Dipartimento di Scienze Politiche e delle Relazioni Internazionali

Cattedra di Sociologia della Comunicazione

Internet garantisce la libertà? Un'analisi dell'*e-governance* e i problemi ad essa relativi.

RELATRICE
PROF.SSA Emiliana De Blasio

CANDIDATA
Federica Fusco
MATR. 077052

ANNO ACCADEMICO 2016/2017

A mia nonna,

INDICE

INTRODUZIONE

Internet ha cambiato la società o quantomeno ci ha offerto degli strumenti per vivere in un modo diverso. Le nuove tecnologie hanno permesso la creazione di una società fortemente interconnessa dove i concetti di spazio e tempo sono contratti. Ciò ha portato allo sviluppo e alla nascita di nuove forme di aggregazione virtuale che si sono poi trasformate in associazioni e forme di protesta reali (Sorice, 2009). L'ottimismo si è subito diffuso insieme all'idea che una società più democratica sarebbe subito nata. Tuttavia la più ampia diffusione del *web* non è stata accompagnata da un maggiore sviluppo dei diritti all'interno del nostro mondo. Nonostante le caratteristiche della rete abbiano dato agli individui-*user* la possibilità di modificare i contenuti e di agire in uno spazio senza confini, alcuni diritti e libertà individuali continuano ad essere a rischio (De Blasio & Sorice, 2016). L'idea che la tecnologia di per sé stessa sia portatrice di miglioramento sociale non trova alcun fondamento nella realtà. Ogni tecnologia può essere utilizzata con fini diversi rispetto a quelli pensati da chi l'ha creata. Lo stesso *Internet* è stato inizialmente concepito per assolvere compiti molto dissimili rispetto a quelli che oggi ci spingono al suo utilizzo (Morozov, 2011). Questo significa che non può esistere uno strumento di comunicazione che cambi le strutture di potere all'interno della società, anzi al contrario è la società che in determinati contesti modifica ciò che ha innanzi a sua immagine e somiglianza (Deibert & Rohozinski, 2010). Questo è ciò che avviene in Cina, ad esempio, dove il *web* è uno strumento con cui lo Stato amplia il suo potere e la sua censura (Morozov, 2011). Bisogna inoltre considerare che il sistema di *governance* che regola *Internet* è fatto di numerosi attori privati che controllano le infrastrutture e i contenuti che circolano *online* (Santaniello & Amoretti, 2013). Ne consegue che siamo innanzi a una vera e propria mancanza di democraticità della quale inoltre pochi individui sono realmente consapevoli. La maggior parte, infatti, degli utenti percepisce il *web* come un luogo privo di minacce. Anche perché molti degli aspetti relativi alla *governance* del *web* sono particolarmente tecnici e spesso, dunque, anche di difficile comprensione per i più. La situazione non è comunque omogenea in tutte le parti del mondo, vi sono luoghi in cui i governi hanno un maggior controllo sulle loro infrastrutture tecnologiche e sui contenuti che circolano *online.* Tuttavia in questi luoghi è la stessa libertà di espressione dei singoli ad essere minacciata. In Occidente vi è un modello di *governance* che è stato definito *multiskateholder* dove diversi sono gli attori che gestiscono il *web*, i governi sono esclusi dal processo di definizione delle regole, o quantomeno dovrebbero esserlo secondo la retorica che alimenta questo modello (Sorice & De Blasio, 2016). Tuttavia nei momenti di forte tensione, soprattutto dopo attacchi terroristici di un certo rilievo, una delle prime reazioni da parte dei governi occidentali è quella di controllare la circolazione di informazioni e dunque il *web*. Un controllo che spesso non viene compreso dai cittadini e che mina il concetto della democrazia stessa. Difatti quanto può dirsi democratica una società che mina alla libertà degli individui, nel luogo in cui questi si sentono più sicuri, in nome della sicurezza?

La protezione della *privacy* degli individui sta diventando uno dei problemi maggiormente dibattuti anche alla luce dello sviluppo di tecnologie che grazie allo sfruttamento di particolari algoritmi riescono a raccogliere informazioni di vario genere sugli utenti che vengono principalmente utilizzate per fini commerciali (Willson, 2016). Questo significa che gli individui in Occidente rischiano di vedere minacciata la loro libertà da più fronti, senza esserne assolutamente coscienti. Una maggiore tutela della *privacy* e della democraticità *online* secondo alcuni potrebbe essere raggiunta attraverso la creazione di una rete completamente neutrale. Si intende neutrale una rete che garantisce l'accesso a tutti senza andare a guardare i pacchetti di informazioni che i singoli si scambiano (Rodotà, 2013).

Dopo il caso Snowden si è incominciato a mettere in discussione, anche a livello di opinione pubblica ma soprattutto accademico, il modello di *governance* attuale del *web.* In particolare si è cercato di vedere come creare un modello maggiormente democratico che garantisca la pubblicità e la trasparenza circa la gestione di *internet*. Uno dei principali attori coinvolto in questo processo è l'*Internet Social Forum*, ente nato subito dopo il caso Snowden. Uno degli altri obiettivi degli ultimi anni è quello di ritrovare lo spirito del primo *web* e utilizzare il mezzo di comunicazione come uno strumento per incentivare la partecipazione dei cittadini alla vita pubblica attraverso pratiche. Probabilmente ciò che concretamente il *web* è riuscito a fare, in questo senso, è stato garantire una maggiore trasparenza dei governi attraverso pratiche di *e-government* e che però rischia di essere fine a sé stessa se non accompagnata da una concreta volontà politica di innovazione democratica. Tutte queste tematiche verranno approfondite nelle pagine a seguire.

I CAPITOLO

La nascita di Internet: le potenzialità del nuovo mezzo di comunicazione.

1.1 Lo spirito delle comunità virtuali: il *cyberottimismo*.

Internet nasce negli anni sessanta con Arpanet un progetto della difesa militare statunitense realizzato dall'agenzia *DARPA* che si occupava dello sviluppo di nuove tecnologie. Siamo nel 1969, in piena guerra fredda, e gli Stati Uniti necessitano di un sistema di telecomunicazioni avanzato che gli permetta di scambiare informazioni sensibili.

Grazie alla diffusione dei primi personal computer, ad opera della Commodore e dell'Ibm, Arpanet ha potuto diffondersi oltre i ranghi accademici e militari, consentendo l'accesso alla nuova tecnologia a sempre più persone. Il momento di svolta si raggiunse grazie alla nascita del *World Wide Web* creato da Tim Berners Lee nel 1991. Lee crea un sistema basato sull'iper-testo che è riuscito a garantire il collegamento a Internet non solo agli enti governativi della difesa, ma anche a industrie, organizzazioni no-profit e, infine, agli individui. Inoltre per favorirne una sempre più ampia diffusione nel 1993 lo scienziato trasforma il *World Wide Web* in un *public domain*. In questo modo un'invenzione nata come mezzo di trasmissione di dati per un'*elites*, si prepara a diventare "*il mezzo di comunicazione rappresentativo della società post-moderna*" (Haigh, Russell, & Dutton 2015, pp.183). Nel corso degli anni '90 Internet ha incominciato a essere parte della nostra vita quotidiana. Tutto inizia a spostarsi on-line e il mondo digitale inizia a diventare uno dei pilastri del mondo, cosiddetto, reale. Se la televisione rappresentava di fatto "*una finestra sul mondo", il Web è da considerarsi "il mondo di per sé stesso"* (Haigh, Russell, & Dutton, 2015, pp. 187). Un universo fatto da milioni di persone interconnesse fra loro che cercano, sempre più spesso, dei modi per diventare protagoniste on-line. Di fatti la peculiarità, non subito colta, del nuovo mezzo è proprio quella di avere dato la possibilità agli utenti di prendere attivamente parte al processo di creazione dei contenuti *on-line*. I tradizionali mezzi di comunicazione ritenevano che Internet fosse un semplice canale di trasmissione di notizie controllate e gestite dai tradizionali *broadcaster.* Al contrario invece la possibilità di generare contenuti aumenterà sempre di più anche grazie alla nascita dei social media[1].

Internet si trasforma pia piano in un non-luogo all'interno del quale ogni singolo individuo si trasforma in giornalista, opinionista ed esperto. Possiamo parlare di auto-comunicazione di massa, secondo il sociologo

[1] I social media nascono già negli anni '90 con i blog che consentivano un'interazione grazie a delle *bulletin board* (bacheche elettroniche). Tuttavia la più ampia diffusione si ha nella prima metà degli anni 2000. Si definisce *social media* uno strumento di Internet basato su presupposti tecnologici, e ideologici che consentono la creazione e lo scambio di contenuti generati dagli utenti. (Kaplan & Haenlein, 2010)

Manuel Castells (Castells, 2009), perché chiunque può produrre contenuti da sé. In generale è proprio la massa a cambiare non è più informe, ma ben definita e sempre più partecipativa. Gli utenti non percependo più quelle che sono le barriere dello spazio e il tempo, che si percepiscono nel mondo reale, sono spinti a creare delle vere e proprie comunità online. Secondo la definizione di Howard Rheingold "*Le comunità virtuali sono aggregazioni sociali che emergono dalla rete quando un certo numero di persone porta avanti delle discussioni pubbliche sufficientemente a lungo, con un certo livello di emozioni umane, tanto da formare dei reticoli di relazioni sociali personali nel ciberspazio*" [2](Rheingold 1993, pp. 1). Chiunque può entrare nella comunità se ne condivide i valori senza incontrare difficoltà. In questo senso, in molti hanno visto la realtà virtuale come un luogo dove si sarebbe potuto avere un dialogo costruttivo, soprattutto a livello politico anche migliore di quello che si ha nella realtà fisica. La facilità di creazione delle comunità avrebbe dato l'input all'azione collettiva per portare avanti forme proteste e azioni di denuncia (Rheingold,1993).

1.2 I Global Movement degli anni 2000 e #OccupyWallStreet ai tempi dei social media.

Alcuni autori hanno notato come lo sviluppo tecnologico sia stato alla base della diffusione dei movimenti di *global justice*[3] (Jeffrey, 2002). Verso la fine degli anni '90 nascono dei movimenti globali che organizzavano la loro azione grazie a forme di *networking*, che incentivavano la nascita di una comunità orizzontale e multiculturale, nella quale le informazioni circolavano liberamente. I *global movements* utilizzavano per comunicare i LISTSERV, dei software di mailing list all'interno dei quali gli utenti potevano scambiarsi opinioni e idee, dare vita a dibattiti e allo stesso tempo mobilitarsi. I LISTSERV hanno rappresentato il principale strumento comunicativo utilizzato da queste comunità e sono stati fondamentali anche per organizzare, nel 1999, le proteste contro il WTO a Seattle[4] o quelle contro la World Bank e il Monetary Found nel 2000 a Praga[5].

I social media[6] favorendo ulteriormente la logica di aggregazione hanno permesso la creazione di comunità più ampie, che riescono a mobilitare un numero maggiore di persone rispetto a quanto i *listserve* erano in grado di fare. Inoltre i nuovi strumenti di comunicazione danno la possibilità agli utenti che stanno partecipando a una manifestazione di potere offrire aggiornamenti in tempo reale, facendo del vero e proprio

[2] In originale*: "Virtual communities are social aggregations that emerge from the Net when enough people carry on those public discussions long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace*"(Rheingold 1993, pp.1).

[3] Per movimenti di *global justice* si intende una rete di movimenti sociali: un movimento di movimenti. Solitamente questi attori agiscono per promuovere un'equale distribuzione delle risorse.

[4] Nel Settembre del 1999 a Seattle durante una riunione dei membri del WTO, dei dimostranti impedirono ai delegati di raggiungere i loro alberghi. Pian piano la protesta si allargò sempre di più fino a degenerare a causa della presenza dei *black block*. Tuttavia il numero dei partecipanti alla manifestazione superò le 40.000 persone, questo numero non era mai stato raggiunto da nessuna protesta all'interno degli Stati Uniti.

[5] Nel Settembre del 2000 a Praga dimostranti provenienti da diverse parti del mondo diedero vita a forme di protesta, anche piuttosto violente, durante un summit della Banca Mondiale e del WTO. I partecipanti furono più di 15.000.

[6] Si veda riferimento 1.

microbroadcasting : coinvolgendo, così, sempre più individui. Le proteste dell'*#Occupymovement* sono emblematiche a questo fine. Il movimento[7] è stato fra i primi a utilizzare Twitter durante delle manifestazioni generando una serie di nuovi effetti. Innanzitutto si è visto come alle dimostrazioni abbia partecipato un numero molto consistente di persone, che non aveva mai sperimentato forme di attivismo politico. Inoltre l'utilizzo dell'hashtag *#Occupy* ha spinto la diffusione di informazioni relative alla protesta e ai suoi motivi, diffondendo così il messaggio dell'organizzazione in tutto il mondo. Questo ha portato ad avere oggi degli *#Occupymovement* in oltre 95 città sparse in 82 paesi del mondo.

Tuttavia proprio *#OccupyWallStreet* ci può offrire degli spunti utili per comprendere i limiti delle forme di aggregazione che nascono online.

1.3 I limiti della logica partecipativa on-line.

Il fine ultimo di tutte le organizzazioni sopra viste era comunque quello di creare delle reti sul territorio, di uscire, dunque, dal Web per agire all'interno della società e del mondo *off-line.* Anche queste nuove forme di attivismo, senza veri e propri *leader*, hanno comunque bisogno di un legame e di una base fisica. Per questo motivo, ad esempio, a Boston nel 2008 *#Occupy* ha speso molte energie per organizzare le attività e i dibattiti fra i manifestanti nelle zone occupate. Inoltre bisogna ricordare che in ogni protesta, fin qui considerata, vi era sempre una porzione di individui fortemente motivata che, però, non aveva alcun legame con il Web. A questo scopo è utile uno slogan dell'*#Occupymovement* di Boston, *"Act in assembly when together, act in network when apart"*[8]*,* che ci suggerisce come i *social network*, in quell'occasione, abbiano solo contribuito ad ampliare un movimento che aveva però delle radici e delle motivazioni storiche ben stabilite.

Non si può, di fatti, considerare il mondo del *Web* come una realtà totalmente avulsa alle logiche del mondo reale. Gli stessi *social media*, tanto esaltati da questi visione, non sono delle entità indipendenti, ma sono perfettamente collocati all'interno di una logica di profitto che non ha legami con la controcultura. Inoltre bisogna tener presente che a giganti come Facebook e Twitter interessa che gli utenti principalmente leggano e consultino i *social* per i propri interessi, piuttosto che questi divengano strumenti per l'approfondimento politico: in quanto è il modo più facile di guadagno grazie all'inserimento di inserzioni commerciali. Da qui la mancata neutralità di questi attori che possono filtrare i contenuti perché contro i valori della piattaforma, o raccogliere dati per fini pubblicitari: innanzi alla totale inconsapevolezza dell'utente (De Blasio, & Sorice, 2016).

[7] #OccupyWallStreet è un movimento di contestazione nato nel Settembre del 2011 a Zuccotti Park a Manhattan. I partecipanti della manifestazione si riunirono nel centro finanziario di New York per protestare contro le ingiustizie del mondo economico. Si voleva fare luce sulle molteplici ombre di Wall Street. Si ebbero forme analoghe di protesta anche Boston.

[8] Tradotto *"Agire in assemblea quando si è riuniti, agire in rete quando si è separati"*

Bisogna dunque non sopravvalutare fenomeni collaborativi come quelli analizzati sopra. Internet, e ciò che vi è al suo interno, nasce e si sviluppa all'interno di una specifica realtà sociale, che come tale è fatta di rapporti di potere non eguali fra loro. L'esistenza del *Web* è garantita da un numero ristretto di attori privati che si occupano di gestirne l'infrastruttura, ma anche le informazioni che vi circolano all'interno. Attori come Google, Yahoo!, Aol , la cui produzione supera il Pil di molte economie sviluppate. Chiaramente, alla luce di quanto visto, la narrativa che alcuni vogliono portare avanti, che vede Internet come il luogo di condivisione e partecipazione orizzontale per eccellenza, non può reggere. Tuttavia il motivo per cui questa visione continua, anche oggi, ad avere forte seguito è che gli stessi grandi protagonisti di cui sopra hanno interesse ad alimentarla e dargli vita. La conseguenza è che solo una ristretta minoranza di utenti è realmente consapevole del reale funzionamento web, si parla di un esiguo 15% (De Blasio & Sorice, 2016). La maggior parte delle persone è *online* solo per divertimento e spesso vede nel web un luogo fortemente democratico e anche più sicuro di quello che è in realtà. Particolarmente emblematico a questo fine è la percezione che gli individui hanno della tutela della *privacy online,* si è visto infatti come la maggior parte degli utenti si senta più protetta di quanto lo sia realmente (DeNardis, 2014). Alcuni autori, come MCchesney, hanno evidenziato come sia necessario agire per cambiare le cose all'interno del sistema mediale, per evitare che fra qualche anno questo diventi autoreferenziale e gli individui sempre meno informati e consapevoli (MCchesney, 2009).

L'opinione pubblica non riesce ad affrontare con facilità i temi relativi al funzionamento e, dunque, alla *governance* di Internet, perché troppo complicati e troppo lontani dalla comune percezione. Nonostante ciò l'*Internet governance* e i conflitti ad essa relativi sono particolarmente rilevanti per comprendere il funzionamento anche della nostra stessa società e il grado di democratizzazione che vi è al suo interno.

II CAPITOLO

Che cosa è l'*Internet Governance*?

2.1 La definizione di *Internet governance.*

"*Comprendere come Internet è governato e modellato da diversi attori è un esercizio di bricolage"*[9] (De Nardis 2014, pp.11). Ogni elemento che governa Internet, proprio come avviene nel *bricolage,* è unico, ha una differente storia ed offre un diverso contributo al sistema. Questo implica che si può parlare di *Internet governance* riferendosi a diversi ambiti e situazioni. Infatti possono dirsi decisioni di *governance*: le modifiche delle infrastrutture tecnologiche o del design, ma anche le regolamentazioni emanate dai governi relative all'uso di Internet da parte degli utenti; taluni trattati internazionali o delle risoluzioni delle Nazioni Unite e così via dicendo. Ogni azione intrapresa in un determinato campo, come ad esempio la definizione di un nuovo *standard* o una nuova regolamentazione sulla *privacy*, si ripercuoterà su tutti gli altri ambiti. Quanti hanno deciso di ricercare una definizione di *Internet governance,* non hanno potuto non tenere conto di questa pluralità.

Nel 2003 le Nazioni Unite hanno cercato di portare l'attenzione a livello globale sulla questione dell'*Internet governance* durante il "*World summit on the Information Society" [10]* organizzato a Ginevra. Alla fine del *summit* i partecipanti emanarono una dichiarazione di principi che avrebbero dovuto rappresentare le linee guida, in materia, per tutti gli Stati membri delle Nazioni Unite. Alcuni dei punti erano di carattere prescrittivo-normativo, altri invece erano di tipo progettuale ovverosia implicavano l'impegno degli Stati per il raggiungimento di determinati obiettivi[11].

Al punto 49 della Dichiarazione viene definita l'*Internet governance* come "*Lo sviluppo e l'applicazione dei governi, del settore privato e della società civile, nei loro rispettivi ruoli, dei pensieri comuni, norme, regole, procedure di decision-making e programmi che espandono la diffusione dell'uso di Internet".*[12] (ITU 2003,

[9] In originale "*Understanding how the Internet is governed and shaped by these diverse actors is an exercise in bricolage"* (Nardis 2009, p.11).

[10] *"The World Summit on the Information society"* è stata una riunione delle Nazioni Unite che ha avuto luogo in due fasi. Una prima svoltasi nel 2003 a Ginevra, alla fine della quale si è redatta una "Dichiarazione di principi" che doveva essere alla base della società informatizzata del nuovo millennio. Una seconda, invece, che si svolse a Tunisi nel 2005, alla fine della quale ci si accordò definitivamente su una comune definizione di *Internet governance*. E' interessante notare che alcuni dei punti su cui il WSIS discusse come ad esempio il *digital divide* o l'*e-learning* sono ancora parte dell'attuale dibattito dopo più di 10 anni.

[11] Vi è una parte della dichiarazione, ad esempio, relativa alla necessità di creare un sistema educativo in grado di trasmettere le abilità necessarie agli individui per essere parti attive nel processo di creazione, di quella che viene definita, la società dell'informazione (ITU, 2003).

[12] In originale "*Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet"* (Geneva Declaration of principles 2003, punto 49)

punto 49). La definizione considera l'interoperabilità dei vari elementi che rendono possibile la gestione di Internet. Si diede particolare attenzione alla definizione di questo concetto, perché il "*World Summit on the Information Society"* doveva dare l'avvio a un sistema di governo aperto, controllato dalle Nazioni Unite, accessibile a tutti, nel quale si sarebbe garantita la protezione dell'utente e dove allo stesso tempo questi avrebbe potuto arricchire la piattaforma con i suoi contributi. I fatti hanno dichiarato il fallimento[13] di questa iniziativa, oggi il maggior peso del controllo di Internet è nelle mani degli Stati Uniti, piuttosto che in quelle delle Nazioni Unite. Inoltre gli utenti non hanno la stessa informazione, o sicurezza, che la Dichiarazione sanciva avrebbero dovuto avere[14]. A questo punto è necessario e capire il funzionamento di alcuni elementi tecnici che ci aiutano a comprendere meglio i differenti livelli della *governance online.*

2.2 Alcuni aspetti tecnici della governance: i DNS e i protocolli.

Internet non potrebbe avere un'ampia diffusione senza i *Domains Name System* (da qui in poi DNS), dei server che trasformano, potremmo dire molto semplicisticamente, i numeri che compongono l'indirizzo IP del *website* in parole, in modo da renderlo comprensibile agli utenti. I DNS non permettono però soltanto ai siti di essere accessibili, ma anche di poter navigare al loro interno. Di fatto non fanno altro che associare e restituire alla richiesta di connessione ad un sito l'indirizzo IP di destinazione, previa la ricerca dell'*hostname* (ad esempio www.google.it), all'interno del database del DNS, che serve ad instaurare la connessione tra le due macchine. La gestione dei domini e dei server che forniscono ai DNS le varie informazioni è affidata all'ICANN (*Internet Corporation for Assigned Names and Numbers*), un'organizzazione *no-profit* che fino all' ottobre del 2016[15] era controllata dalla "*National Telecommunications & Information Administration"*[16] degli Stati Uniti. Nonostante ormai il dipartimento abbia formalmente perso il controllo, l'influenza del governo continua ad essere molto forte. L'importanza di questi *server* è data dal fatto che questi possono garantire, o meno, l'accesso ai siti. Infatti, in taluni casi, si potrebbe decidere di chiudere, attraverso l'utilizzo dei DNS l'accesso a specifici siti (come avviene spesso con i *website* legati alla pirateria). Chi controlla questi *server* gestisce ciò che agli utenti è permesso vedere. Per questo motivo tutti i provvedimenti che si cerca di emanare in materia sono molto controversi e provocano grandi tensioni all'interno della comunità informatica.

[13] Tuttavia vi sono degli esempi di organizzazioni con procedure aperte di governance. Particolarmente rilevante è l'*Internet Engineering Task Force* (da ora in poi IETF's), un'organizzazione internazionale che ha l'obiettivo di creare standard completamente aperti e accessibili. Chiunque può accedere e partecipare ai *meeting* della *community*: l'unico limite è quello della conoscenza individuale. Il modo di operare dell'organizzazione, che nel corso degli anni ha creato numerosi standard (alcuni particolarmente rilevanti come quello in maniera di privacy), non è particolarmente condiviso.

[14] In alcuni punti la dichiarazione sottolinea come gli utenti debbano essere informati e capaci di accedere al web con consapevolezza (ITU, punti 29 e seguenti). In altri si parla della protezione della privacy e dei dati personali dell'individuo che dovevano essere garantiti dalla *governance* (ITU, punto 35)

[15] Il primo Ottobre 2016 il governo degli Stati Uniti (nonostante le proteste di alcuni senatori repubblicani come il noto Ted Cruz) ha ceduto il controllo dei DNS all'ICANN. Il provvedimento era da anni fortemente invocato soprattutto da Cina e Russia. Il loro non essere paesi democratici aveva però ulteriormente bloccato le autorità dal prendere alcun provvedimento

[16] Il Dipartimento delle telecomunicazioni e infrastrutture tecnologiche.

Un altro elemento tecnico, e allo stesso tempo politico, è rappresentato dai protocolli: un insieme di regole standardizzate che permette di compiere diverse azioni. Un protocollo si definisce politico perché incorpora una serie di regole, che hanno in sé dei valori trasmessi successivamente alla tecnologia (Nardis, 2009). Per comprendere meglio basti pensare al protocollo *peer-to-peer,* che permette il funzionamento di BITTORRENT. Lo standard consente lo scambio di file fra due individui, in modo diretto, con due computer. Di fatto vi è un rifiuto di un sistema gerarchico, e la promozione di uno scambio democratico di sapere fra individui, che si riflette nel design. I protocolli si dicono fondamentali anche perché garantiscono l'interoperabilità tra differenti *devices*. Infatti offrono una serie di regole comuni che permettono a macchine diverse di comunicare. Agli inizi di Internet, proprio per raggiungere una sempre maggiore interconnessione, in molti cercavano di creare standard comuni e di garantirne una maggiore diffusione possibile.[17] La stessa nascita del Web si basa su un protocollo: lo standard TCP/IP[18]. Questo è da dirsi fondamentale per il funzionamento di Internet, perché permette la connessione dell'utenza mondiale. Un protocollo, come questo sopra visto, funziona perché universale, facilmente identificabile e aperto a tutti. La crescita di Internet, anche in termini di maggiore accessibilità, può essere garantita solo con la creazione di protocolli totalmente aperti (De Nardis,2009).

Questi elementi tecnici ci dimostrano come l'organizzazione dell'infrastruttura tecnologica abbia in sé delle implicazioni politiche molto forti. Di fatto il controllo di un server o la creazione di un protocollo incidono sulla democraticità o meno della società.

2.3 La *governance* attraverso gli algoritmi e la loro presenza nel nostro quotidiano.

Finora si è guardato agli elementi che formano l'infrastruttura tecnologica e che permettono a Internet stesso di esistere. Adesso si guarderà a quelle che possiamo definire come l'insieme di istruzioni che permettono ai *software* di esistere e di far compiere ai computer determinate *task*: gli algoritmi (McKevey, 2014).

Un algoritmo non è nient'altro che un procedimento che risolve un determinato problema attraverso una serie di procedimenti elementari, grazie all'utilizzo della matematica e della logica astratte in istruzioni. A un algoritmo vengono delegate, nello specifico, una serie di *task* o un processo, come ad esempio l'organizzazione dei *trend* di Twitter. Il modo in cui l'algoritmo interagisce con il problema e il modo in cui organizza i dati a sua disposizione variano il tipo di risultato. Difatti alle specifiche *queries* (richieste) un algoritmo risponde attraverso l'utilizzo e la manipolazione di specifici dati che gli vengono offerti. Attraverso questa azione deleghiamo una consistente parte della nostra vita quotidiana a un processo matematico e logico che ovviamente ne cambia alcuni elementi. Questa automazione aumenta quelle che possono essere le possibilità di ogni singolo individuo, permettendogli dunque di fare azioni più velocemente rispetto a quanto accadeva in

[17] Si guardi riferimento (10)
[18] Transmission Control Protocol/Internet Protocol.

passato. Per fare in modo che taluni algoritmi lavorino al meglio gli individui devono condividere una serie di informazioni e di dati personali con il sistema, solo in questo modo difatti si potrà avere l'*output* richiesto. Ad esempio guardiamo per un attimo come funziona il famoso sito di *e-commerce* Amazon: nel momento (ma anche prima e durante la navigazione), in cui l'utente decide di acquistare un determinato oggetto il sito gli raccomanda altri oggetti simili a quello visualizzato. Amazon.com riesce a fare ciò perché cataloga, anche grazie all'utilizzo dei *cookies*[19]quelle che sono le varie e differenti esperienze di acquisto o anche le semplici ricerche dei suoi utenti. In questo modo ogni volta l'algoritmo e i *cookies*, che lo sfruttano, utilizzati da Amazon possono, attraverso uno specifico procedimento, interpretare quelle che potrebbero essere le possibili preferenze di un individuo e suggerirgliele (Willson, 2016). Questo però ha una serie di importanti implicazioni, difatti l'algoritmo in questione non ci sta aiutando a risolvere uno specifico problema, ma ci sta influenzando e manipolando in qualche modo. Gli algoritmi di questo tipo hanno un potere manipolativo, dunque, che può essere anche sfruttato per finalità commerciali e pubblicitarie più invasive rispetto a quelle che abbiamo fin qui visto. Un esempio ci viene offerto dalla *newsfeed* di Facebook; grazie all'algoritmo che vi è alla base, questa mostra di *default*[20] agli utenti le notizie solo in base ai loro interessi e non più seguendo un ordine cronologico. Di fatto questo tipo di algoritmi creano uno specifico ambiente e anche una specifica cornice per gli individui (Willson, 2013). Nel 2013 a questo proposito un team di ricercatori di Facebook ha condotto una serie di esperimenti dimostrando come attraverso l'utilizzo di un algoritmo[21], che modificava la *newsfeed,* del famoso social si potessero influenzare e manipolare gli stati d'animo delle persone. Partendo dell'assunto che la "*News feed rappresenta il primo canale attraverso cui le persone possono vedere i contenuti condivisi dagli amici*"[22](Kramer, Guillory & Hancock, 2014, pp.3), i ricercatori hanno ipotizzato che questo potesse essere il primo strumento di contagio di emozioni basato su una comunicazione attraverso l'uso del computer e allo stesso tempo che le emozioni si potessero predire. Attraverso l'utilizzo di un software[23] le parole degli stati degli utenti venivano analizzate e divise in "positive" e "negative", in questo modo si potevano andare a catalogare i vari *post* in base alle emozioni che si riteneva trasmettessero e allo stesso tempo i ricercatori potevano non leggere i *post* degli utenti. Una volta divisi i post in categorie, in

[19]I cookies fanno sì che le inserzioni pubblicitarie on-line siano legate alle nostre tendenze di ricerca, di acquisto e anche ovviamente ai nostri dati personali anagrafici e non. I cookies sono dei file di testo inviati durante la navigazione in Internet utilizzati dai browser per salvare informazioni come dati di accesso, cronologia dei siti visitati o impostazioni utilizzate e ricerche dell'utente. In questo modo vengono "tracciati" i gusti e gli interessi di chi naviga on-line. Così è possibile creare le cosiddette "pubblicità intelligenti" grazie all'utilizzo di specifici algoritmi. Queste ci mostrano ciò che potrebbe interessarci o che comunque è relativo alle nostre ultime ricerche. Tuttavia nel momento del loro concepimento servivano ai browser per motivazioni puramente tecniche. Esistono quattro tipi di pubblicità intelligenti principalmente: quelle legate al "contesto" in cui l'utente si trova" quindi ad esempio relative al sito che lui sta visitando, quelle legate al comportamento dell'utente nel tempo basate sui tipi di ricerca operati dagli utenti, quelle basate sulla posizione geografica dell'utente e quelle legate al comportamento sui *social* degli *user.* (De Nardis, 2014).

[20] Gli utenti possono cambiare comunque questa impostazione, organizzando così la loro timeline diversamente, guardando le notizie in ordine cronologico.

[21] N = 689,003

[22] In originale "News Feed is the primary manner by which people see content that friends share" (Kramer, A, Guillory, E., Hancock, J 2014, pp.3)

[23] Il Linguistic Inquiry and Word Count.

maniera del tutto casuale, si è deciso di mostrare a una serie di utenti solo status che trasmettevano emozioni positive e ad altri solo quelli che comunicavano sensazioni negative. In questo modo il *team* di Facebook ha confermato le sue ipotesi iniziali, in quanto si è osservato che gli individui erano più inclini a scrivere pensieri positivi su Facebook se nella loro *home* erano stati omessi i post negativi e viceversa (Kramer, Guillory & Hancock 2014, pp.3).[24] Non soltanto le notizie, gli stati degli amici, ma ovviamente anche le inserzioni pubblicitarie seguono questa logica.

Hal Ronald Varian, *chief economist* di Google, specializzato proprio nell'economia dell'informazione scrive: *"[…] Io condivido moltissime informazioni private con il mio dottore, il mio avvocato, il mio commercialista, il mio personal trainer e così via. Lo faccio perché ricevo benefits tangibili e io mi fido che loro agiscano portando avanti i miei interessi. […] Perché io sto volontariamente condividendo tutte queste informazioni private? Perché ottengo qualcosa in cambio*"[25] (Varian 2013, pp.). In questo modo l'economista risponde a quanti si preoccupano dell'eccessivo potere che gli algoritmi di Google (di cui poi si vedrà brevemente in seguito) sostenendo che i vantaggi di queste tecnologie superano gli svantaggi. Difatti quello che un tempo bisognava chiedere e ricercare oggi ci viene subito servito dai nostri *devices* che, ad esempio, senza una nostra richiesta, automaticamente ci avvisano quando uscire di casa per arrivare a un incontro puntuali, semplicemente guardando nel nostro calendario (Varian, 2013). Dall'altro lato però numerosi sono i *bias*[26] che queste tecnologie possono causare, proprio perché, nonostante siano sistemi automatizzati, sono comunque ideati e concepiti dall'uomo. Questi nel caso degli algoritmi possono essere non voluti, ma talvolta lo sono. Le conseguenze possono avere degli effetti sfavorevoli per l'utente. Ad esempio alcuni studi condotti negli Stati Uniti hanno mostrato come vi fosse una curiosa associazione, all'interno del Google Play Store, fra le applicazioni per uomini gay single e quelle relative ai reati a sfondo sessuale. Ciò ci mostra quali possano essere gli effetti distorsivi che un'errata progettazione degli algoritmi può causare alimentando pregiudizi lesivi, in questo caso dell'identità omosessuale.

Da un punto di vista di *governance* gli attori che hanno un maggiore accesso ai dati e che allo stesso tempo possono contare su delle elevate competenze tecniche possono scrivere algoritmi particolarmente funzionali e allo stesso tempo incisivi nelle nostre vite. Basti guardare a Google la cui pervasività nelle nostre vite è tale che ad oggi esiste addirittura un verbo in inglese, *to google,* per indicare l'azione di ricerca attraverso il famoso

[24] All'esperimento hanno partecipato circa 155,000 utenti che utilizzavano Facebook in inglese, selezionati in modo causale. Sono state analizzate 121 milioni di parole, 4 milioni di post che trasmettevano emozioni positive e 1 milione che al contrario potevano definirsi come negativi. A questi utenti si è affiancato un gruppo a cui sono stati oscurati post in modo del tutto casuale, al fine di creare così un gruppo di controllo, cioè un gruppo che non sottoposto all'esperimento, poiché non modifica il suo comportamento, riesce a confermare le ipotesi alla base dell'esperimento.

[25] In originale "I share highly private information with my doctor, lawyer, accountant, trainer, and others because I receive identifiable benefits and I trust them to act in my interest. Why am I illing to share all this private information? Because I get something in return".

[26] I *bias* sono dei giudizi o dei pregiudizi cognitivi che non necessariamente corrispondono all'evidenza. Ad esempio, avere timore di prendere un aereo e non di viaggiare in macchina, nonostante siano più frequenti gli incidenti in auto rispetto a quelli aerei. (Oliverio, 2015)

sito (Willson, 2013). Google ha creato dei *database* enormi, che difatti per questo motivo vengono utilizzati anche da altri attori. Allo stesso tempo continui sono gli esperimenti che l'azienda fa sugli utenti in modo da trovare i migliori modi per manipolare, stimolare o semplicemente rendere più facile la vita quotidiana degli individui. Da qui il grande impegno profuso da Google nella creazione di un assistente personale all'interno dei vari *devices*, come ad esempio Google Now, che riesce a suggerire all'individuo i percorsi migliori per raggiungere i luoghi dei suoi appuntamenti senza che questi lo richieda direttamente (Varian, 2013).
Allo stesso tempo i test vengono condotti anche per spingere gli utenti in una determinata direzione, negli ultimi anni l'azienda, si è impegnata nello sviluppare algoritmi in grado di rendere adatte ai *mobile devices* la maggior parte dei contenuti offerti da Google. (Varian, 2013) A questo punto appare sempre più evidente che il potere di Google sia immenso, e le sue potenzialità possono dirsi più ampie rispetto a quelle dei governi stessi. La capacità di fare continui test sugli utenti, il grande patrimonio di informazioni che Google riesce ad acquisire ha offerto la possibilità all'azienda di guadagnare sfruttando i dati in suo possesso, creando pubblicità e vendendoli di fatto al miglior offerente. (Zuboff, 2016). Difatti il principale obiettivo dell'azienda è in assoluto massimizzare i suoi profitti, come ad esempio ha dimostrato la scelta di piegarsi alle regole del governo cinese censurando alcuni contenuti, pur di non perdere una delle fette di mercato più consistenti del mondo. (De Blasio & Sorice, 2016).

Alla luce di quanto si è finora visto si può concludere che il problema della *governance* di Internet sia legato al fatto che vi è una forte mancanza di democraticità, legata soprattutto all'opacità entro la quale tutti i vari meccanismi sono inseriti e al fatto che la maggior parte degli attori che gestiscono questo potere sono privati. Come si è visto il controllo di un server, la scrittura di un protocollo e la gestione di specifici dati incidono sulla democraticità della nostra società (Nardis, 2014). Emblematico, come si è visto, è il caso degli algoritmi i cui effetti sono fortemente incisivi, ma il cui funzionamento è totalmente lontano dai fruitori del web. La inconsapevolezza di questi ultimi non è soltanto legata alla mancanza di competenze tecniche, ma anche al fatto che, per l'appunto, la routine e il funzionamento dei vari meccanismi vengono in tutti modi oscurati agli utenti. I cittadini, spesso, non possono neanche immaginare il sistema che vi è dietro, e decidere dunque di conoscerlo meglio e di studiarne il funzionamento. Dall'altro lato i ricercatori e gli studiosi interessati in questo campo hanno difficoltà ad analizzare questi elementi in quanto la maggior parte di essi sono brevettati e non totalmente disponibili. Da qui la necessità di chiedersi quanto gli individui siano liberi e quanto sia necessario fare per rendere la *governance* del *web* il più trasparente e vicina ai cittadini.

Prima di passare a vedere talune possibili soluzioni è necessario guardare all'attuale situazione degli utenti al loro grado di libertà e a cosa stanno facendo attualmente i governi per tutelarli.

III CAPITOLO

Le minacce alla libertà degli individui in rete

3.1 Il ruolo degli intermediari privati e il loro rapporto con i governi.

Quanto visto finora ci ha fatto comprendere che sono i privati i principali intermediari di contenuti all'interno del Web. Agli albori di Internet non era necessaria l'esistenza di quelli che oggi sono definiti come i *content aggregation sites*, questi sono nati nel momento in cui sono da un lato aumentati i contenuti prodotti per il Web e dall'altro, soprattutto, il numero degli utenti. Difatti il maggior numero di utenti ha reso necessaria la fine del classico rapporto *end-to-end* tipico degli albori di Internet, questo perché diventava troppo difficile per i singoli accedere e trovare i contenuti e, allo stesso tempo, per il grande numero di elementi che grazie a questo tipo di siti possono essere finalmente ordinati. Ad oggi dunque attori come Google, Yahoo! o Bing sono i principali intermediari di contenuti a livello mondiale e quindi responsabili da un punto di vista soprattutto sociale del livello di informazione degli utenti. Infatti sono loro che materialmente ci permettono di informarci e di avere accesso a determinati contenuti piuttosto che ad altri. Tuttavia questi siti non sono legalmente responsabili per i contenuti che ospitano; questo è un elemento fondamentale che permette loro di dare spazio a quante più voci possibili, in altro modo il processo di controllo dei singoli elementi renderebbe più difficile il processo e incentiverebbe delle forme di censura da parte di attori come Google, dettate dalla paura di un qualsivoglia procedimento legale (De Nardis, 2014). Guardando nello specifico a Google, che rappresenta la più grande e la più importante di queste realtà, si può osservare che più volte la compagnia è stata chiamata a rispondere sul tema, questo perché spesso i governi o i giudici dei vari Paesi nel mondo si rivolgono all'azienda per far sì che questa rimuova taluni contenuti per le più svariate ragioni, come si vedrà a breve. In generale, bisogna tenere a mente che per rispettare le diverse legislazioni nazionali Google (così come tutti gli altri colossi del Web) è costretto a mettere in pratica dei provvedimenti anche tecnici non sempre di facile attuazione. Allo stesso tempo, nel caso di richieste provenienti da Stati non propriamente democratici la compagnia deve valutare con maggiore attenzione la situazione, in quanto acconsentire a determinate richieste può provocarle un danno di immagine notevole. Nel 2007 la compagnia scrive un post nel suo blog spiegando la sua posizione e la sua filosofia in merito "*Google non è, ne dovrebbe essere l'arbitro di ciò che deve apparire nel web. Questo ruolo appartiene a tribunali e ai governi regolarmente eletti*" (GOOGLE BLOGSPOT, 2007). Tuttavia, sempre nello stesso post, la compagnia spiega che ogni giorno è costretta ad affrontare determinate scelte anche per andare incontro a quelle che sono le richieste dei governi e delle varie aziende che vedono in alcuni contenuti una lesione dei loro diritti, sempre cercando di garantire la libertà di espressione e allo stesso tempo evitando di fare un controllo preventivo dei singoli contenuti (2007). In generale si può concludere che la *policy* di Google in materia è abbastanza liberale, sulla carta, tutelando gli

individui rispetto alle richieste degli Stati che sono legate magari a una esigenza del governo di turno. Nello specifico vediamo che gli Stati democratici, solitamente, tendono a richiedere che il colosso rimuova i contenuti che non sono conformi alla legge nazionale, quelli legati a casi di diffamazione (talvolta presunti) o legati a segreti di Stato. La compagnia cerca di essere abbastanza trasparente mostrando in un report (ad oggi aggiornato al 2015) le richieste dei singoli Stati e quante di queste richieste sono state accettate o approvate. Le statistiche che vengono condivise da Google comunque non riflettono il reale numero delle domande e delle decisioni che l'azienda deve prendere relativamente ai contenuti presenti *on line.* Difatti talvolta la compagnia rimuove i contenuti perché riceve delle richieste da parte di privati o per seguire alcune sue regole. Tuttavia, ciò che è maggiormente preoccupante è il fatto che gli Stati continuino a non volere rendere pubbliche questo tipo di richieste e che debba essere una compagnia privata, in nome della libertà di espressione e della trasparenza, a farlo (De Nardis, 2014).

Un altro esempio interessante ai nostri fini è legato al mondo delle applicazioni per dispositivi mobili; è sotto gli occhi di tutti il fatto che oggi siamo sempre più dipendenti e legati alle *app* per occuparci delle più svariate attività. Secondo gli studi della società di ricerca OVUM lo sviluppo di *app* arriverà a oltre 79 bilioni di dollari nel 2020 e anche gli stessi download aumenteranno considerevolmente, si parla di 378 bilioni sempre nel 2020 (OVUM, 2016). Da ciò ne consegue che attori come Apple o la stessa Google, che detengono il controllo di quello che può essere ospitato o meno nei loro *store*, di fatto hanno il potere di bloccare o meno l'innovazione in uno specifico settore. E' interessante guardare alla *policy* di Apple per comprendere quanto ampia sia la discrezione che l'azienda californiana ha in materia. Difatti leggiamo nell'introduzione alla guida per gli sviluppatori di Apple che la compagnia si rifiuta di accettare contenuti che superino un certo "limite" e, scrivono i membri dell'azienda *"a chi ci chiede qual è il confine noi rispondiamo, come rispose una volta un giudice della Corte Suprema, quando lo supererai lo saprai*" (APPLE POLICY, 2017), sottolineando così il grande potere dell'azienda.

Come si è visto nel capitolo precedente, gli attori che compongono il web, grazie all'utilizzo di specifiche tecnologie, riescono a raccogliere varie informazioni sugli utenti per le finalità sopra esposte. Questo comporta che, nel momento del bisogno, gli Stati chiedano a queste aziende di consegnare i dati degli *user*, perlopiù in nome della sicurezza nazionale. Una volta ancora sono dei privati a fungere da intermediari, anche da garanti talvolta, della privacy dei cittadini in un contesto globale. Guardando al *Google Trasparency Report* si osserva che le principali motivazioni che spingono i governi a questo tipo di richieste sono legate a procedimenti di tipo penale o a casi di antiterrorismo. L'azienda prima di dare i dati alle autorità vede se la richiesta è conforme alla sua *policy* e se la legge glielo consente comunica all'utente la trasmissione dei dati; inoltre tecnicamente la compagnia vuole che vengano fatte richieste il meno generali possibili in modo da potere, anche nel momento della cessione dei dati, garantire comunque la privacy dell'utente. È importante in questa sede comprendere quanto questa materia sia da dirsi rilevante e allo stesso tempo delicata per queste compagnie,

che soprattutto quando si trovano ad avere rapporti con Stati non democratici rischiano, se agiscono in modo sbagliato, di perdere fortemente la loro credibilità, ancora di più che nel caso della rimozione di contenuti. Difatti la cessione di dati personali a terzi va a minare quel rapporto di fiducia che sempre più l'utente medio ha con il web visto come un luogo sicuro dove potere esprimere le proprie opinioni quasi sempre (secondo quella che è ovviamente la visione comune) in totale anonimato (De Nardis, 2014). A questo proposito è interessante guardare quanto è successo a Yahoo! fra il 2002 e il 2004. In questo lasso di tempo l'agenzia di telecomunicazioni ha consegnato alle autorità cinesi i dati di un giornalista e di un ingegnere sostenitori della democrazia che sono stati successivamente condannati. Per queste condanne Yahoo! è dovuta comparire innanzi a una corte (vani sono stati i tentativi da parte dell'azienda di venire assolta) ed è stata costretta a pagare al tribunale una somma che ad oggi continua a non essere nota. Inoltre l'immagine della compagnia è stata danneggiata gravemente subendo anche attacchi da diversi giornali e organizzazioni di diritti umani.

A questo punto prima di andare a vedere quali sono le politiche che i governi hanno attuato negli ultimi anni servendosi del web, talvolta sfruttando la collaborazione degli attori fin qui analizzati, è necessario concentrarci per un attimo sulla privacy degli individui on-line. Fin qui abbiamo infatti visto come si manifesta il potere di attori terzi sulle vite degli utenti senza però guardare nello specifico alla condizione di quest'ultimi. Cosa possono fare i singoli per tutelarsi? Cosa si intende per privacy? Quanto è effettivamente importante una sua tutela?

3.2 La privacy online: l'erosione dell'anonimato.

E' evidente il fatto che siamo all'interno di un flusso ininterrotto di dati e informazioni di cui siamo consumatori e produttori allo stesso tempo. Da ciò deriva la necessità di proteggere questo patrimonio e di non lasciarne la tutela a terzi, in quanto farlo equivarrebbe lasciare a qualcun altro il controllo della nostra vita e di come questa debba essere organizzata, anche alla luce del potere manipolativo che certe tecnologie hanno. Per essere realmente padrone di sé stesso ognuno di noi dovrebbe avere la possibilità di accedere con facilità ai propri dati, di conoscere come questi vengono impiegati e anche di decidere, quando lo si ritiene opportuno, di non cederli a talune organizzazioni (Rodotà, 2013).

Quando Internet nacque, agli inizi degli anni '90, vi era l'opinione diffusa che questo fosse un luogo dove chiunque avrebbe potuto esprimere le proprie opinioni in totale anonimato (De Nardis, 2014). Il primo web era caratterizzato in generale da un "*latente anonimato […] si accedeva alla rete con uno pseudonimo, un nickname, arbitrario e caratterizzante, ma non sempre (anzi, quasi mai) riconducibile alla identità offline*" (Caliandro, 2011). Talvolta in caso di specifiche richieste da parte dell'autorità giudiziaria, ad esempio, un *provider* poteva, attraverso l'indirizzo IP, fornire delle informazioni personali sui singoli. Oggi l'esistenza dei social network ha causato una serie di problemi particolarmente rilevanti per quanto riguarda l'anonimato. All'interno dei *social* permettere agli individui l'utilizzo di pseudonimi può essere lesivo dei diritti di alcuni.

Emblematici sono a questo proposito i casi di cyberbullismo che sempre più spesso finiscono per avere dei contorni drammatici. Tanti i casi di giovanissimi che decidono di porre fine alla loro vita in seguito alle minacce e agli insulti ricevuti online, e solitamente dopo avvenimenti del genere vi sono delle vere e proprie richieste, anche dal basso, in favore di una minore libertà. Nel 2013 in seguito al suicidio di una giovane nel Regno Unito vi è stata una mobilitazione per far sì che *ask.fm*, un social network che permette agli utenti di farsi domande in totale anonimato, fosse chiuso. Un altro problema è legato al fatto che nel momento in cui gli individui decidono di agire anonimamente online spesso si "ricreano" un'identità utilizzando immagini di altri che sono assolutamente inconsapevoli e senza alcun potere innanzi ai fatti. Il problema è che, come spiega Laura De Nardis "*gli individui sono liberi di scegliere in che modo essere attivi nei social media, ma tuttavia anche chi non ne ha mai fatto parte può essere fotografato ed identificato online"* (De Nardis 2014, pp.237). Vi sono vari episodi che provano quanto affermato dalla De Nardis, come ad esempio il caso del blogger Tom MacMaster che durante il periodo delle rivolte in Medioriente ha creato un blog, molto seguito, sotto falso nome facendo finta di essere una ragazza americana di nascita, residente in Siria ed omosessuale utilizzando le immagini di una donna che, ignara, viveva a Londra. L'evento sollevò molte polemiche e fece emergere quelli che erano gli ovvi problemi legati all'utilizzo di un'identità falsa *online*. Allo stesso tempo la vicenda mostra come sia difficile controllare i contenuti una volta che questi diventano virali, difatti le immagini della ragazza londinese verranno per sempre associate al personaggio di finzione inventato da MacMaster. Infine, soprattutto all'interno dei *social network*, l'obbligo di identificarsi può essere un deterrente all'avvio da parte degli utenti di discorsi che incitano all'odio e alla violenza. Per queste ragioni attori come Google+ e Facebook stanno portando avanti le *real name policy* obbligando gli *user* a utilizzare il loro vero nome al momento della registrazione.

Bisogna, però, tenere a mente che l'anonimato rappresenta una *"precondizione della libertà di manifestazione del pensiero"* (Rodotà 2013, pp.392) quando siamo all'interno di regimi non democratici, dunque, nel momento in cui questo viene negato è la stessa libertà di espressione ad esserlo. La Cina, ad esempio, è il primo Stato ad aver obbligato tutti i suoi utenti a identificarsi per accedere ad Internet e allo stesso tempo il governo cinese opera dei controlli anche sui contenuti stessi che vengono messi *online*. Non soltanto gli Stati non democratici, ma anche le democrazie sviluppano ogni anno di più una propensione per il controllo come il *Google Transparency Act* ci mostra. Infine bisogna ricordare che nel momento in cui gli individui entrano all'interno di piattaforme utilizzando il loro vero nome danno automaticamente la possibilità a quest'ultime di acquisire altri dati riguardo la loro identità. L'anonimato impedisce ai poteri del web come Facebook e Google di acquisire le informazioni più attraenti da un punto di vista commerciale (Rodotà, 2013).

In questo modo dunque l'individuo che online condivide dati relativi alla sua vera identità si trasforma in un oggetto dal quale possono essere continuamente estratte informazioni, che molto pericolosamente potrebbero

spingere attori terzi a manipolarne i gusti. Per non parlare degli effetti lesivi per la democrazia se questi dati venissero manipolati per spostare il consenso dei cittadini su un candidato piuttosto che su quello di un altro.

Tutti questi elementi fin qui visti vanno ad attaccare il concetto di privacy come viene tradizionalmente inteso. Se prima la privacy era il diritto di ognuno ad essere lasciato da solo, e dunque si doveva tutelare l'individuo da ingerenze esterne, oggi al contrario bisogna guardare e proteggere il singolo da quanto avviene all'interno della sua stessa casa innanzi agli schermi dei suoi *devices*. Per questo motivo se in passato una violazione della privacy individuale poteva essere facilmente individuabile e sanzionabile, oggi è più difficile andare a rimarcare i confini di cosa sia una violazione, di quello che è comunque in modo assolutamente innegabile un diritto della persona umana. Tuttavia non sembra che l'individuo sia completamente inconsapevole di quanto avviene, difatti le politiche dei vari social media, e non, impongono ai siti di informare e far accettare agli utenti quelle che sono le norme in materia di privacy. Obbligando così chi vuole accedere a un determinato contenuto in rete, a cedere una parte di sé e trasformando gli utenti in "*vittime consapevoli*" (Rodotà 2013, pp. 395).

Dunque così il web che è nato come il luogo della condivisione e della libertà, e che puntava a divenire una comunità orizzontale si è trasformato, o si sta trasformando, in una comunità gerarchica in cui il privato dell'individuo è diventato la merce di scambio (Rodotà, 2013). A questo problema non si riescono a trovare semplici soluzioni perché il principale guadagno per gli attori che dominano, e di fatto governano, il web, è legato al mondo delle pubblicità che sempre più si sta sviluppando attorno allo sfruttamento dei dati personali dei singoli sui quali ormai direttamente vengono costruiti gli annunci pubblicitari. D'altronde il *business model* su cui si fonda Internet è basato sulla totale gratuità dei suoi contenuti, per cui in qualche modo le grandi compagnie che li gestiscono dovranno guadagnare, e questo è sicuramente il metodo più veloce ed attualmente più efficace, per cui una modifica delle procedure alla base di questo potrebbe mettere in crisi tutto il sistema.

Qualche passo è stato mosso per bilanciare le diverse esigenze, cercando di tutelare i singoli. Si è principalmente cercato di proteggere alcune informazioni ritenute particolarmente sensibili, come ad esempio, quelle relative alla salute o alle finanze personali. Allo stesso tempo tutti i grandi attori di Internet hanno sviluppato delle *policy* per proteggere i bambini *online* sia dai contenuti che da determinati tipi di *advertising*. Inoltre si sono imposte delle limitazioni per quanto riguarda la cattura di immagini per la creazione di mappe o altro. Google (e non solo) opera una certa sorveglianza sulle fotografie che utilizza per Google Maps in modo da evitare che immagini di individui si diffondano senza che questi ne abbiano dato il consenso in modo specifico. Infine l'Unione Europea ha sempre dato una grande attenzione alle tematiche relative alla privacy per cercare di garantire la libertà dei suoi cittadini, con la *Data Protection Directive* del 2016 l'EU è diventata la zona del mondo in cui si dà maggiore attenzione ai diritti della privacy online.

A questo punto è giunto il momento di andare ad analizzare quelle situazioni in cui gli individui sembrano aver perso la loro libertà in rete.

3.3 La censura ad opera dei regimi autoritari nel Web 2.0

Fino a questo momento abbiamo visto come i maggiori poteri all'interno del web sono in mano ad attori che non detengono alcuna legittimità democratica, in quanto privati. In un certo senso sono loro a esercitare, quando lo ritengono necessario, forme di censura e i governi, come si è visto nelle pagine precedenti, devono sottostare a quanto questi decidono. La passività e l'incompetenza sono in questo senso condizioni standard dei governi. Seguendo questo ragionamento, possiamo dunque affermare che un governo che volesse attuare delle forme di censura, sarebbe costretto a chiudere completamente l'accesso al web. Quest'ultimo, difatti, sarebbe incompatibile con la sua visione. Allo stesso tempo però un'economia che rinuncia a Internet è assolutamente inadatta a fronteggiare le sfide di un mondo globalizzato. Questa idea che i dittatori siano in una posizione dilemmatica, dove da un lato vi è la tecnologia e dall'altro il loro bisogno di alimentare il regime attraverso la censura, si è sviluppata durante la Guerra Fredda. Nel 1985 George Schultz segretario di Stato statunitense, fu uno dei primi a portare avanti pubblicamente questa tesi, affermando che i regimi totalitari saranno costretti a scegliere fra la tecnologia e il regime. La caduta del muro di Berlino, e l'ottimismo che ne è conseguito, ha contributo a rafforzare questo pensiero che si fonda sull'assunto che il capitalismo e lo sviluppo siano intrinsecamente legati e destinati a un inevitabile trionfo. In questo modo si è portati a guardare al web come a un'entità astratta e decontestualizzata, senza andare a considerare come questo possa esistere ed essere utilizzato in diverse zone del mondo culturalmente diverse dalla società occidentale che l'ha ideato e concepito. Da ciò si può evincere, facilmente, la pericolosità di questo pensiero, che spinge a non pensare a come determinate tecnologie possano essere manipolate per andare a creare forme di censura più sofisticate (Morozov, 2011). Inoltre questo assunto non spiega come sia possibile come tutti i regimi autoritari del nostro tempo, eccezion fatta per la Corea del nord, garantiscano l'accesso alla rete globale e continuino ad esistere. Da un punto di vista pratico questa tesi non considerava il fatto che potesse esistere una forma di censura in grado di bloccare l'accesso ai contenuti. Si partiva dal presupposto che una volta che si fosse ottenuto l'accesso a Internet chiunque avrebbe potuto visualizzare qualsivoglia contenuto. Tutto questo è stato smentito dai fatti, un governo può bloccare l'accesso a specifici siti e così proibirli alla società civile. Inoltre le tecnologie, che abbiamo analizzato in precedenza, permettono di tracciare i profili dei singoli che hanno provato a visualizzare determinati siti e allo stesso tempo possono impedirgli di accedere ai contenuti che stanno cercando. In generale così come abbiamo visto sia possibile una personalizzazione della pubblicità, è allo stesso tempo fattibile applicare le stesse tecnologie e gli stessi meccanismi per vedere se un individuo all'interno di un regime autoritario sia un sostenitore di idee democratiche. Appreso ciò, si può agire al contrario di come si fa nel caso delle pubblicità, oscurando i siti ai singoli. I *social network* possono incentivare questo processo rendendo chiaramente visibili le amicizie e gli interessi delle persone. In questo modo non soltanto siamo

innanzi a forme di "censura personalizzata", e quindi più potente, ma è anche più difficile per un osservatore terzo potere avere dati specifici o maggiormente rilevanti. Un altro elemento tecnico che può aiutare nuove forme di censura si ritrova nella struttura basilare del web globale. Difatti questo è formato sugli *hyperlink* che sono dei collegamenti ipertestuali che permettono a un singolo di essere rinviato a uno specifico contenuto. L'ipertesto può rendere possibile la deduzione di alcune informazioni sui singoli, senza guardare direttamente al contenuto di ciò che questi ultimi stanno visionando. Proviamo a immaginare che un gruppo di individui sospetti inizi a scambiarsi un file in PDF, il governo potrebbe decidere di impedirne l'accesso senza nemmeno visionarlo, attraverso e grazie all'URL presente nell'ipertesto. Ovviamente anche in questo caso i *social network* rendono più veloce il processo perché la maggior parte di loro, come si è visto, obbligano gli utenti a utilizzare il loro vero nome, rendendo così possibile il lavoro di identificazione e di censura ai governi sugli individui. Il motivo per cui oggi ancora si può avere ancora una minima protezione online da queste forme di censura è legato alla possibilità degli utenti di accedere anonimamente alla maggior parte dei contenuti (Morozov, 2013). Ma il desiderio, e la necessità, di profitti sempre maggiori stanno spingendo le forze economiche occidentali a modelli di marketing che necessitano delle informazioni degli individui, i quali sono disposti sempre più ad accettare la situazione senza vederne la pericolosità né per sé stessi, né ovviamente per i cittadini dei regimi autoritari d'Oriente e non. Questo lega il futuro di Internet e dei dati personali alle esigenze economiche dell'Occidente. Un altro elemento che rende particolarmente efficiente questa nuova censura 2.0 è il fatto che è delegata ad attori terzi che materialmente agiscono in aiuto dei governi. Nei paragrafi precedenti si è visto come in Occidente i governi spesso siano costretti ad accettare le decisioni di Google, o di altri attori analoghi del web, difatti sono questi grandi colossi ad avere l'ultima parola sulla rimozione o meno di specifici contenuti sempre cercando di essere coerenti con le loro linee di principio. Questo comporta che nel momento in cui Google e Facebook devono rapportarsi con dei regimi autoritari, tendono comunque a non assecondare tutte le richieste. Non rinunciano a queste grandi fette di mercato, perché sarebbe economicamente sconveniente tuttavia cercano di assecondare le loro richieste con riserva per tutelare la loro immagine ed evitare lesioni di questo genere. Questo non rappresenta un ostacolo per i governi che possono decidere di servirsi di sistemi di controllo locale o in generale di sviluppare localmente delle alternative alle *start-up* della Silicon Valley. In questo senso si trovano *software* elaborati e applicazioni che riproducono i famosi *social network*, rendendoli conformi alle norme culturali, direttamente prodotti in questi Paesi. Ne consegue che vi possono essere varie piattaforme, controllate da diversi attori, che operano la censura per il governo senza avere alcuna remora nell'agire nel modo più oppressivo possibile, in quanto non vanno incontro ad alcun tipo di danno di immagine (Morozov, 2013). Tuttavia quest'ultimo elemento può rappresentare una forza, ma allo stesso tempo una debolezza per il regime. Guardiamo per un attimo al caso della Cina, che è da considerarsi sotto questo punto di vista un modello (soprattutto per ciò che riguarda le operazioni di controllo dei contenuti). Il governo ha emanato una legge sulla censura, stabilendo che cosa e che tipo di documenti non possono essere presenti online, tuttavia lascia completamente libere le varie compagnie private di agire. Dunque sono le compagnie che decidono, ad esempio, quali tipi di parole sono da

considerarsi a rischio e così via dicendo. Si è osservato che questo permette l'esistenza e la sopravvivenza di alcuni *blog* contro il regime. Difatti da un lato chi scrive questo genere di contenuti è pronto ad evitare la censura e ne conosce bene i meccanismi, dell'altro le compagnie private non sempre ritengono o sono in grado di vedere contenuti a rischio. Infine, sempre rimanendo nell'ambito del *blogging*, visto che il contenuto rimane nelle mani completamente di compagnie locali terze, che hanno come unico obbligo quello di eliminare contenuti, e non di produrne, non vi è alcuna presenza di propaganda nei vari *blog* (MacKinnon, 2009).

Una forma più sofisticata di agire è la censura basata sulla collaborazione della società civile con il governo. Ad esempio in Cina vengono redatte delle vere e proprie liste di volontari che hanno il compito di segnalare al governo i contenuti che possono essere considerati di disturbo e per questo sono talvolta pagati. Pratiche analoghe esistono anche in Thailandia dove esiste un *blog* in cui i cittadini possono segnalare gli articoli o i post che accusano o denigrano la posizione del sovrano (la lesa maestà è lì un reato gravissimo). Queste forme di tecnologie sono utilizzate e sperimentate anche all'interno delle nostre democrazie. Basti pensare, ad esempio, alla recente iniziativa portata avanti dal fondatore di Wikipedia, Jimmy Wales, di creare uno spazio dove giornalisti e volontari contribuiscano, anche economicamente, al mantenimento del sistema. I volontari e lo staff dovranno di fatto controllare e verificare la veridicità dei vari contenuti prima di pubblicarli (Fiveash, 2017).

Infine l'ultima forma di censura nel Web, e anche la più pericolosa, è legata agli attacchi DDos. Per comprendere che cosa è un attacco DDos bisogna partire dal presupposto che i server che ospitano i siti hanno una differente capacità di gestire un numero finito di utenti. Dunque un sito come CNN.com, che è uno dei siti che può ospitare il maggior numero di persone al mondo contemporaneamente, riesce a sopportare che più utenti entrino nello stesso momento offrendo a tutti lo stesso servizio, ma al contrario piccole realtà no. Un attacco DDos è basato principalmente su questo, cioè attraverso dei *malware* che permettono l'utilizzo di più computer contemporaneamente, si fanno più accessi a un sito di quanti il server che lo ospita sia in grado di sostenere, in modo da mandare in fumo, letteralmente, tutto il sistema. Questi attacchi vengono spesso promossi dai governi, per oscurare i contenuti di determinati siti e per bloccarli del tutto, o anche da soggetti che sono semplicemente fedeli a una causa e che vogliono spegnere, letteralmente coloro che si dicono contrari a quest'ultima. Il vantaggio di utilizzare questi attacchi, è che sono particolarmente economici, infatti esistono individui che si offrono su Ebay di farne alcuni a pagamento. Un altro elemento a favore è legato al fatto che è una forma di censura difficile da tracciare, perché il sito continua a esistere, solo che materialmente non può funzionare. Infine il quantitativo di denaro che i proprietari del sito devono pagare per risolvere i danni causati dall'attacco, può anche fiaccare loro gli animi e rendergli sempre più difficile trovare nuovi server che li ospitino. Gli attacchi DDos rappresentano un modo per buttare fuori da Internet chi dà fastidio, levandogli ogni capacità di agire. Quest'ultima forma di censura è la più sottovalutata e anche la più pericolosa proprio perché particolarmente allettante anche da un punto di vista economico. Le *policy* che cercano di combattere

direttamente il problema sono pressoché nulle perché l'attenzione viene data principalmente a quelle che sono le tecniche di filtraggio dei contenuti che sono le più facili da aggirare.

Finora si sono analizzati i problemi legati alla censura che può nascondersi anche dietro a un considerevole flusso di informazioni e non è un fenomeno da dirsi incompatibile con lo sviluppo della infrastruttura tecnologica in determinati paesi. Sicuramente la censura online e quanto visto finora rappresenta una delle più grandi e pericolose minacce. I governi di questi luoghi utilizzano e plasmano il web sul loro modello di società chiusa, fiaccando il potere di aggregazione di quest'ultimo.

Tuttavia anche i governi delle nostre democrazie consolidate, hanno messo e mettono a rischio la libertà online in nome per lo più della sicurezza nazionale e della paura del terrorismo.

3.4 Gli ostacoli per la piena libertà degli individui in Occidente: il problema della sicurezza.

Vi sono dei casi in cui Google, e ovviamente anche altri grandi colossi, è costretto a piegarsi alle policy nazionali, tradendo la sua stessa filosofia. Questo avviene principalmente nel caso di richieste che vengono fatte dai governi per acquisire informazioni circa i dati personali di sospettati al terrorismo. Il problema del terrorismo al giorno d' oggi è che siamo innanzi a terroristi irrazionali che lavorano in piccoli gruppi o anche soli. Questi "nuovi terroristi" non considerano l'effetto di lungo termine delle loro azioni, ma semplicemente agiscono sacrificando la loro vita per un obiettivo più grande. Ne consegue che la prevenzione, data l'irrazionalità che caratterizza gli attacchi, diviene sempre più difficile da attuare. La maggior parte degli individui tuttavia accetta i provvedimenti anti terrorismo, nonostante questi minino chiaramente alla privacy. Questo perché solitamente le persone accettano queste restrizioni affermando di non avere nulla da nascondere. Non si comprende il cuore del problema, che non è legato a ciò su cui lo Stato indaga ma alla libertà dei singoli. La questione tuttavia non è legata ai controlli *online* e non, a cui ormai siamo abituati, ma al fatto che la società veda i cittadini che rispettano la legge come potenziali terroristi senza però fare qualcosa di realmente concreto per proteggerli dalle minacce del terrorismo come l'*escalation* di attacchi in Europa nell'ultimo periodo testimonia (Garfinkel, 2000). Per comprendere meglio questa minaccia alla libertà individuale dei singoli bisogna tornare indietro agli attacchi terroristici del Settembre del 2001. Dopo questi tragici avvenimenti, sono state emanate delle leggi di carattere esecutivo con lo specifico obiettivo di andare a combattere il terrorismo internazionale, cercando principalmente di prevenire i possibili attacchi. Le nuove forme di terrorismo hanno profondamente trasformato i metodi per combattere il nemico, che non è più possibile sconfiggere utilizzando metodi classici e previsti dalle vecchie strategie militari, in quanto questo può essere ovunque e non è facilmente identificabile. Questa paura ha portato gli Stati Uniti a emanare il *"Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*" (da qui in poi "*Patriot Act*") una legge il cui impatto è stato controverso, sui diritti e sulle libertà dei cittadini degli Stati Uniti d'America.

Principalmente si tratta di forme di sorveglianza che hanno offerto la possibilità ai sistemi di intelligence americana, in particolare all'NSA , di raccogliere informazioni sui cittadini, semplicemente sulla base di un sospetto, senza la necessità di un mandato, guardando al loro comportamento *online* , alle loro *mail* private e così via dicendo. La legge creava anche un sistema di alleanze particolarmente forte fra l'intelligence statunitensi e quelle estere. Nonostante la sua particolare invasività, le statistiche hanno mostrato come raramente i sospettati di terrorismo, poi si rivelassero realmente affiliati con le organizzazioni terroristiche e inoltre si è riscontrato che nella maggior parte dei casi si utilizzava questa legge per potere compiere indagini più approfondite su criminali comuni (Banks, 2011). Dopo il caso Snowden[27] , nell'estate 2013, le compagnie private come Google, Facebook, Yahoo! e Microsoft hanno cercato di fare chiarezza rendendo pubblici il numero di dati che avevano condiviso con il governo, in nome della sicurezza nazionale (GUARDIAN, 2014). Google inoltre ha creato un sistema di criptaggio delle sue *mail* in modo da proteggere ulteriormente i suoi utenti (Velazco, 2014). È chiaro che il caos generato da Snowden ha necessariamente mobilitato i grandi colossi del web nello scegliere una posizione e ad essere più trasparenti, per paura che il rapporto di fiducia con i clienti si incrinasse eccessivamente. Oggi la legge è stata sostituita dall'USA Freedom Act, provvedimento emanato dall'amministrazione Obama, che va a porre talune limitazioni all'azione delle agenzie americane, soprattutto per quanto riguarda la raccolta di metadata sugli utenti o di informazioni che servono a tracciare il comportamento degli utenti (Byers, 2015). Inoltre l'NSA ha deciso di non raccogliere più le email private dei cittadini statunitensi (Conditt, 2017). Tuttavia nonostante questi progressi, dettati anche dalle pressioni sempre maggiori dell'opinione pubblica e delle organizzazioni non governative, siamo ancora davanti al problema etico di come affrontare il terrorismo senza andare a ledere i diritti dei singoli.

E' interessante osservare che lo stesso tipo di misure sono state portate avanti in Francia dopo gli attacchi terroristici alla redazione del giornale "Charlie Ebdo" nel 2015. In Francia si sono autorizzate delle misure che consentono al governo di raccogliere i dati degli individui per osservarne il comportamento, di guardare che tipo di pagine web sono solitamente cercate o consultate dai singoli, in modo da poter giudicare se una persona sia sospetta o meno. Il provvedimento è stato fortemente contestato dalla società civile guidata dalla organizzazione non governativa "Amnesty International", che ha giudicato il provvedimento come lesivo dei diritti dei francesi e che ha avuto una modalità d'azione "sproporzionata" secondo gli attivisti (AMNESTY, 2016). Questo ci testimonia come in nome della sicurezza internazionale la libertà degli individui *online* può, di fatto, essere limitata, senza che gli individui se ne accorgano.

Anche in Gran Bretagna sono state presi provvedimenti negli ultimi anni in nome della tutela della sicurezza che hanno portato delle minacce per la sicurezza dei cittadini. Nel Regno Unito le misure di sorveglianza maggiormente restrittive sono state prese al di fuori di una formale dichiarazione di Stato di emergenza. Nel

[27] Edward Snowden era un agente dell'NSA che ha deciso di svelare al mondo il funzionamento di alcuni programmi di sorveglianza, ideati dall'*intelligence* americana, che venivano usati per spionare i cittadini.

2004 fu emanato il *"Civil Contingencies Act"* , dal governo di Tony Blair che riteneva non adeguata la legislazione precedente alla gestione delle nuove sfide che la situazione internazionale poneva. La caratteristica di questa legge era la generalità e l'ampiezza con cui si definiva un'emergenza e dunque con cui si autorizzavano misure speciali di sicurezza. Si intende come emergenza anche una calamità naturale o un evento ad essa collegato. Nel 2011 viene emanato il "*Terrorism prevention and investigation measures Act"* una legge che autorizza forme speciali di controllo nei confronti di coloro sospettati di essere minacce per la sicurezza del Paese. Alcune parti del provvedimento sono state ritenute troppo restrittive della libertà dei singoli e per questo motivo sono state bocciate dalla Corte Suprema del Regno Unito. Tuttavia non si è abbandonato completamente l'atto, ma al contrario si è deciso di applicare determinate forme di controllo nei momenti in cui si è innanzi a situazioni di generale "necessità". La vaghezza di questa legislazione, voluta dal parlamento, ha sollevato molte critiche da parte dei più svariati attori. Nel Novembre 2016 è stata emanato l'"*Investigatory powers act"* definito da Amnesty International come una delle misure di sicurezza più radicali dell'Europa e del mondo. La legge istituzionalizza la sorveglianza e lo spionaggio di massa, autorizza intercettazioni su larga scala, l'accesso a dati e informazioni personali. Una caratteristica del provvedimento che rappresenta una minaccia per gli individui è legata al fatto che le autorizzazioni per commettere questo tipo di sorveglianza possono essere date con grande facilità. Possono essere concesse, ad esempio, quando si è innanzi a individui che condividono gli stessi obiettivi all'interno di un gruppo specifico. In questo modo non si riesce facilmente a individuare i criteri per indicare chi sia effettivamente un potenziale terrorista e chi no, in quanto troppo generici. Tutti questi poteri possono essere autorizzati dal Primo ministro e da una commissione giudiziaria composta da membri scelti dal capo di governo stesso. Quest'ultimo elemento solleva forti dubbi circa l'indipendenza del giudizio del caso. L'atto è passato nonostante i numerosi dubbi sollevati in merito dalle commissioni parlamentari, le industrie di telecomunicazioni, la società civile e lo stesso garante per la *privacy* delle Nazioni Unite (AMNESTY, 2017).

In Germania invece nel 2015 si sono dati maggiori ai poteri ai servizi di *intelligence* soprattutto per quanto concerne le forme di controllo *online.* Si era provato anche ad attuare forme di controllo all'interno delle case delle persone tedesche e non. Tuttavia il provvedimento è stato bloccato dalla Corte Costituzionale tedesca perché non stabiliva dei criteri chiari per la sua attuazione. Nell'Ottobre del 2016 il parlamento ha adottato una legge sui servizi di sorveglianza che ha autorizzato il controllo delle comunicazioni dei cittadini stranieri. Nello specifico si autorizzano i servizi segreti a intercettare e raccogliere dati dei cittadin non tedeschi, qualora questi ultimi siano sospettati di terrorismo o di agire contro l'interesse tedesco. La legge è stata attaccata da più parti, anche dalle Nazioni Unite che in un rapporto sul diritto alla *privacy* l'ha definita sproporzionata e non necessaria. La legge autorizza anche l'intercettazione dei cittadini tedeschi nei casi di prevenzione al terrorismo. I principali dubbi sono legati alle modalità di raccolta dei dati dei cittadini all'estero, in quanto sono dati non controllatati in alcun modo. Inoltre vi è il fondato timore che un provvedimento di questo tipo mini la libertà dei giornalisti stranieri presenti sul suolo tedesco. Infine tutte queste forme di sorveglianza

possono avvenire senza che sia necessaria una qualsivoglia forma di autorizzazione giudiziaria (AMNESTY, 2017).

E' interessante notare come alcuni dei più importanti Paesi membri dell'Unione Europea abbiano preso una serie di provvedimenti così incisivi e invasivi per la *privacy* dei cittadini. Nonostante l'Unione Europea rappresenti una delle zone in cui il diritto alla *privacy online,* come si è visto, dovrebbe essere maggiormente garantito.

Internet è un luogo dove dovremmo sentirci sicuri di scrivere e di agire come vogliamo, perché rappresenta, data la nostra dipendenza sempre crescente dal mezzo, un'estensione della nostra persona sotto forma di dati (Rodotà, 2013). Tuttavia il web è anche il luogo che permette ad organizzazioni terroristiche come Al Qaeda di organizzarsi e di preparare nuovi attacchi terroristici. Questo ovviamente crea grandi difficoltà e spinge spesso alla violazione della privacy dei singoli. Le grandi trasformazioni che il web ha portato nella nostra società non l'hanno ancora spinta a trovare delle soluzioni concrete né a comprendere in che misura il web incida sui diritti dei singoli, come ad esempio quello alla privacy. Rimane tuttavia il fatto che ciò che mettiamo su Internet o in generale come usiamo i nostri *devices* non può essere usato contro di noi, pertanto dobbiamo essere sicuri e potere fidarci del nostro mezzo di comunicazione più usato (Clinton, 2010).

IV CAPITOLO

Il futuro del web: metodi, teorie e principi per garantire una più ampia libertà agli utenti.

4.1 La *Network Neutrality*

Quando si parla di *Network neutrality*, da un punto di vista tecnico si fa riferimento alle reti a banda larga e al modo in cui queste possono offrire un accesso all'*Internet* globale senza rallentare o bloccare taluni contenuti. Da un punto di vista politico la *net-neutrality* è il principio secondo cui bisogna consentire l'accesso al *web* a tutti gli individui in egual modo, considerando prima le loro esigenze piuttosto che quelle dei *provider.* Si tratta di un principio, dunque, che vuole che l'accesso ad *Internet* sia universale perché considera quest'ultimo come una risorsa fondamentale. Una società in cui si permette che esista il *digital.-divide*, non è da considerarsi giusta.

E' importante ricordare che un *provider* può bloccare l'accesso a determinati siti, spesso ciò avviene nel caso di pirateria, materiale pornografico e così via dicendo. Vi possono essere dei casi in cui per interessi di tipo prevalentemente economico i *provider* privilegino delle informazioni in forma di video, piuttosto che in forma di testo, o limitino la potenza di navigazione degli utenti spingendoli a utilizzare, ad esempio, diversi tipi di *devices*. Inoltre la rete, secondo quanti sostengono la *net neutrality*, non dovrebbe rendere maggiormente accessibili determinati pacchetti di informazioni[28], piuttosto che altri in quanto un *provider* che agisce in questo modo, potrebbe anche essere in grado di andare a guardare all'interno dei pacchetti di informazioni dei singoli utenti. In questo modo potrebbe offrire un abbonamento *ad hoc* in base al tipo di fruizione del *web* degli *user*. Per questo motivo i sostenitori della *net neutrality* ritengono che questo principio potrebbe portare anche a una più piena tutela della *privacy* individuale. Quando si parla di neutralità della rete non si parla di un principio astratto, ma di concreti provvedimenti legislativi. Difatti si tratta di una serie di azioni che i governi dovrebbero intraprendere proibendo tramite la legge ai *provider* di compiere delle discriminazioni di trattamento (De Nardis, 2014). Alcuni vedono nella neutralità della rete un modello di gestione del *cyberspace* improntato a una maggiore competitività economica (Sylvain, 2010). Difatti garantire a tutti il medesimo accesso e la stessa visibilità è un modo per favorire la competitività e l'emergere di nuovi attori nel *web*.

[28] Nel momento in cui ci si connette ad *Internet*, tramite un *provider,* avviene uno scambio di informazioni fra due terminali. Le informazioni vengono suddivise e inviate dal mittente sotto forma di pacchetti in modo da poter essere usufruite dal destinatario. Questo processo è definito come commutazione di pacchetto. I pacchetti vengono indirizzati secondo un percorso, che non è necessariamente lineare ma che al contrario è legato alla locazione dei *router* che sono incaricati di "instradare" i pacchetti (Kurose & Ross, 2003).

Grandi colossi come Amazon.com, Facebook, Google e Yahoo! non sarebbero potuti esistere se non fosse esistita la parità nel trattamento dei contenuti. Dunque una rete neutrale può essere un antidoto contro la creazione di grandi monopoli gestiti direttamente dalle grandi compagnie di telecomunicazioni. In questa visione sono degli obiettivi economici che fanno da traino per la creazione di uno spazio virtuale migliore (Sylvain, 2010). Molte *business company* in competizione con le grandi compagnie telefoniche sostengono la *net neutrality* appellandosi a una retorica fondata sul rispetto dei diritti umani e l'abbattimento del *digital-divide,* che una rete non neutrale è portata a creare. Tuttavia è importante sottolineare che queste compagnie hanno il fondato timore che i loro contenuti e alcuni servizi da loro offerti, come ad esempio le chiamate WhatsApp, vengano rallentati dai *provider*.

Per quanto riguarda le *policy* da prendere in merito il più grande problema è legato al fatto che devono essere i singoli Stati a decidere di attuare uno specifico provvedimento in materia, questo va a creare delle differenze in base alla parte del mondo in cui ci si trova. All'interno dell'Unione Europea dal Novembre 2015[29] viene garantita e tutelata la neutralità tecnologica. Il regolamento dell'U.E tiene conto di quelli che possono essere i limiti tecnici che talvolta possono impedire una piena neutralità della rete. Difatti, spesso, quando ad esempio vi sono utenti che consumano un'eccessiva quantità di banda, gli *Internet Services Providers* (ISPs) sono costretti a rallentare il traffico anche per evitare che le decisioni di alcuni loro clienti vadano a lederne altri. La più comune forma di discriminazione, è infatti legata al traffico degli individui (De Nardis, 2014). Inoltre il regolamento dell'Unione dispone che sono accettabili talune discriminazioni se in conformità con la legge o per mantenere e tutelare l'integrità del *network*[30]. Negli Stati Uniti la situazione è più complessa ed incerta; fino al 2015 non vi era alcuna concreta regolazione. In quell'anno la FCC ha emanato dei provvedimenti in materia in modo da assicurare la neutralità della rete[31]. Una legge che è stata vista in linea con il primo emendamento della costituzione americana che sancisce la libertà di espressione, difatti un mancato o parziale accesso limita le manifestazioni di pensiero degli individui. Tuttavia l'amministrazione Trump attraverso il nuovo capo del dipartimento delle telecomunicazioni Ajit Varadaraj Pai sta facendo dei passi indietro. Nonostante ancora non abbia elaborato un concreto piano d'azione Pai si è detto pronto, in nome della tutela del mercato a tornare indietro per quanto riguarda la *net neutrality* (Kargan, 2017).

Chi si dice contrario alla *net neutrality* lo fa appellandosi al fatto che certi tipi di discriminazioni sono da dirsi necessarie da un punto di vista tecnico. Un'ampia e incontrollata neutralità metterebbe in crisi un modello di *business*, comunque a vantaggio di grandi compagnie del *web* che sono in competizione con gli ISPs. Inoltre come si è visto, la neutralità tecnologica è un problema che deve essere affrontato attraverso l'azione dei governi. In questo modo in nome della neutralità si permetterebbe a degli Stati di controllare il *web* e di minare, volendo, anche alla qualità di un servizio. Sono preferibili le scelte portate avanti da chi opera nel mercato,

[29] Regolamento (UE) 2015/2120 del Parlamento Europeo e del Consiglio.
[30] Si veda riferimento 27.
[31] *Open Internet Order* del Marzo 2016.

piuttosto che quelle dei governi perché le prime sono considerate più indipendenti e paradossalmente più neutrali secondo quest'ottica (De Nardis, 2014). Un'altra critica alla *net neutrality* muove dall'assunto che detta *policy* non assicurerà automaticamente la democraticità all'interno del *web.* Una rete neutrale non è per forza democratica. La garanzia di accesso a dei contenuti rappresenta solo un modo di facilitare la comunicazione fra individui, senza tuttavia guardare concretamente alla qualità della democrazia all'interno del *cyberspace* (Sylvain, 2010).

Il diritto all'accesso rappresenta, comunque, lo strumento attraverso cui gli individui possono esercitare i loro poteri in rete. Come tutti i diritti anche il diritto all'accesso implica un dovere che va ad attaccare alcuni luoghi del potere. Non si può lasciare il mondo del *web* privo di una regolamentazione, in quanto troppi sono gli interessi che vi sono coinvolti, vi è bisogno di una serie di provvedimenti che vadano a creare un equilibrio fra le parti. Dunque una rete neutrale può essere il presupposto e la base per la costruzione di una rete democratica. Una rete in cui i diritti sono amplificati e universali, proprio perché il popolo del *web* soffre gli stessi problemi ovunque (Rodotà,2013).

Negli ultimi anni i discorsi in merito alla *net neutrality* e ai diritti del *web* sono aumentati, soprattutto dopo il caso Snowden il problema della democrazia digitale e della *governance* del *cyberspace* ha catturato anche l'attenzione di una parte dell'opinione pubblica.

4.2 Lo sviluppo dell'idea di un modello democratico di *web* nell'era post-Snowden.

In questi anni alcuni studiosi ritengono si stia affrontando una fase di transizione della *governance* della rete, ci si è resi conto che il mantenimento dello *status quo* non è più possibile. Bisogna dunque trovare un modello di *governance* che concili gli interessi degli Stati, delle aziende tutelando i cittadini e rendendoli, anche partecipi di quanto avviene *online* (Sorice & De Blasio, 2016).

Nella sua prima fase, fra gli anni '60 e '90, il *cyberspace* era dominato dagli attori che contribuivano a crearlo materialmente, da ciò ne conseguiva un'ampia partecipazione e discussione fra i membri al suo interno e una quasi totale esclusione dei governi. Nonostante, i primi sviluppi in questo campo si debbano ai finanziamenti del governo statunitense che hanno dato ai pionieri di Internet la possibilità di sviluppare le loro idee. Negli anni '90 tuttavia il modello va in crisi e si avvia la privatizzazione del *web,* con le conseguenze fin qui viste. "*L'intermediazione fra l'uomo e la macchina viene a collocarsi all'interno di scatole nere, seguendo regole sottratte al pubblico"* (Sorice & De Blasio 2016, pp.74) nonostante ci si sia continuati a nascondersi dietro una retorica a sostegno dell'anarchia del *web* e di una sua più totale deregolamentazione. Questo modello di gestione del *cyberspace* si definisce di *multiskateholder* perché tanti sono gli attori che ne hanno il controllo, allo stesso tempo i governi hanno un potere che varia in base alle infrastrutture che possono controllare. Paesi come la Cina possono avere un vero e proprio dominio sul loro *cyberspace* perché cercano in tutti i modi di essere svincolati dai giganti internazionali. Ovviamente questo dominio lede al quantitativo dell'informazione

e alla qualità della democrazia dell'intero sistema. Dall'altro lato altri Paesi, più liberi, non avendo il controllo delle loro infrastrutture sono delle vere e proprie province di un impero dominato dagli Stati Uniti. Nonostante i vari tentativi di organizzazioni come ad esempio l'Unione Europea per internazionalizzare la rete. Dopo il caso Snowden, tuttavia, il modello *multiskateholder* è entrato definitivamente in crisi mostrando i suoi evidenti limiti. Il modello che era nato in contrasto alla gestione di Internet dei paesi autoritari come Cina e Russia, aveva contribuito e permesso lo sviluppo di un sistema di sorveglianza di massa che aveva portato alla lesione dei diritti umani di milioni di cittadini in tutto il mondo. Il caso Snowden ha mostrato gli effetti politici della privatizzazione del *cyberspace* fatto da un'infrastruttura centralizzata e collocata solo nel territorio americano. Nel quale vi è anche il piccolo, ma potente, gruppo di aziende come Google, Apple, Microsoft, Yahoo! e così via. Questo ha permesso a un solo Paese la creazione di un programma come PRISM che leggeva e raccoglieva i dati dei singoli in modo incondizionato. Dall'altro lato la logica di profitto che ha portato alla diffusione dei *software* proprietari, che non permettono di leggere le istruzioni all'interno del codice sorgente[32], ha portato alla scrittura di programmi come OPTIC NERVE in grado di attivare la *webcam* di un computer senza che il proprietario se ne accorga. Nell'immediato gli Stati Uniti hanno cercato di occuparsi della crisi promuovendo una serie di conferenze internazionali volte a favorire il dialogo fra i vari attori: privati, membri di spicco dell'accademia, esponenti della comunità tecnica, rappresentanti della società civile e così via. L'ICANN insieme al governo brasiliano nel 2015 ha promosso l'organizzazione di un meeting (NetMundial) che si è svolto in Brasile nell'Aprile di quell'anno. Durante l'incontro si è iniziato a delineare il grande problema che ancora oggi rappresenta un limite alla creazione di un modello democratico di gestione del *web.* Infatti sono emerse delle visioni sovraniste, sostenute soprattutto dal governo brasiliano, che volevano imporre un controllo autonomo e indipendente delle infrastrutture (Sorice & De Blasio, 2016). La paura e lo sgomento post- Snowden hanno spinto molti governi a ripensare un modello di *governance* basato sulla gestione autonoma delle infrastrutture, che come si è visto, porta alla creazione di un sistema non democratico dove l'informazione è controllata (Santaniello & Amoretti 2013). In generale comunque questi forum sono finiti per diventare dei grandi parlatoi dove non si riesce a portare avanti un'azione concreta.

Nonostante nessun governo o Stato adotti un modello democratico di *governance* vari attori in diversi contesti stanno iniziando a discutere e a guardare allo sviluppo della *Net Democracy*. Lo sviluppo di questo modello passa attraverso la creazione dell'*Internet Social Forum*[33] (ISF da qua in poi). L'obiettivo è quello di creare uno spazio dove si possa discutere circa il futuro della *governance* di *Internet* in modo da promuovere un *web* decentralizzato nella sua architettura ma che tuteli e garantisca a tutti gli stessi diritti. In particolare offrendo ai cittadini il controllo dei propri dati e dell'informazione che passa per il *web* (ISF, 2015). L'ISF vuole distinguersi rispetto agli altri *forum* precedenti perché vuole produrre dei risultati concreti per la tutela dei

[32] Si definisce codice sorgente l'insieme delle istruzioni che compongono un programma.

[33] Il progetto si sviluppa nel 2015 con il preciso intento di porre fine alla sorveglianza di massa. Nasce all'interno del *World Social Forum* un incontro annuale di organizzazioni che rappresentano la società civile. Il principio che muove l'ISF è che il *web* appartiene a tutti gli individui e che per questo motivo questi ultimi devono avere un controllo su di esso. La paura è, infatti, che il cyberspace si stia muovendo sempre più verso una logica antidemocratica.

cittadini. Le violazioni dei diritti del *cyberspazio* non sono sempre tutelabili da un punto di vista legale, soprattutto quando si tratta di violazioni legate a programmi di sorveglianza di massa (Sorice & De Blasio, 2016). La produzione di norme necessita di un concreto impegno politico da parte di vari attori. Degno di nota è l'impegno dell'Unione Europea in merito che sostiene attraverso la Commissione un approccio sintetizzato dall'acronimo COMPACT "*che vede Internet come uno spazio di responsabilità civiche, organizzato in modo da costituire un'unica risorsa non frammentata secondo un modello di governance multipartecipativo, un mezzo per promuovere la democrazia e i diritti umani, una rete basata su una solida architettura tecnologica in grado di conquistare la fiducia degli utenti e di agevolare una governance trasparente, sia dell'infrastruttura soggiacente sia dei servizi da questa veicolati"* (COMMISSIONE EUROPEA 2014, pp.4). L'U.E promuove un modello multipartecipativo, che coinvolga i vari Stati membri, e che abbia un'unica legislazione di riferimento che sia parallela e non dissimile a quella che regola le azioni della nostra vita quotidiana al di fuori del web. In questo modo Internet non sarà più un luogo frammentato, ma al contrario unito dagli stessi principi a livello globale che ne guidano la legislazione. Per fare questo l'organizzazione regionale ritiene necessario promuovere un dialogo su specifiche tematiche e definire, soprattutto, il ruolo delle autorità pubbliche in questo contesto. Inoltre subito dopo il caso Snowden la Commissione dell'U.E. ritiene che sia fondamentale riconquistare la fiducia degli utenti del *web* che quindi non devono essere esclusi da questo processo di ricerca e dialogo sulla *governance.* Per questo motivo la Commissione europea propone che i processi multipartecipativi rispettino i seguenti requisiti: trasparenza, inclusività, equilibrio e *accountability.* In questa visione la trasparenza servirebbe come garanzia delle varie parti coinvolte in questo processo ed eviterebbe che terzi agiscano per parti silenziose; l'*accountability,* invece, dovrebbe essere garantita attraverso una rendicontazione periodica da un lato, ma anche dalla possibilità di ricorso in caso di mancato adempimento dei doveri da parte delle istituzioni intergovernative coinvolte. Per quanto riguarda l'inclusività e l'equilibrio l'obiettivo è quello di raggiungere "*tutte le parti interessate da una determinata questione, offrendo loro opportunità eque e accessibili affinché possano partecipare e contribuire a tutte le fasi cruciali del processo decisionale, evitando che nel processo prendano il sopravvento una parte interessata dominante o interessi di parte"* (COMMISSIONE EUROPEA 2014, pp. 7). Quest'ultimo obiettivo ha portato alla creazione di GIPO (*The Global Internet Policy Observatory*) che vuole rendere accessibili a tutti coloro che sono interessati gli ultimi risultati in ambito di *Internet governance.* GIPO permette anche l'attiva partecipazione degli utenti promuovendo il dialogo e lo scambio di idee.

Allo stesso tempo chi sostiene un modello di *governance* democratico, promuove anche lo sviluppo della giustizia sociale e della partecipazione attraverso il web. Bisogna infatti che il web recuperi il suo scopo originale, le varie innovazioni tecnologiche non hanno portato alla creazione di un mondo più giusto, anzi al contrario nuove sfide sono innanzi alle democrazie. Per questo motivo l'Internet Social Forum si propone di creare uno spazio per la promozione della giustizia sociale, con l'obiettivo di agire come attore intermedio

all'interno della società. Il mondo digitale influenza molti settori importanti della società, tuttavia un'azione concreta non può esistere se non vi è una struttura centralizzata che agisca da intermediario e che coltivi le azioni. In questo scenario, dunque, si colloca l'ISF che, sempre nella sua pagina web, elenca i vari punti della sua azione tutti finalizzati a creare un legame fra la giustizia sociale e il web (ISF, 2017). In quest'ottica le tecnologie e i *media* ridiventano strumenti in grado di aumentare la "densità" di una democrazia fornendo la possibilità ai soggetti di partecipare alla vita pubblica. Possono essere varie le posizioni, più o meno estreme, in questo campo ma tutte in generale vedono le tecnologie come uno strumento, in potenza, facilitatore della partecipazione (Sorice & De Blasio, 2016).

Talvolta si confonde il concetto di *e-democracy* con il concetto di *e-governement*, visto da molti come una delle potenzialità maggiori del *web* per alimentare la democraticità all'interno della società. Quando parliamo di *open governement* parliamo di un concetto "*solo in parte sovrapposto alle forme di e-democracy*" in quanto si tratta di "*un processo gestionale aperto e trasparente dell'amministrazione pubblica"* da ciò dunque si evince che siamo innanzi a una procedura, a un modo di governare (De Blasio 2014, pp. 34). Il Web 2.0 offre la possibilità ai governi di potere cambiare il loro modo di governare e anche di rendicontare le loro azioni innanzi all'elettorato. In questo modo Internet potrebbe diventare un luogo di condivisione e apertura dove le istituzioni governative al posto di raccogliere dati sui singoli, ne condividono altri per renderli partecipi e maggiormente consapevoli. Questo almeno in una visione puramente ideale. I cittadini diventano capaci in questo modo di monitorare l'operato del governo direttamente, a differenza di quanto avveniva in passato non ricevono un semplice stimolo a cui rispondere, ma possono partecipare in modo attivo. Ciò che rende possibile tutto questo è ovviamente la volontà politica di rendere *open* i dati relativi alla pubblica amministrazione. Una volta disponibili i dati possono essere riutilizzati in svariati modi dai cittadini e anche dalle Organizzazioni non governative interessate allo studio di determinate situazioni. Allo stesso tempo anche i cittadini, con le competenze tecniche adeguate, possono creare dei loro personali *database* denunciando problematiche su cui vogliono che lo Stato o il governo locale si focalizzi. Per fare ciò si tendono comunque a utilizzare maggiormente i *social media*, soprattutto Twitter (Vanhomerig & Karré,2014). Nei paesi anglofoni, Canada, Stati Uniti e Gran Bretagna il sistema di *open data* è stato implementato. Puntare agli *open data* significa puntare alla trasparenza, e dunque in qualche modo combattere la sorveglianza di massa. Tuttavia non saranno semplicemente dei dati a risolvere i problemi di fiducia che attualmente i cittadini avranno nei confronti dei governi. Nonostante ciò queste pratiche di governo incentivano un utilizzo del *web* maggiormente in linea con gli scopi e gli obiettivi iniziali per cui era stato creato.

4.3 Il modello di società del *free software movement.*

Si ritiene interessante concludere la ricerca sui possibili metodi e modelli attraverso cui garantire la libertà agli individui *online* guardando all'esperienza della *free software foundation.* La fondazione fondata da Richard

Stallman nel 1985 rappresenta un classico esempio di subcultura[34] che mira a cambiare il rapporto produttivo rendendo attivamente partecipi i consumatori-utenti ridandogli la possibilità di potere essere protagonisti della loro esperienza. Alcuni vedono talune analogie fra il *free software movement* e le comunità che sono fiorite fra gli anni '60 e '70 in California. Difatti vi è lo stesso *background* culturale e fra gli appartenenti al movimento di Stallman vi è lo stesso spirito comunitario che li spinge a diffondere i loro valori e la loro etica il più possibile nella società.

L'associazione ha come obiettivo quello di promuovere l'uso globale del *free software* cioè un software che offre la possibilità di essere studiato, modificato e redistribuito grazie all'utilizzo di un particolare tipo di licenza che rende disponibile il codice sorgente[35]. Questo metodo di *licensing* è definito, con un neologismo creato dalla stessa fondazione, *copyleft*. Secondo Stallman, che è il *leader* e la voce del movimento ancora oggi, l'utilizzo del *copyleft* è uno strumento attraverso il quale si può promuovere la libertà di informazione fra gli individui. Vi è una visione fortemente utopica che ritiene che attraverso la tecnologia si possa cambiare radicalmente la società andando a intaccare le grandi compagnie capitalistiche, come Microsoft, che vengono accusate dal *Free Software Movement* di avere privato gli utenti della libertà costringendoli attraverso l'utilizzo del *copryright* a un'ignoranza forzata. E' una visione che in questo senso idealizza la tecnologia perché vede in quest'ultima lo strumento per il cambiamento radicale della società anche *offline* (Elliot & Scacchi, 2008). La società dell'informazione in cui viviamo oggi ha delle potenzialità infinite, nonostante ciò, vi è un ampio *digital divide* in quanto non soltanto vi sono delle parti del mondo in cui non vi sono determinate tecnologie, ma anche perché vi è una grande ignoranza circa il funzionamento delle tecnologie, dalle quali siamo sempre più dipendenti. La visione del movimento per il *software* libero va contro la globalizzazione accusando questo processo di avere privato le persone del loro potere trasferendolo alle grandi compagnie, che adesso controllano con grande facilità le nostre vite. Per avere una società in cui gli individui sono liberi bisogna trattarli come agenti attivi e non come passivi recipienti importanti solo nel momento dell'acquisto. Il movimento di Stallman ha resistito a ogni tentativo di omologazione e si esprime attraverso i suoi sostenitori sparsi in giro per il mondo che cercano anche di personalizzare le idee del *free software* per adattarle zona per zona (Thomas, 2010).

La *free software foundation* e i suoi seguaci ritengono che vi sia una stretta correlazione fra le minacce che gli individui incontrano *online* e la diffusione dei *software* non liberi. Infatti il primo passo, si legge nel sito della fondazione, per acquisire la libertà è avere il controllo del proprio dispositivo in questo modo si potranno evitare alcune forme di sorveglianza e controllo. Tuttavia per quanto riguarda le minacce alla privacy degli

[34] Si definisce subcultura "*l'insieme delle pratiche sociali provocate anche dalla fruizione dei media, i cui contenuti sono spesso riutilizzati in chiave oppositiva-quando non apertamente trasgressiva- degli appartenenti della subcultura stessa"* (Sorice 2009, pp. 254).

[35] Un esempio di *software* libero è rappresentato dal *kernel* Linux creato dallo svedese Linus Torvalds. Linux è il primo esempio di *software* libero esistente. Tuttavia Stallman tiene a sottolineare le differenze fra il suo movimento e l'*Open Source Initiative*, che ha portato alla diffusione di Linux, in quanto il primo si pone delle domande etiche e propone anche una specifica filosofia e non soltanto un determinato tipo di *software* (Elliot & Scacchi, 2008).

individui e alla raccolta di dati da parte dei governi Stallman suggerisce uno specifico atteggiamento da seguire. La proposta di Stallman è radicale e si fonda sull'assunto che gli individui "*devono rifiutare di usare sistemi di comunicazione che esigono che gli utenti usino il loro vero nome: anche se questo non costituisce un problema per l'individuo in sé, mette pressione agli altri affinché cedano la propria privacy*" (Stallman, 2013). Dunque bisogna boicottare tutte quelle forme di servizi *online* che vogliono acquisire informazioni, anche minime, su di noi[36]. Per Stallman non si può arrivare a una soluzione senza un mutamento totale all'interno della società. Fino a quando non vi sarà un cambiamento strutturale, con l'utilizzo e la diffusione del *free-software* e della sua filosofia, bisognerà boicottare tutti i servizi *online* sui quali gli individui non possono avere controllo. Per questo motivo lo stesso *leader* invita i suoi seguaci a manifestare le loro scelte e a diffondere la filosofia al prezzo, spesso, di un vero e proprio isolamento (GNU, 2017).

[36] All'interno della pagina personale di Stallman vi sono degli spazi relativi a vari colossi del *web*, come Amazon, Airnb e così via dicendo. All'interno di queste pagine il *leader* del movimento spiega le ragioni per cui queste aziende e i loro servizi vanno boicottati.

CONCLUSIONI

Internet si è presentato a noi come un (non) luogo dalle mille contraddizioni che non può più a lungo essere ignorato e dall'opinione pubblica e, soprattutto, dai governi. Ogni aspetto della nostra vita ormai è collegato alle nuove tecnologie. La dipendenza crescente degli individui rispetto alle tecnologie è legata a un rapporto di fiducia, sempre più forte, fra i singoli e la scienza tecnologica. Un rapporto che diventa più forte ogni giorno di più, in quanto più ci si affida alla tecnologia per la risoluzione dei problemi quotidiani più si ha fede in essa. La conseguenza è un cambiamento totale all'interno della società, difatti se prima il concetto di fiducia era strettamente legato all'esperienza diretta e a un rapporto con gli altri, oggi non sembra essere più così. Questo mutamento ha influenzato per sempre anche i rapporti all'interno della nostra società, soprattutto quello fra cittadini e figure professionali. Si sta assistendo a una de-professionalizzazione della nostra società, soprattutto nel rapporto pubblico-privato. Gli individui non si affidano più a terzi "agenti"[37] per risolvere alcuni problemi della loro vita, ma cercano attraverso il web di affrontarli. L'aumento di informazioni a nostra disposizione fa sì che spesso, ad esempio, un medico incontri un paziente che ha consultato e studiato una serie di informazioni specialistiche che potrebbero portarlo a contrastare quanto il dottore gli prescrive. Ciò rappresenta una sfida per la nostra società che dovrebbe riuscire a guardare e ad analizzare la qualità delle informazioni che da ogni dove ci inondano. Ogni gruppo e categoria professionale non può più ignorare le sfide che il *web* sta ponendo innanzi ai nostri occhi. Al giorno d'oggi i governi occidentali non riescono a cogliere questo vuoto di *policy*, né la necessità di innovare (Margetts, 2009). Si è principalmente deciso di utilizzare il web per incrementare la trasparenza rendendo pubblici la maggior parte dei dati relativi all'amministrazione della cosa pubblica. La trasparenza è un concetto che va a toccare vari aspetti della *governance* e ha in sé molte varianti. Difatti si può parlare del rapporto e della necessità di trasparenza quando si parla di sicurezza, ma anche quando si parla di *accountability*. La diffusione dell'uso di Internet ha incentivato la trasparenza delle amministrazioni pubbliche occidentali. In questo senso Internet diviene il luogo della democrazia per eccellenza consentendo a tutti tramite la possibilità di consultare i dati e di essere, dunque, perfettamente informati. Tuttavia, alcuni studi hanno mostrato che la possibilità di consultare tutte le informazioni relative alla pubblica amministrazione ha spesso portato i cittadini a perdere fiducia nelle istituzioni perché viste come incompetenti. In secondo luogo quando si parla di *open data* spesso si è innanzi ad organizzazioni terze che guadagnano, pubblicando determinati dati, quella fiducia che i governi hanno perduto. Dunque talvolta bisogna per fare ciò, ancora una volta, affidarsi a terzi, che con specifiche competenze tecniche pubblicano i dati in nome della trasparenza, come avviene con il *Google Transparency report.* Questo riporta alla luce il grande problema che è alla base del problema della *governance* di *Internet* e dei suoi effetti sulla nostra vita: la mancanza di competenze

[37] Si intende per rapporto di agenzia "*una species dei rapporti di potere sociale fra un soggetto principale e un soggetto agente che compie azioni, diciamo pure azioni di rappresentanza, per suo conto"* (De Mucci 1999, pp-190). Relazioni di questo tipo si manifestano quando gli individui comprendono che per massimizzare i loro interessi è necessario affidarsi a terzi (De Mucci, 1999).

tecniche. Difatti tutte queste pratiche attraverso cui si vuole garantire la democraticità, dipendono da terze entità che spesso non hanno alcun interesse nel massimizzare *l'accountabilitiy* democratica. Vi è dunque, ancora una volta, un problema di interpretazione per i cittadini ordinari e per i governi. Da qui la necessità di implementare l'utilizzo e la conoscenza di Internet in tutte quelle che sono le *policy* dei nostri tempi in modo da offrire ai cittadini la possibilità di trarre in modo concreto dei vantaggi dal nuovo mezzo di comunicazione, che al contrario di quanto affermavano i *cyber* ottimisti necessita di una regolamentazione in tutti quegli ambiti e quelle problematiche nuove spesso imprevedibili (Margetts, 2011). E' proprio l'impossibilità di prevedere dove l'innovazione porterà e la mancanza di linearità del progresso che rende difficile l'azione in questo campo (Sorice, 2009). L'idea, inoltre, che la tecnologia di per sé stessa sia portatrice di cambiamento e di miglioramento sociale è da dirsi erronea, come i casi qui sopra visti ci hanno testimoniato. Fino a quando si darà per scontato un cambiamento sociale, questo non avverrà e la libertà degli individui sarà in balia delle contingenze e delle esigenze dei governi, o di terzi attori, che se da un lato pubblicano tutti i dati delle pubbliche amministrazioni, dall'altro sviluppano programmi di sorveglianza di massa all'oscuro dei cittadini. Nel momento in cui si comprenderanno le implicazioni che il web ha per lo stesso modo di fare *policy*, si potrà finalmente avere un nuovo tipo di politiche pubbliche che si focalizzerà su nuovi temi per garantire diritti e tutele più piene ai cittadini.

SYNOPSIS

Who rules the Internet? Who controls the information flow? There are no easy answers to those questions, although the net governance's choices consistently affect the level of democracy of our society. This essay will analyze the e-governance and some related issues, in order to provide those answers.

To begin with, the first chapter breaks down the history of Internet. At the beginning there was a technical governance regime which means that the Internet was directly controlled by the material creators of the entire system. In 1992 the situation dramatically changed when the Cern scientist Tim Barners Lee created the World Wide Web. Lee generated a system based on the hypertext which offered the possibility to non-governamental organizations, as well as individuals, to access the web.

Virtual online communities emerged, which are definied as "*social aggregations that emerge from the Net when enough people carry on those public discussions long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace"* by the sociologist Howard Rheingold (Rheingold 1993, pp.1). Rheingold represents the cyber-positive or utopian thinking that was widespread during the '90s. It seems that their expectations were met by the global justice movements who organized their protest online through the list-server. Also, the birth and spread of social networks made the development of political aggregation forms even easier. The case in point is represented by the *#OccupyWallStreet* movement. The association was created in 2011 at Zucotti Park in New York with the purpose of fighting the financial and economic world of Wall Street. It was the first movement using Twitter to organize a protest and to share updates about it. An incredible number of people joined the demonstrations. Even citizens, who had never experimented political activism before, decided to participate. Nevertheless, the protest would not have existed without the grass roots activism offline. In order to make a real change in our society, it is always necessary to have the effort of the people offline.

The second chapter will critically examine and offer a definition of Internet governance in order to understand the logic of power of the Internet. Nowadays, academics tend to agree on the definition of *e-governance* given by "The World Summit of Information society" in 2003. According to the Summit : " *Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision making procedures, and programmes that shape the evolution and use of the Internet"* (Geneva declaration of principles 2003, article 49). In order to understand how the governance works, the essay focuses the attention on the players controlling the Internet resources in terms of

infrastructure. First of all, technical aspects are to be analyzed to understand how the Internet connection works. Therefore it is essential to know what the DNS are.

The Domain Name Systems translate the numbers from the websites' addresses in words understandable by humans. In this way DNS allow the access at a mainstream level. Nowadays, DNS are managed by of the ICANN, a nonprofit organization based in the USA. This organization is independent since 2016, before this date it was under the control of the government of the United States. However, the influence of the United States government is still considerable. The concern related to the DNS is caused by the fact that these technologies can even be used to block the access to certain contents. As a consequence, who is in control of DNS could even decide to restrict the user's freedom *online*.

The protocol is another very important technical part. A protocol is a system of rules governing the Internet. Protocols embed values which reflect the idea of their creators. The issue here is the fact that it is not easy to identify who is creating a new protocol and why.

The latest part of the second chapter will focus upon the issue of the control of online contents. This control is exercised by big companies such as Google, Yahoo and Bing. They are able to do that thanks to the algorithms. An algorithm is a procedure which solves a problem through elementary steps, thanks to the mathematics. Algorithms are currently used to customize websites' homepages, which we frequently visit, or to create intelligent forms of advertising. Overall, they are mainly used to collect users' data for commercial purposes. On one side, this kind of actions are needed by the companies to earn money while maintaining the access to their contents free. On the other side, the more personal data are collected, the less privacy is granted to the users.

In this regard, the third chapter of the essay will be focused on the level of protection guaranteed to online users. It will highlight the threats to their freedom. Once again, it is essential to look at the role of the big companies, such as Google, in the managing of online contents. Those private companies have a substantial moral responsibility for what they are hosting. By allowing the greatest number possible of contents in their site, they would be considered as defenders of the online freedom. At the same time, they have to respect the different national legislations of every country having access to them. Moreover, they have to face governments' requests who force them to violate the privacy or the freedom of opinion of their users. Sometimes governments ask for the removal of specific online contents. Other times they are concerned about certain individuals and they ask for their datas. Certainly, companies such as Google are in a delicate position,

especially when these requests come from non democratic countries. In order to gain the trust of the user, Google publishes every year a report of those kind of requests. However, the main concern is related to the fact that governments tend to hide and avoid to explain to the public opinion their demands.

Even other type of private companies have a great responsibility in our society. Apple, for instance, has a critical importance in controlling the innovation: as an example we could think of the AppStore rules for Apps, specifically referring to the reasons why an app could be rejected or accepted. Those rules are not clearly defined, but we can read the following lines: "*We will reject apps for any content or behavior that we believe is over the line. What line, you ask? Well, as a Supreme Court Justice once said, "I'll know it when I see it". And we think that you will also know it when you cross it.*" (APPLE POLICY, 2017).

Another threat to online freedom of persons is related to privacy. Nowadays, the Internet and the new technologies have changed what privacy means. Privacy is traditionally the right to be left alone. However, it is currently more difficult to understand when privacy is violated. In fact, we are constantly threatened by our devices that collect information about us without us knowing. People sometimes waive their right to privacy since social networks or other kind of web sites force them to use their real identity.

When the Internet made its first appearance, an important shared belief was that new media fostered the use of anonymous identity. In fact, people typically used pseudonyms within online forums. This practice has become harder to realize since the creation of social networks. Phenomena such as cyberbullying led companies such as Facebook or Google to adopt *real name policies*. On one side, this seems the only way to recognize the responsible of online crimes. On the other, the most part of data that are requested by those companies are used for commercial purposes. Moreover, anonymity is fundamental for those persons who live in non-democratic countries such as China. As a consequence, fostering people to use their real identity could represent a violation of human rights. Real name policies enacted by the Chinese government represent the clearest example of this idea.

Thus, the third chapter will start by focusing on how governments use the Internet to control and limit their citizens' lives. Firstly, it is analyzed the situation in non-democratic countries. The idea that technology can shape democracy is widespread in western societies. However, the current situation is denying this common thinking. The case in point is represented by China, which has exploited the Internet to limit even more the freedom of expression of its citizens. They are sometimes helped by the Western companies, such as Google, that prefer to sacrifice their philosophy in order not to lose Chinese customers. Nevertheless, when American companies refuse to collaborate with the authorities, the government refers to local companies, that have no

reason to refuse those requests, to provide services, to create social networks or to control infrastructures. In fact, it is easier for the government to control the Internet user by using local companies. For this reason, it exists in China several web sites that are a reproduction of the western ones, but still controlled by the government.

Another form of control and censorship on the Internet is based on the collaboration of civil society with the government. In certain cases, authoritarian governments ask to volunteers to control the internet contents and to report any violation of the rules to the authorities. These people are generally well payed for those activities.

Furthermore, the more sophisticated form of censorship is represented by the DoSS attack. A DDoSS attack disrupts temporarily or indefinitely a server which hosts the site. This can happen through the use of some types of malware. DDoSS is the cheapest kind of attack, mostly used to undermine the enemy. In order to repair the damage caused by the attack, the web site's owners have to spend a consistent amount of money.

Finally, the third chapter will critically analyze the degree of online users' protection in our Western democracies. The recent terrorist attacks have been fostering the United States and the European countries to enact extraordinary legislations that authorize massive surveillance. Those measures make it possible to collect data about suspected users without them knowing. It is interesting to see that most part of European countries have adopted these types of law, even though the EU represents the world areas where there is the higher degree of privacy protection in terms of legislation.

The final chapter will deal with some models, theories and policies conceived how remedies for guaranteeing a better degree of freedom protection to the users. First of all, the chapter will examine the network neutrality issue. The network neutrality is a juridical principle which claims to guarantee to everyone the online access without any sort of discrimination. A society where it is enabled the existence of the digital divide can never be considered as a democratic one. Moreover, a neutral network offering to everyone the same visibility fosters an economic competition inside the web.

The democratic model will be the subject of the other part of the chapter. The model has been theorized by some scholars who claim about the current governance of the Internet. The development of this model should be realized with the support of the Internet Social Forum. The main purpose of the forum is to create a space where people and experts can discuss about the future of the Internet governance. The ISF would

generate a model of governance which guarantees the user rights. In particular, it would offer to every citizens the possibility of monitoring their online datas. Moreover, the ISF would that the Internet encourage the movements of social justice . By involving those groups the ISF will foster the democratic participation inside the society.
Instead, some policy makers have exploited the Internet to increase the degree of participation inside their countries. This is the case of the open data policies that consist in the disclosure of the informations about the government work.

The last part of the fourth chapter will be focused on the extremist position of the free software movement. The Richard Stallman association has the main purpose of promoting the global use of the free software. The free software makes accessible his source code. Thus, the software can be studied, modified and redistributed in the society. By using the free software the freedom of expression will be guaranteed to everyone. It is an utopist vision that considers technology as the main instrument for a radical change in the society. The Free Software movement accuses the big companies, as Microsoft, of stealing the user freedom by forcing them to the use of software with closed source code. The free software foundation claims that there is a correlation between the closed source code and the threats to freedom that people have to suffer online.

In conclusion, in order to make a real change in our society it is necessary that our policy makers understand the role that Internet has in our life and how it uses to make a better society. This will occur only when it is understood that innovation is not linear.

BIBILIOGRAFIA

Byers, A. (2015): "Usa Freedom Act vs. Usa Patriot Act", *Politico*, Disponibile in: http://www.politico.com/story/2015/05/usa-freedom-act-vs-usa-patriot-act-118469

Caliandro, A. (2011): [On-line], Uno sguardo sociologico sulla costruzione dell'identità *online*, Disponibile in: http://www.etnografiadigitale.it/2011/01/uno-sguardo-sociologico-sulla-costruzione-dellidentita-online/.

Carr, M. (2013): [On-line] Internet freedom, human rights and power, Australian Journal of International Affairs, 67:5, 621-637, http://dx.doi.org/10.1080/10357718.2013.817525.

Castells, M. (2009): *Comunicazione e potere*. Milano: Università Bocconi Editore.

De Blasio, E. (2014): *La democrazia digitale.* Roma: Luiss University Press.

De Blasio, E., Sorice, M. (2016): *Innovazione Democratica.* Roma: Luiss University Press.

De Nardis, L. (2009): *Protocol politics: The globalization of Internet governance*. Cambridge: The Mit Press.

De Nardis, L. (2014): The Global War for Internet Governance. United States: Yale University Press.

Elliott,M.,Scacchi,W. (2008) "Mobilization of software developers: the free software movement",Information Technology & People, Vol. 21 Issue: 1, pp.4-33, Disponibile su: http://dx.doi.org/10.1108/09593840810860315.

Fiveash,K. (2017): [On-line] Wikitribune is Jimmy Wales' attempt to wage war on fake news, *Ars technica,* Disponibile in: https://arstechnica.com/business/2017/04/jimmy-wales-wikitribune/

Garfinkel, S. (2000): *Database Nation: the death of privacy in 21st century*, Bejing- Cambridge-Farnham-Koln-Paris-Sebastopol-Taipei-Tokio: O'Reilly.

Greenwald, G., MacAskill, E., Poitras, L. (2013): Edward Snowden: the whistleblower behind the NSA surveillance revelations, *The Guardian,* Disponibile in: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Haigh, T, Russell, A, & Dutton, W (2015): [On-line] 'Histories of the Internet: Introducing a Special Issue of Information & Culture', Information & Culture, 50, 2, pp. 143-159. Disponibile in: Academic Search Complete doi. 0.7560/IC50201.

Juris, J. S. (2012): Reflections on #Occupy Everywhere: Social media, public space, and emerging logics of aggregation. [On-line] American Ethnologist, 39: 259–279. doi:10.1111/j.1548-1425.2012.01362.x

Kang, C. (2017):[On-line] Trump's F.C.C. Pick Quickly Targets Net Neutrality Rules, The New York Times, Disponibile in: https://www.nytimes.com/2017/02/05/technology/trumps-fcc-quickly-targets-net-neutrality-rules.html

Kaplan Andreas M., Haenlein Michael, (2010): [On-line] Users of the world, unite! The challenges and opportunities of social media, Business Horizons, 53: 59-68. Disponibile in: http://michaelhaenlein.eu/Publications/Kaplan,.

Kramer,A.,Guilloryb,J.& Hancoock, J. (2014): [On-line], PNAS "Evidence of massive-scale emotional contagion through social networks", Disponibile in: http://www.pnas.org/content/111/29/10779.1.

La France, A. (2017): [On-line] The Problem with WikiTribune, *The Atlantic,* Disponibile in: https://www.theatlantic.com/technology/archive/2017/04/wikipedia-the-newspaper/524211/

Margetts, H. (2009): [On-line] "The Internet and Public Policy", "Policy and Internet", Vol.1, Iss 1, Article 1, Disponibile in: www.psocommons.org/policyandinternet.

Margetts, H. (2011): "The Internet and Trasparency", The Political Quarterly, Vol.82, No.4, October-December.

MacKinnon, R. (2009): [On-line], China's censorship 2.0: How companies censors bloggers, First Monday, Volume 14 Numero 2, Disponibile in: http://firstmonday.org/article/view/2378/2089.

McChesney, R. (2009): [On-line], My Media Studies: thoughts from Robert W. McChesney, Television & New Media, Volume 10 Numero 1. Disponibile in: http://journals.sagepub.com/home/TVN.

McKelvey, F (2014): Algorithmic Media Need Democratic Methods: Why Publics Matter.
Canadian Journal of Communication, Volume 39, Business Premium Collection pg. 597.

Morozov, E. (2011): *The Net delusion.* Stati Uniti: Public Affairs.

Oggolder, C (2015):'From Virtual to Social: Transforming Concepts and Images of the Internet', Information & Culture, 50, 2, pp. 181-196, Academic Search Complete, EBSCOhost, visto 10 Marzo 2017.

Oliverio, A. (2015) *Individuo, natura, società. Introduzione alla filosofia delle scienze sociali*. Milano: Mondadori.

Regolamento (UE) 2015/2120 del Parlamento Europeo e del Consiglio.

Rheingold, H (1993): *The Virtual Community: Homesteading on the Electronic Frontier*. Cambridge: The Mit Press.

Rodotà, S. (2012): *Il diritto di avere diritti,* Bari: Editori LaTerza.

Santaniello, M. & Amoretti, F. (2013): Electronic Regimes: Democracy and Geopolitical
Strategies in Digital Network. Policy and Internet, Vol, 5, No 4.

Thomas, B. (2010): Participation in the Knowledge Society: the Free and Open Source Software (FOSS) movement compared with participatory development , Development in Practice, Volume 20, Number 2, pp. 270-276.

Sylvain, O. (2010): Internet Governance and Democratic Legitimacy: Federal Communications Law Journal; Vol, 62, No, 2. Businesse Premium Collection: pg.205.

Sorice, M. (2009): *Sociologia dei mass media.* Roma: Carocci.

Wauters, R. (2009): [On-line] China's Social Network QZone Is Big, But Is It Really The Biggest?, *Teccrunch*, Disponibile in: https://techcrunch.com/2009/02/24/chinas-social-network-qzone-is-big-but-is-it-really-the-biggest/

Willson, M. (2016): [On-line], Algorithms (and the) everyday. Information, Communication & Society. Disponibile in: http://dx.doi.org/10.1080/1369118X.2016.1200645

Vanhoring. I & Karré. P (2013) : [On-line], Public accountability in the Internet age: changing roles for governments and citizens, International Review of Public Administration, 2014 Vol. 19, No. 2, 206–217, Disponibile in: http://dx.doi.org/10.1080/12294659.2014.928477.

Varian, H. (2013): Beyond Big Data [Working paper] Transcript of keynote given at NABE meeting, Sept 2014, San Francisco.

Zuboff,S (2016): [On-line], The Secrets of Surveillance Capitalism, Frankuferter Allemagine, Disponibile in: http://www.faz.net/-gsf-8eaf4

SITOGRAFIA

AMNESTY INTERNATIONAL (2016): *L'impact disproportionné de l'État d'Urgence en France,* Disponibilein:https://amnestyfr.cdn.prismic.io/amnestyfr%2F775c2444-b422-41f0-83e8-0cb6e2a2953f_aif+-+vies+bouleversees+etat+urgence+france.pdf.

AMNESTY INTERNATIONAL (2017) : *Dangerously, Disproportionate* : the ever expanding of National security in Europe. Disponibile in: www.amnesty.org .

BBC (2012): *China dissident Wang jailed on Yahoo information freed*, Disponibile in: http://www.bbc.com/news/world-asia-china-19432800.

CNN (2013): *Chinese journalist Shi Tao released after 8 years in prison,* Disponibile in: http://edition.cnn.com/2013/09/08/world/asia/shi-tao-journalist-free/.

COMMISSIONE EUROPEA (2014): *Governance e politica di internet: il ruolo dell'Europa nel forgiare il futuro della governance di Internet,* Disponibile in: http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52014DC0072&from=en.

ENGADGET (2014): *Google makes Gmail more secure in light of NSA snooping,* Disponibile in: https://www.engadget.com/2014/03/20/gmail-https-nsa-snooping/

ENGADGET (2017): *NSA will stop illegally collecting American emails,* Disponibile in: https://www.engadget.com/2017/04/28/nsa-will-stop-illegally-collecting-american-emails-report/.

GUARDIAN (2014): *Microsoft, Facebook, Google and Yahoo release US surveillance requests,* Disponibile in: https://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests.

GUARDIAN (2015): *France passes new surveillaince law in wake of Charlie Ebdo attack*, Disponibile in: https://www.theguardian.com/world/2015/may/05/france-passes-new-surveillance-law-in-wake-of-charlie-hebdo-attack.

INTERNET SOCIAL FORUM (2017): *Internet Social Forum: Why the Future of the Internet Needs Social Justice Movements,* Disponibile in: http://internetsocialforum.net/isf/?page_id=1402.

INTERNET SOCIETY (2012): *History of Internet Governance | Internet Society*, Disponibile in: https://www.internetsociety.org/history-internet-governance.

ITU (2003): *Declaration of Principles Building the Information Society: a global challenge in the new Millennium*, Disponibile in: http://www.itu.int/net/wsis/docs/geneva/official/dop.html.

GOOGLE BLOOGSPOT (2007): *Free expression and controversial content on the web*, Disponibile in: https://googleblog.blogspot.it/2007/11/free-expression-and-controversial.html.

GOOGLE TRANSPARENCY REPORT (2015): *Richiesta di rimozione di contenuti da parte dei governi*, Disponibile in: https://www.google.com/transparencyreport/removals/government/?hl.

OVUM (2016): *App Revenue to Double by 2020, Outpacing Download Growth*, Disponibile in: https://www.ovum.com/press_releases/ovum-app-revenue-to-double-by-2020-outpacing-download-growth/.

APP STORE REWIEV GUIDELINES (2017): *App store rewiev guidelines*, Disponibile in: https://developer.apple.com/app-store/review/guidelines/.

VIDEOGRAFIA

Clinton-Rodham, H. (2010)*: Secretary Clinton Speaks on Internet Freedom*, Disponibile in: https://www.youtube.com/watch?v=ccGzOJHE1rw&t=102s, Visualizzato 8/03/17 Youtube U.S.A Department of State.

Ringraziamenti

Alla fine di questi tre anni mi sembra doveroso ringraziare chi mi ha supportato in questo percorso. Innanzitutto come promesso il primo “grazie” va a Roberto che ha creduto in tutto questo prima di me. Poi ovviamente secondi, ma non per importanza, i miei genitori che lo hanno materialmente reso possibile e senza i quali non sarei la persona che sono oggi. Grazie mamma, in particolare, per il tuo supporto in ogni momento della mia vita da che io ricordi; grazie papà per avermi insegnato quanto può fare la forza di volontà. Un ringraziamento a Gabriele per le sue consulenze tecniche e per il suo sostegno durante quest’ultimo anno davvero difficile. Infine un grazie a William, lui saprà il perché, lo sa sempre.