Luiss Guido Carli

Dipartimento di Scienze Politiche

Cattedra: Sociologia della Comunicazione

“La zona d’ombra della democrazia post-moderna”

La manipolazione di massa tra tecnologie avanzate, big-data e algoritmi

Prof. Sorice

Relatore

Pantellini Lorenzo, matr. 0844772

Candidato

Anno Accademico 2019/2020

Alla mia Comunità Militante,
manipolo di fratelli, vigili sotto la bandiera che insieme difendiamo,
fautori della persona che sono oggi, fiaccole nell'oscurità
che indicano la strada, nel solco della Giustizia e della Verità.

A mio nonno Giorgio,
che venuto a mancare all'inizio del mio percorso universitario,
avrei voluto presente in questi giorni nei quali ne sto completando la prima parte,
terminando la laurea triennale.
Consapevole e mai dubitante di averlo al mio fianco,
proseguo il mio corso di studi anche nel suo nome, così come ho portato a termine questo primo ciclo.

Ringrazio:

I miei genitori,
per i loro preziosi e vitali consigli di fronte ad ogni mia scelta di vita,
per il sostegno totale che mi assicurano davanti a ogni difficoltà,
per l'amore che nutrono e quotidianamente coltivano verso la mia persona,
per l'interesse, e mai il rifiuto, nei confronti di ciò che abbraccio
e di ciò in cui credo.

La mia Amica Agata,
che più che un'amica, definirei sorella.
Una persona per cui trovo difficilissimo trovare qua delle parole,
per le tante che già le ho dedicato in questi tre anni, al termine dei quali
non sarei mai giunto senza di lei… o con te o con nessuno, come si dice.
Al mio fianco nei momenti più belli passati insieme,
fidata spalla in quelli più difficili, luce della luna che illumina le strade di Roma
nelle mille nottate prima degli esami, che nonostante i diversi percorsi magistrali,
non sono certo finite.
Ad maiora, Agi.

Alex e Stefano, amici e compagni di infinite notate.

A Stefano, in particolare, va il mio pensiero nel completare questa tesi,
termine del mio percorso triennale che avrebbe sicuramente voluto vedere,
ringraziandolo per il suo supporto, per i suoi consigli
e per la sua ricchissima compagnia nelle notti di Viale Romania.

Il vostro Lorenzo

INDICE

Introduzione

"Il ministero della Verità (Miniver, in neolingua) differenziava in maniera sorprendente da qualsiasi altro oggetto che la vista potesse discernere. Era un'enorme struttura piramidale di cemento bianco e abbagliante che s'innalzava, terrazza dopo terrazza, fino all'altezza di trecento metri, da dove si trovava Winston era possibile leggere, ben stampati sulla bianca facciata in eleganti caratteri, i tre slogan del partito:
LA GUERRA E'PACE
LA LIBERTA' E'SCHIAVITU'
L'IGNORANZA E'FORZA."

-George Orwell, 1984

E' una serata estiva, fuori il caldo mi costringe a ritardare la mia uscita in centro, e sono al lavoro per portare avanti alcune ricerche riguardanti la tesi che qua si appresta ad essere introdotta. Nel mentre, decido di riempire il vuoto che mi ci circonda mettendo un po' di musica su Spotify, applicazione che ho direttamente scaricato nel computer, e così sarà Hans Zimmer con le sue strepitose colonne sonore a farmi compagnia.
Ad un certo punto, lo schermo del mio cellulare sul tavolo si accende, è la chiamata di un'amica.
Opto per la risposta in vivavoce per continuare a scrivere, ed entrambi affamati, cominciamo a confrontarci su cosa ordinare per cena. Dopo qualche minuto per decidere se mangiare hamburger o meno, la prima opzione perde, e scegliendo qualcos'altro, ordiniamo e chiudo la chiamata.
Intanto, in sottofondo, la playlist di Zimmer è giunta al terzo brano, e secondo il funzionamento dell'applicazione, è il turno della pubblicità: sono passati non più di due minuti da quando ho riattaccato al telefono e la voce dell'inserzione che esce dal computer è McDonald's che mi consiglia i suoi "inconfondibili ed inimitabili hamburger *Crispy McBacon*." Mi stranisco per qualche secondo, ma torno poi tranquillamente al lavoro… dopo tutto è da qualche tempo che i nostri dispositivi ci sono vicini, anzi, sembrerebbero addirittura ascoltarci a dire il vero, assecondandoci nelle decisioni quotidiane. Stasera il mio computer, per esempio, sembrerebbe aver saputo cosa ho ordinato per cena, e nonostante questo, ha cercato comunque di darmi un consiglio in materia… ma che gentile!
Se al lettore che si approccia a questa tesi, nella lettura delle precedenti righe, potrebbe venir voglia di chiudere il documento perché ritenuto frutto di un "complottista" piuttosto che di un "paranoico digitale", non ce ne meraviglieremmo.
Ed è proprio questo il punto che vogliamo andare ad evidenziare, partendo dalla data che oggi segna il calendario.

E'il 2020, l'era della modernità e delle sue invenzioni rivoluzionarie è ben superata, siamo infatti nell'era in cui il soggetto rivoluzionato non è la materia per mano dell'uomo, ma l'uomo per mano di ciò che materia neanche più è. Siamo nella "*quarta rivoluzione industriale":* intelligenza artificiale, tecnologia avanzata e *IOT ("Internet of Things")*. Se in passato l'uomo è riuscito a rivoluzionare limitati aspetti della sua quotidianità, come poteva essere il riuscire a spostarsi più velocemente per mezzo dell'automobile, oggi a variare è lo stesso mondo in cui egli si ritrova a vivere, un oceano informatico e digitale nel quale è catapultato e da cui sembra non trovare via d'uscita. Dal mondo reale, tangibile, autentico della materia e dei contatti personali fra individui, oggi si è proiettati nel campo di studio entro il quale questa tesi intende andare ad indagare: il "*cyber-space",* il mondo del web, il mare magnum dei miliardi di click al secondo, dell'infinità dei dati in cui ogni persona è "*internauta".*

La navigazione nel web, i profili Facebook, i miliardi di mail quotidianamente inviate da una parte del pianeta all'altra, l'incalcolabile numero di click che ogni secondo decretano una qualsiasi decisione di ogni individuo, in due parole, i *"Big-Data"*. La portata della rivoluzione, che quotidianamente avanza, in cui oggi l'uomo vive non ha eguali nella storia, superata è addirittura anche la digitalizzazione in sé: oggi è la *"datizzazione"* di ogni aspetto della vita, quest'infinito fiume di informazioni, a rappresentare l'energia che traina lo stesso mondo intero, la cui "fonte di vita" (di profitto?) è l'uomo stesso. Dall'inevitabile proiezione nel web di ogni sua azione, pensiero, emozione e volontà, derivano dati. Ma a chi servono? Chi riesce a controllare una tale mole di informazioni? A che scopo? Nel "*cyber-space",* gli individui stessi (gli *"internauti"*) rappresentano la principale, nonché vitale, risorsa primaria di quelle potenze che, come analizzeremo, sono definite *"cyber-lobbies"*: multinazionali, immense aziende e giganti digitali nell'ambito informatico che detengono il monopolio nel mercato dei *"Big-data",* essendo essi stessi gli unici raccoglitori di quest'ultimi, scopo per il quale sono nati e per cui, secondo la seguente tesi, detentori del reale potere nell'era del sovvertimento dell'istituzione meramente politica da parte del processo della digitalizzazione della vita di ogni individuo.

Individuando i quattro ambiti portanti dell'argomento che andremo a trattare, la tesi è divisa in altrettanti capitoli. Il primo, dedicato alla figura dei mass-media, analizzerà l'impatto che la rivoluzione digitale ha avuto sul rapporto tra cittadini, società e potere, nell'era dove le notizie non si ricevono solo all'ora di cena accendendo l'unica televisione della casa, ma ci appaiono autonomamente sullo schermo del telefono che abbiamo in mano. Nel secondo capitolo vedremo il ruolo cruciale dei *"Big-Data"* nella loro funzione di quello che potremmo definire "il nuovo oro" dell'era post-moderna. Dall'attività digitale quotidiana di ogni cittadino, analizzeremo come le *"Cyber-lobbies"* - in primis *Google* - ne sfruttano il potenziale, raccogliendo i dati e trasformandoli in oggetto di scambio nel mercato degli stessi e in risorsa primaria per i giganti dell'ultra-capitalismo. Proseguendo, vedremo come governi ed istituzioni militari possono attuare enormi operazioni di controllo di massa col mezzo dei dati, grazie al progressivo sviluppo della tecnologia,

nonchè come le aziende di cui sopra vi collaborino, ricoprendo ruoli chiave in materia: a tale scopo, abbiamo scelto il prezioso lavoro, nel ruolo *whistleblower* dell'agenzia di sicurezza interna statunitense, di Edward Snowden, che dette vita al *Datagate.* Infine, svilupperemo la scienza della "psicometria" e di come tramite la renderizzazione dei dati sia possibile influenzare le dinamiche socio-politiche, arrivando al principale caso al riguardo: lo scandalo di *Cambridge Analytica* e i dati quali vere e proprie armi in chiave elettorale. I diritti e la privacy dei cittadini, nel tempo in cui la digitalizzazione totale ha fornito nuove armi per l'arsenale delle multinazionali, in chiave consumistica e di profitto, e altrettante fonti di potere e controllo alle istituzioni governative, sono tutt'altro che ben saldi e garantiti rispetto a quanto raccontano le carte costituzionali fondanti delle democrazie odierne. Nuove e ben più potenti forme di *governance* dalle portate planetarie, sembrano avere la possibilità, certamente il potenziale, di sostituirsi alle istituzioni politico-amministrative tradizionali.

L'irresistibile fame di profitto, che ha ormai raggiunto cifre incalcolabili, di queste *"cyber-lobbies"* e la loro fuori uscita da ogni regolamentazione sugli standard di privacy dell'individuo, le ha ormai poste in cima alla piramide del potere nella società dell'ipertecnologia e dei *"big-data"*, arrivando, come vedremo, a superare le sfere più alte delle istituzioni governative. Ma a che costo? Di quali armi predispongono questi nuovi detentori, ormai non più del mero potere politico e decisionale, bensì del controllo della vita umana stessa? Che ruolo ricoprono nei tavoli della *governance*, a partire dagli ambiti dei singoli stati sino alle questioni di portata planetaria? Come piattaforme *"social-network"* quale Facebook, o software di ricerca come *Google*, sono riusciti ad acquisire una posizione di rilievo primario, nel lavoro di ricerca di Servizi Segreti e istituzioni governative? Quanto un sistema fondato sul controllo della quotidianità dell'uomo quale risorsa primaria del potere è compatibile con i principi democratici, sui cui la maggior parte delle istituzioni si fonda e dei quali si dichiara garante? Il mondo parallelo, invisibile, digitale e quindi distaccato dalla realtà, rappresenta il campo di scontro dal quale scaturirà il futuro dell'uomo o la sua fine per come l'abbiamo sempre conosciuto?

Sono questi gli interrogativi che ci siamo posti iniziando ad osservare gli aspetti della realtà in cui quotidianamente siamo immersi ed a cui non molti, troppo pochi a nostro avviso, sembrano fare caso.

E'partendo dalla domanda che almeno ognuno di noi si è posto almeno una volta nella vita che siamo giunti ad analizzare quanto in questa tesi è sostenuto: chi comanda il mondo in cui abitiamo? Chi influenza le decisioni di milioni persone, una volta dimostrato, come vedremo, che è lecito domandarsi se in determinate circostanze esista ancora la "libera scelta"?

Capitolo 1 – Il ruolo dei *mass-media*: la rivoluzione digitale come punto di non ritorno

"Il servo, lavorando, dà al padrone ciò di cui ha bisogno. Il padrone non riesce più a fare a meno del servo. Dunque, la subordinazione si rovescia. Il padrone diviene servo, poiché è strettamente legato al lavoro del servo, mentre il servo diviene il padrone (con la sua attività produttiva) del padrone." [1]

-Hegel, *Fenomenologia dello spirito*

1. La Quarta Rivoluzione Industriale e la sua portata

Allo scopo di indagare il mondo che ci siamo posti di analizzare in questa tesi, inevitabile diviene partire dall'assunto fondamentale per il quale la rivoluzione che ne ha portato la nascita non ha eguali nella storia: è un taglio netto con ogni ordine ad esso preesistente, un punto di non ritorno. Immaginiamo che l'avanzare della tecnica, e del dominio dell'uomo in tale ambito, avesse seguito un percorso ascendente rappresentato dai gradini di una scala condominiale. Nonostante l'innegabile portata delle prime rivoluzioni industriali, dalle quali si svilupparono nuove fonti di energia, nuove risorse, sino alla nascita delle città modernamente intese col massiccio spostamento di massa dalle zone rurali, il cambiamento che registriamo con l'affermarsi della "*Quarta rivoluzione industriale"*, non ha nulla a che fare con i gradini di cui prima: nel giro di un ventennio, è come se fosse stato scalato l'intero Empire State Building. Dai primi anni del 21esimo secolo, nei quali i mercati "*dot.com"* iniziavano ad affermarsi grazie all'uso dei primi computer, non ancora comunque diffusi a livello di massa e limitati fino a quel momento in ambito prettamente militare, siamo giunti, in soli diciannove anni, alla nostra quotidianità di cittadini del 2020, capaci di farci fare un caffè dalla macchinetta, ordinandoglielo col controllo vocale.

1.1 La digitalizzazione e l'uomo: l'*internauta* e la vita *"smart"*

Il coinvolgimento dell'uomo nella sua totalità esistenziale in tale rivoluzione, è ciò che differenzia quest'ultima dalle precedenti: un paradigma è stato ribaltato, ruoli sconvolti, l'individuo stesso proiettato in una dimensione altra. L'era dell'ipertecnologia ha edificato un mondo parallelo rispetto a quello reale fino ad ora conosciuto, nel "*Cyber-space"* l'uomo è *"Internauta",* fluttua costantemente tra i miliardi dati e di input che la tecnica dominante, o per meglio dire, a nostro avviso soffocante, gli imprime e che non sembra più in grado di controllare. La tecnologia, gli schermi degli *smartphone,* i *social-media* sono i diventati il filtro attraverso cui l'individuo del 21esimo secolo guarda una realtà che tale non è più definibile. *"Egli non la "vive", quindi la rende inautentica: la realtà, sostanzialmente, diventa il frutto di una mediazione. La tecnica moderna – che è l'unica ad agire direttamente nel mondo – si «emancipa» dal suo controllo,*

[1] HEGEL G.W.F. (2000), Fenomenologia dello spirito, Armando Editore

diventando sempre più autonoma e governando la natura. Viceversa, l'uomo tecnicizzato – dandosi ai progressi tecnoscientifici per rendere la propria esistenza più godibile – si impigrisce, finchè i ruoli si rovesciano. Esso diventa il servo, rendendosi totalmente dipendente dalla tecnica moderna."[2]

2. Dai *mass media* ai *social media*: il ribaltamento del paradigma e i nuovi poteri

Il binomio da noi preso in considerazione, risiedente nel rapporto tecnica-uomo, ha comportato con l'affermazione del *"Cyber-space"* e della società globalizzata una condizione di totale e crescente dipendenza del secondo fattore – uomo - rispetto al primo – tecnica. In questo capitolo, analizzeremo come il progresso della tecnologia, tramite *mass* media e altre tecniche avanzate, hanno contribuito a creare l'uomo interconnesso, dipendente, a nostro avviso, schiavizzato. Il ribaltamento del paradigma che abbiamo citato nelle righe precedenti, non è altro che il riflesso di tanti e svariati sconvolgimenti di ruoli che gli attori della società odierna hanno subito. Nascenti con la mera funzione informativa, i *mass media*, hanno da sempre occupato un posto di rilievo negli equilibri del potere costituito: è tramite essi, infatti, che le persone vengono a conoscenza di quanto accade nel mondo in cui vivono, dagli ambiti loro più vicini come le notizie locali, sino alle dinamiche di ordine planetario, come può essere una testata di geopolitica internazionale. Tuttavia, dopo l'affermazione della società del consumo, instaurata dall'incontrarsi dell'incremento della produzione a catena, che permetteva alle aziende di offrire una quantità industriale di prodotti alle masse, e l'esplosione dell'economia di profitto che sfruttò a pieno le potenzialità del nuovo fenomeno, la logica economica del mero sostentamento iniziò a svanire. Le enormi potenzialità che un tale sistema offriva ai capitalisti in chiave di profitto, portò all'affermazione di una nuova e necessaria logica che sarebbe dovuta intercorrere tra produttore, prodotto e cliente: il cliente, non avrebbe dovuto semplicemente acquistare il prodotto "*perché necessario"*, bensì lo avrebbe dovuto desiderare "*perché bello, nuovo e alla moda"*, e sempre in maggiori quantità. E'a questo punto che le strategie di marketing e le potenziali entrate delle aziende, diedero vita all'era del consumismo: un fenomeno prettamente moderno, figlio dell'economia di profitto, centrale nella società che ci apprestiamo in questa tesi ad analizzare.

2.1 L'ultra-consumismo ai tempi del *Cyber-space*

Ed è proprio con la "Quarta rivoluzione industriale" che la macchina dell'ultra-capitalismo, la società del consumo sfrenato ed "inevitabile", si afferma in ogni ambito della vita dell'uomo moderno: oggi, con le iper-tecnologie, con la totale connessione globale, nell'era di *Google* e di *Amazon*, possiamo decretare la vittoria totale di queste logiche su quell'uomo ormai perso nei meandri di miliardi di dati, che varia il suo umore quotidiano in base ai "Mi *piace*" ricevuti su *Facebook.* Tramite l'onnipresenza dei *mass media* nella nostra quotidianità, questo sistema è riuscito a sfruttare al massimo le armi che in tale ambito il progresso gli

[2] TENNENINI R. (2019), Schiavi Digitali, Passaggio al Bosco Edizioni

ha fornito: studi sulla psicologia umana, come vedremo successivamente, hanno permesso la creazione di vere e proprie formule di marketing da parte delle aziende, che tramite questi canali riescono a non stancare mai il consumatore studiandone le mosse in anticipo, osservandolo, e bombardandolo letteralmente con pubblicità *ad hoc* e contenuti personalizzati. Illuminanti, in tale chiave di analisi, le parole di Hal Varian, responsabile delle scelte economiche di *Google*: *"Personalizzazione e customizzazione sono il terzo "nuovo uso" delle transazioni mediate dai computer. Anziché dover chiedere a Google, è Google a dover sapere cosa volete, e a dirvelo prima ancora che ve lo domandiate."*[3] Nel *Cyber-space*, non vi è più la singola televisione come mezzo di diffusione delle notizie, delle pubblicità e dei programmi di intrattenimento, ad essa si sono aggiunte le figure dei *Social Network* e delle piattaforme digitali: il ribaltamento del paradigma, si afferma ancora una volta nel fondamentale passaggio dai *mass media* tradizionali all'utilizzo delle nuove moderne forme di diffusione mediatica, i *social media*, appunto. Tale dinamica, nel suo aspetto negativo e pericoloso, è ben descritta da Tennenini, in "*Schiavi Digitali": "Nel primo caso, si tratta di imporre un condizionamento attraverso un intrattenimento determinato dalla pubblicità, dagli show televisivi, dai reality, dai film, dai telegiornali o dai quiz. Interrompere tale incantesimo, però, è relativamente semplice: basta spegnere la televisione o uscire di casa. Nel secondo caso, invece, è quasi impossibile: l'intrattenimento è dappertutto, seguendoci con il nostro smartphone. […] Con l'estensione planetaria del fenomeno, tutti sono ingoiati – direttamente o indirettamente – nel cyber-space: il lavoro, l'informazione, l'intrattenimento, il tempo libero, le relazioni e gli equilibri sociali ne risultano compromessi. La rivoluzione digitale – infatti – non si è portata dietro solo le innovazioni, i dispositivi tecnici e il bagaglio culturale cibernetico ad esse correlato, ma anche numerose «malattie del benessere»: narcisismo, voyeurismo, nomofobia, vamping, disformismo, depressione, deficit d'attenzione, tendenza al suicidio e demenza digitale. Un baratro senza fine, che minaccia miliardi di individui. Le nuove cyber-lobby divengono autonome, mentre la massa – trasformata in followers – si aliena: il contegno dell'uomo tecnicizzato, in ambito sia teorico che pratico, assume nuove forme di assuefazione dai dispositivi smart. La complessità di queste cyber-lobby è talmente grande – e i suoi meccanismi così complessi – da non essere definibile con precisione. Lo stesso progresso tecnico, così rappresentato in tale contesto storico, diventa un meccanismo vuoto e sterile, che tradisce la sua natura: quella che doveva essere la "liberazione dell'umanità" dai vincoli del lavoro – infatti – si è trasformata in una gabbia ancora peggiore."*[4]

[3] ZUBOFF S. (2019), *Il Capitalismo della Sorveglianza*, LUISS University Press

[4] TENNENINI R. (2019), *Schiavi Digitali*, Passaggio al Bosco Edizioni

2.2 Il *marketing* digitale: la pubblicità intelligente e l'invasione dei *Cookies*

Per comprendere le dinamiche che questa gabbia contribuiscono a creare, la cui pericolosità consiste nel fatto che essa non appare ma rimane invisibile, è possibile partire dall'analisi di alcuni messaggi che ognuno di noi riceve ogni volta che accede un sito, a cui inevitabilmente deve aver fatto caso. Ed è proprio da questa impossibilità nel non incontrarli che partiremo: essi infatti ci appaiono sullo schermo e ci vengono fatti visualizzare automaticamente, senza che noi abbiamo mai chiesto nulla. Stiamo parlando dei "*cookies*, quelle finestre che ad ogni nostro accesso su un qualsiasi sito ci appaiono domandandoci se vogliamo "accettarli" o meno. Ma cosa sono? Chi li gestisce? A che scopo? Per rispondere a tali quesiti è bene inanzitutto evidenziare un concetto fondamentale che potremmo definire il minimo comun denominatore dell'agire dei *Social Network* e delle *Cyber Lobbies*, quelle aziende dal fatturato ad almeno nove zeri che ne determinano il funzionamento: la tecnologia artificiale, nonché l'uso degli algoritmi e dei *Big Data*, sfruttando i miliardi di dati che ognuno di noi produce semplicemente utilizzando il proprio smartphone, riesce a captare automaticamente l'oggetto delle nostre ricerche, in modo da indirizzare, per le volte successive, le proposte che lo stesso web ci proporrà su potenziali argomenti di nostro interesse. Il *"cookie"*, qua ora trattato, funziona esattamente così nel momento in cui noi clicchiamo "accetta" alla sua comparsa: memorizza il sito su cui stiamo navigando, in modo da proporcene di simili, o addirittura di complementari, nelle prossime nostre sessioni di ricerca. Vi è di più, tale processo si riversa su ogni inserzione pubblicitaria che incontreremo, a prescindere dall'*app* che staremo utilizzando o dal sito che staremo visitando. Ecco spiegato uno dei principali esempi di come la tecnologia avanzata, tramite algoritmi, che con formule matematiche memorizzano ed elaborano i nostri *data* e gli forniscono una direzione a seconda dei nostri interessi personali – ormai nel *Cyber space* ridotti a meri impulsi digitali -, riesca a far funzionare al massimo grado e in mole incalcolabole di dati, il sistema moderno della pubblicità: non più cartelloni 5x3 metri lungo le strade, ma inserzioni personalizzate ed automatiche in ogni momento di utilizzo del nostro smartphone. A chi non è mai capitato di parlare al telefono con amici, magari di una bella moto da poter comprare, e poi si è ritrovato, tra i più eclatanti e comuni esempi, la bacheca *Facebook* intasata di inserzioni su rivenditori di moto?

2.3 I *Cookies* arma delle multinazionali: il caso *Verizon*, i *Supercookies* e la privacy violata

Di fronte a meccanismi dalle portate come questo, possiamo evincere il ruolo di rilievo che nel mondo del marketing e dei mercati siano giunti a ricoprire i giganti del web, ideatori di strumenti come i "*cookies"*. L'utilizzo degli algoritmi, e lo sfruttamento dei *Big data* in tale chiave, ha creato veri e propri mercati di quest'ultimi a sè stanti: il profitto di un'azienda passa oggi inevitabilmente da queste logiche, l'asso nella manica di un imprenditore che opera ai tempi del *Cyber space* non è più la geniale invenzione di un oggetto, bensì, per esempio, proprio la quantità di inserzioni che riesce a controllare e a far giungere agli individui

più appetibili. Tuttavia, l'aspetto oscuro del nuovo marketing digitale, risiede nella creazione mirata dei suoi strumenti, composta da operazioni che molto spesso coincidono con veri e propri furti di dati sensibili. Il raccoglimento massiccio dei nostri *Big-Data* resta infatti una delle principali questioni riguardanti la possibilità di far convivere la fame di profitto dei giganti del web con il rispetto della privacy dei cittadini. *"Proprio qui risiede il nuovo tipo di politica governativa – denominato «regolamentazione algoritmica» – ordito dall'establishment della Silicon Valley. Esistenze efficenti, in un verkehrte Welt con quel tipo di politica anch'essa intelligente, in cui i nostri comportamenti quotidiani vengono registrati, analizzati e sollecitati, mentre le leggi sono dirette da sensori e meccanismi di feedback. L'obiettivo dell'Idra della Silicon Valley, nella Dürftige Zeit, è esattamente questo: tagliare i costi, anticipare i desideri del consumatore, automizzare le fabbriche, controllare i lavoratori e ridurre costantemente i tempi. Si tratta di una forma di controllo dei nostri dati e dei nostri cervelli atta a riformulare un nuovo tipo di comportamento, che sia coerente con la logica del nuovo capitalismo smart. La nostra presenza sui molteplici social network – del resto – facilita il loro intento."*[5] A dimostrazione di quanto appena esposto, interessante risulta l'accusa rivolta dalla *F.C.C. (Federal Communications Commission)* nei confronti del colosso *Verizon,* azienda statunitense fornitrice di banda larga e di telecomunicazioni. Dopo aver raggiunto tale livello sul mercato, rilevando *Yahoo* per 4,8 miliardi di dollari nel 2015 e fondendola con *AOL,* creando nel 2017 la seconda azienda per fatturato nelle comunicazioni dopo *AT&T*, ha dovuto pagare l'ammenda di 1,35 milioni di dollari in seguito al fatto che le indagini la decretavano rea di aver rubato, a loro insaputa, dati sensibili di milioni di persone tramite l'utilizzo di "*supercookies",* seguendo le logiche della moderna scienza di *"targeting technology"*.[6] Verizon, inoltre, come vedremo nei prossimi capitoli, fu anche l'azienda che collaborò con l'*NSA* (*National Security Agency)* durante il periodo del programma di sorveglianza "*PRISM",* fornendo all'agenzia di sicurezza interna statunitense i tabulati telefonici di milioni di persone, risultando così coinvolta nel *DATAGATE*.[7]

Risulta evidente, quindi, che nel mega mercato che tratta "l'oro del 21secolo", la reale vittima resti, come le logiche dell'intera società digitale sembrano confermare, l'uomo quale individuo, ormai neanche più sovrano della sua stessa vita privata. In quest'ultima chiave, il processo che lo porta a ritrovarsi coinvolto in violazioni di diritti come quello della privacy, nonché nelle ricezioni di quelle possiamo definire "pubblicità imposte", senza che egli abbia mai chiesto niente al riguardo se non cliccando "*accetta*" al comparire dei *"termini di servizio"* di fronte a un *cookie* o nella registrazione a un sito, è ben riassunto dalla frase proveniente dal documentario *Netflix* "*The Social Dilemma"*, nel quale: *"Se non stai pagando per il*

[5] TENNENINI R. (2019), *Schiavi Digitali,* Passaggio al Bosco Edizioni

[6] KASTRENAKES J. (March 7, 2016), *"FCC fines Verizon $1.35 million over 'supercookie' tracking"*, The Verge https://www.theverge.com/2016/3/7/11173010/verizon-supercookie-fine-1-3-million-fc

[7] SOLDAVINI P. *"Tutto quello che avreste dovuto sapere sul Datagate/Come è emerso il Datagate?"*, Il Sole 24ore https://st.ilsole24ore.com/art/notizie/2013-10-23/tutto-quello-che-avreste-voluto-sapere-datagate--come-e-emerso-datagate-225948.shtml?uuid=AB6tNuY

prodotto, allora il prodotto sei tu."[8] Il mondo del mercato globale, infatti, ha come merce di scambio dei dati, ma essi, in fondo, siamo noi stessi. Il nostro click è il nostro pensiero, ciò che digitiamo ci rende cosa siamo per i giganti di *Silicon Valley* e i suoi clienti: l'ultra-capitalismo della società digitale globalizzata e globalizzante, che tutto connette e tutti traccia, ha ridotto gli individui dalla loro più profonda ed autentica unicità, a cartelle di impulsi elettronici, a numeri di un algoritmo, pronti ad essere venduti come prodotti al miglior offerente.

3. Le *Cyber Lobbies*: tra consapevolezza e spinta verso il progresso

Nonostante la natura e le modalità con cui i giganti del web si muovono nel mercato globale, che abbiamo introdotto in questa prima parte della tesi, non manca la consapevolezza dei vertici rispetto a quanto le aziende che gestiscono rappresentano nel *Cyber space*, e sull'impatto che le loro innovazioni hanno portato in ambito umano e sociale. Da quando ci si è resi conto che il progresso tecnologico del 21esimo secolo sarebbe stato un processo irreversibile, dalla portata che abbiamo in precedenza descritto, costante e accesissimo è divenuto il dibattito riguardo il compromesso che esso dovrebbe trovare (se, può trovarlo!) con taluni aspetti in materia di diritti umani e con la natura umana stessa. Quest'ultimi, infatti, erano stati ritenuti intaccabili da ogni sorta di innovazione che l'uomo si sarebbe potuto anche solo mai immaginare: in primis, citiamo i risvolti accertati che in ambito patologico molti dispositivi tecnologici provocano all'organismo, partendo da quelli dei campi elettromagnetici generati dai cellulari, ma se vogliamo, ancor prima, dai cavi del trasporto della corrente. Tuttavia, non sembra essere bastato il fatto che le innovazioni avanguardistiche nella sfera della tecnologia, colonna portante nel *leit motiv* secondo il quale "il progresso è sempre volto a migliorare l'uomo", abbiano di fatto compromesso la cosa più preziosa che egli possiede, nonché la vita stessa, la sua salute. L'avanzamento della rivoluzione portata avanti nell'era digitale, guidata dai giganti di *Silicon Valley*, sembra infatti aver superato tale dilemma con una soluzione alternativa: il dibattito in tema si è spostato dalla salvaguardia della salute umana, alla possibilità di trasmutare l'uomo stesso in qualcosa che umano più non è. Nella realtà digitale, dove tutto è interconnesso e ognuno ha effettivamente una vita parallela rispetto a quella reale, dai profili *Facebook*, agli *Avatar* nei videogiochi, per citare qualche esempio, l'uomo è stato distaccato dalla sua dimensione più autentica e fisica: l'Intelligenza Artificiale e *l'Internet of Things*, lo sta già sostituendo in molte di quelle azioni quotidiane che, in molti casi, ormai neanche riuscirebbe a compiere senza il supporto del suo *smartphone*, reso indispensabile proprio in tale chiave. Al riguardo, le parole di Elon Musk, CEO e CTO di *SpaceX*, non destano dubbi: *"La percentuale dell'intelligenza che non è umana è in crescita. Alla fine, noi saremo una percentuale molto piccola dell'intelligenza. Io ho provato a convincere le persone a rallentare un po' l'Intelligenza Artificiale,*

[8] *"The Social Dilemma"* (2020), Netflix https://www.netflix.com/watch/81254224?trackId=254015180&tctx=0%2C0%2C1092ea01-d1dd-4dd1-8105-79f77c5f19a9-48274619%2C2b0f362e-3fdc-425c-a1c7-2cd844e63e92_42721550X20XX1600106810112%2C2b0f362e-3fdc-425c-a1c7-2cd844e63e92_ROOT%2C

a regolarla, ma è stato inutile. Ci ho provato per anni. Ci sarà sempre una qualche nuova tecnologia che causerà danni o morte. Ci sarà del clamore, ci saranno delle indagini, ci sarà una qualche tipologia di comitato di approfondimento. Essi scriveranno delle regole, quindi ci sarà sorveglianza: col tempo ci saranno regolamentazioni. Tutto questo porterà via molti anni; questo è il normale corso delle cose. Questo lasso di tempo non è significativo per l'Intelligenza Artificiale. Non puoi aspettare 10 anni per affrontare ciò che è pericoloso. È troppo tardi. Infatti, è una cosa che di sicuro non controlleremo. Il tuo cellulare è già un'estensione di te. Tu sei già un cyborg: anche se non te ne rendi conto, sei già un cyborg. Se il tuo cellulare è un'estensione di te, è così. "[9]

[9] ELON MUSK, *Fondatore, CEO e CTO di Space Exploration Technologies Corporation (SpaceX), co-fondatore, CEO e product architect di Tesla, co-fondatore e CEO di Neuralink. Presidente di SolarCity, fondatore di The Boring Company e co-fondatore di PayPal e OpenAI.*

Capitolo 2 - I *Big-Data*: il controllo di massa nel *cyber-space*

"*Questo è quello che ogni impresa ha sempre sognato, avere la garanzia che se viene inserita una pubblicità, avrà successo. E'così che fanno affari, vendendo certezza.*
Per poter avere successo in questo settore devi solo saper fare grandi previsioni, le grandi previsioni hanno un imperativo: servono molti dati."[10]

-Shosana Zuboff, *"The Social Dilemma" (Netflix, 2020)*

1. L'uomo *"Internauta"* come fonte primaria di dati

Nel seguente capitolo analizzeremo cosa i *Big Data* rappresentano nel mercato delle *Cyber Lobbies*, le fasi che ne vedono la raccolta, il loro utilizzo da parte di quest'ultime e il ruolo che l'uomo ricopre nell'era della connessione globale. Centrale, a tale scopo, sarà l'attenzione che dedicheremo al "capitano di *Silicon Valley*" *Google*, che secondo l'illuminante parallelismo della Zuboff *"sta al capitalismo della Sorveglianza come la Ford Motor Company e la General Motors stanno al capitalismo manageriale della produzione di massa"*[11]. Allo scopo di arrivare a descrivere i *Big Data*, riteniamo necessario far riflettere i lettori su quanto l'argomento, apparentemente "troppo enorme", "da livelli alti del potere", li riguardi invece da molto più vicino di quanto essi credano. Non vi è infatti la necessità di appartenere alla cosiddetta *"Generazione Z"*[12] per non essersi imbattuti personalmente in qualche dinamica che ci ha fatto storcere la bocca e dubitare di una possibile sorveglianza, navigando sul web. Prendendo l'esempio più diffuso delle dinamiche di cui sopra, non potremmo non aver fatto caso, almeno una volta, che dopo aver effettuato alcune ricerche su un determinato oggetto, che magari vorremmo acquistare, le inserzioni pubblicitarie che ci compaiono su ogni altro sito riguardano lo stesso oggetto della ricerca precedente, se non altri simili o comunque funzionali a quest'ultimo e al suo acquisto. Vi è di più, la stessa cosa può accadere, come nell'introduzione di questa tesi è stato riportato per esperienza personale, senza che nessuno di noi abbia mai digitato riguardo l'oggetto in questione, ma semplicemente parlandone in prossimità del nostro dispositivo, sia esso lo *smartphone* con cui abbiamo effettuato direttamente la chiamata, sia esso un computer, come nel caso del sottoscritto, che si trovava nelle vicinanze. Nel paragrafo che segue, andremo a introdurre il meccanismo che sta dietro alla comparsa di tali inserzioni.

[10] SHOSHANA ZUBOFF (2020),*"The Social Dilemma*", Netflix

[11] ZUBOFF S. (2019), Il Capitalismo della Sorveglianza, LUISS University Press

[12] *"Significato di Generazione Z",* Inside Marketing https://www.insidemarketing.it/glossario/definizione/generazione-z/

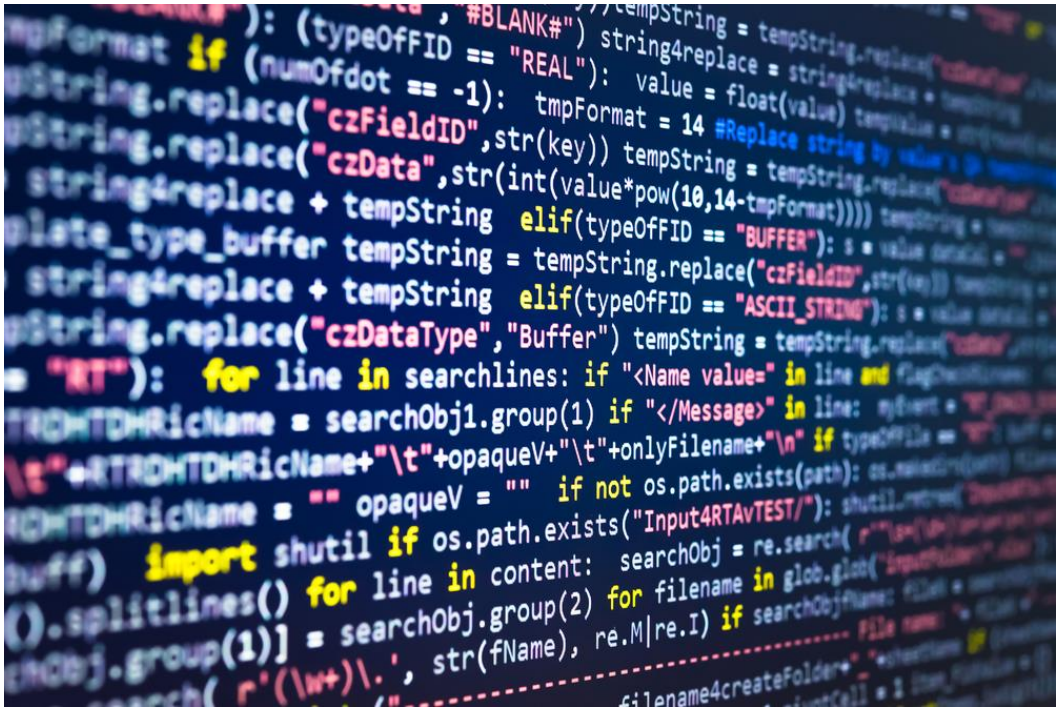
1.1 I *Big Data*: dalla raccolta all'elaborazione, il ruolo degli algoritmi

La logica informatica che sta dietro a tutto questo vede quattro principali attori: i dati, gli algoritmi, un'azienda, e noi. L'uomo del 21esimo secolo infatti, costantemente connesso in ogni suo aspetto della quotidianità, è *"Internauta"* nel *Cyber Space*: ogni sua digitazione corrisponde a un dato. Quest'ultimo viene registrato e raccolto da enormi e potentissimi *software,* che tramite formule matematiche, ed ecco che entrano in gioco gli *algoritmi*, viene elaborato insieme alle altre migliaia prodotti da ogni altra sua azione sul web. Tramite la fase dell'elaborazione, che consiste nel dare un senso, una direzione al lavoro compiuto dall'algoritmo, il *software* può estrapolare gli ambiti di interesse dell'*Internauta*, a seconda delle sue ricerche più frequenti, nonché di quelle istantanee, provengano esse da siti visitati o dai *social network* da questi utilizzati. E'così, che si arriva al quarto agente di tale "macchina da pubblicità": l'azienda. Essa, oltre a quella che si occupa direttamente dell'aspetto tecnico-informatico, prima fra tutte *Google,* come vedremo nei prossimi paragrafi, può principalmente essere rappresentata da quella multinazionale che tratta il prodotto che abbiamo cercato, e che tramite l'avanzata tecnologia dell'algoritmo, "venendo a sapere" che ad esso siamo interessati, ci compare sullo schermo nel contenuto di quell'inserzione che almeno una volta ci ha spaventati, facendoci domandare se qualcuno ci ascoltasse o meno.

1.2 Dai *click* su un sito alla comparsa delle inserzioni: i prodotti siamo noi

Avendo introdotto il funzionamento dell'algoritmo, quale strumento di elaborazione dei dati, e il ruolo ricoperto dalle aziende in tale meccanismo, è inevitabile giungere alla conclusione che, se quest'ultime hanno la possibilità di venire a conoscenza dei nostri interessi, è perché nel nostro essere *internauti* siamo direttamente noi stessi a fornirli, senza neanche rendercene conto: da ogni attività che svolgiamo sui nostri dispositivi, qualsiasi azienda è potenzialmente coinvolta quotidianamente nel volerci proporre i suoi prodotti, tramite le inserzioni. Considerata l'automatizzazione di questo processo digitale, ci si chiede se vi possa essere ancora uno spiraglio di libero arbitrio e di privacy nel mondo del *Cyber Space*. In conclusione, la fonte dei *Big Data* da cui migliaia di transazioni, variazioni strategiche di marketing, virate politiche, scelte aziendali ogni giorno dipendono, siamo noi stessi. Ogni nostro click, alla fine dei conti, non è altro che il prodotto delle nostre personali riflessioni, pensieri, volontà, emozioni, che riversate in rete sono trasformate, sotto impulsi elettrici, in migliaia di dati pronti ad essere utilizzati nel mercato dei *Big Data,* nel quale constatiamo come il prodotto possa essere solo uno: la vita stessa dell'uomo nella sua totalità. Nell'era digitale, in virtù del fatto che l'uso quotidiano di *smartphone* e altre tecnologie sempre più avanzate è divenuto indispensabile, viene messa in dubbio anche la possibilità di una "fuga" da tali dinamiche, che come vedremo prossimamente, nascondono logiche ben più profonde e sinistre di una semplice strategia di marketing digitale. Logiche di fronte alle quali rimane difficile stabilire quanto controllo saremo in grado di operare, questione alla quale, con grande lungimiranza, aveva già accennato Martin Heidegger, secondo il quale *"…Ciò che è veramente inquietante non è che il mondo si trasformi in un completo dominio della*

tecnica. Di gran lunga più inquietante è che l'uomo non è affatto preparato a questo radicale mutamento del mondo. Di gran lunga più inquietante è che non siamo ancora capaci di raggiungere, attraverso un pensiero meditante, un confronto adeguato con ciò che sta realmente emergendo nella nostra epoca."[13]



Un esempio di *Algoritmo*[14]

[13] HEIDEGGER M. (1995), *L'abbandono,* Il Nuovo Melagnolo

[14] *"Gli algoritmi minacciano il libero arbitrio? Due tesi al confronto"*, Agenda Digitale https://www.agendadigitale.eu/cultura-digitale/gli-algoritmi-minacciano-il-libero-arbitrio-due-tesi-al-confronto/

2. Da *Silicon Valley* fino a casa tua: Google, il padre dell'*algoritmo intelligente*

"Le nuove logiche economiche e i loro modelli commerciali vengono scoperti in un tempo e in un luogo determinati, e poi migliorano attraverso una serie di tentativi.
Nella nostra epoca Google è stata l'azienda che ha guidato, scoperto, elaborato, sperimentato, messo in pratica e diffuso il capitalismo della sorveglianza."[15]

-SHOSHANA ZUBOFF, Il Capitalismo della Sorveglianza

Una volta descritta la centrale e strategica funzione che l'utilizzo dell'algoritmo svolge nella vita *smart* dell'uomo-*internauta*, cerchiamo di scavare nella storia più recente al fine di comprendere come siamo giunti a tutto questo, e quali logiche hanno portato alla creazione delle nuove armi in mano all'ultra-capitalismo, trovando l'origine dell'*"oro del 21esimo secolo"*. A tale scopo, inevitabile diviene l'analisi del processo che ha portato *Google* ad essere definito*"il pioniere del capitalismo della sorveglianza"*[16], il colosso la cui *holding Alphabet*, è diventata a gennaio scorso la quarta società statunitense a raggiungere mille miliardi di dollari di capitalizzazione[17], alla distanza di appena 16 anni dal suo debutto sugli indici di *Wall Street*, datato 19 agosto 2004. A tal proposito, riteniamo indicativo in chiave di lettura del mondo in questa tesi analizzato, il fatto che le prime e uniche aziende quotate in borsa a raggiungere la stessa capitolazione erano state *Apple* e *Amazon* nell'estate del 2018, seguite da *Microsoft* nell'aprile dello scorso anno.[18] In merito a quest'ultima osservazione, pur riconoscendo il fatto che non è di nostra competenza la lettura dal filtro economico-finanziario di ciò che stiamo trattando, ne evidenziamo l'importanza per chi ne volesse portare avanti approfondimenti personali, ricordando soltanto l'influenza che le sfere economiche e finanziarie hanno sul mondo che ci circonda.

2.1 Gli algoritmi strumento di miglioramento delle ricerche web: il reinvestimento dei dati

Nata nel 1988, fondata da Larry Page e Sergey Brin, due laureati di Stanford, la prima fase di *Google* conobbe una grande crescita nel mercato informatico grazie all'efficienza del motore di ricerca che, lavorando secondo gli innovativi metodi di ricerca di Amit Patel, aveva contribuito a creare un equilibrio tra l'azienda e la persona, tra *Search* e l'*user* del web. Tale equilibrio era garantito dal fatto che tali tecnologie erano ancora in fase sperimentale, quindi, nell'economia dei due attori, l'uno serviva all'altro: *"Search aveva bisogno di persone dalle quali apprendere, e le persone avevano bisogno di apprendere da Search."*[19]

---

[15] ZUBOFF S. (2019), Il Capitalismo della Sorveglianza, LUISS University Press
[16] Ibidem
[17] *"Alphabet, la holding che controlla Google, è diventata la quarta società statunitense a raggiungere mille miliardi di dollari di capitalizzazione"*, Il Post https://www.ilpost.it/2020/01/17/alphabet-googl-mille-miliardi-capitalizzazione/
[18] Ibidem
[19] ZUBOFF S. (2019), Il Capitalismo della Sorveglianza, LUISS University Press

Ma fu proprio questa dinamica a scaturire un processo di miglioramento nella qualità della navigazione, continua a tal proposito la Zuboff: *"Questa simbiosi consentì agli algoritmi di Google di imparare a produrre ricerche sempre più rilevanti e complete: più query significavano apprendimento; più apprendimento produceva più rilevanza; più rilevanza significava più ricerche e più utenti."*[20] Tuttavia, rimane fondamentale evidenziare il fatto che in questa prima fase della futura punta di diamante di *Silicon Valley*, lo studio e la raccolta dei dati rimaneva volto esclusivamente al beneficio degli utenti: infatti, il valore che l'azienda offriva si limitava al mero miglioramento nelle funzionalità dei suoi servizi, rimanendo perciò nel contesto di quello che è stato definito*"reinvestimento del valore comportamentale"*[21].
Non si conoscevano pertanto logiche di profitto, non avendo fisici prodotti da vendere, ma semplicemente servizi da offrire secondo una logica di miglioramento reciproco.

2.2 La svolta verso il controllo totale: il *surplus comportamentale* e la pubblicità *targetizzata*

"Per poter continuare a contare qualcosa negli anni a venire non basterà più dimostrare di sapere far soldi. Serviranno bensì profitti duraturi ed esponenziali.". Parlava così Kara Swisher nel suo articolo[22] apparso sul *The Wall Street Journal* il 19 novembre del 2000. E' infatti nel periodo più buio per gli azionisti del settore informatico, colpiti duramente dalla bolla finanziaria delle *dot.com*[23] nata dalla loro estrema fiducia nelle potenzialità del settore, che Brin e Page dovettero mettere in discussione il sistema fino a quel momento adottato da *Google* al fine di trovarne uno sostitutivo. La soluzione, inevitabilmente, restava una sola: interrompere il rapporto di collaborazione e di reciprocità con gli utenti, che caratterizzava il sistema del *reinvestimento del valore comportamentale*, nel nome di una nuova strategia che aumentasse il profitto dell'azienda. Si presentò quindi la necessità di un cambiamento radicale nell'uso della pubblicità, serviva un incremento della stessa: le modalità per cui si optò, avrebbero cambiato per sempre non solo il destino dell'azienda, ma la vita delle persone. Avrebbero rivoluzionato il mondo intero, che si sarebbe di lì a poco spostato nella dimensione altra, nel *Cyber space*. La nuova strategia di *advertising*, infatti sarebbe stata quella che oggi definiamo *targetizzata*, cioè posta *ad hoc* per ogni utente a seconda dei suoi personali interessi. Fu allora che i dati degli utenti divennero la risorsa necessaria a tale fine. Il miglioramento e l'aumento della precisone nella loro raccolta, diventarono la chiave di svolta per la sopravvivenza di *Google* nei primi anni del secolo. Quell'incremento di dati da raccogliere non sarebbe più stato limitato allo scambio reciproco volto ad una sempre maggior qualità del servizio, bensì alla conoscenza totale, da parte dell'odierno colosso di *Silicon Valley*, della personalità più profonda di ogni persona: ad ognuno sarebbe dovuta giungere la pubblicità perfetta, "quel che voleva, quando voleva, dove lo avrebbe voluto". Nasce così il *surplus comportamentale*, il sempre più massiccio accumulamento di dati sensibili necessario a rendere

[20] Ibidem
[21] Ibidem
[22] SWISHER K. (19 dicembre 2000), *"Dot-Com Bubble Has Burst; Will Things Worsen in 2001?",* The Wall Street Journal https://www.wsj.com/articles/SB97709118336535099
[23] *"Lo scoppio della bolla delle c.d. DOTCOM",* Consob.it http://www.consob.it/web/investor-education/la-bolla-delle-c.d.-dotcom

sempre più precisa la pubblicità, per fare in modo che l'inserzionista che ne avrebbe voluto usufruire, avrebbe pagato una somma sempre maggiore per accaparrarsela: in poche parole, la mercificazione totale della vita umana, ridotta ad impulsi elettronici (*Big-Data*), vitali per l'esponenziale incremento del profitto delle multinazionali e delle *Cyber Lobbies*. La logica che vi sta dietro è ben espressa, ancora una volta, dalla Zuboff: *"E' l'invenzione stessa a dimostrare il ragionamento dietro alla scelta di soggiogare ai calcoli commerciali il ciclo di rinvestimento del valore comportamentale. Prima i dati comportamentali venivano "usati" per migliorare la qualità della ricerca a beneficio degli utenti, ora erano divenuti la materia prima – detenuta esclusivamente da Google – per la costruzione di un mercato dinamico dell'advertising online. Google era in grado di assicurarsi più dati comportamentali di quanti gliene servissero per soddisfare i propri utenti. Tale surplus* […] *era il bene gratuito che venne dirottato dal miglioramento del servizio a un mercato di scambio molto remunerativo.* - ma soprattutto- […] *La nuova Google ignorava le pretese di autodeterminazione e non poneva limiti a quel che poteva trovare e prendere. Respingeva la morale e il valore legale del diritto individuale a decidere, ridefinendo la situazione secondo l'opportunismo tecnologico e il proprio potere unilaterale. La nuova Google assicura i propri reali clienti che farà tutto il necessario per trasformare la naturale insondabilità del desiderio umano in un dato scientifico, e proclama di essere indipendente dalle norme sociali e dall regole che ne ostacolano il cammino. E'la superpotenza che impone i propri valori e segue i propri obiettivi aggirando e ignorando i contratti sociali che vincolano gli altri."*[24] Nacque ufficialmente l'era del capitalismo della sorveglianza, l'ultima frontiera nello scontro tra la tecnica e l'uomo. Fu così che il guanto di sfida a ciò che rimane oggi dell'autenticità della vita umana, con le sue mille particolarità e varietà di colori, fu gettato nel nome del profitto e del dominio mondiale dipendente da un algoritmo, un numero su uno schermo: è così che ebbe inizio l'era dei *Big Data*.

2.3 Dal computer fisso agli *smartphone*: i *Data* tra *Google Maps* e *Social Netwrok* nel 2020

In seguito all'analisi dell'incremento del funzionamento dei sistemi di sorveglianza e raccolta dati, giungiamo infine agli esempi anticipati all'inizio del paragrafo precedente.
Nel 2020, nel mondo del *Cyber Space* ormai affermato a 360º nella vita delle persone e della società, tale meccanismo ha raggiunto potenzialità mai viste prima.
Pensiamo solamente al ruolo chiave che l'approdo di *Social Network* come *Facebook* o *Instagram* hanno rappresentato nello studio del *surplus comportamentale*.
Basati sulla creazione di personali *Profili*, in cui ognuno condivide e scrive contenuti a seconda dei propri interessi, i padri del tasto *Mi Piace*, rappresentano oggi l'avanguardia nell'ambito della raccolta di *Big Data*: la diffusione totale di tali piattaforme e il loro funzionamento permettono una precisione tale da poter manipolare fenomeni sociali, come vedremo nel prossimo capitolo analizzando il caso di *Cambridge Analytica*, quali elezioni e movimenti di massa di qualsiasi genere.

[24] ZUBOFF S. (2019), Il Capitalismo della Sorveglianza, LUISS University Press

Nello specifico, pensiamo soltanto a quante informazioni i *Database* di *Silicon Valley* riescono a captare da un profilo *Facebook*. Dalle pagine che seguiamo, ai *like* che mettiamo, dai *gruppi* in cui ci aggiungiamo, forniamo letteralmente una planimetria totale delle nostre attività e interessi personali. Vi è di più: lo sviluppo tecnologico del 2020, permette a tali aziende di comprendere, per esempio, quando dormiamo e quanto. Basti pensare alla possibilità che il nostro stesso *smartphone* ci offre, di vedere quante ore abbiamo passato in un determinato giorno su una *app* rispetto a un'altra, nonché a statistiche quali i numeri di volte che abbiamo sbloccato lo schermo e la relativa attività generale.
Se prima, ai tempi precedentemente analizzati di *Search*, le fonti di *Data* che potevamo fornire si "limitavano" alle nostre ricerche sul web, oggi l'infinità di *app* di cui possiamo usufruire dovrebbero farci riflettere, se viste secondo il filtro che questa tesi vuole apportare agli occhi del lettore, su quante informazioni le *Cyber Lobbies* sono diventate in grado di aggiungere quotidianamente ai propri *server*.
Continuando con gli esempi, a chi non è mai capitato di visitare un ristorante, o un luogo qualsiasi di interesse, ed aver ricevuto, magari il giorno dopo, un messaggio di *Google Maps* che ci chiedeva "*se quel posto ci era piaciuto*" consigliandocene altri simili? Anche gli spostamenti, non vengono risparmiati.
Il tutto segue una logica sola: conoscere sempre meglio l'*Internauta* per proporgli una sempre maggior quantità di contenuti personalizzati e sempre più precisi, ineguagliabile in tale chiave la voce che appare che su *YouTube*, ma non solo, accanto ai video che stiamo visualizzando "*Potrebbe interessarti anche.",* o ancora gli onnipresenti *"Consigliati per te*". E'questa l'intelligenza artificiale applicata al *target marketing* spietato dell'ultra-capitalismo, l'algoritmo che si perfeziona giorno dopo giorno grazie all'incremento esponenziale dei *Big Data* che noi stessi gli forniamo e che si nutre oggi più che mai di miliardi dati giornalieri. *"Proprio qui risiede il nuovo tipo di politica governativa – denominato «regolamentazione algoritmica» – ordito dall'establishment della Silicon Valley. Esistenze efficienti […] con quel tipo di politica anch'essa intelligente, in cui i nostri comportamenti quotidiani vengono registrati, analizzati e sollecitati, mentre le leggi sono dirette da sensori e meccanismi di feedback. L'obiettivo dell'Idra della Silicon Valley è esattamente questo: tagliare i costi, anticipare i desideri del consumatore, automizzare le fabbriche, controllare i lavoratori e ridurre costantemente i tempi. Si tratta di una forma di controllo dei nostri dati e dei nostri cervelli atta a riformulare un nuovo tipo di comportamento, che sia coerente con la logica del nuovo capitalismo smart.*
La nostra presenza sui molteplici social network – del resto – facilita il loro intento."[25]
Gli esempi che potremmo ulteriormente riportare sono svariati. Tuttavia non è nostra intenzione sviluppare una lista che presenti tutti i modi in cui le *Cyber Lobbies* ci conoscono ogni giorno sempre di più, cosa che senz'altro può risultare interessante, ma che riteniamo potenzialmente ridondante in questa sede.
Ciò su cui vogliamo soffermarci, è l'importanza di un cambiamento di filtro nel guardare il *Cyber space* nel quale viviamo, azione con cui invitiamo, sollecitandolo, il lettore verso tale cambio di prospettiva nella sua

[25] TENNENINI R. (2019), Schiavi Digitali, Passaggio al Bosco Edizioni

analisi in tale ambito, a partire dalla sua stessa quotidianità. La presa di coscienza di fronte alle "ombre della democrazia" che scendono ogni giorno, silenziosamente, e per questo diventando sempre più pericolose, deve infatti partire da questi, da ognuno di noi.

Capitolo 3 – I *Data* in mano al governo: Edward Snowden e il *DATAGATE*

1. Il *Dati* come arma di controllo: l'attacco alle *Twin Towers* come punto di non ritorno

Ora che abbiamo visto la nascita del sistema che "regola" il *capitalismo della sorveglianza*, riteniamo necessario, con l'aiuto di qualche esempio pratico di vita quotidiana, sottolineare la mancanza di un punto d'arrivo negli obiettivi delle *Cyber Lobbies* che operano in questo settore.
Al fine *capitalizzare* sempre più profitti, vi era la conseguente necessità di migliorare costantemente la macchina degli algoritmi e della *pubblicità* targetizzata. Per far si che tale sistema avanzasse secondo ritmi esponenziali, *Google* e i giganti di *Silicon Valley* avevano bisogno di una sola cosa: il perfezionamento nella raccolta di dati, l'accrescimento vertiginoso del numero di quest'ultimi.
Il rapporto proporzionale che si venne a creare tra questa necessità e l'avanzamento costante dei sistemi tecnologici permise alle aziende del settore di registrare una crescita in quella direzione che non si sarebbe mai fermata: la quantità e la qualità dei *Big Data* raccoglibili sarebbe stato direttamente proporzionale al progresso e al perfezionamento degli strumenti digitali.
Prima di giungere ai giorni nostri, ricordiamo quanto il contesto storico nel quale le *Cyber Lobbies* dalle odierne capitalizzazioni a più di nove zeri le abbia aiutate nei primi anni della loro ascesa: impossibile tralasciare il punto di non ritorno che rappresentò, nella collaborazione tra agenzie governative e colossi dell'informatica, l'11 settembre del 2001.
Se già in precedenza, come abbiamo visto, *Google* e colleghi non credevano di dover badare troppo alla *privacy* dei loro utenti, gli anni che succedettero all'attacco delle *Twin Towers*, sbarrarono le porte alla più totale deregolamentazione in chiave di controllo su questi: la minaccia (la scusa?) del terrorismo dette il via libera ad una strettissima collaborazione tra gli organi di sicurezza nazionale *(NSA, CIA, Pentagono)* e strumenti di estrazione di dati come *Google*. Al fine di comprendere quanto già all'epoca quest'ultimo ricoprisse una posizione strategica potentissima, basti pensare al fatto che le sue tecnologie e strategie di raccolta dati furono prese da modello, nonché da strumento, dalle agenzie governative: l'apparato di difesa degli Stati Uniti, chiese espressamente aiuto ai tecnici di *Silicon Valley*, detentori delle più avanzate tecnologie in campo di raccolta *Big Data*, finanziando *startups* e investendo in altrettanti programmi di sviluppo digitale, come l'*ARDA (Advanced Research and Development Activity)*[26]. Quest'ultimo progetto

[26] *"Attività di ricerca e sviluppo avanzate"*, Wikipedia
https://www.sourcewatch.org/index.php/Advanced_Research_and_Development_Activity

del Pentagono ricevette un finanziamento di 64 milioni di dollari per l'incremento della ricerca di *Big Data* da parte dei servizi di intelligence. Per comprendere la forte collisione, che vide coinvolte la sfera privata dell'alta tecnologia e le stanze del Pentagono, riportiamo la presentazione dell'ex ammiraglio a capo dell'*NSA* John Poindexter, del *TIA (Total Information Awareness)*, un programma che come scriveva Disharon L.Crenson, il 18 febbraio del 2003, era "*..finanziato da oltre 20 milioni di dollari in contratti governativi,-* e grazie al quale - *i ricercatori stavano compiendo i primi passi verso lo sviluppo di un sistema che potrebbe vagliare le cartelle finanziarie, telefoniche, di viaggio e mediche di milioni di persone nella speranza di identificare i terroristi prima che colpiscano."*[27]

Queste, le parole di Poindexter: *"Se un'organizzazione terroristica è intenzionata a pianificare ed eseguire un attacco contro gli Stati Uniti, dovrà fare degli acquisti, lasciando le proprie tracce nello spazio informatico. […] Dobbiamo saper isolare tali tracce in mezzo a tutto il rumore, […] l'informazione rilevante estratta da simili dati dev'essere disponibile in archivi di larga scala con un contenuto semantico potenziato che consenta di analizzarli."*[28]

Abbiamo quindi, di fronte a noi, lo strumento del *surplus comportamentale* al servizio delle agenzie di sicurezza nazionale, il piano di analisi, diventa ora militare: il mix dell'avanzamento della tecnologia digitale e le potenzialità di raccolta ed elaborazione dati che si destavano mese dopo mese dalla collaborazione tra *Pentagono* e *Silicon Valley* segnò il punto di non ritorno nell'entrata nell'era della sorveglianza totale.

1.1. I tabulati di *Verizon* richiesti dalla *NSA*: l'inizio del *Datagate*

Il 5 giugno 2013, sul Guardian appaiono alcune liste di ordini segreti che la *FISC (Foreign Intelligence Surveillance Court)* impartiva ad alcuni dipartimenti della *Verizon Communication*, la quale gli avrebbe dovuto fornire una raccolta di *"metadati"* ricoprenti gli interi tabulati telefonici statunitensi, dalle chiamate interne, a quelle in uscita dagli USA.

Il giorno dopo, il 6 giugno, al Guardian si aggiunge il Washington Post con le rilevazioni riguardo all'esistenza di *PRISM*, un segreto sistema elettronico di sorveglianza in mano alla *NSA*, che permetteva all'agenzia di sicurezza interna americana di accedere a miliardi di dati sensibili di milioni di cittadini: dalle e-mail e le chiamate, fino alle ricerche sul web, in tempo reale.

E' l'inizio del *Datagate*, lo scandalo che vide protagonista l'agenzia di sicurezza interna americana (*NSA*) la quale, con la complicità di svariate aziende nel settore comunicativo e informatico, come verrà decretato alla fine, raccoglieva i dati sensibili dei milioni di cittadini, dal 2001 fino ad almeno il 2011.

---

[27] CRENSON L.S. (February 18, 2003) , *"Researchers Working on Total Information Awareness Program"* Government Technology https://www.govtech.com/security/Researchers-Working-on-Total-Information-Awareness.html

[28] Ibidem

Come abbiamo analizzato nel paragrafo 3 del Capitolo 2 di questa tesi, una volta che i sistemi di intelligence e le agenzie di sicurezza entrarono in stretta collaborazione coi pionieri dell'informatica, si eette ufficialmente vita all'era della sorveglianza totale e "legittimata"[29].

A tal proposito riteniamo importanti le parole del giurista Stefano Rodotà, che intervistato dall'*Espresso* il 12 maggio del 2015, proprio nei giorni in una corte d'appello federale di New York decretava "illegali" le attività di spionaggio portate avanti dall'*NSA* durante il *Datagate*[30], così rispondeva riguardo al pericolo della limitazione delle libertà e della privacy con la scusa della sicurezza nazionale decantata dalle istituzioni: *"Sta accadendo, e non è la prima volta, che utilizzando come argomento, o meglio, come pretesto, fatti riguardanti il terrorismo o la criminalità organizzata si dice "l'unico modo per tutelare la sicurezza è quello di diminuire le garanzie e di aumentare le possibilità di controllo che le tecnologie rendono sempre più possibile". E questo è sempre avvenuto, è avvenuto in particolare dopo l'11 settembre, vicenda che ho vissuto in prima persona perché all'epoca presiedevo i garanti europei e ho avuto una serie di contatti continui con gli Stati Uniti che chiedevano un'infinità di informazioni da parte dell'Europa, cui abbiamo in parte resistito."*[31]

Il logo dell'NSA (*National Security Agency*), l'agenzia di sicurezza interna statunitense

[29] Vedi paragrafo 1 Capitolo 3

[30] SAVAGE C. and WEISMAN J. (May 7, 2015), *"N.S.A. Collection of Bulk Call Data Is Ruled Illegal"*, New York Times https://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html?_r=0

[31] ROSSANO A. (12 maggio 2015), *"Con la scusa del terrorismo ci tolgono i diritti" Stefano Rodotà denuncia la deriva europea"*, L'Espresso https://espresso.repubblica.it/attualita/2015/05/12/news/con-la-scusa-del-terrorismo-ci-tolgono-i-diritti-stefano-rodota-denuncia-la-deriva-europea-1.212058

1.2 Cos'è *PRISM:* il programma centrale dell'*NSA*

"Non voglio vivere in un mondo in cui tutto ciò che faccio o dico viene registrato. Questo è qualcosa che io non sono disposto ad accettare o sostenere."

-EDWARD SNOWDEN, intervista a *The Guardian - "'The US government will say I aided our enemies - NSA whistleblower"*[32]*, Youtube*

Per *PRISM* intendiamo il programma usato dall'agenzia di sicurezza nazionale interna americana con cui, grazie alla collaborazione di svariate aziende del settore informatico, nonché dei principali *Social Network,* come vedremo tra poco, il governo americano ha raccolto miliardi di dati sensibili di cittadini statunitensi e non a partire dal 2001 fino ad almeno il 2011.
Il 7 giugno del 2013, quando *The Guardian* e *Washington Post* escono allo scoperto dichiarando *"che l'Nsa ha anche accesso diretto ai dati degli utenti di Google, Facebook, Apple e altre aziende tecnologiche statunitensi per controllarne le conversazioni"*[33]*,* l'inchiesta, che di lì a poco avrebbe assunto una portata planetaria e senza precedenti nell'era del *Cyber space*, fornì le prime informazioni dettagliate riguardo al funzionamento di tale sistema.
Fungendo da programma di sorveglianza elettronica e *cyberwarfare* fu messo in funzione dalla *NSA* già dal 2007 e, caratterizzato dalla massima segretezza, svolse un'attività di *"data mining"*: una titanica operazione di rastrellamento delle informazioni provenienti dalle azioni degli *user* sul web, con la complicità di fornitori di servizi elettronici, dalle chiamate ai messaggi, dai post sui *Social* alle transazioni bancarie, in tempo reale.
Lo strumento col quale l'attività di *"data mining"* veniva svolta venne identificato nel così *detto "Boundless Informant"*, il quale era in grado di descrivere dettagliatamente e di riferire le coordinate geografiche delle informazioni che recepiva. Al fine di farci un'idea della portata e delle potenzialità d'infiltrazione di tale "arma di controllo", ne riportiamo la descrizione fornitaci dallo stesso *The Guardian*, nell'articolo pubblicato l'11 giugno del 2013: *"L'obiettivo dello strumento interno dell'NSA è il conteggio e la classificazione dei record delle comunicazioni, noti come metadati, piuttosto che il contenuto di un'e-mail o di un messaggio istantaneo. I documenti di Boundless Informant mostrano che l'agenzia ha raccolto quasi 3 miliardi di informazioni dalle reti informatiche statunitensi in un periodo di 30 giorni che termina a marzo 2013. Un documento afferma che è progettato per fornire ai funzionari della NSA risposte a domande come "Che tipo di copertura abbiamo sul paese X "in" quasi tempo reale chiedendo all'infrastruttura SIGINT*

---

32 *"Edward Snowden interview: 'The US government will say I aided our enemies' - NSA whistleblower"*, YouTube, The Guardian https://www.youtube.com/watch?v=Q_qdnyEqCPk

33 *"Cos'è il datagate e com'è cominciato"* (25 giugno 2015), L'Internazionale https://www.internazionale.it/notizie/2015/06/25/datagate-snowden-spionaggio

[intelligence dei segnali] ". Una scheda informativa della NSA sul programma […] *dice: "Lo strumento consente agli utenti di selezionare un paese su una mappa e visualizzare il volume dei metadati e selezionare i dettagli sulle raccolte per quel paese."*[34]

Inoltre, il sistema forniva agli operatori dei servizi statunitensi, come si legge nello stesso articolo, una mappa di calore basata sull'intensità del controllo che la *NSA* applicava ad una data regione, indicato a livello crescente dal colore verde, sfumando dal giallo all'arancio, fino al rosso.

La mappa di calore del "Boundless Informant[35]

1.3 *PRISM e* il ruolo di aziende e *Social Network:* i *metadati*

Se poco fa abbiamo parlato del "rastrellamento" di miliardi di dati, riteniamo necessario analizzare la natura di quest'ultimi per quanto riguarda il contesto di cui stiamo parlando.

A tale scopo, definiremo per prima cosa i *metadati,* termine che è atterrato per la prima volta nella discussione pubblica proprio grazie ad Edward Snowden e alle sue dichiarazioni, per poi andare a descrivere il ponte che ha permesso alla *NSA* di raccogliere tali dati: la collaborazione tra *PRISM* e varie aziende nel settore tecnico-informatico. Al fine di sintetizzare il seguente paragrafo, lo schematizzeremo dividendolo in due punti, ognuno corrispondente alle due domande centrali volte alla comprensione dell'intero sistema di sorveglianza in questo capitolo analizzato:

1) Che informazioni esattamente estraeva la *NSA*: cosa sono i *metadati*?

Il progresso tecnologico e la conseguente digitalizzazione sempre più progressiva hanno inevitabilmente, con un evidente incremento della praticità nella loro gestione, sia chiaro, sostituito la materia cartacea nella

34 *"Boundless Informant: the NSA's secret tool to track global surveillance data"*, TheGuardian.com https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

35 *"Boundless Informant heat maps"*, Edward Snowden.com https://edwardsnowden.com/2014/05/14/boundless-informant-heat-maps/

raccolta di qualsiasi tipo di dati: ogni fase della "vita" di quest'ultimi, dalla produzione all'archiviazione, si è resa registrabile a livello informatico, divenendo quindi indelebile.
Al fine di una sempre migliore gestione di tali documentazioni, sono stati inventati degli strumenti digitali volti ad una classificazione precisissima di queste immense quantità di dati al fine di poterli rintracciare nella loro singolarità, operazione che risulterebbe altrimenti impossibile da affrontare: i *metadati*.
Nel linguaggio informatico, tale termine indica un insieme di informazioni sui singoli dati, in poche parole, le coordinate di ogni dato che ne permettono la rintracciabilità, in una prima fase, e l'analisi della natura in una seconda.
Al fine di comprendere cosa il sistema di sorveglianza statunitense stesse raccogliendo in quantità incalcolabili ogni giorno, prendiamo l'esempio del ruolo che i *metadati* svolgono solamente nell'ambito della Pubblica Amministrazione, dove essi sono *"per esempio il vostro NOME ed il vostro COGNOME: che vi chiamiate "Mario Rossi" o "Giuseppe Verdi" non importa, il metadato NOME o COGNOME, descrive come Mario sia un nome, quindi ha una certa lunghezza in caratteri, e lo stesso vale per il vostro COGNOME.* […] *Hanno degli identificatori univoci, nel senso che non si può fare confusione tra oggetti della stessa categoria. Ad esempio il nostro "Mario Rossi" sarà nato da qualche parte, in una certa data. Con il suo codice fiscale possiamo, ragionevolmente, identificarlo in maniera del tutto univoca, quindi la nostra entità anagrafica avrà questo identificatore unico ed irripetibile.*"[36]
Un *metadato*, in conclusione, è lo strumento informatico che permette di dare una connotazione, sotto ogni punto di vista, dal luogo e dall'orario in cui è stata fatta, dal mittente al ricevente, e così via, ad ogni singola azione svolta da una persona sulla rete: sia essa un *Like* su *Facebook* o, più banalmente, un *SMS* alla propria ragazza. Possiamo quindi immaginare, nonché decretare, la mole di informazioni che la *NSA*, grazie all'accesso a tali strumenti, sia stata in grado di raccogliere per mezzo di *PRISM*.

2) Le modalità di raccolta: le aziende quali ponte tra la *NSA* e i nostri dati sensibili

"Google tiene molto alla sicurezza dei dati dei nostri utenti. Divulghiamo i dati degli utenti al governo in conformità con la legge e esaminiamo attentamente tutte le richieste di questo tipo. Di tanto in tanto, le persone affermano che abbiamo ha creato una "porta di servizio" del governo nei nostri sistemi, ma Google non ha una porta di servizio per il governo per accedere ai dati degli utenti privati ".

-*Google* per *The Guardian,* 7 giugno 2013

[36] GROSSO R. (8 marzo 2018), *"Dati e metadati per la PA, a che servono e come migliorano il rapporto con il cittadino."*, AgendaDigitale.eu https://www.agendadigitale.eu/cittadinanza-digitale/dati-metadati-la-pa-servono-migliorano-rapporto-cittadino/

Nel paragrafo 2.3 del capitolo 1 della seguente tesi, abbiamo incontrato il colosso delle telecomunicazioni statunitensi *Verizon*, citando la multa che dovette pagare per l'abuso di *supercookies* durante la sua spietata campagna online di pubblicità targetizzata.
La multinazionale, tuttavia, era già apparsa sulle testate d'inchiesta riguardanti proprio il *Datagate.*
La sua complicità, in ambito della comunicazione telefonica nell'operazione di sorveglianza della *NSA*, era l'oggetto del primo articolo del *Guardian* alla nascita dell'intera inchiesta.
Parlava così, infatti, il 6 giugno del 2013: *"La National Security Agency sta attualmente raccogliendo i tabulati telefonici di milioni di clienti statunitensi di Verizon, uno dei maggiori fornitori di telecomunicazioni americani, in base a un ordine del tribunale top secret emesso ad aprile.*
L'ordine, una copia del quale è stata ottenuta dal Guardian, richiede a Verizon "su base giornaliera e continuativa" di fornire alla NSA informazioni su tutte le chiamate telefoniche nei suoi sistemi, sia negli Stati Uniti che tra gli Stati Uniti e altri paesi."[37]
Verizon, in effetti, fu il primo esempio tra le aziende che collaborarono con l'*NSA*, fornendo nel suo caso *metadata* sotto forma di tabulati telefonici, che Edward Snowden riportava nel primo documento rilasciato.
Non passarono le ventiquattr'ore e le stesse testate[38], il 7 giugno del 2013, svelarono i documenti dell'ex dipendente della *NSA e* della *Booz Allen Hamilton,* una società americana di consulenza in materia di gestione e tecnologia dell'informazione[39], riguardanti il coinvolgimento di ulteriori aziende tra le quali, in primis, *Google*, *Facebook* e *Microsoft.* Il ruolo dei giganti di *Silicon Valley* nell'operazione di spionaggio di massa messa in atto da *PRISM* è ben spiegata dal *Sole24ore*, come abbiamo già visto in precedenza, comunque, non dovrebbe essere difficoltoso comprendere l'importanza dei loro server quali fonti di dati sensibili[40]: *"… il cuore del programma Prism è incentrato sulla collaborazione con i colossi del web che hanno aderito allo schema nel corso degli anni. Secondo la ricostruzione fatta dal Guardian sulla base della documentazione riservata (e in parte pubblicata) al programma collaborano Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, Aol e, ultima in ordine di tempo, Apple. Queste aziende avrebbero messo a disposizione di Prism i loro server, dai quali passa la gran parte del traffico globale di internet. Bisogna tenere conto della particolare struttura della rete e soprattutto del fatto che i pacchetti di bit che portano le informazioni lungo le connessioni del web viaggiano su percorsi che non necessariamente sono lineari, ma che di solito seguono il criterio dell'economicità. Proprio per questo gran parte del traffico*

---

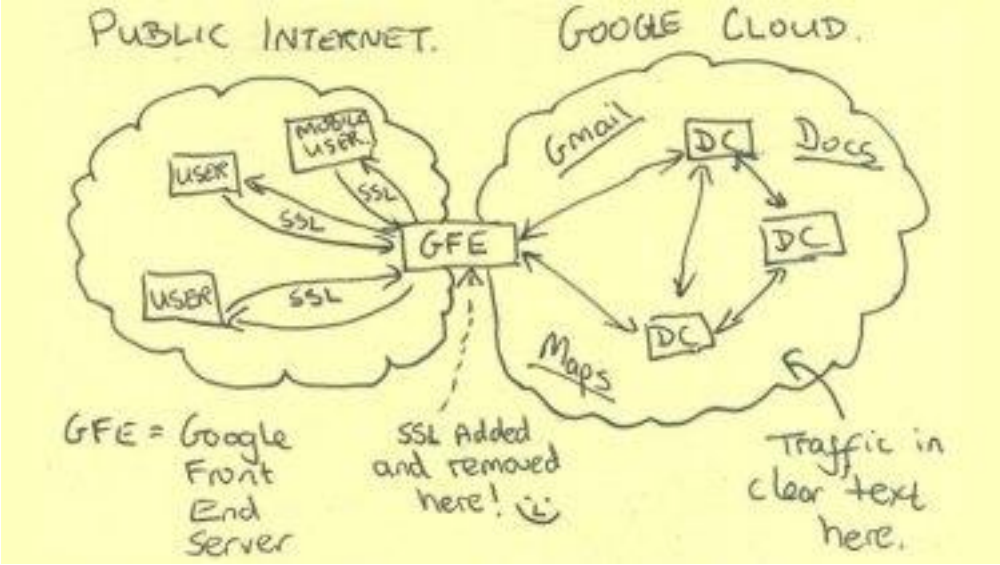
37 *"NSA collecting phone records of millions of Verizon customers daily"*, TheGuardian.com https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

38 *"NSA Prism program taps in to user data of Apple, Google and others"*, The Guardian.com https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

39 *Booz Allen Hamilton*, Wikipedia.org https://en.wikipedia.org/wiki/Booz_Allen_Hamilton

40 Vedi paragrafo 2.3 del Capitolo 2

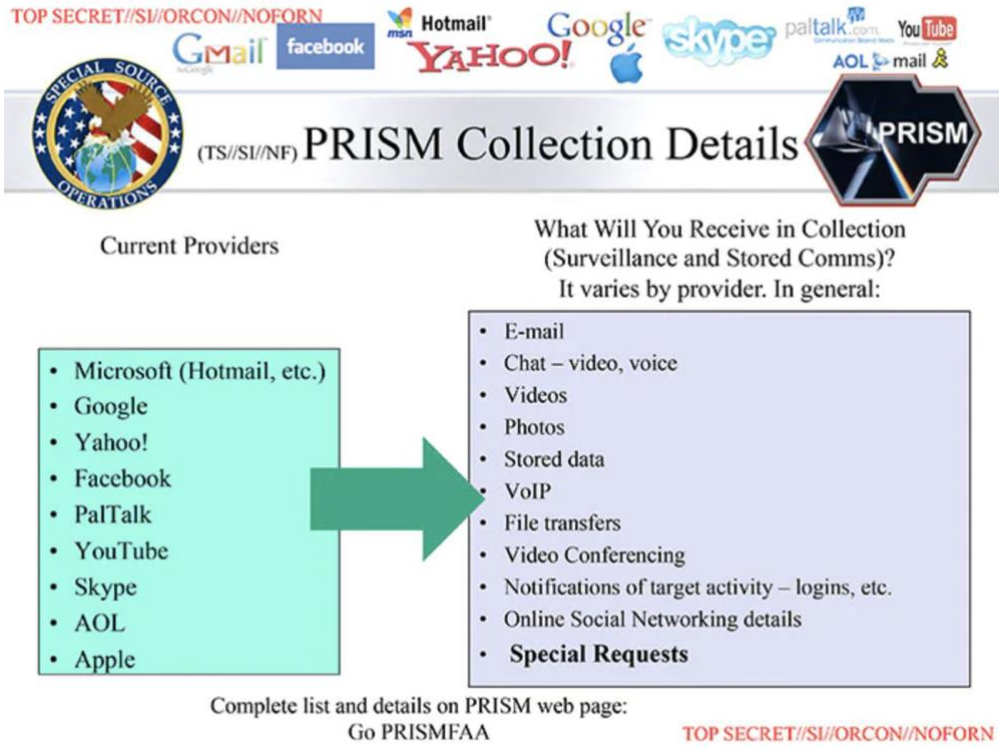
mondiale passa per gli Stati Uniti appoggiandosi si server dei loro internet provider. Ed è per questo che Prism riesce a catturare anche le comunicazioni provenienti da stati stranieri, senza varcarne i confini."[41] Siamo quindi di fronte al perfezionamento del "sistema di scambio di servizi" tra agenzie governative e multinazionali del settore informatico che pone le sue radici nei programmi di sorveglianza post 11 settembre 2001: è l'inarrestabile avanzata del levitano invisibile dello "spionaggio legittimo", la messa a punto dell'odierno trionfo del capitalismo della sorveglianza. Nelle due immagini che seguono, il punto d'incontro tra il programma della NSA e le relative risorse rappresentate dai suoi "fornitori di dati".



In questa diapositiva tratta da una presentazione della National Security Agency su "Google Cloud Exploitation", uno schizzo mostra dove "Internet pubblico" incontra "Google Cloud" interno dove risiedono i dati degli utenti. Due ingegneri con stretti legami con Google sono esplosi in parolacce quando hanno visto il disegno.[42]

[41] SOLDAVINI P. *"Datagate, ecco come funziona il nuovo spionaggio globale"* sez. 3, IlSole24Ore https://st.ilsole24ore.com/art/2013/2013-10-23/tutto-quello-che-avreste-voluto-sapere-datagate--come-vengono-intercettate-informazioni-222331.shtml?uuid=ABY8FuY#navigation

[42] GELLMAN B. and SOLTANI A. (October 30, 2013) *"NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say"*, New York Times https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html



Lo schema di come la NSA e l'FBI hanno raccolto dati come audio, video, fotografie, e-mail e documenti dai server interni di nove importanti società tecnologiche, da una diapositiva tra le 41 di una presentazione sulla sicurezza ottenuta dal Washington Post e The Guardian.[43]

2. I tentacoli del *Big Brother*: *SSO*, il progetto *Tempora* e *Stellar Wind*

Dopo aver affrontato schematicamente il coinvolgimento dei *Social Network* e delle multinazionali nel fenomeno *Datagate*, affrontando quest'ultimo dal punto di vista più da noi ritenuto più idoneo per la nostra tesi, quello del ruolo dei *data*, riteniamo necessario citare ulteriori programmi in merito.
Lo scopo del corrente paragrafo è, sì di incrementare l'argomentazione, ma soprattutto fornire al lettore ulteriori spunti nel caso volesse svolgere un approfondimento in merito, nonché dimostrare brevemente la grandezza del fenomeno che stiamo analizzando, che si estende ben oltre quanto in questa sede descritto. Procederemo quindi per una classificazione ancor più schematizzata della precedente in merito:

1) *SSO (Special Source Operations)*: Descritta dallo stesso Snowden "il gioiello della NSA"[44], è la divisione speciale dell'agenzia di sicurezza interna americana. Era tramite essa che i servizi statunitensi gestivano i rapporti con le aziende private, dalle quali si rifornivano dei relativi *data*, a seconda dei vari settori che ognuna di esse rappresentava. Alcuni *partner*, infatti, non facevano parte dello stesso grado nella

[43] SEIFERT B. (June 6, 2013) *"Secret program gives NSA, FBI backdoor access to Apple, Google, Facebook, Microsoft data"*, TheVerge.com https://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism

[44] *"The Guardian NSA files: decode"*, Section 3, TheGuardian.com https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/3

scala gerarchica dei complici della *NSA*. Al riguardo, parla così il ricchissimo dossier sul sito dello stesso *Guardian:"I nomi di molti dei "partner aziendali" della NSA sono così sensibili da essere classificati come "ECI" - Informazioni controllate eccezionalmente - un livello di classificazione più elevato rispetto alla copertina dei documenti Snowden.*
Ma alcune delle società Internet vengono nominate nel briefing sulle operazioni di origine speciale sull'accesso ai partner aziendali. Un grafico che confronta i rapporti settimanali che coinvolgono le aziende elenca alcuni dei fornitori di Prism. Altre società presenti nell'elenco sono protette dai nomi di copertina ECI. Artifice, Lithium e Serenade sono elencati in altri documenti come nomi di copertina per i partner aziendali SSO, mentre Steelknight è descritto come una struttura partner della NSA."[45]

2) Progetto *Tempora*: portato avanti dal "fratello britannico" della *NSA* dal 2011, il *GCHQ (Government Communications Headquarter)*, che a sua volta aveva accesso ai dati raccolti dall'agenzia a stelle e strisce, si occupava dell'intercettazione delle comunicazioni estere correnti sui cavi sottomarini e sulle grandi infrastrutture internazionali. Tramite tale sistema, a partire da conversazioni telefoniche ed e-mail, dai messaggi su Facebook a qualsiasi altra attività via web, si decretò il passaggio in rassegna di circa *"600 milioni di dati telefonici al giorno, filtrando il flusso di telefonate attraverso oltre 200 cavi in fibra ottica."*[46]

3) *Stellar Wind*: fuoriuscito al pubblico nella pubblicazione da parte del *Guardian*[47] in data 27 giugno 2013, rappresenta il nome del programma della *NSA* col quale, sotto la presidenza Obama (che ne aveva autorizzato il funzionamento prorogando nel 2012 la legge del *Foreign Intelligence Surveillance Act* del 1978, reintrodotto già prima da Bush nel 2004)[48], erano stati intercettati *metadata* riguardanti le e-mail. Nello specifico, l'operazione vide lo specifico raccoglimento *"dei campi "Da:", "A:" e "Cc:" di ogni email scambiata sulla rete statunitense fra cittadini locali e stranieri, una massiccia raccolta dati avviata nel 2001 sotto l'amministrazione Bush."*[49]

---

[45] Ibidem

[46] *"Che cos'è Tempora: il programma di sorveglianza elettronica britannico"* (24 ottobre 2013), Polisblog.it https://www.polisblog.it/post/166503/che-cose-tempora-il-programma-di-sorveglianza-elettronica-britannico

[47] *"NSA collected US email records in bulk for more than two years under Obama"*, TheGuardian.com https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama

[48] *"Cos'è il datagate e com'è cominciato"* (25 giugno 2015), L'Internazionale https://www.internazionale.it/notizie/2015/06/25/datagate-snowden-spionaggio

[49] MARUCCIA A. (1 luglio 2013) *"Datagate, le intercettazioni dell'era Bush"*, Punto-informatico.it https://www.punto-informatico.it/datagate-le-intercettazioni-dellera-bush/

3. La "Giurisprudenza della sorveglianza": La Legge sugli emendamenti *FISA* del 2008

Chiudendo la nostra analisi riguardante il *Datagate*, in questo paragrafo affronteremo lo scandalo riguardante le attività di spionaggio di massa delle agenzie di sicurezza nazionali, in primis statunitensi e britanniche[50], dal punto di vista del diritto. Riteniamo opportuno specificare che, non essendo l'ambito giurisprudenziale la materia della seguente tesi, abbiamo optato, anche in questo paragrafo, per una schematizzazione del relativo oggetto, cercando comunque di svolgere la più esaustiva analisi di un aspetto che prevediamo poter (e dover!) essere fonte di un vitale dibattito negli anni a venire, più di quanto già fino ad oggi esso già non sia stato: il diritto alla *privacy* e la regolamentazione della gestione dei *Data*, quali prime fonti di dati sensibili, nel mondo del *Cyber space.*

1) La *NSA* e il *FISA*: Il *FISA* (*Foreign Intelligence Surveillance Act)* è un atto normativo degli Stati Uniti d'America, emanato nel 1978 in seguito allo scandalo *Watergate*[51], che vide il presidente Nixon coinvolto per intercettazioni telefoniche illegali. In esso sono stabilite le procedure volte alla sorveglianza fisica ed elettronica, nonché alla raccolta di informazioni di intelligence straniera.
Citiamo anche, in tale chiave, l'istituzione della Corte di sorveglianza dei servizi segreti esteri degli Stati Uniti (FISC), una speciale corte federale che tiene sessioni non pubbliche per valutare l'emissione di mandati di perquisizione ai sensi della FISA. I procedimenti davanti alla FISC sono ex parte, il che riconosce il governo quale partito presente.[52] Giungendo all'aspetto che a noi più riguarda in questa sede, è bene sottolineare che, come dal titolo del seguente paragrafo abbiamo cercato di introdurre, anche il *capitalismo della sorveglianza* ha una "sua giurisprudenza": segue cioè determinate logiche e adotta altrettante strategie al fine di farsi largo tra le possibili limitazioni che può trovare in tale materia.
L'evoluzione della "Legge sulla sorveglianza dei servizi segreti stranieri" è ritenuto da noi un esempio perfetto per comprendere le dinamiche appena accennate.
Dopo il primo aggiornamento subito sotto la presidenza Reagan nel 1981, con *l'Ordine esecutivo 1233*[53] , la svolta decisiva si ha nel 2001, quando in seguito agli attacchi dell'11 settembre, l'allora presidente Bush, tramite il *Patriot Act, "modificò la FISA* – alle sezioni 214 e 216 - *consentendo la raccolta di determinati metadati di comunicazione via cavo o elettronica per comunicazioni rilevanti per un'indagine di terrorismo o spionaggio invece di comunicazioni che potrebbero essere quelle di un terrorista o di una spia. […]* –

[50] Vedi Paragrafo 1.2 (*PRISM)* e 2 (*Tempora)* Capitolo 3

[51] HISTORY.COM EDITORS (Uptated: sep 25, 2019 – original: oct 29, 2009), *"Wategate Scandal",* History.com https://www.history.com/topics/1970s/watergate

[52] *"The Foreign Intelligence Surveillance Act of 1978 (FISA)",* U.S. Department of Justice, Justice Information Sharing https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286

[53] Più recentemente modificata dal presidente Bush nel 2004, questa ordinanza autorizzava ampiamente la raccolta di tutte le informazioni ai fini della "difesa nazionale" non proibita da altre leggi applicabili.

nonché consentiva, alla sezione 215 - *al governo di ordinare la raccolta di "cose tangibili" che aiutano in un'indagine su terrorismo o spionaggio.* - tali cose non avrebbero dovuto e potuto - *necessariamente riguardare direttamente un obiettivo, ma essere rilevanti solo per un'indagine."*[54]

Tuttavia, il ruolo chiave che riguarda la *NSA* nel *Datagate*, arriva in merito al successivo aggiornamento della *FISA*: nel 2008, introdotta dalla Casa Bianca con a capo Barack Obama, la legge sui relativi emendamenti, si legge ancora sul dossier del *Guardian*, alla sezione 702 *"modifica la Fisa e richiede l'istituzione di procedure per il targeting di persone non statunitensi all'estero. Il governo potrebbe non prendere di mira intenzionalmente una persona statunitense, ma la NSA ha rivelato che raccoglie involontariamente le comunicazioni americane […]* – inoltre, alle sezioni 703 e 704 – *stabilisce procedure per prendere di mira le persone statunitensi all'estero. In questi casi, la sorveglianza di una persona statunitense può essere autorizzata senza mandato perché la persona statunitense si trova fuori dal paese."*[55] E'infatti la sezione 702 che *l'NSA* avrebbe "interpretato a modo suo", come dimostreranno in seguito anche le profonde contraddizioni riscontrate dallo stesso Tribunale *FISA* quando verrà a conoscenza nel gennaio del 2009 di interrogazioni non autorizzate[56] dell'agenzia di sicurezza da cui era completamente all'oscuro. La *NSA*, a sua volta, avrebbe cercato di difendersi contando sul fatto che in ogni caso, anche gli stessi atti del Tribunale appartenevano ad una giurisprudenza totalmente segreta (vedi nota 49). La sezione 702, prevedeva infatti due modalità d'operazione in chiave di sorveglianza elettronica: la prima era volta allo spionaggio di *foreign power*[57], la seconda, prevedeva la possibilità di coinvolgimento anche di soggetti comuni, per esempio cittadini di uno stato.

Il punto centrale, in virtù di quanto in questo capitolo è stato analizzato e di quanto dimostrato nella stessa intera inchiesta riguardante la mole di informazioni che la NSA riuscì ad estrapolare dai suoi stessi cittadini (si ricordi anche solo quanto riportato alla nota 31, in riferimento al *Boundless Informant),* consiste nel fatto che secondo quanto previsto dalla sezione 702, alle operazioni di sorveglianza potevano essere sottoposte esclusivamente soggetti stranieri (*"foreign power",* paragrafo *1801)*.

2) Il *GCHQ* e il *RIPA*: Tramite il relativo progetto *Tempora*, che abbiamo visto nel paragrafo 4.3, anche il *GCHQ (Government Communications Headquarter)* britannico è ritenuto da noi degno di nota nell'analisi dal filtro giurisprudenziale. Parallelamente, e in stretta collaborazione, con la *NSA*, anche il servizio d'intelligence della Corona si è dovuto confrontare con il suo corrispettivo della FISA americana.

---

[54] "The Guardian NSA files: decode", Section 5, TheGuardian.com https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/5

[55] Ibidem

[56] Ibidem

[57] *"Il paragrafo 1801 include nella definizione di "foreign power" non solo i governi e le istituzioni di uno Stato straniero, ma anche organizzazioni politiche situate all'estero purché non composte da personale americano…"*

SENIOR M. (november 25, 2013) *"Il datagate ed i limiti del diritto"*, Medialaws.eu http://www.medialaws.eu/il-datagate-ed-i-limiti-del-diritto/

Il raggio d'azione, nonché le conseguenti modalità, dell'*GCHQ,* sono infatti regolate da un atto del Parlamento volto alla regolamentazione delle attività di sorveglianza, in materia di indagini e intercettazioni riguardanti le comunicazioni, degli enti a queste predisposti: Il *Regulation of Investigatory Powers* Act (*RIPA)* del 2000. Tramite questo strumento, si disciplinano le modalità con le quali è possibile condurre operazioni di sorveglianza, nonché l'accesso alle comunicazioni elettroniche di una specifica persona. Brevemente: proprio come la FISA, il *RIPA* distingue a sua volta tra *"internal ed external communications"*[58]: nel il primo caso, quindi per comunicazioni interne alla nazione, la sezione 8 dell'atto normativo prevede l'applicazione di svariati passaggi e la necessità di altrettante verifiche in merito all'operazione di sorveglianza che l'ente è intento a svolgere. Nel secondo, di fronte a materiale di analisi estera, le disposizioni restano generiche e vi si riscontra quindi la totale assenza della necessità di identificazione di una persona specifica e della relativa monitorizzazione.
Esattamente come l'*NSA,* il servizio britannico, ha tuttavia bypassato completamente le procedure per la sorveglianza interna disciplinate dalla sezione 8 del *RIPA,* andando ad acquisire dati sensibili di milioni di cittadini del Regno Unito, proprio per mezzo della sua possibilità di accesso, che dalle rivelazioni di Snowden risale a giugno 2010, ai *database* del programma americano *PRISM.*

[58] Ibidem

"Se foste nella mia posizione privilegiata, se viveste in un paradiso come le Hawaii, e faceste un sacco di soldi, cosa potrebbe spingervi a lasciarvi tutto alle spalle?' La mia più grande paura riguardo alle conseguenze per l'America di queste rivelazioni è che non cambi nulla. Ho paura che la gente venga a conoscenza di tutte queste cose dai media, comprenda fino a che punto il governo è in grado di spingersi unilateralmente per esercitare un maggiore controllo sulla società americana e globale, ma che alla fine non sia disposta a correre i rischi necessari per contrastare questo stato di cose e costringere i propri rappresentanti ad agire sul serio nel suo interesse. E nei prossimi mesi, nei prossimi anni, non potrà che peggiorare, se non verrà il giorno in cui cambieranno le politiche. Perché l'unico limite alle attività di sorveglianza dello stato sono le politiche. Anche quando si fanno accordi con altri stati sovrani, siamo portati a pensare che siano frutto di politiche anziché di leggi. Ed è così che, quando verrà eletto un nuovo leader, ci diranno: 'Per via della crisi, per via dei rischi che corriamo nel mondo, di una nuova minaccia imprevista, abbiamo bisogno di esercitare una maggiore autorità, abbiamo bisogno di più potere'.
E a un certo punto, nessuno potrà fare più niente per opporsi, perché il potere sarà diventato una tirannia."

-Edward Snowden

-Edward Snowden, video-intervistato da Glenn Greenwald, *The Guardian*[59]

[59] Brignardello R. "*Traduzione della video-intervista con Edward Snowden"* https://alaskahub.org/traduzione-della-video-intervista-con-edward-snowden/

Capitolo 4 - Tecnologia e potere: i dati come arma politica, il caso Cambridge Analytica

«Il caso che è esploso è quello delle presidenziali 2016, ma la società era grande, lavoravamo su molte elezioni in giro per il mondo. Sviluppavamo anche progetti commerciali, non solo politici. Trump era uno dei tanti clienti. Importante, ma uno dei tanti."

-Britanny Kaiser, ex Direttrice del settore buisness di *Cambridge Analytica*[60]

Nel terzo capitolo di questa tesi, dopo aver visto il ruolo dei *Data* in chiave di sorveglianza e spionaggio, andremo ad analizzare la loro potenzialità in chiave elettoriale, quindi, la loro declinazione di una vera e propria arma politica. Al fine di condurre tale ricerca, era inevitabile descrivere lo scandalo riguardante *Cambridge Analytica,* una società di raccolta dati che nel 2018 è stata accusata, dopo le dichiarazioni del suo *whisthleblower*, nonchè ex dipendente Christopher Wylie, di aver *"utilizzato informazioni personali prese senza autorizzazione all'inizio del 2014 per costruire un sistema che potesse profilare singoli elettori statunitensi, al fine di indirizzarli con annunci politici personalizzati."*[61]
Il contesto in cui ci muoveremo, infatti, saranno le elezioni presidenziali statunitensi del 2016, nelle quali, come vedremo, *Cambridge Analytica* svolse un ruolo chiave nella vittoria di Donald Trump, proprio grazie ad un sistema di manipolazione e condizionamento di milioni di cittadini americani "incerti" riguardo al voto tramite lo strumento della *psicometria*, conoscendone cioè le personalità al fine di creare contenuti social *ad hoc* per lo scopo appena descritto.

1. La personalità delle persone come fonte di dati: la scienza della *psicometria*

"Abbiamo sfruttato Facebook per raccogliere milioni di profili di persone. E abbiamo costruito modelli per sfruttare ciò che sapevamo su di loro e prendere di mira i loro demoni interiori. Questa era la base su cui è stata costruita l'intera azienda. "

-Christopher Wylie, ex dipendente di *C.A.*, in seguito informatore dell'*Observer*[62]

Dalle parole dell'ex dipendente della società inglese, oltre ad annunciare l'altro complice principale nella vicenda, *Facebook,* si rivelano ben evidenti gli strumenti usati e le relative modalità di operazione che furono messi in campo. A tal proposito, al fine di comprendere come *Cambridge Analytica* sia riuscita ad influenzare

60 GAGGI M. (15 novembre 2019), Corriere.it *"L'ex ragazza di Cambridge Analytica «Manipolavamo tutto: voti, comportamenti e coscienze»"* https://www.corriere.it/sette/esteri/19_novembre_15/ex-ragazza-cambridge-analytica-manipolavamo-tutto-voti-comportamenti-coscienze-b754fc80-055d-11ea-a1df-d75c93ec44da.shtml
61 *"Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach"*, TheGuardian.com https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
62 Ibidem

circa un quarto degli elettori americani, diviene necessario partire dalla scienza sui cui si è fondata la potenza della società ai cui vertici erano l'A.D. Alexander Nix e il suo vice Steve Bannon (il quale, una volta lasciato tale ruolo, sarebbe andato a coordinare l'intera campagna elettorale dell'attuale presidente statunitense): la *psicometria*. Dalla Treccani leggiamo che per tale metodo scientifico si intende*"L'insieme dei metodi d'indagine psicologica che tendono al raggiungimento di valutazioni quantitative del comportamento umano o animale."*[63] E' proprio su tale "indagine", volta alla sempre più completa conoscenza della psicologia e della personalità delle persone, che *Cambridge Analytica* fondava la sua ricchezza nel mercato dei *Data*, nonchè il suo quotidiano lavoro. Tuttavia, nello svolgere un'indagine, qualunque essa sia, si ha la necessità di avere delle fonti dalle quali estrarre informazioni, ed ecco che il ruolo dei *Data* nella vincenda si fa chiaro: l'immenso contenitore dal quale la società di Nix e Bannon estraeva miliardi di dati sensibili, giungendo poi a condizionare più di 50 milioni[64] di elettori negli USA, fu individuato in *Facebook*. Infatti, al fine di operare al meglio in chiave di *"microtargeting comportamentale"*, ovvero l'inserimento massiccio di pubblicità altamente personalizzata su ogni persona (concretizzati poi in contenuti a scopo elettorale sugli individui staunitensi al fine condizionarne la scelta di voto), *Cambridge Analytica* riuscì ad estrapolare i *big data* tramite i profili che ognuna di esse possedeva sulla piattaforma di Zuckerberg. Per comprendere al meglio l'efficenza che tramite i *Social Networks* la *psicometria* è oggi riuscita a raggiungere, dai tratti inquietanti ma quantomai esplicativi, riportiamo le parole di Vesselin Popov, del *Cambridge Psychometrics Centre*: *"Oggi la maggior parte delle domande che uno psicologo porrebbe ha già una risposta in forma digitale. Non è più necessario stendere le persone su un lettino, basta che condividano i loro profili social. Monitorando la loro attività online puoi persino diagnosticare malattie: la depressione, per esempio. Ma puoi capire tanti altri aspetti della loro personalità. Si possono addirittura fare analisi predittive, scoprire delle cose prima che le sappiano i diretti interessati. Il caso più clamoroso è di una catena di supermercati americani che è riuscita a dedurre che una donna fosse incinta semplicemente analizzando i dati dei suoi acquisti. Le hanno proposto via mail prodotti per neonati prima ancora che lei sapesse di aspettare un bambino."*[65]

63 Voce *"psicometria",* Enciclopedia Treccani https://www.treccani.it/enciclopedia/psicometria/

64 *"Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach",* TheGuardian.com https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

65 RAI (22 marzo 2018) "*Cambridge Analytica. La psicometria ai tempi dei social network*, YouTube https://www.youtube.com/watch?v=n9F8glhhw5w

1.2 L'arma della *psicometria* a *Cambridge Analytica*: *Facebook* e *l'app* di *Kogan*

"Non lavoriamo con i dati di Facebook e non abbiamo i dati di Facebook".[66]

-Alexander Nix, Amministratore Delegato di *Cambridge Analytica*

Una volta appurato il sistema di raccoglimento dei *data*, scaviamo nel 2014 allo scopo di comprenderne la nascita ed analizzarne tecnicamente lo svolgimento. In quell'anno, infatti, tra le aule dell'Università di Cambridge, il professor Aleksandr Kogan portava a termine la realizzazione di una particolare *app* che si sarebbe poi rivelata, come ora vedremo, il "cavallo di Troia" di *C.A.* per accedere alle informazioni degli utenti *Facebook*: *"thisisyourdigitallife"* (*"Questa è la tua vita digitale"*). All'utente che la scaricava veniva fornito, analizzandone l'attività sul web, un personale profilo dal punto di vista della psciologia, nonchè probabili previsioni attitudinali: in poche parole, le persone si sarebbero sottoposte ad una "seduta online" di *psicometria*, senza però poter comprendere a chi realmente sarebbero giunte le informazioni in ultima istanza. Lo sfruttamento del *Social Network* n.1 di *Silicon Valley* da parte dell'invenzione di Kogan veniva attuato secondo le modalità di accesso delle persone alla stessa app. Spiegava a tal riguardo Emanuele Menietti per il *Post:"Per utilizzarla, gli utenti dovevano collegarsi utilizzando Facebook Login, il sistema che permette di iscriversi a un sito senza la necessità di creare nuovi username e password, utilizzando invece una verifica controllata da Facebook. Il servizio è gratuito, ma come spesso avviene online è in realtà "pagato" con i dati degli utenti: l'applicazione che lo utilizza ottiene l'accesso a indirizzo email, età, sesso e altre informazioni contenute nel proprio profilo Facebook."*[67] (Di queste parole, oltre al fatto di rendere quantomai idonea la definizione dell'app che abbiamo dato all'inizio della seguente pagina, ne sottolineamo l'importanza dal momento in cui descrivono, nel finale, la commercializzazione totale dei dati degli utenti, quindi, della loro stessa vita). L'*app*, utilizzata da Kogan tramite l'azienda *Global Sciences Research*[68] di cui era direttore, sarebbe giunta a "fare sue vittime" inizialmente circa 270mila utenti *Facebook*. Utilizziamo il termine "inizialmente" perché, venendo al punto centrale della questione, l'operazione di rastrellamento di dati sensibili svolta, come sarebbe poi stato rivelato durante l'inchiesta, avrebbe coperto non solo i diretti iscritti all'*app*, bensì anche tutti gli *amici Facebook* di quest'ultimi: l'invenzione del professore, così agendo, violava *tout court* le politiche di regolamentazione in materia della piattaforma, le quali consentivano il reperimento dei dati al solo scopo di incrementare la qualità del prodotto e del servizio offerti a coloro che la scaricavano. Tuttavia, le conseguenti limitazioni apportate da *Facebook* in materia, giunsero troppo tardi: il sistema elaborato da Kogan, sulla base dei 270mila iscritti, riuscì a costruire un archivio, contenente qualsiasi tipo di

66 "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", TheGuardian.com https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

67 MENIETTI E. (Lunedì 19 marzo 2018), *"Il caso Cambridge Analytica, spiegato bene"*, IlPost.it https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/

68 CARISSIMO J. (APRIL 22, 2018) *"Who is Aleksandr Kogan?"*, Cbsnews.com https://www.cbsnews.com/news/aleksandr-kogan-who-is-university-of-cambridge-lecturer-facebook-cambridge-analytica-scandal-2018-04-21/

informazione utile a scopi psicometrici, di circa 50 milioni di profili, che non tardarono a passare nelle mani di *Cambridge Analytica*, violando il regolamento del *Social Network* che prevede il divieto per i *"proprietari di app di condividere con società terze i dati che raccolgono sugli utenti."*[69] L'arma da "guerra elettorale" di Nix e Bannon, che avrebbe portato Donald Trump a capitanare la Casa Bianca nel 2016 aveva ora la sua arma, al resto, ci avrebbero pensato gli algoritmi.

1.3 Quei "due anni di troppo" e la complicità di *Facebook*

"Potrebbero avere molti dati ma non saranno i dati degli utenti di Facebook. Potrebbero essere dati sulle persone che sono su Facebook che hanno raccolto da soli, ma non sono dati che abbiamo fornito ".[70]

-Simon Milner, direttore delle politiche britanniche di Facebook

Insieme a *Cambridge Analytica*, l'azienda di Zuckerberg si è ritrovata al centro dell'inchiesta. Il coinvolgimento "non ortodosso" del *Social Network* più diffuso al mondo, è stato messo in luce dalle dichiarazioni del *whistleblower* dell'agenzia inglese, dalle quali si evince che esso sarebbe stato al corrente dell'enorme traffico sui suoi dati già a partire dalla messa in funzione dell'*app* di Kogan. Nonostante il reperimento di dati che quest'ultima portava avanti, con il sistema "dati dell'utente = dati di tutti gli amici dell'utente" come abbiamo visto nel precedente paragrafo, fosse in linea con le condizioni d'uso di *Facebook*, il problema si pose in un preciso momento della storia. Infatti, non appena Kogan condivise l'archivio che era riuscito a creare con *Cambridge Analytica*, bypassò letteralmente il regolamento dell'azienda di *Silicon Valley*, che vietava espressamente alle *app* di fornire i suoi dati ad elementi terzi. Considerato ciò, *Facebook* avrebbe potuto, (nonchè dovuto, in quanto chiara era la violazione in tal caso), agire in chiave di sospensione dell'account reo della condivisione dei *data*. Tuttavia, tale provvedimento nei confronti di *Cambridge Analytica* sarebbe giunto solo due anni più tardi. Vi è di più: secondo quanto ammesso in seguito dai legali dell'azienda, come leggiamo nella ricostruzione de *Il Post*[71], fu la stessa *C.A.* ad autodenunciarsi con *Facebook*, evidemente ben consapevole riguardo alla possbilità di subire la sospensione di cui prima. E' quindi a questo punto che s'innalza l'alone di dubbio sull'effettivo coinvolgimento di *Facebook*, in quanto non risultò chiaro perché la definitiva sospensione[72] di *C.A.* giunse solo venerdì 16 marzo 2018, proprio in prossimità della pubblicazione delle testate d'inchiesta al riguardo.

---

69 https://www.facebook.com/terms/

70 "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", TheGuardian.com https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

71 MENIETTI E. (Lunedì 19 marzo 2018), "Il caso Cambridge Analytica, spiegato bene", IlPost.it https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/

72 GREWAL P. (16 MARZO 2018), *"Suspending Cambridge Analytica and SCL Group From Facebook", aboutfb.com* https://about.fb.com/news/2018/03/suspending-cambridge-analytica/

"Questa per me è stata la cosa più sorprendente. Hanno aspettato due anni e non hanno fatto assolutamente nulla per verificare che i dati fossero stati cancellati. Tutto quello che mi hanno chiesto di fare è stato barrare una casella su un modulo e rispedirlo. "[73]

-Christopher Wylie, whistleblower ed ex dipendente di *C.A.*

2. Dalla raccolta all'azione: i *data* nella campagna elettorale

Dopo aver analizzato come *Cambridge Analytica* sia riuscita ad immagazzinare gli archivi di dati corrispondenti a circa 50 milioni di utenti *Facebook*, andiamo ora a vedere come questi sono stati utilizzati come una vera e propria "arma politica" a scopo elettorale nelle presidenziali USA del 2016.

2.1 Dai finanziamenti di Mercer al *Progetto Alamo*: l'organizzazione

Alla base della "macchina da guerra elettorale" di Trump, Steve Bannon svolse un ruolo chiave, proprio dopo aver lasciato la poltrona di vice di Alexander Nix, in *Cambridge Analytica*. Agendo da mente nell'organizzazione che avrebbe portato l'attuale presidente USA a trionfare sulla Clinton, aveva iniziato a preparare il campo di battaglia ben prima del 2016. Il sistema di raccolta dati dell'azienda di Nix, che abbiamo analizzato precedentemente, fu infatti finanziato[74] da Bannon nel 2014 tramite un'investimento pari ad 1 milione di dollari per l'acquisto di quest'ultimi. Inoltre, da quanto riportato dal Washington Post grazie alle dichiarazioni del whistleblower di *C.A.*, la consapevolezza di Bannon riguardo alla potenzialità che i *data* avrebbero potuto avere in chiave elettorale, fu confermata dal fatto che ricevette *"dalla Cambridge Analytica* è […] *oltre 125 mila dollari in compensi per le sue consulenze."*[75] Tuttavia, il ciclo di finanziamenti che la società inglese ricevette non si limitò alla volontà del suo stratega e vice-presidente: vista la rilevanza che *Cambridge Analytica* stava assumendo nel possedere quel capitale milionario di dati sensibili, incrementò la potenzialità di quest'ultimi, aggiungendo alla preziosa consulenza di Steve Bannon, l'appoggio del repubblicano Robert Mercer[76], che da parte sua, investì la cifra di 15 milioni di dollari nel progetto. Eravamo davanti alla defintiva presa di coscienza che la fase elettorale di una campagna politica, poteva essere portata avanti grazie allo strumento della psicometria, assicurato in quel caso da *Cambridge Analytica:* gli interessi di influenti uomini d'affari e quelli dell'alta tecnologia si incontrarono alla perfezione dando vita al sistema che avrebbe rivoluzionato il modo di fare politica in un contesto dalla portata delle presidenziali statunitensi,

---

[73] "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", TheGuardian.com https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[74] (21 marzo 2018)*"Bannon, l'ex stratega di Trump, "mente" di Cambridge Analytica. Tajani: "Zuckerberg deve spiegare"*, Sezione "Esteri" LaRepubblica.it https://www.repubblica.it/esteri/2018/03/21/news/bannon_l_ex_stratega_di_trump_la_mente_di_cambridge_analytica-191810903/

[75] Ibidem

[76] ROSENBERG M., CONFESSORE N. and CADWALLADR C. (March 17, 2018) *"How Trump Consultants Exploited the Facebook Data of Millions"* New York Times https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

ma che allo stesso tempo, avrebbe messo in forte dubbio il rispetto di diritti quali la *privacy* di milioni di cittadini, intaccando le fondamenta del sistema democratico moderno. Arriviamo quindi a metà del 2016, quando a San Antonio, Texas, Bannon e l'allora gestore dell'ambito *social* di Trump Brad Parscale, danno vita al *Progetto Alamo*[77]. Una votla che si possedevano dati riguardanti 50 milioni di potenziali elettori americani, corrispenti a circa un quarto del totale, non restava che sfruttare le efficentissime tecniche psicometriche di *C.A.* perchè degli algoritmi ne influenzassero il voto.

"Le regole non contano per loro. Per loro, questa è una guerra, ed è tutto giusto."[78]

-Christopher Wylie

2.2 La vittoria di Trump: tra *fake news* e inserzioni targetizzate

L'applicazione della psicometria a scopo elettorale fu l'asso nella manica di Bannon e compagni per portare Trump a raggiungere la Casa Bianca. Conoscendo il profilo psicologico e prevedendo i comportamenti di milioni di statunitensi cui il profilo *Facebook* fu reso un vera e propria fonte di informazione, nonchè un campo di manipolazione, il *Progetto Alamo* riuscì a spostare le percentuali andando ad agire minuziosamente sui *social network* di quest'ultimi. Lo schema di indirizzamento di voto, infatti, si basava sul concetto di "stanare", allo scopo di condizionarne la scelta di voto, quegli elettori che risultavano ancora non convinti del candidato su cui riporre la propria fiducia: coloro che il team di C.A. individuò quali *"persuadables"*, appunto, gli "indecisi". In un articolo[79] su *epolitcs.it* risalente a luglio scorso, Lucrezia Lela spiega quantomai esaustivamente ed in pochissime parole come dagli uffici di Parscale e Bannon si lavorava alla manipolazione di tali individui, inondando letteralmente le loro bacheche *Facebook* di messaggi personalizzati (solo di questi se ne contavano circa 100mila al giorno[80], secondo le tecniche di Parscale), post riportanti *fake news* e altrettanti contenuti pubblicati da profili falsi, noti come *bot*, cioè, automaticamente generati *ad hoc*. E' così, che, profondamente studiate divise per regioni ben definite al fine di comprendere dove operare e in quale intensità, le "prede" della macchina elettorale basata sulla psicometria e sul targeting altamente personalizzato, "scelsero" il loro candidato. Il trionfo del modello di campagna elettorale, pensata da Bannon, armata da *Cambridge Analytica*, si basò infatti su una fortissima collaborazione delle principali piattaforme *social*, che come abbiamo visto, rappresentano la primaria fonte di *data*, non a caso già definiti "l'oro del 21esimo secolo".

---

[77] D'ALESSANDRO J. (10 aprile 2018) "Dal Progetto Alamo di Trump a Cambridge Analytica, cosa c'è da sapere" Repubblica.it https://rep.repubblica.it/pwa/evergreen/2018/04/10/news/facebook_zuckerberg_cambridge_analytica-193519143/

[78] Ibidem

[79] LESA L., (7 luglio 2020), *"Facebook e Cambridge Analytica per Trump 2016"*, https://www.epolitics.it/articolo/69

[80] POLITANO' M., (1 marzo 2018), *"Chi è Brad Parscale, l'arma segreta di Trump per le elezioni del 2020"*, https://www.panorama.it/news/chi-e-brad-parscale-arma-segreta-trump-elezioni-usa-2020

A tal proposito, quanto accadeva negli uffici gestiti dal *guru* conservatore e Parscale, e animati dalle menti dei *social*, citiamo il consigliatissimo documentario[81] *Netflix* "*The Great Hack"*, basato sul libro[82] della seconda whistleblower di *Cambridge Analytica* Britanny Kaiser: *"Durante il periodo di maggiore attività del "Progetto Alamo" si investiva 1 milione di dollari al giorno in inserzioni pubblicitarie su Facebook. I rappresentanti di Facebook, YouTube e Google lavoravano tutti qui, erano nostri colleghi. In pratica, ci spiegavano come utilizzare le piattaforme al massimo delle loro possibilità."* In conclusione, la spiegazione della democrazia nell'era del *Cyber Space*: per gli indecisi sul voto non vi è problema, a loro penserà qualcuno di molto premuroso. Qualcuno che, come abbiamo potuto constatare, se ne prende cura talmente tanto bene da conoscerli più di quanto essi stessi non si conoscano. Tu non possiedi un cellulare con *Google* e un profilo *Facebook*, sono loro a possedere te.

Conclusioni

"I gotta admit that I'm a little bit confused, sometimes it seems to me as if I'm just being used."[83]

-*Dogs*, Pink Floyd (Animals, 1977)

Scrivevano così i Pink Floyd in studio registrando *Animals*, il capolavoro concepito dal genio di Waters che, ispirandosi alla fattoria di orwelliana memoria, continuava la serie di *concept albums*, iniziato con *The Dark Side of the Moon* nel '73, volti alla critica dell'alienante società capitalista. In effetti, al termine della ricerca da noi portata avanti al fine di strutturare la tesi che conosce qua il suo epilogo, ci sentiamo anche noi *"un po' confusi"* ed anche a noi pare, ancor più di prima, che *"a volte è come se fossimo solo usati"*. In chiunque possieda una sensibilità verso ciò che, secondo quanto da noi fin'ora sostenuto, la società del *Cyber space* sta minando dalle fondamenta, cioè la più autentica e profonda naturale identità dell'uomo, confidiamo la speranza che possa sentirsi come noi. Anzi, non ne dubitiamo affatto. Il tema che ci siamo posti di analizzare nelle sue principali declinazioni, è infatti ritenuto da noi una delle sfide più rilevanti che la generazione alla quale apparteniamo ha il dovere di affrontare. Come abbiamo potuto vedere, con il ribaltamento dei paradigmi in chiave di rivoluzioni e soggetti rivoluzionati, i tempi che corrono ci pongono di fronte al più che fondato dilemma riguardante il futuro della libertà umana, ormai quasi irreversibilmente compromessa da un sistema di ultra-capitalismo e di sorveglianza totale - e totalizzante - che trova la sua risorsa vitale nell'annientamento della spontanietà psico-critica delle persone stesse. Dalla dipendenza creata dagli strumenti che tale sistema

81 **"***The Great Hack - Privacy violata – Trailer Ufficiale",* (2019), Netflix Italia: https://www.youtube.com/watch?v=d2ob6ALzSLk

82 KAISER B. (2019), *La dittatura dei dati",* Harper Collins

83 *"Testo, Traduzione e Significato di Dogs",* Legendary Cover,it https://legendarycover.it/testi-traduzioni/pink-floyd/dogs/#:~:text=Significato%20di%20Dogs,-Dogs%20non%20%C3%A8&text=In%20Animals%2C%20invettiva%20dei%20Pink,ottenere%20denaro%2C%20potere%20e%20prestigio.

offre quali "servizi di connessione e condivisione" tra le persone (in primis i *Social Network),* fino al divenire a loro volta quest'ultimi strumenti di raccolta di dati sensibili, diviene inevitabile constatare quanto la pericolosità in chiave di violazione della *privacy*, nonchè di manipolazione delle scelte quotidiane di milioni di persone, superi in gran lunga i risvolti in chiave di comodità e praticità da essi provenienti. Dalla lettura sotto il filtro critico rivolto all'aspetto consumistico, quindi dell'uomo quale costante fonte di dati in quanto reso consumatore assetato di acquisti su *Amazon* o visualizzatore "a tempo indeterminato" di contenuti *"consigliati per te"*, fino all'analisi della moderna possibilità di pilotare la scelta elettorale, come il caso *Cambridge Analytica*[84] ci ha dimostrato, valori quali il libero arbitrio e la consapevolezza delle scelte quotidiane di milioni di personi non possono che essere messi in dubbio al termine di questo "viaggio" nel *Cyber space*. Ma secondo le logiche del *Capitalismo della sorveglianza*, non ci siamo fermati certo qua: il progresso tecnologico e la diabolica forza calcolante degli algoritmi, hanno dato la possibilità alle agenzie di sicurezza nazionali e alle istituzioni governative di mettere in piedi programmi di spionaggio e controllo che hanno superato di gran luga il *Big Brother* di *1984*, per citare ancora Orwell, dalle portate non precisamente quantificabili. Considerando infatti che, secondo quanto visto nel Capitolo 3 prendendo in analisi il *Datagate*, le relative operazioni della *NSA* e complici furono organizzate in base alle "possibilità" tecnologiche circoscrivibili al primo decennio del secolo corrente, è compito del lettore che si approccia all'argomento da noi trattato andare oltre la mera descrizione di ciò "che è stato", approcciandosi a quest'ultimo con la domanda rivolta a ciò che "è diventato oggi", per passare quindi alla previsione di ciò che "potenzialmente potrà essere domani". Questo, allo scopo di assumere un'approccio attivo nei confronti di un fenomeno dalla crescita esponenziale, le cui potenzialità sono dai noi ritenute dover essere tradotte in "pericolo". Infatti, di fronte al futuro che possiamo prevedere seguendo tali logiche critiche e di analisi, constatando l'esponenziale e apparentemente indomabile corsa verso un futuro di dittatura digitale, diviene essenziale, dopo la presa di coscienza in una prima fase, non perdere la bussola, dirigendo la propria rotta nella direzione contraria allo stato di inconsapevolezza in cui ancora i più dormono sogni troppo tranquilli. A tal proposito, ritroviamo le parole della Zuboff nel rammenarci che *"l'inevitabilità della tecnologia ci viene ripetuta come una sorta di mantra, ma si tratta di un sonnifero esistenziale che serve a farci rassegnare: un sogno che ci narcotizza lo spirito."* Quindi, che fare? Con la volontà di chiudere l'ultima sezione di questa tesi offrendo delle personali e dirette considerazioni dedicate a coloro i quali potrebbero non aver inquadrato l'importanza del tema fino in fondo, elencheremo una serie di spunti operativi, da attuare a partire dalla propria quotidianità. Agiamo in tal senso allo scopo non solo di rendere il nostro lavoro una descrizione delle forze che oggi gettano ombre sui "principi democratici ed inviolabili" sui quali esse stesse dichiarano di fondarsi e per il cui mantenimento opererebbero, ma anche, se non soprattutto, per porre chiunque ne abbia la volontà, nelle condizioni di poter accedere ad un determinato modo di pensare, per poi necessariamente in tal senso agire, in un mondo che già da troppo tempo sta soffocando tale aspetto dell'uomo: il filtro libero con cui osservare ciò che lo circonda, svincolato da ogni dogma imposto, agente in conformità con l'ordine naturale delle cose, nel solco dei rapporti

[84] Vedi paragrafo 2.2, Capitolo 4

autentici e profondi tra i suoi simili, contro la sua degradazione in *internauta*, individuo che insorge contro il destino, che terzi hanno già scritto per lui, di automa strisciante di carte di credito e battitore di tasti davanti a quello che più che uno schermo, è oggi una gabbia. 1) Recuperare uno spirito critico: osservare ciò che abbiamo davanti prima di interargirci. Navigare con la consapevolezza che sul *web*, prima che essere noi a fare una ricerca, è qualcun altro che sta cercando di conoscere noi. Sviluppare la capacità di saper leggere cosa può celarsi dietro al *click* che stiamo per fare, conoscerne la provenienza e lo scopo di chi ne ha deciso la posizione e il momento in cui apparire. 2) E' la pubblicità che viene da noi, non noi a cercare il prodotto: grazie alla *psicometria* e alla sempre più efficiente pubblicità targetizzata, la macchina consumistica ci contatta continuamente. Evitare di acquistare oggetti che realmente non ci servono solo perché *"in offerta solo oggi",* o perdere tempo in siti che non avremmo mai visitato se non ci fossero stati "proposti". *"Le cose che possiedi, alla fine, ti possiedono."*[85] 3) Autodeterminarsi e dominarsi: rimanere presenti a se stessi durante l'uso dei nostri smartphone, riuscire a conoscersi per comprendere se siamo veramente noi stessi a voler vedere determinati contenuti. Alcune *app*, programmate secondo studi neurologici, ci tengono attaccati allo schermo: leggerne e captare il senso dei tasti e dei simboli ad esse collegati, svelarne la reale natura, distaccarsene quando necessario. 4) Recuperare i legami autentici e reali: la nostra quotidianità, seppur non possa prescindere dall'uso degli strumenti tencologici, non deve tuttavia esserne scandita. Se siamo in compagnia, usiamo il meno possibile i nostri dispositivi: guarda negli occhi il tuo amico, interagisci con lui autenticamente, gli schermi alterano i rapporti tra persone. 5) Ritrovare se stessi: nella frenetica vita *smart* del cittadino del 2020, gli *smartphone* ci ricordano anche quando abbiamo riunioni o se dobbiamo prendere medicine, siamo noi ad esserci scordati di noi stessi. Quando possibile, distacchiamocene, torniamo a vivere il mondo che ci circonda nella sua profonda ed autentica realtà, facciamo una passeggiata iun montagna, torniamo nel verde, parliamo con noi stessi: distacchiamoci dal grigiore delle città e dell'illuminazione 24 ore su 24 degli schermi. Ritroviamo un centro e diamoci una direzione, solo allora i *capitalisti della sorveglianza* nulla potranno su di noi.

"Non tocca a noi dominare tutte le maree del mondo; il nostro compito è di fare il possibile per la salvezza degli anni nei quali viviamo, sradicando il male dai campi che conosciamo, al fine di lasciare a coloro che verranno dopo terra sana e pulita da coltivare."[86]

-Gandalf il Grigio, *Il Signore degli Anelli*

[85] TYLER DURDEN, (1999), *Fight Club*

[86] TOLKIEN J.R.R. (2003), *Il Signore degli Anelli*, Bompiani

Abstract

If the reader who approaches this thesis might want to close the document because it is considered the result of a "plotter" rather than a "digital paranoid", we would not be surprised.
And this is precisely the point we want to highlight, starting from the date that today marks the calendar.
It is 2020, the era of modernity and its revolutionary inventions is well over, we are in fact in the era in which the revolutionary subject is not matter at the hands of man, but man at the hands of what matter no longer is. We are in the "fourth industrial revolution": artificial intelligence, advanced technology and IOT ("Internet of Things"). If in the past man has managed to revolutionize limited aspects of his everyday life, such as being able to move faster by car, today the world in which he finds himself living, a computer and digital ocean in which he is catapulted and from which he seems to find no way out, varies. From the real, tangible, authentic world of matter and personal contacts between individuals, today he has projected himself into the field of study within which this thesis intends to investigate: the "cyber-space", the world of the web, the magnum sea of billions of clicks per second, of the infinity of data in which each person is "internauts". Web surfing, Facebook profiles, the billions of e-mails sent daily from one part of the planet to another, the incalculable number of clicks that every second decrees any decision of any individual, in two words, the "Big-Data". The scope of the revolution, which is advancing daily, in which man lives today is unparalleled in history, is even surpassed by the digitisation itself: today it is the "dataisation" of every aspect of life, this infinite river of information, that represents the energy that drives the whole world itself, whose "source of life" (of profit?) is man himself. From the inevitable projection on the web of his every action, thought, emotion and will derive data. But who needs them? Who can control such a mass of information? For what purpose? In the "cyber-space", the individuals themselves (the "internauts") represent the main, as well as vital, primary resource of those powers which, as we shall analyse, are defined "cyber-lobbies": multinationals, immense companies and digital giants in the information technology field that hold the monopoly in the "big-data" market, being themselves the only collectors of the latter, a purpose for which they were born and for which, according to the following thesis, they hold the real power in the era of the subversion of the merely political institution by the process of digitisation of each individual's life. By identifying the four main areas of the subject we are going to deal with, the thesis is divided into as many chapters. The first one, dedicated to the figure of the mass media, will analyse the impact that the digital revolution has had on the relationship between citizens, society and power, in an era where news is not only received at dinnertime by turning on the only television in the house, but appears autonomously on the screen of the telephone in our hands. In the second chapter we will see the crucial role of the "Big-Data" in what we might call the "new gold" of the post-modern era. From the daily digital activity of every citizen, we will analyse how the "Cyber-lobbies" - first of all Google - exploit their potential, collecting data and transforming it into an object of exchange in the market of the same and as a primary resource for the giants of ultra-capitalism. Going on, we will see how governments and military institutions can carry out huge mass control operations using data, thanks to the progressive development of

technology, as well as how the above mentioned companies collaborate with them, playing key roles in this field: for this purpose, we have chosen the valuable work, in the whistleblower role of the US Homeland Security Agency, of Edward Snowden, who gave birth to Datagate. Finally, we will develop the science of 'psychometrics' and how, through data rendering, it is possible to influence socio-political dynamics, arriving at the main case in point: the Cambridge Analytics scandal and data as real weapons in electoral terms. The rights and privacy of citizens, at a time when total digitization has provided new weapons for the arsenal of multinationals, in terms of consumerism and profit, and as many sources of power and control to government institutions, are far from being well established and guaranteed compared to what the founding constitutional charters of today's democracies tell us. New and much more powerful forms of governance with a planetary scope seem to have the possibility, certainly the potential, to replace the traditional political-administrative institutions. The irresistible hunger for profit, which has by now reached incalculable figures, of these "cyber-lobbies" and their outflow from any regulation on the privacy standards of the individual, has now placed them at the top of the pyramid of power in the society of hyper-technology and "big-data", reaching, as we shall see, beyond the highest spheres of government institutions. But at what cost? What weapons are these new holders of, now no longer of mere political and decision-making power, but of control over human life itself? What role do they play in the tables of governance, from the spheres of individual states to issues of planetary importance? How have "social-network" platforms such as Facebook, or search software such as Google, managed to gain a leading position in the research work of secret services and government institutions? How compatible is a system based on the control of man's everyday life as a primary resource of power with the democratic principles on which most institutions are founded and of which they declare themselves guarantors? Does the parallel world, invisible, digital and therefore detached from reality, represent the field of confrontation from which man's future or his end as we have always known it will come? These are the questions we have asked ourselves by beginning to observe the aspects of reality in which we are immersed daily and to which not many, too few in our opinion, seem to pay attention. It is starting from the question that at least each of us has asked ourselves at least once in our lives that we have come to analyse what is supported in this thesis: who is in charge of the world in which we live? Who influences the decisions of millions of people, once it has been demonstrated, as we shall see, that it is legitimate to wonder whether "free choice" still exists in certain circumstances? The theme that we have set ourselves to analyse in its main forms is in fact considered by us to be one of the most important challenges that the generation to which we belong has a duty to face. As we have seen, with the overturning of paradigms in terms of revolutions and revolutionized subjects, the times we are facing are the most well-founded dilemma concerning the future of human freedom, now almost irreversibly compromised by a system of ultra-capitalism and total surveillance - and totalizing - which finds its vital resource in the annihilation of the psycho-critical spontaneity of people themselves. From the dependence created by the tools that such a system offers as "connection and sharing services" between people (first of all Social Networks), to becoming in turn the latter tools for the collection of sensitive data, it becomes inevitable to see how much the danger in terms of violation of privacy, as well as manipulation of

the daily choices of millions of people, far outweighs the implications in terms of comfort and practicality coming from them. From reading under the critical filter aimed at the consumerist aspect, therefore of man as a constant source of data as a consumer made thirsty for purchases on Amazon or "indefinitely" viewer of contents "recommended for you", to the analysis of the modern possibility of driving the electoral choice, as the Cambridge Analytica case has shown us, values such as free will and awareness of the daily choices of millions of people can only be questioned at the end of this "journey" into Cyber space. But according to the logic of surveillance capitalism, we have not stopped there: technological progress and the diabolical calculating power of algorithms have given the possibility to national security agencies and government institutions to set up espionage and control programmes that have greatly surpassed the Big Brother of 1984, to quote Orwell again, whose scope is not precisely quantifiable. Considering, in fact, that, according to what we saw in Chapter 3, taking the Datagate into consideration, the relative operations of the NSA and its accomplices were organized according to the technological "possibilities" that can be circumscribed to the first decade of the current century, it is the reader's task to go beyond the mere description of what "has been", approaching the latter with the question of what "has become today", and then move on to the prediction of what "potentially could be tomorrow". This, in order to take an active approach to a phenomenon of exponential growth, whose potential we believe must be translated into "danger". In fact, in the face of the future that we can predict by following such critical and analytical logics, noting the exponential and apparently indomitable race towards a future of digital dictatorship, it becomes essential, after becoming aware in a first phase, not to lose the compass, directing one's course in the opposite direction to the state of unconsciousness in which most still sleep too peaceful dreams. In this regard, we find Zuboff's words in reminding us that "the inevitability of technology is repeated to us like a sort of mantra, but it is an existential sleeping pill that serves to make us resign ourselves: a dream that narcotizes our spirit". So, what to do? With the desire to close the last section of this thesis by offering personal and direct considerations dedicated to those who may not have grasped the importance of the topic to the end, we will list a series of operational cues, to be implemented starting from their daily life. We act in this sense with the aim not only of making our work a description of the forces that today cast shadows on the "democratic and inviolable principles" on which they themselves claim to be based and for whose maintenance they would operate, but also, if not above all, to put anyone who has the will to do so, in the conditions of being able to access a certain way of thinking, and then necessarily act in this sense, in a world that has been suffocating this aspect of man for too long: the free filter with which to observe what surrounds him, freed from any imposed dogma, acting in conformity with the natural order of things, in the wake of the authentic and profound relationships between his fellow men, against his degradation as an internaut, an individual who rises up against destiny, which third parties have already written for him, as an automaton crawling with credit cards and beating keys in front of what, more than a screen, is today a cage.

Bibliografia

Monografie:

- HEGEL G.W.F. (2000), *Fenomenologia dello spirito*, Armando Editore
- HEIDEGGER M. (1995), *L'abbandono,* Il Nuovo Melagnolo
- KAISER B., (2019), *La dittatura dei dati*, Harper Collins
- ORWELL G. (2016), *1984*, Mondadori
- TENNENINI R. (2019), *Schiavi Digitali*, Passaggio al Bosco Edizioni
- TOLKIEN J.R.R. (2003), *Il Signore degli Anelli*, Bompiani
- ZUBOFF S. (2019), *Il Capitalismo della Sorveglianza*, LUISS Universtiy Press

Documenti multimediali:

- *"Edward Snowden interview: 'The US government will say I aided our enemies' - NSA whistleblower"*, YouTube, The Guardian https://www.youtube.com/watch?v=Q_qdnyEqCPk

- *"Fight Club"* (1999), David Fincher

- RAI (22 marzo 2018) *"Cambridge Analytica. La psicometria ai tempi dei social network",* YouTube https://www.youtube.com/watch?v=n9F8glhhw5w

- *"The Great Hack - Privacy violata – Trailer Ufficiale",* (2019), Netflix Italia https://www.youtube.com/watch?v=d2ob6ALzSLk

- *"The Social Dilemma"* (2020), Netflix https://www.netflix.com/watch/81254224?trackId=254015180&tctx=0%2C0%2C1092ea01-d1dd-4dd1-8105-79f77c5f19a9-48274619%2C2b0f362e-3fdc-425c-a1c7-2cd844e63e92_42721550X20XX1600106810112%2C2b0f362e-3fdc-425c-a1c7-2cd844e63e92_ROOT%2C

Documenti in rete:

- *"Alphabet, la holding che controlla Google, è diventata la quarta società statunitense a raggiungere mille miliardi di dollari di capitalizzazione"*, Il Post https://www.ilpost.it/2020/01/17/alphabet-googl-mille-miliardi-capitalizzazione/
- *"Attività di ricerca e sviluppo avanzate"***,** Wikipedia https://www.sourcewatch.org/index.php/Advanced_Research_and_Development_Activity
- *"Boundless Informant heat maps"*, Edward Snowden.com https://edwardsnowden.com/2014/05/14/boundless-informant-heat-maps/
- *"Boundless Informant: the NSA's secret tool to track global surveillance data",* TheGuardian.com https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

- *"Che cos'è Tempora: il programma di sorveglianza elettronica britannico"* (24 ottobre 2013), Polisblog.it https://www.polisblog.it/post/166503/che-cose-tempora-il-programma-di-sorveglianza-elettronica-britannico
- *"Cos'è il datagate e com'è cominciato"* (25 giugno 2015), L'Internazionale https://www.internazionale.it/notizie/2015/06/25/datagate-snowden-spionaggio
- *"Gli algoritmi minacciano il libero arbitrio? Due tesi al confronto"*, Agenda Digitale https://www.agendadigitale.eu/cultura-digitale/gli-algoritmi-minacciano-il-libero-arbitrio-due-tesi-al-confronto/
- *"Lo scoppio della bolla delle c.d. DOTCOM"*, Consob.it http://www.consob.it/web/investor-education/la-bolla-delle-c.d.-dotcom
- *"NSA collected US email records in bulk for more than two years under Obama"*, TheGuardian.com https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama
- *"NSA collecting phone records of millions of Verizon customers daily"*, TheGuardian.com https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
- *"NSA Prism program taps in to user data of Apple, Google and others"*, The Guardian.com
- *"Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach"*, TheGuardian.com https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
- *"Significato di Generazione Z"*, Inside Marketing https://www.insidemarketing.it/glossario/definizione/generazione-z/
- *"Testo, Traduzione e Significato di* ***Dogs"*****, Legendary Cover,it** https://legendarycover.it/testi-traduzioni/pink-floyd/dogs/#:~:text=Significato%20di%20Dogs,-Dogs%20non%20%C3%A8&text=In%20Animals%2C%20invettiva%20dei%20Pink,ottenere%20denaro%2C%20potere%20e%20prestigio.
- *"The Foreign Intelligence Surveillance Act of 1978 (FISA)"*, U.S. Department of Justice, Justice Information Sharing https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286
- *"The Guardian NSA files: decode"*, Section 3, TheGuardian.com https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/3
- "The Guardian NSA files: decode", Section 5, TheGuardian.com https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/5
- (21 marzo 2018)*"Bannon, l'ex stratega di Trump, "mente" di Cambridge Analytica. Tajani: "Zuckerberg deve spiegare"*, Sezione "Esteri" LaRepubblica.it https://www.repubblica.it/esteri/2018/03/21/news/bannon_l_ex_stratega_di_trump_la_mente_di_cambridge_analytica-191810903/
- *Booz Allen Hamilton*, Wikipedia.org https://en.wikipedia.org/wiki/Booz_Allen_Hamilton
- Brignardello R. *"Traduzione della video-intervista con Edward Snowden"* https://alaskahub.org/traduzione-della-video-intervista-con-edward-snowden/
- CARISSIMO J. (APRIL 22, 2018) *"Who is Aleksandr Kogan?"*, Cbsnews.com https://www.cbsnews.com/news/aleksandr-kogan-who-is-university-of-cambridge-lecturer-facebook-cambridge-analytica-scandal-2018-04-21/
- CRENSON L.S. (February 18, 2003) , *"Researchers Working on Total Information Awareness Program"* Government Technology https://www.govtech.com/security/Researchers-Working-on-Total-Information-Awareness.html
- D'ALESSANDRO J. (10 aprile 2018) "Dal Progetto Alamo di Trump a Cambridge Analytica, cosa c'è da sapere" Repubblica.it https://rep.repubblica.it/pwa/evergreen/2018/04/10/news/facebook_zuckerberg_cambridge_analytica-193519143/
- GAGGI M**.** (15 novembre 2019), Corriere.it *"L'ex ragazza di Cambridge Analytica «Manipolavamo tutto: voti, comportamenti e coscienze»"* https://www.corriere.it/sette/esteri/19_novembre_15/ex-ragazza-cambridge-analytica-manipolavamo-tutto-voti-comportamenti-coscienze-b754fc80-055d-11ea-a1df-d75c93ec44da.shtml
- GELLMAN B. and SOLTANI A. (October 30, 2013) *"NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say"*, New York Times https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html
- GREWAL P. (16 MARZO 2018), *"Suspending Cambridge Analytica and SCL Group From Facebook", aboutfb.com* https://about.fb.com/news/2018/03/suspending-cambridge-analytica/
- GROSSO R. (8 marzo 2018), *"Dati e metadati per la PA, a che servono e come migliorano il rapporto con il cittadino."*, AgendaDigitale.eu
- HISTORY.COM EDITORS (Uptated: sep 25, 2019 – original: oct 29, 2009), *"Wategate Scandal"*, History.com https://www.history.com/topics/1970s/watergate
- https://www.agendadigitale.eu/cittadinanza-digitale/dati-metadati-la-pa-servono-migliorano-rapporto-cittadino/
- https://www.facebook.com/terms/
- https://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html?_r=0
- https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
- KASTRENAKES J. (March 7, 2016), *"FCC fines Verizon $1.35 million over 'supercookie' tracking"*, The Verge https://www.theverge.com/2016/3/7/11173010/verizon-supercookie-fine-1-3-million-fc
- LESA L., (7 luglio 2020), *"Facebook e Cambridge Analytica per Trump 2016"*, https://www.epolitics.it/articolo/69
- MARUCCIA A. (1 luglio 2013) *"Datagate, le intercettazioni dell'era Bush"*, Punto-informatico.it https://www.punto-informatico.it/datagate-le-intercettazioni-dellera-bush/
- MENIETTI E. (Lunedì 19 marzo 2018), *"Il caso Cambridge Analytica, spiegato bene"*, IlPost.it https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/
- POLITANO' M., (1 marzo 2018), *"Chi è Brad Parscale, l'arma segreta di Trump per le elezioni del 2020"*, https://www.panorama.it/news/chi-e-brad-parscale-arma-segreta-trump-elezioni-usa-2020
- ROSENBERG M., CONFESSORE N. and CADWALLADR C. (March 17, 2018) *"How Trump Consultants Exploited the Facebook Data of Millions"* New York Times https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

- ROSSANO A. (12 maggio 2015), *"Con la scusa del terrorismo ci tolgono i diritti"*
- SAVAGE C. and WEISMAN J. (May 7, 2015), *"N.S.A. Collection of Bulk Call Data Is Ruled Illegal",* New York Times
- SEIFERT B. (June 6, 2013) *"Secret program gives NSA, FBI backdoor access to Apple, Google, Facebook, Microsoft data"*,
- SENIOR M. (november 25, 2013) *"Il datagate ed i limiti del diritto"*, Medialaws.eu http://www.medialaws.eu/il-datagate-ed-i-limiti-del-diritto/
- SOLDAVINI P. *"Tutto quello che avreste dovuto sapere sul Datagate/Come è emerso il Datagate?"*, Il Sole 24ore https://st.ilsole24ore.com/art/notizie/2013-10-23/tutto-quello-che-avreste-voluto-sapere-datagate--come-e-emerso-datagate-225948.shtml?uuid=AB6tNuY
- *Stefano Rodotà denuncia la deriva europea",* L'Espresso https://espresso.repubblica.it/attualita/2015/05/12/news/con-la-scusa-del-terrorismo-ci-tolgono-i-diritti-stefano-rodota-denuncia-la-deriva-europea-1.212058
- SWISHER K. (19 dicembre 2000), *"Dot-Com Bubble Has Burst; Will Things Worsen in 2001?",* The Wall Street Journal https://www.wsj.com/articles/SB977091183365350 99
- TheVerge.com https://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism
- Voce *"psicometria",* Enciclopedia Treccani https://www.treccani.it/enciclopedia/psicometria/