαίνει πως είναι τεμπέλης και άρα θα μειωθούν οι πόντοι του σε αντίθεση με κάποιον που έχει παιδί και αγοράζει πάνες που σημαίνει πως πιθανότατα είναι ένας καλός υπεύθυνος γονιός οπότε θα έχει αύξηση πόντων. Η έκταση αυτού του συστήματος δεν μένει μόνο στις συνήθειες του ατόμου αλλά και στις συναναστροφές του. Δεν έχει και πολλή σημασία λοιπόν αν ο προαναφερθείς "υπεύθυνος γονιός" αγοράζει πάνες για το παιδί εφόσον την ίδια στιγμή συναναστρέφεται (μιλάει ή έχει φίλους στα social media) ανθρώπους με "κακή φήμη" που μπορεί να εκδηλώνουν αρνητική άποψη για την κυβέρνηση. Με αυτόν τον τρόπο δεν ασκείται έλεγχος στις συνήθειες ενός ανθρώπου αλλά και στις συναναστροφές του επιβάλλοντας έτσι έναν -μεταμοντέρνο θα λέγαμε- εξοστρακισμό. Για να επιβληθεί αυτό το point system όμως δεν αρκεί η προσθαφαίρεση εικονικών πόντων αλλά και η υλική του πραγμάτωση. Κάποιος με χαμηλό αριθμό πόντων λοιπόν θα υποστεί χαμηλές ταχύτητες στο internet, επιπλέον γραφειοκρατία για απλές υπηρεσίες, αποκλεισμό από καλά ξενοδοχεία, αποκλεισμό των παιδιών του από σχολεία που θεωρούνται καλά[35], διαπόμπευση σε δημόσιες λίστες κακών πολιτών, αποκλεισμό από θέσεις εργασίας που θεωρούνται καλές μέχρι και απαγόρευση χρήσης

34. https://en.wikipedia.org/wiki/Social_Credit_System
https://media.ccc.de/v/34c3-8874-gamified_control

35. https://yro.slashdot.org/story/18/07/16/1515254/a-student-was-rejected-by-a-college-because-of-chinas-social-credit-system

ΜΜΜ και απαγόρευση εξόδου από την χώρα[36]. Αντίστοιχα κάποιος με υψηλό σκορ θα φαίνεται πιο ψηλά σε υπηρεσίες online dating, θα έχει φθηνότερους λογαριασμούς, θα μπορεί να νοικιάζει χωρίς να προπληρώνει και θα έχει καλύτερα επιτόκια από τις τράπεζες. Σε αντίθεση με τους (συνήθως) λιγότερο ορατούς τρόπους καταστολής και κοινωνικού ελέγχου που είδαμε να συμβαίνει στα "δημοκρατικά δυτικά κράτη", και την οφθαλμοφανή καταστολή που κάποια αυταρχικά καθεστώτα κατά καιρούς έχουν εφαρμόσει όταν η χρήση των ηλεκτρονικών υπηρεσιών ξεφεύγει του "φυσιολογικού", το Social Credit System είναι το απόλυτο παράδειγμα εξόφθαλμης καταστολής και κοινωνικού ελέγχου μέσω του λεγόμενου gamification[37] που μπορεί να ασκήσει κάποιος που έχει έλεγχο του internet αλλά και των ηλεκτρονικών υπηρεσιών[38]. Η Κίνα σε γενικές γραμμές είναι πρωτοπόρα στη χρήση της τεχνολογίας για την επιβολή της τάξης και των ρυθμών ζωής που το κράτος θέλει να επιβάλλει στους πολίτες σε σημεία που αγγίζουν οργουελιανά σενάρια.

36. Το συγκεκριμένο μέτρο απαγόρευσης ταξιδιών ήδη εφαρμόζεται και έχει ακυρώσει πτήσεις ανθρώπων 11 εκατομμύρια φορές και διαδρομές με το τρένο 4 εκατομμύρια φορές: http://uk.businessinsider.com/china-social-credit-system-blocked-people-taking-flights-train-trips-2018-5

37. Η παρουσίαση ενός συστήματος με όρους που θυμίζουν κάποιο παιχνίδι. Μια πλατφόρμα σχεδιασμένη να μοιάζει με ηλεκτρονικό παιχνίδι που χρησιμοποιεί επιβράβευση με πόντους και "αγγαρείες" είναι ένα παράδειγμα gamification

38. Ένα παράδειγμα ενός παρόμοιου gamified συστήματος με πόντους που μοιάζει υπερβολικά στο σύστημα της Κίνας που αποδεικνύει το πως μπορούν συνήθειες και κοινωνικοί αποκλεισμοί να επιβληθούν παρουσιάζεται στη σειρά "επιστημονικής φαντασίας"(?) Black Mirror στο επεισόδιο Nosedive (https://en.wikipedia.org/wiki/Nosedive)

Παράρτημα 1

Πώς συλλέγονται τα δεδομένα;

Για να επιτευχθεί η συλλογή όλων αυτών των δεδομένων, έχει αναπτυχθεί και επιστρατευτεί μια **πληθώρα υπηρεσιών, ιστοσελίδων και συσκευών**.

Μηχανές αναζήτησης: Για κάθε μας αναζήτηση, οι εταιρίες που παρέχουν την υπηρεσία, αποθηκεύουν τις επερωτήσεις που κάνουμε, από ποιες σελίδες ήρθαμε και ποιες σελίδες επισκεφτήκαμε μετά, μοναδικά στοιχεία της σύνδεσής μας για να μας αναγνωρίσουν σε μελλοντικές συνδέσεις. Τελικά συνδυάζουν τα νέα δεδομένα με το προφίλ που ήδη έχουν για εμάς.

email: Σε αντάλλαγμα της δωρεάν υπηρεσίας email οι χρήστες δίνουμε στις εταιρίες την άδεια να διαβάσουν την αλληλογραφία μας, εξάγοντας πληροφορίες για εμάς και τους ανθρώπους που επικοινωνούμε. Από τα μεταδεδομένα των μηνυμάτων, δηλαδή τους παραλήπτες, την ώρα αποστολής, τη συχνότητα που επικοινωνούμε με το κάθε άτομο, την ώρα που συνδεόμαστε στο email, τι θεωρούμε spam και ποιο περιεχόμενο μας τραβάει περισσότερο την προσοχή, κλπ. – οι εταιρίες συμπληρώνουν το προφίλ μας, χτίζουν το κοινωνικό μας κύκλο και μαθαίνουν τις καθημερινές μας συνήθειες, πότε εργαζόμαστε, πότε κοιμόμαστε, πότε είμαστε σπίτι κ.ο.κ.

maps (χάρτες): Εφαρμογές χαρτών και πλοήγησης μαθαίνουν πού, πώς και πότε κινούμαστε, τα καθημερινά μας δρομολόγια, τις περιοχές που βγαίνουμε, που παρκάρουμε κλπ. . Με αυτά τα δεδομένα οι εταιρίες πίσω από τους χάρτες μπορούν να κατασκευάσουν μοτίβα κίνησης και συμπεριφοράς ξεκινώντας από μεμονωμένα άτομα και φτάνοντας στο επίπεδο του πληθυσμού μιας ολόκληρης πόλης ή χώρας. Μπορεί να μας φαίνεται "βολικό" όταν το google maps μας ενημερώνει για μποτιλιάρισμα στο δρόμο, όμως οι πληροφορίες για τις (μετα)κινήσεις του πλήθους είναι σίγουρα εξίσου πολύτιμες για τον έλεγχό του (πχ αστυνομία).

smartphones: Ίσως η χειρότερη μέχρι τώρα έκφανση εργαλείου κοινωνικού ελέγχου, είναι τα κινητά τηλέφωνα γενικά και τα smartphones ειδικά. Όλα τα κινητά τηλέφωνα, χρειάζονται κάποιον πάροχο τηλεφωνίας για να λειτουργήσουν. Οι πάροχοι αυτοί, έχουν τυπικά πρόσβαση σε όλα τα δεδομένα τηλεφωνίας. Εκτός από το περιεχόμενο των συνομιλιών, το πότε και με ποια άτομα συνομιλούμε), γνωρίζουν ανά πάσα στιγμή και την τοποθεσία μας. Μάλιστα οι πάροχοι τηλεφωνίας υποχρεούνται από την ελληνική νομοθεσία να διατηρούν για 1 χρόνο όλα τα metadata τηλεφωνίας (όλα τα χαρακτηριστικά μιας κλήσης εκτός από το περιεχόμενο: ποιός τηλεφώνησε, πότε, σε ποιο γεωγραφικό σημείο). Την τελευταία δεκαετία τα smartphones έχουν κάνει την κατάσταση ακόμα πιο πολύπλοκη για τους χρήστες. Εκτός από τηλέφωνο, παρέχουν πρόσβαση στο διαδίκτυο, έχουν κάμερα, μικρόφωνο, και διάφορους ακόμη αισθητήρες. Όλα τα παραπάνω σκιαγραφούν ένα πολύ εχθρικό περιβάλλον, για μία μόνο συσκευή, που αν

ήταν άνθρωπος θα την ονομάζαμε ρουφιάνο. Παρόλα αυτά την κουβαλάμε πάντα μαζί μας και περνάμε πολύ χρόνο χρησιμοποιώντας την.

Social media και κινητό τηλέφωνο: Η δυνατότητα πρόσβασης στο internet και τα social media από τα κινητά τηλέφωνα, πρακτικά ορίζει την online παρουσία των χρηστών σε 24ωρη βάση. Εκτός από το περιεχόμενο που δημοσιεύουμε, βλέπουμε ή προωθούμε, μεταδεδομένα όπως η τοποθεσία από την οποία γίνεται η σύνδεση γίνονται πλέον ορατά μέσω του κινητού. Τα smartphones δίνουν ακόμα σημαντικές πληροφορίες που προκύπτουν από τη μη χρήση τους: αφού το κινητό είναι ανενεργό (ή είναι ενεργό αλλά χωρίς δραστηριότητα) για μεγάλο διάστημα, μπορεί να σημαίνει π.χ. ότι κοιμόμαστε, εργαζόμαστε ή οδηγούμε. Το κινητό λοιπόν προδίδει ακόμη περισσότερα στοιχεία για τις δραστηριότητές μας, τα οποία συνδυάζονται με επίσημα στοιχεία που έχουμε δώσει οικειοθελώς. Εξάλλου μέσω της κάρτας SIM ο πάροχος τηλεφωνίας διαθέτει τα πλήρη στοιχεία μας.

mobile apps: Οι εφαρμογές των λεγόμενων "έξυπνων" τηλεφώνων, κατά την εγκατάσταση, ζητάνε την άδεια μας ώστε να έχουν πρόσβαση στα προσωπικά μας αρχεία, την κάμερα, το μικρόφωνο ή ακόμα και στην γεωγραφική μας θέση μέσω του ενσωματωμένου gps τους. Αυτό μπορεί πριν λίγα χρόνια να μας φαινόταν αδιανόητο, παρόλα αυτά συναινούμε καθημερινά στις απαιτήσεις των εφαρμογών αυτών ώστε να μπορούμε να χρησιμοποιήσουμε τις "δωρεάν" υπηρεσίες τους. Στον αντίποδα, υπάρχουν εμπορικά apps που διαφημίζονται ως ασφαλή καθώς παρέχουν από άκρη σε άκρη κρυπτογράφηση των μηνυμάτων[1]. Δεν είναι όμως μόνο το ίδιο το περιεχόμενο της συνομιλίας που έχει σημασία. Τα μεταδεδομένα της επικοινωνίας μας είναι εξίσου πολύτιμα ως προϊόν, όπως έχουμε προηγουμένως περιγράψει.

Παράρτημα 2: Άλλες σημειώσεις

Cookies: Τα cookies έχουν τρεις βασικές χρήσεις:

1. Διαχείριση session (της σύνδεσης δηλαδή σε μια ιστοσελίδα)
2. εξατομίκευση ιστοσελίδας (προτιμήσεις όπως πχ αλλαγή χρώματος background σε μια ιστοσελίδα)
3. tracking (παρακολούθηση)

Οι πρώτες δυο κατηγορίες συνήθως είναι βασικές για κάποιες λειτουργικότητες μιας ιστοσελίδας, ενώ το tracking είναι το προβληματικό.

Περισσότερα: https://en.wikipedia.org/wiki/HTTP_cookie#Tracking

Κρυπτογράφηση: όταν μιλάμε για κρυπτογράφηση, το βασικότερο σημείο είναι η εμπιστοσύνη. Στον ψηφιακό κόσμο η κρυπτογράφηση γίνεται συνήθως με ζεύγη κλειδιών. Αν μια υπηρεσία προσφέρει κρυπτογράφηση ενώ κρατάει η ίδια τα κλειδιά, υπάρχει σοβαρό πρόβλημα εμπιστοσύνης. Επίσης δεν ξέρουμε πως υλοποιείται η κρυπτογράφηση, αν δεν είναι δηλαδή ανοικτού κώδικα, τότε πάλι δεν είναι εμπιστοσύνης.

Κοινωνικός γράφος: Διάγραμμα που απεικονίζει το δίκτυο συσχετισμών και προσωπικών σχέσεων μεταξύ ανθρώπων.

1. https://www.bestvpn.com/guides/signal-private-messenger

Παράρτημα 3

Σενάριο με τεχνικές λεπτομέρειες

Έχουμε ήδη τονίσει το πόσο σημαντική είναι η χρήση ελεύθερου λογισμικού εν γένει και ειδικά όταν μας απασχολεί η ιδιωτικότητά μας. Θα εξετάσουμε μια υποθετική περίπτωση που θέλουμε να αναρτήσουμε ένα κείμενο ανώνυμα στο διαδίκτυο, που έχει συνοδευτικά αρχεία εικόνας ή βίντεο. Παραθέτουμε τα βασικά σημεία προσοχής:

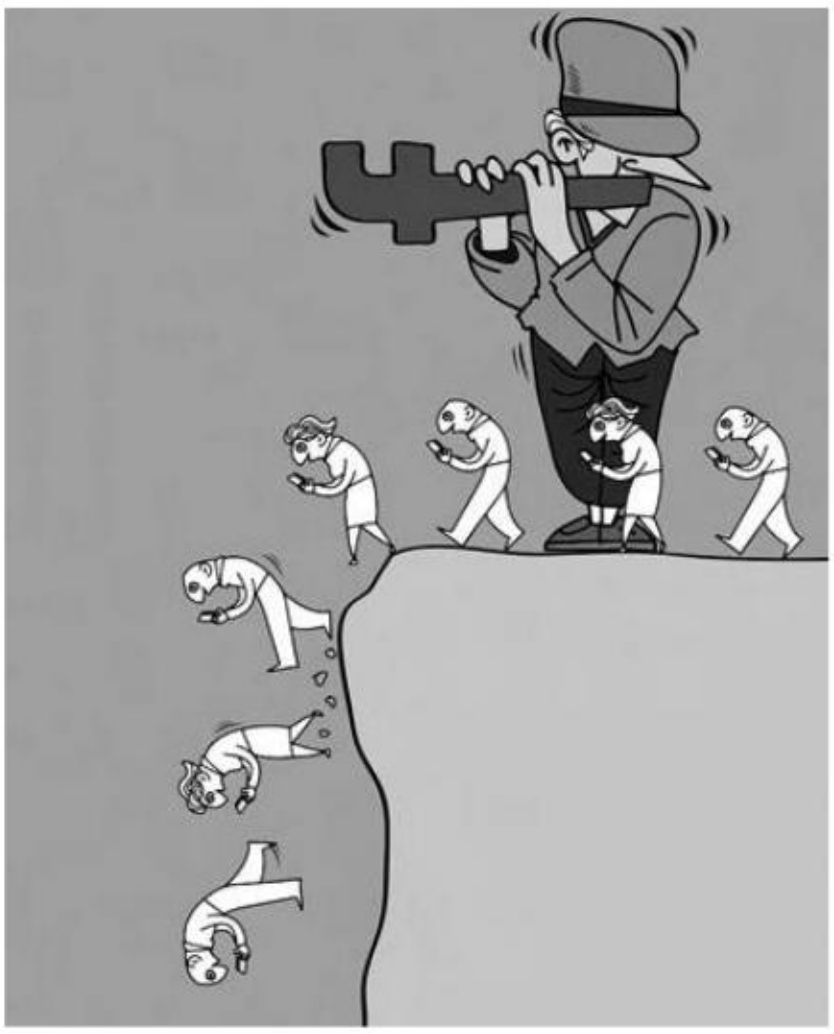
- **IP address:** Η ηλεκτρονική διεύθυνση της συσκευής που χρησιμοποιούμε. Αυτή είναι μοναδική. Υπάρχει η εσωτερική ενός δικτύου και η εξωτερική. Πχ στο οικιακό δίκτυο, υπάρχει μία εξωτερική IP, αυτή που μας δίνει ο πάροχος, και αντιστοιχεί στο ρούτερ μας, και πολλές εσωτερικές, που δίνει το ρούτερ στις διάφορες συσκευές. Στο διαδίκτυο, όλες οι συσκευές εμφανίζονται με την εξωτερική IP, για την οποία ο πάροχος ξέρει ανά πάσα στιγμή σε ποιο άτομο αντιστοιχεί, οπότε είναι επώνυμο στοιχείο.
- **MAC address:** κάθε κάρτα δικτύου έχει μια μοναδική MAC address, έτσι ώστε να μπορεί να αντιστοιχεί μια IP address σε αυτή. Τις MAC addresses τις ορίζουν οι κατασκευαστές hardware, οπότε σε περίπτωση που τους ζητηθεί, μπορούν να αντιστοιχήσουν μια MAC address σε πχ ένα laptop, και μετά αυτό το laptop να βρεθεί που πουλήθηκε, οπότε πάλι προκύπτει ένα επώνυμο στοιχείο.
- **Metadata:** πολλή συζήτηση γίνεται για τα metadata, τις πληροφορίες που συνοδεύουν ένα αρχείο, μια ηλεκτρονική επικοινωνία, και γενικά όλες τις κινήσεις στον ψηφιακό κόσμο. Εδώ θα μας απασχολήσουν κυρίως τα metadata των αρχείων που θα επισυνάπταμε. Όλα τα αρχεία περιέχουν ημερομηνία δημοσίευσης/τροποποίησης, στοχεία του δημιουργού (όνομα χρήστη υπολογιστή, το πρόγραμμα που τα δημιούργησε). Φωτογραφίες τραβηγμένες από εμάς, περιέχουν τα στοιχεία της φωτογραφικής κάμερας ή του κινητού), πιθανά γεωγραφικά στοιχεία για το που τραβήχτηκε, κλπ κλπ. Επίσης είναι δυνατό να προσθέσουμε παραπάνω μετα-δεδομένα σε ένα αρχείο. Συχνά το συναντάμε σε αρχεία μουσικής, που περιέχουν την ιστοσελίδα που δημοσιεύτηκαν πρώτη φορά. Είναι προφανές ότι για ανώνυμη δημοσίευση, χρειάζεται να καθαριστούν όλα αυτά.
- **Κρύψιμο προσώπων σε φωτογραφίες:** Ένα ακόμη σημείο που θέλει προσοχή, είναι το κρύψιμο προσώπων αλλά και χαρακτηριστικών (πχ μια ιδιαίτερη μπλούζα) σε φωτογραφίες πριν ανεβούν. Ο καλύτερος τρόπος είναι να αφαιρούμε τελείως την πληροφορία σβηνοντας τα πρόσωπα τελείως και μετά να βάζουμε κάτι από πάνω για να μην είναι creepy. Χρησιμοποιώντας μόνο 1 φίλτρο, θεωρητικά μπορεί να αντιστραφεί η διαδικασία. Ειδικά για ανέβασμα μεγάλου αρχείου όπως ένα βίντεο, θέλει προσοχή γιατί είναι μια κίνηση που μπορεί να ανιχνευθεί, ακόμη και αν έχουμε χρησιμοποιήσει το δίκτυο tor. Το δίκτυο tor αποκρύπτει από τον πάροχό μας τι κάνουμε, Δείχνει όμως ότι το κάνουμε μέσω του tor. Σε τέτοια περίπτωση, καλό είναι να χρησιμοποιήσουμε ένα μη επώνυμο δίκτυο (όχι από το σπίτι δηλαδή).
- **Παράλληλη χρήση άλλων υπηρεσιών:** Μεγάλος κίνδυνος είναι η παράλληλη χρήση άλλων υπηρεσιών τη στιγμή που θέλουμε να κάνουμε κάτι ανώνυμα. Και εδώ υπάρχουν τεχνικές που μπορούν να βρουν από την επώνυμη χρήση μας, τι κάναμε ανώνυμα.

Είναι πολλά τα σημεία που μπορεί να μας προδώσουν. Ο καλύτερος τρόπος είναι η χρήση της Linux διανομής Tails (https://tails.boum.org), και η σωστή επιλογή του σημείου που θα συνδεθούμε στο διαδίκτυο. Αυτά καλύπτουν όλα τα παραπάνω, εκτός από το καθάρισμα των metadata. Και εδώ όμως χρειάζεται μεγάλη προσοχή και σωστή ενημέρωση πριν τα χρησιμοποιήσετε.


dead zuckerbergs
στην τροχιά της cybrigade


the revolution
won't be
social-media-lized
antisocial.espivblogs.net

Επίλογος



Σε αυτή την έκδοση προσπαθήσαμε να αποτυπώσουμε κάποιους προβληματισμούς με αφετηρία την χρήση των social media στην καθημερινότητα και στην κινηματική δράση συντροφισσών και συντρόφων. Επιχειρήσαμε να περιγράψουμε κάποια από τα βασικά τους τεχνικά χαρακτηριστικά, τα οποία είναι εν πολλοίς κοινά και τα οποία θεωρούμε ότι συνιστούν μια σημαντική εξέλιξη στην χρήση του ίντερνετ και στο πως αυτό επιδρά στην καθημερινότητα μας. Αν φυσικά τα χρησιμοποιούμε. Προσπαθήσαμε επίσης να αποδομήσουμε κάποιες από τις πιο κοινές αυταπάτες γύρω από τη χρήση τους και τις δυνατότητες που δίνουν στην επικοινωνία.

Ωστόσο, όπως αναφέραμε και στην αρχή, το ζήτημα έχει πολλές διαστάσεις και μέσα από τις συζητήσεις που κάναμε το διάστημα μέχρι αυτή την έκδοση βρεθήκαμε να μιλάμε για πράγματα όλο και λιγότερο τεχνικά, με ή χωρίς εισαγωγικά. Η τεχνολογία γενικότερα και το ίντερνετ ειδικότερα, έχουν μπει για τα καλά στις ζωές μας και μια συζήτηση που δεν θα μιλά για την κοινωνική, ψυχολογική και πολιτική τους διάσταση είναι τουλάχιστο ελλιπής.

Σκοπεύουμε σε μια επόμενη έκδοση να μπορέσουμε να μιλήσουμε για αυτά, και να έχουμε μια πιο ολοκληρωμένη ανάλυση και κριτική. Αυτός είναι και ένας από τους λόγους που επιλέξαμε, προς το παρόν, να μην κάνουμε συγκεκριμένες αντι-προτάσεις, αν και η χρήση μη εμπορευματικών, κινηματικών υποδομών, όπου αυτές υπάρχουν, είναι για εμάς αυτονόητη.

dead zuckerbergs (στην τροχιά της cybrigade)
12/2018

// dead zuckerbergs [στην τροχιά της cybrigade] //
// antisocial@espiv.net — antisocial.espivblogs.net //