Scienza e Pace, Vol. 4, N° 3 (2013)

Quale libertà nel tempo del controllo globale delle informazioni?

di ***Federico Quadrelli***

Alcune riflessioni sul "caso Snowden"

1. La guerra non dichiarata alla libertà in nome della sicurezza

Libertà, democrazia, sicurezza, *privacy*. Sono alcune tra le parole più controverse, ma anche più dense di significato, che vengono utilizzate nelle scienze sociali e nel discorso pubblico, mediatico e politico, contemporaneo. Da secoli sulla definizione e la messa in pratica dei concetti di "*libertà*" e "*democrazia*" si sono impegnati, con posizioni e risultati diversi, intellettuali e militanti. Per difendere libertà e democrazia si sono combattute guerre di resistenza, per preservarle e realizzarle si sono scritte le costituzioni moderne. Oggi, la tranquillità dei Paesi occidentali ha reso la maggioranza dei cittadini poco sensibili, e forse inconsapevoli, rispetto al fatto che i pericoli per la democrazia e la libertà non sono affatto svaniti, malgrado l'assenza di una guerra guerreggiata sul territorio europeo, fatta di carri armati e di bombardamenti aerei. Tali pericoli sono sempre presenti, ma agiscono in modo più subdolo perché sono pericoli "invisibili" che le autorità hanno interesse a coprire o minimizzare, per mantenere intatto il senso comune liberal-democratico e la fiducia nello Stato di diritto.

Nei paesi occidentali, la "guerra" alla libertà e alla democrazia si gioca ormai su altri piani, tra cui assume rilievo crescente la dimensione immateriale dell'esistenza, ossia il "virtuale" e il controllo delle informazioni personali. Da qui, nel corso degli ultimi vent'anni, l'emergere del dibattito sulla società sorvegliata (Lyon 2002), sulla "*privacy*" e sull'istituzione di apposite *autority* per la sua tutela. Da qui anche un continuo conflitto tra i principi di tutela dell'integrità e della dignità personali, garantiti dalle norme sulla *privacy*, e le richieste di deroga a tali principi e a tali norme in nome della "*sicurezza*". Tale conflitto è stato innescato e acuito, in particolare, dalle reazioni degli Stati Uniti e dei paesi alleati agli attacchi dell'11 settembre 2001. In nome della sicurezza e della "guerra globale al terrorismo" sono state adottate legislazioni come il Patriot Act, e si sono diffuse pratiche in materia di raccolta e analisi di dati personali che hanno sostanzialmente messo tra parentesi i principi di tutela e rispetto della vita privata delle persone, specie nel caso di informazioni sensibili. Questo lato immateriale della violazione dei diritti ha poi avuto il suo contraltare materiale nelle pratiche di reclusione a tempo indefinito dei sospettati in attesa di processo e di tortura dei prigionieri di guerra, in violazione delle convenzioni di Ginevra, pratiche di cui la prigione di Guantanamo ha rappresentato l'esempio più noto ma non l'unico. A giustificazione di queste deroghe sistematiche ai principi del diritto è stata

costantemente invocata la "sicurezza nazionale", come una sorta di diritto assoluto e superiore rispetto alla dignità della persona e della sua integrità, sia fisica che virtuale.

È in questo scenario che conviene inquadrare il "caso Snowden" e quanto ne è seguito, compreso il recente datagate rivelato dal *Guardian* e da *Le Monde*, secondo cui almeno 35 capi di stato e di governo mondiali sono stati in questi ultimi anni spiati *dalla National Security Agency* (NSA) statunitense.

2. Il caso Snowden

Edward Snowden, classe 1983, è un esperto di sicurezza informatica che ha lavorato prima per la CIA, poi per la NSA ed infine per una società privata denominata Booz Allen Hamilton, un appaltatore del governo statunitense.

Attraverso la collaborazione con Glenn Greenwald, giornalista del *Guardian* che ha pubblicato una serie di denunce sulla base di sue rivelazioni avvenute nel giugno 2013, Snowden ha rivelato diverse informazioni su numerosi programmi di intelligence secretati, tra cui il programma di intercettazione telefonica tra Stati Uniti ed Unione europea riguardante i metadati delle comunicazioni, il PRISM, Tempora e programmi di sorveglianza Internet. Snowden ha affermato che le rivelazioni costituiscono uno sforzo "per informare il pubblico su ciò che viene fatto in loro nome e quello che è fatto contro di loro". Come ha dichiarato egli stesso in un'intervista concessa al *South China Morning Post*, Snowden ha cercato lavoro presso la Booz con il preciso intento di procurarsi materiale sulla NSA e dunque su dati "riservati" del suo paese, così da renderli pubblici. Si tratta di un progetto sicuramente molto bene architettato, l'esito di una pianificazione che, come spiegato bene da Manjoo (2013), deve far riflettere.

L'attività di *hacking* di Snowden ha messo in evidenza una falla nel sistema di sicurezza della NSA, che è stata "ingannata" da un suo dipendente. Manjoo si chiede quanti altri *hacker* meno integerrimi di Snowden (assumendo che abbia agito per un principio etico, come da lui affermato) possono esserci nella NSA e soprattutto quante informazioni personali possono essere già state "rubate" per scopi meno nobili del far sapere al mondo che siamo tutti sotto il grande orecchio e la lente di ingrandimento degli statunitensi.

Come accade in queste vicende c'è sempre chi si schiera a favore e chi contro. Ci sono quelli che osannano Snowden come un "eroe" (Guetta 2013), mentre altri lo definiscono un "traditore". Al di là della vicenda personale e dei risvolti penali delle azioni di Snowden, occorre riflettere attentamente su alcune questioni sollevate dal caso. In primo luogo occorre riflettere sulle finalità del programma di "*micro-macro spionaggio*" del governo degli Stati Uniti denominato PRISM; in secondo luogo, è necessario indagare quella che io definisco "*la premessa sociale*" che ha prodotto le circostanze su cui è nato il caso Snowden, ossia la diffusione di internet quale nuovo spazio della vita sociale e politica delle persone. Questo doppio piano consente di mettere in luce le illusioni di libertà che un pensiero acriticamente "internet-centrico" (Merozov 2012) ha generato nel corso degli ultimi quindici anni.

3. Il programma PRISM

Almeno dal 2007 la NSA raccoglie informazioni attraverso un "programma di sorveglianza" denominato PRISM. Edward Snowden ha deliberatamente sottratto all'agenzia per cui lavorava dei documenti "top secret", che ha poi diffuso per mezzo della stampa, allo scopo di far sapere al mondo che gli Stati Uniti stanno violando la privacy globale dei cittadini. Dai documenti rivelati si evince che PRISM è abilitato alla sorveglianza in profondità delle comunicazioni e del traffico internet mondiale. Le informazioni che PRISM può raccogliere passano attraverso ogni attività virtuale conosciuta: email, chat, chat vocali, videochat, video e foto pubblicate online, conversazioni VoiP (ossia una conversazione telefonica realizzata attraverso internet), trasferimento e condivisione di file, e notifiche d'accesso sui social network.

PRISM è dunque un programma di spionaggio diffuso e approfondito di ogni *attività umana mediata dalla tecnologia*, ossia la quasi globalità delle attività quotidiane dei cittadini statunitensi e di una parte crescente della popolazione mondiale. Il suo potere e i suoi effetti di controllo sono sconcertanti e impressionanti, sia per l'estensione della violazione del diritto alla privacy, sia per il superamento dei concetti stessi di "controllo" e "sorveglianza", per come li avevamo intesi sino ad oggi e per come erano stati limitati e regolamentati nella cornice dello Stato di diritto.

Le domande che, a questo punto, sorgono con maggiore insistenza sono: come ha potuto PRISM raccogliere questa immensa mole di informazioni? E ancora: come ha potuto raccogliere dati personali "protetti" (dai provider e dalle leggi) di milioni di utenti senza mai essere "scoperto"?

Una parte delle informazioni è stata recuperata sfruttando il "routing", ossia il percorso virtuale che un utente effettua quando si collega ad alcuni siti. La maggior parte dei percorsi passa per gli Stati Uniti o per ISP (*internet service provider*) statunitensi, e questo ha consentito a PRISM di recuperare molte informazioni senza dover violare nessuna legge/regola formale.

L'altro aspetto controverso della vicenda è quello che vuole la "collaborazione" da parte dei principali service provider del globo, cioè Google, Facebook, Microsoft, Skype, Apple, Youtube, ecc. Immediata, dopo le rivelazioni di Snowden, la risposta di questi provider, che hanno ammesso le richieste ufficiali da parte del Governo, ma nessuna diffusione d'informazioni private dei propri utenti. In particolare i vertici di Google e Facebook sono intervenuti tempestivamente per rassicurare i propri utenti e prendere le distanze da questo progetto di spionaggio.

A questo punto della storia emergono almeno due elementi, utili per mettere a fuoco le ambivalenze delle nozioni di democrazia e libertà oggi accettate dal senso comune: un programma super-tecnologico di spionaggio globale messo in piedi da un governo *democratico*, ovvero gli Stati Uniti, e la collaborazione, almeno richiesta e sollecitata dal governo statunitense, allo scambio di informazioni private da parte dei principali provider

internet, la cui filosofia aziendale è da sempre ispirata alla promozione delle *libertà* fondamentali (di informazione, di comunicazione, di opinione, ecc.).

4. Privacy e controllo, i paradossi di Internet

Commentando un'inchiesta del *Wall Street Journal*, Alberto Flores D'Arcais (2012) ha scritto di come le nostre vite siano divenute oggetto di commercializzazione da parte dei provider internet più noti. Scaricando alcune applicazione dai social network, infatti, l'inchiesta del WSJ ha rilevato che "tra i dati personali richiesti ci sono non solo l'indirizzo email o la località, ma anche gli orientamenti sessuali, politici e religiosi. E non solo degli utenti che scaricano l'applicazione, ma anche dei loro "amici" di Facebook. Tra i casi citati ci sono celebri società come Yahoo e Skype e altre meno conosciute, tutte con un obiettivo comune: saperne di più della nostra vita e dei nostri interessi".

Il concetto di privacy viene messo in discussione già dall'uso che questi provider fanno dei nostri dati personali. Polemicamente, vorrei far notare che lo scandalo generato dalla vicenda Snowden non si è ripetuto quando è stato reso noto che questi provider commercializzavano le nostre informazioni per scopi di marketing. Le ragioni del profitto, come e più di quelle relative alla sicurezza, sembrano prevalere sul rispetto dei diritti fondamentali legati alla riservatezza e all'identità personali.

L'intreccio tra rete e profitto si è spinto negli anni ben oltre quanto qui accennato. Oltre ai casi di commercializzazione di alcune informazioni private, ma anonime, ossia senza citare nome e cognome dell'utente, ci sono casi di vere e proprie violazioni dei diritti. Come ha scritto Rodotà: "Si sono, infatti, moltiplicate negli ultimi anni le violazioni dei diritti su internet. Il caso più clamoroso è quello delle grandi società di Internet – Google, Microsoft, Yahoo – che accettano richieste censorie da parte di Stati autoritari, giustificandosi con il fatto che, altrimenti, si vedrebbero precluso l'accesso ai mercati che, come quello cinese, sono economicamente importantissimi" (Rodotà 2009, 7).

La rete, dunque, è tutt'altro che un paradiso terrestre di libertà e democrazia. Internet, essendo spazio non geograficamente limitato, e non disponendo né di ingresso né di uscita fisicamente delimitati, ha generato l'illusione collettiva secondo cui lo spazio virtuale in cui ci muoviamo è "senza controllo" e "senza gestori". Errore fatale, dato che internet ha un creatore e soprattutto numerosi gestori. In taluni casi, i governi possono essere sia proprietari che gestori degli accessi, come nel caso della Cina (eigenLab, 2012).

La collaborazione tra provider e governi (autoritari e democratici) emersa dopo la vicenda Snowden conferma quanto era già noto, amplificandone semmai la portata negativa. Mentre prima erano note le pressioni da parte di governi autoritari, ad esempio per far cadere l'anonimato su giornalisti che diffondono notizie critiche o chiedere la rimozione di video sgraditi (Rodotà 2009, 8), ora lo sono anche le pressioni dei governi democratici.

Il governo degli Stati Uniti si è giustificato spiegando che le informazioni raccolte sono "solo" dei "metadati" e che il diritto alla privacy e alla libertà di espressioni non sono in pericolo. Ma è davvero così?

Ha scritto a rigiardo Jaron Lanier (2013) che "*metadata system are said to gather only tags and skeletal informations, but not "content" is the aspect of data that programs can most reliably understand. It's the topical stuff. The distinction is instrumental rather than substantial (…) Metadata is the aspect of data that programs can most reliably understand. It's the topical stuff that is regimented into a standard structure, like the blanks filled in on a form. In order to treat real-world events as metadata, certain actions of people, rather that their expression, are used to fill in those blanks. For instance, programs cannot understand the meaning of ordinary conversation, but a program can log when a call is made, and to whom*".

In sintesi: la linea che separa un'informazione da una meta-informazione è assai labile, e questo confine si sposta facilmente da una parte all'altra in base a ciò che si sta cercando. Dopotutto, si è già detto, la collezione di dati personali diretta o indiretta, è pratica nota e diffusa, con grande risultato economico, specie per le imprese internet.

Il governo statunitense ha in generale uno scopo differente da quello delle imprese: ossia non c'è un diretto interesse economico, bensì un interesse di "sorveglianza". Per quanto tra le informazioni "sottratte" possano ben essercene alcune relative a segreti industriali. Il problema è che, dopo l'11 settembre, l'allarme sicurezza costruito abilmente dai governi contro la minaccia del terrorismo globale ha allentato le resistenze alle violazioni dei diritti e delle libertà personali. In un recente sondaggio il PewResearch Center ha evidenziato come il 62% degli americani reputi corretto, da parte del governo, dare una priorità alla sicurezza del paese piuttosto che al rispetto della privacy. Solo il 32% si è detto di opinione opposta.

Questa idea è stata ribadita anche dal "padre" di internet, Vincent Cerf, in una recente intervista a *la Repubblica*. Alla domanda dell'intervistatore, su come si sentisse davanti ad uno scandalo come il datagate, che usa proprio la rete per spiare i cittadini, Cerft ha risposto: "credo che dobbiamo riflettere su un punto e tornare a quello che accadde l'11 settembre. Uno Stato in cui la privacy è totalmente rispettata è uno Stato insicuro. Uno Stato in cui al contrario chi governa sa tutto dei propri cittadini è il massimo della sicurezza. Ma non credo che nessuno voglia vivere in questi due estremi. *Dobbiamo trovare un equilibrio fra privacy e sicurezza*".

Si tratterebbe dunque di individuare i "confini" della sicurezza o, meglio, i confini delle azioni che un governo è legittimato a intraprendere per difenderla. In che misura uno Stato che si proclama democratico (il problema si pone in modo diverso, evidentemente, per i governi autoritari), può spingersi nel violare la privacy e le libertà dei suoi cittadini? In che misura è consentito e tollerabile un controllo così massiccio delle informazioni scambiate tra privati e liberi cittadini? Da come si risponde a queste domande, deriva una diversa configurazione di internet come spazio di libertà e democrazia.

Mettendo tra parentesi le questioni normative, è un fatto che negli ultimi dieci-dodici anni la privacy come diritto ha ceduto il passo alla sicurezza e al controllo. Alla luce di questo processo, come hanno scritto Alberto Flores D'Arcais e Jaron Lanier in due ben distinti articoli, potrebbe emergere in un prossimo futuro una nuova idea di privacy, basata "sulla "libertà dall'essere identificati/profilati" in maniera sistematica.

Alla luce del caso Snowden, la distinzione tra "tecnologie della libertà" e "tecnologie del controllo" è in pratica meno netta che in teoria. Occorre dunque riaprire la questione della regolamentazione di internet, affrontata periodicamente ma troppo superficialmente nel dibattito politico italiano. In uno Stato democratico di diritto il rispetto della dignità della persona, del suo corpo fisico come del suo "corpo elettronico", dei suoi diritti e delle sue libertà fondamentali, costituiscono principi guida derogabili solo in casi eccezionali, per periodi limitati di tempo, rispetto a circostanze appurate e circoscritte, e comunque sotto il controllo della magistratura e di altri enti autonomi di garanzia. Come afferma Rodotà, "nel momento in cui la tecnologia viene sempre più massicciamente impiegata per la creazione di una società della sorveglianza, della classificazione e del controllo, bisogna in ogni momento definire le condizioni necessarie per evitare che la tecno-politica si risolva nel controllo autoritario, nella discriminazione, in vecchie e nuove stratificazioni sociali produttive di esclusione, nel dominio pieno di una logica di mercato che cerca un'ulteriore legittimazione proprio nella tecnologia" (Rodotà 2009, 7).

A fronte dei numerosi e sistematici casi di di violazione dei diritti dei cittadini, anche nello spazio virtuale, da parte di attori privati e pubblici, a fini di profitto o di "sicurezza", si rende sempre più necessario un "*bill of rights*" per il governo e l'uso di internet. Una carta che sancisca a livello globale e nazionale, diritti, doveri e soprattutto limiti rigorosi e inequivocabili, sia per gli Stati che per i provider. L'obiettivo è quello di mantenere fermo il "quadro della democrazia e dei diritti di libertà" in un contesto sociale in continuo mutamento, proprio a causa (o per merito) di un progresso tecnologico potente e sempre in espansione.

Conclusioni

Il caso Snowden ha il fascino tipico di un romanzo fantascientifico. Si potrebbero fare congetture di ogni genere: credere che Snowden abbia operato al soldo della Cina per danneggiare l'occidente; oppure pensare che sono gli USA ad aver manovrato Snowden per poter generare nelle persone un maggior senso di insicurezza e per creare, in modo paradossale, una maggiore richiesta di controllo proprio da parte dei cittadini. Dopo tutto il 62% dei cittadini statunitensi reputa prioritaria la sicurezza e non la privacy.

Come i romanzi fantascientifici, però, il caso Snowden ci costringe a riflettere su aspetti fondamentali del modo di organizzarci politicamente che chiamiamo "democrazia". Anche perché non di *fiction* si tratta, ma di realtà.

Quello che i fatti ci hanno indicato è che il controllo globale sulle nostre vite è già stato realizzato. La premessa sociale è stata data dal fatto che miliardi di persone utilizzano

internet come nuovo spazio del vivere sociale, condividendo spontaneamente ogni aspetto della propria vita. Da questo punto di vista è difficile non essere d'accordo col sociologo e politologo Evegeny Morozov: l'internet-centrismo ha generato una illusione e il "soluzionismo tecnologico" che è disceso da questa idea "salvifica" e acritica di internet ha prodotto effetti negativi non trascurabili nelle nostre vite e nelle nostre società.

Ora che sappiamo di essere controllati in (quasi) ogni aspetto della nostra vita, anche e soprattutto in rete, attraverso i nostri post sui social networks, le nostre condivisioni di contenuti, attraverso l'uso di applicazioni e giochi virtuali, attraverso i tweet e i re-tweet, cosa possiamo fare? Praticamente poco o niente, se non utilizzare gli strumenti tecnologici con responsabilità e senso critico, e promuovere una regolamentazione che metta al centro la tutela dei soggetti più deboli, ossia gli utenti privati, contro il potere dei soggetti più forti, ossia le imprese internet e gli Stati. Lo strumento della rete, di per sé, non è né buono né cattivo, ma è appunto l'uso che se ne fa a qualificarlo di volta in volta in un modo o nell'altro (Quadrelli 2013).

Il dibattito continua, e continua il conflitto sul governo della rete. In ultima analisi, la vicenda Snowden non è affatto la conclusione di un processo, bensì l'inizio di una fase di "modernizzazione riflessiva" (Beck *et al*. 1999) in cui, consapevoli dei limiti del *web* e della notevole fragilità delle istituzioni liberal-democratiche, continuiamo a sperimentare forme di libertà e soprattutto di democrazia in e *attraverso* la rete.

Riferimenti bibliografici

Beck, U., Giddens, A. e Lash, S., *Modernizzazione riflessiva. Politica, tradizione ed estetica nell'ordine sociale della modernità*, Asterios, Trieste, 1999.

Flores D'Arcais, A., "Ecco come Facebook ci vende alle aziende", *la Repubblica*, 8 aprile 2012.

Lanier, L., "The meta Question", *The Nation*, 17 giugno 2013.

Lyon, D., *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002.

Manjoo F., "Il sistema è fragile", *Internazionale.it*, 28 giugno 2013.

Morozov E., *L'ingenuità della rete*, Codice Edizioni, Torino, 2012.

Quadrelli, F., "La democrazia in rete e le nuove forme della partecipazione", *Scienza&Pace*, IV, 1, 2013.

Rodotà, S., "Tecnopolitica", in *Enciclopedia Treccani*, versione online, 2009.