CRIMINALIZZARE LA CRITTOGRAFIA

L'INGRESSO DELLO STATO NELLE SPAZIALITÀ CIFRATE

Paolo Andreozzi

Sommario

L'insieme delle dinamiche politiche successive all'attacco del 7 gennaio 2015 presso la sede del settimanale *Charlie Hebdo* di Parigi ha ricordato, per certi aspetti, il periodo del dopo 11 settembre americano. In particolare è emersa, nell'ambito della guerra dell'occidente al terrore, l'ipotesi di rendere illegali alcune tecniche crittografiche che ostacolino l'attività di controllo da parte delle autorità governative dei dati scambiati dagli utenti in rete. Questo lavoro prende in considerazione un fatto sociale, sintetizzato nell'espressione «criminalizzazione della crittografia», con degli strumenti sociologici. In proposito sono stati distinti due piani principali: quello individuale e quello statale. Per quanto riguarda il piano individuale, è stata affrontata una ricostruzione concettuale del termine di riservatezza, a partire dai concetti sviluppati in ambito etnometodologico di territorialità e informazione per comprendere successivamente quale sia il ruolo giocato dall'insieme di tecniche crittografiche nel garantirla; si delinea così l'idea di spazialità cifrate come risultato dell'impiego di tecniche crittografiche con lo scopo di proteggere la propria riservatezza. A livello statale, si affronta, con gli strumenti concettuali della sociologia politica e della devianza, la dinamica di criminalizzazione, privilegiando in particolare un'ontologia dello Stato di matrice bourdieusiana. Si arriva infine a rilevare come i due piani siano strettamente connessi da una cinghia di trasmissione logica: l'argomento *if you've got nothing to hide, you've got nothing to fear* si presenta come l'elemento fondamentale di comprensione della dinamica di criminalizzazione della crittografia. Il lavoro rivela dunque la possibilità di portare il dibattito in corso, sul controllo e la sorveglianza, dal campo giuridico della privacy, verso dimensione puramente sociologica, aprendo dunque alla possibilità di uscire dalla dinamica del bilanciamento fra diritti, quale unico mezzo per la risoluzione del conflitto.

Indice

Introduzione

Appena una settimana dopo gli attacchi di Parigi del gennaio 2015, il Primo Ministro del Regno Unito David Cameron incontra a Washington il Presidente statunitense Barack Obama per discutere delle possibilità di ottenere, da parte delle autorità governative, i dati degli utenti della rete internet intercettabili attraverso i loro *Internet Service Provider*[1]; in particolare, sulla questione dell'accesso ai contenuti cifrati scambiati in rete, emerge la possibilità di rendere illegali alcune tecniche crittografiche in grado di impedire questa attività di controllo[2]. La criminalizzazione della crittografia, ossia la proibizione delle tecniche crittografiche che impediscano *de facto* l'accesso delle autorità governative ai messaggi e alle informazioni scambiate, ha delle radici profonde nella storia degli ultimi cinquant'anni e trova il suo più significativo antenato nel *Foreign Intelligence Surveillance Act* statunitense del 1978. Questa nuova ondata di dichiarazioni politiche ha così riaperto un intenso dibattito sul rapporto tra *privacy* e sorveglianza; tuttavia è possibile notare come gli ultimi anni abbiano visto, nel campo giuridico in cui tale dibattito si svolge, una netta retrocessione dei partigiani della *privacy*, i quali si trovano in una condizione di difficoltà sempre maggiore nel fronteggiare la questione del *bilanciamento* tra diritti in conflitto e l'argomento «*if you've got nothing to hide, you've got nothing to fear*». Questo lavoro si pone dunque l'obiettivo di sottoporre la questione della criminalizzazione della crittografia ad uno studio sociologico, in particolare attraverso la ricostruzione di un insieme di concetti autonomi dal campo del diritto. Questo permetterebbe la riapertura di un nuovo dibattito nel seno delle scienze sociali, con la possibilità di guardare dall'esterno lo stesso sillogismo sotteso dall'argomento *nothing to hide*, mettendone in evidenza le logiche stesse che lo sorreggono.

È apparso opportuno distinguere due piani principali di analisi: quello individuale e quello statale. Per quanto riguarda l'individuo, l'idea chiave da ricostruire è quella di *privacy*: pochissimi risultano i tentativi in ambito sociologico di definizione di questo concetto, probabilmente a causa di un monopolio decennale della questione da parte del mondo accademico civilistico; si procede così ad una costruzione di quegli attrezzi concettuali necessari per la definizione di una nozione di *riservatezza*, a partire dai concetti di spazialità e informazione sviluppati a partire dagli anni cinquanta in ambito etnometodologico. Successivamente, ci si preoccupa di selezionare le specifiche tecniche crittografiche che siano oggetto di tale attività di criminalizzazione e di comprendere quale sia il loro ruolo rispetto al

[1] Zezima e Jaffe 2015.
[2] Price 2015.

concetto di riservatezza definito. Relativamente al livello statale si è proceduto ad una specifica ontologia dello stato e del sociale, con riferimento esplicito al lavoro di Pierre Bourdieu: si individua così uno spazio sociale abitato da logiche morbide che, in particolare nei periodi di forte scuotimento emotivo che caratterizzano gli anni della guerra dell'occidente al terrore, si riadattano e si trasformano, arrivando a consolidarsi in specifiche possibilità concettuali di ragionamento. La criminalizzazione della crittografia diventa così un processo bilaterale, il luogo dinamico di incontro tra l'individuo e lo stato in uno stesso spazio sociale, dove cinghia di trasmissione concettuale è l'argomento *nothing to hide*. Infine, un'appendice sul ruolo giocato dalle grandi aziende dei servizi *internet*, come Google, Facebook o Yahoo, è l'occasione per imbracciare l'insieme di concetti elaborati nel corso del lavoro, avvicinandosi così alle questioni ancora aperte sui rapporti tra colossi privati, *privacy* e sorveglianza.

Il lavoro tenta così di dimostrare la possibilità di discutere del rapporto tra *privacy* e sorveglianza anche al di fuori del dibattito giuridico, data la connessione tra un concetto di *riservatezza* di derivazione antropologica e la dinamica stessa di criminalizzazione; il passaggio porta con sé degli aspetti importanti, proprio in quanto struttura un campo del dibattito che non guarda più alla riservatezza come a un diritto da «bilanciare», ma come un aspetto profondamente antropologico riconnesso a dinamiche molto più evidenti e quotidiane di ritiro, mantenimento del segreto e interazione tra gli individui diffusamente adottate e presumibilmente condivise.

L'unico e la sua spazialità

Centro di gravità analitica sul ruolo della crittografia nell'individuo è il concetto di *riservatezza*. Le fondamenta teoriche che questa sezione cerca di edificare affondano le radici nella sola idea di un legame ferreo tra utilizzo di tecnologie crittografiche da parte dell'individuo e una sua «pretesa» di riservatezza. Malgrado la copiosa letteratura scientifica in campo giuridico, quell'idea che è stata ivi codificata come *privacy* trova ancora poco spazio teorico[3] nelle altre scienze sociali[4]. Pertanto si impone qui uno sforzo di costruzione concettuale relativamente al termine scelto di «riservatezza», perché rimanga ben distinto dall'associato concetto giuridico di *privacy*[5]. Si accetta qui l'idea che il terreno iniziale sia quasi più psicologico che sociale, dal momento che «riservatezza» attiene primariamente a un insieme di fattori culturali e storici relativi alla maniera in cui l'individuo struttura il mondo e vi si colloca[6]. Tuttavia, una volta completata la cassetta degli attrezzi concettuali relativi alla «riservatezza» si accede alla necessità di sciogliere il nodo del ruolo della crittografia per l'individuo: qual è il potenziale offerto dalla tecnologia nella preservazione delle varie spazialità? Solo successivamente è possibile procedere ad affrontare il primo sillogismo «complesso» preso in esame in questo lavoro: la formula eminentemente sociale del «non ho nulla da nascondere».

Costruzione di un concetto

Come punto di partenza intuitivo per il non-ancora-concetto «riservatezza» prendiamo una semplice nozione *geografico-spaziale*. L'idea è quella di tracciare, attraverso l'assunto geografico, un'area confinata attorno all'individuo in cui gli oggetti sociali presi in esame si muovono, mutano e interagiscono. Punto di riferimento in letteratura è l'ambito etnometodologico. Nel 1967 lo studioso americano Harold Garfinkel pubblica i suoi *studies in ethnomethodology*, nei quali descrive alcuni

[3]Vedi *e.g.* Sassen 2002, *passim* e Callero 2003, p. 126

[4]Ciò viene notato anche da Alan Bates, il quale si interroga circa l'utilità del concetto di *privacy* in campo sociologico e psicologico, dove è stato studiato particolarmente poco(Bates 1964, p. 423). Queste considerazioni, che non trovano difficile collocazione nello stato dell'arte degli anni '60, sono probabilmente valide ancora oggi.

[5]Pur non esistendo un modello di legislazione sulla privacy globalmente accettato, è possibile individuare nella formulazione presente all'articolo 12 della Dichiarazione Universale dei Diritti Umani del 1948 la struttura essenziale del diritto alla *privacy*:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

[6]Bates 1964, p. 429.

«breaching experiments»[7]: si tratta di esperimenti che ruotano attorno all'idea di rottura delle attese e della spazialità dell'individuo, intesa come sfondamento di quel senso comune che abita esteticamente il sociale; è questa una concezione di stabilità rispetto a un'attitudine che Simmel vedeva come più *reattiva*[8] che attiva.

Quest'idea di *spazialità* dell'individuo, accolta con un approccio «prossemico» in ambito antropologico[9], è scandagliata da Erving Goffman attraverso una progressione concettuale per gradi di astrazione che parte da quelli che chiama «territori del sé» per arrivare a definire territorialità *non strettamente* spaziali, ossia non **fisicamente** delimitate; alla base del concetto di spazialità si trova l'individuo, concepito al tempo stesso come «unità veicolare» nello spazio e «unità partecipativa» delle relazioni sociali. A tale idea di spazialità si tenta di associare altri potenti concetti, quelli di *informazione* ed *entropia*, presi in esame in ambito sociologico soprattutto tra gli anni '40 e '50 a partire dalle loro definizioni fisiche e ingegneristiche.

Spazialità del sé

In *Relations in Public* Goffman sviluppa un concetto di *territorialità* articolato nei vari *territories of the self* secondo linee che l'autore considera «non spaziali», ossia non più ancorate al fisico. L'operazione intrapresa dal sociologo americano consiste nel risalire per gradi di astrazione concettuale dal territorio in senso stretto fino all'area di «preservazione» riguardante, in senso ampio, *informazioni*. Di nostro interesse è un concetto di «spazialità» del tutto aderente a quello di «territory» formulato da Goffman, mentre qui per territorio intendiamo ciò che egli considera «spaziale», ossia ciò che è fisico, tangibile, concreto nel senso comune del termine: la traduzione in questo caso è semplicemente terminologica; per non creare confusione lasceremo pertanto il termine *territory*, nel senso dato dal sociologo americano, non tradotto. Goffman arriva a includere tra i «territories of the self» un'*informational* e una *conversational preserve*, definite come

> l'insieme dei *fatti concernenti se stessi* sui quali l'individuo si aspetta di **controllare** l'accesso quando in presenza di altri[10]

e

[7] Garfinkel 1967, pp. 35 e ss.

[8] Davis 1973, p. 323.

[9] *Cfr.* su questo Hall et al. 1968. Lasciando da parte gli interessanti tentativi di quantificazione(Sheppard 1996) delle varie organizzazioni del «microspazio» affrontate in ambito *prossemico*, tale approccio si rivela esplosivo nell'analisi sul controllo e sugli effetti più politici della gestione dello spazio.

[10] Goffman 1971, p. 39.

> il diritto di un individuo a esercitare qualche **controllo** su chi può chiamarlo in una conversazione e su quando egli possa essere chiamato; e allo stesso tempo il diritto di un insieme di individui già impegnati in una conversazione a proteggere il loro intorno dall'ingresso o dall'ascolto di nascosto da parte di altri[11].

Elemento base centrale in entrambe le definizioni è quello del **controllo**. È anche importante notare che il termine *right*, diritto, impiegato in queste definizioni ha il significato di *claim*[12], **pretesa**, qualcosa di preliminare rispetto al concetto di «diritto»: non implica alcun presupposto statale, né giusnaturalistico. Spazialità è dunque un concetto che presuppone la possibilità di indicare degli spazi, siano essi fisici o virtuali, di pensare in termini geografici il sociale, ciò che permetta poi di definire un'attività di controllo su qualcosa che lo attraversi. L'approccio spaziale dà la possibilità di ragionare per «regioni», aree, porzioni **delimitate**, confinate, di spazio; un'idea compresa nelle parole spazialità (al plurale), spazi[13] e territori, che guardano allo spazio sociale come intimamente, continuativamente, dinamicamente regionalizzato. Spazio sociale è luogo di possibilità e individuazione di tutti gli oggetti che assumiamo siano sociali sempre e solo in quanto interazione di (almeno) due individui, aderendo ad un'idea di interazione sociale fondamentale inclusa nel concetto di «sociazione» in Simmel[14]. Tale interazione è all'origine di una *dinamica*, ossia di una *dynamis* che modifica lo stato di un sistema, in questo caso specifico, sociale, in quanto non può fare altro che mobilitare concetti sociali, dunque modificare (o confermare) il suo stato. La banale conclusione è che ogni individuo, nella misura in cui *inter*-agisce, ha una certa «possibilità» o «capacità» di azione sociale, in termini di possibilità di agire o non agire, chiaramente nel rifiuto di ogni presupposto deterministico.

Spazio sociale è dunque l'*intra* che risiede tra gli individui, che però, suggerisce Goffman, può essere tale anche se svincolato dalla sua prepotente accezione fisica. Osservare il sociale in termini di spazialità significa cercare di costruire in termini spaziali i concetti sociali; il geografico è qui una determinazione specifica, fisica, dello spaziale. Agendo, il «self» si estende necessariamente su di un'area che può essere incidentalmente fisica ovvero anche solamente concettuale, ma che è sempre almeno in potenza individuabile; questa semplice considerazione è alla base delle

[11] Ibid., p. 40.
[12] Ibid., p. 28.
[13] Nel mettere in parallelo i lavori di Erving Goffman e Michel Foucault, Robert Leib opta per l'espressione «spaces of the self», anziché «territories»(Leib 2013).
[14] Simmel 1906a, p. 40 e seguenti.

idee di invasività, sconfinamento, rispetto e «inappropriatezza situazionale»[15] che popolano intere famiglie di quesiti psichiatrici e antropologici. Non appare tuttavia corretto considerare questa linea di ragionamento come un'adesione all'idea di «cyberspazio» che ha invaso i dibattiti sulla rete dei giuristi di tutto il mondo. Se da una parte l'idea spaziale qui introdotta riguarda prevalentemente un problema epistemologico e non una codificazione giuridica, dall'altra essa non ha nemmeno vocazione a trattare dello «spazio virtuale» della rete, essa non delinea alcuno spazio cartesiano[16] e, pur trattando senza dubbio di una «esperienza di spazialità mediata cognitivamente»[17], si pone al di là di tutto un insieme di problematiche riguardanti le intersezioni geografiche del «cyberspazio».

Informazione ed entropia

Il «self» di Goffman è una costruzione *intersoggettiva* dell'interazione sociale, che discende dall'idea di persona-maschera diffusamente adottata in ambito etnografico[18]; le aree, i territori, riguardano il «self». Individuo è invece la consapevolezza stessa dei vari «sé», che si incarica di «gestirli» e organizzarli: in tal senso è *autodeterminazione*. La costruzione concettuale precedente trova una conferma nella capacità di lettura dei termini «attacco», «invasione», «sconfinamento» e «marcatori territoriali»[19] anche quando applicati a spazialità sempre meno fisiche: il controllo dell'informazione *disseminata* o *disincarnata*[20] volontariamente. Il concetto di *informational preserve* include infatti quello di informazione, intesa come «facts about the self»[21]. Nella prospettiva «spaziale» le informazioni si muovono in uno spazio inteso come luogo delimitato, come potrebbe essere un cassetto di effetti personali. Come già visto, l'elemento strettamente fisico non è necessario e anzi, superarlo è un passaggio fondamentale nella descrizione del sociale qui affrontata.

[15] È Goffman stesso a considerare come punto di partenza questa espressione, comune presso gli psichiatri per descrivere una famiglia di comportamenti osservati in alcuni pazienti. Il metro di paragone per quanto riguarda tale «inappropriatezza» è evidentemente lo psichiatra stesso, che formula un giudizio di *gusto* sulla condotta del paziente. L'insieme di studi psichiatrici sull'inappropriatezza esplora e indaga *chi* attacca, invade, perfora le regole e le norme situazionali, senza tuttavia concentrare l'attenzione su queste ultime(Goffman 1966, pp. 3, 232).

[16] Non si tratta infatti di uno spazio identificato da assi orientati. In tal senso non può in nulla essere affiancato alla «spazialità [concettuale] del sé» definita da *Charles Taylor*, spazio di definizione morale e identitaria del sé. Il concetto fisico che più vi si avvicina è probabilmente quello di *campo*, definito in funzione dello spazio, dunque delle distanze, tra gli oggetti sociali e il sé.

[17] Cohen 2007, p. 210.

[18] Vedi *e.g.* Singer 1980, *passim* e Attewell 1974, *passim*.

[19] Goffman 1971, pp. 44 e ss.

[20] Goffman 1966, pp. 14 e ss.

[21] vedi *supra*, definizione citata.

Oltre al «coinvolgimento situazionale» e alle «barriere di coinvolgimento»[22], Goffman introduce i concetti di informazione «incarnata» o «disincarnata»[23], come preliminari alla lettura del suo lavoro. L'individuo è *vehicular unit*, unità veicolare di informazioni, che possono essere **incarnate** nell'essere, nell'apparire, nel movimento stesso del soggetto, dunque disseminate involontariamente o inevitabilmente, oppure disincarnate, volontariamente emesse e destinate ad altri. Appare adeguato riportarsi al tentativo di *teoria sociologica dell'informazione* formulato da *Harold Garfinkel* nel 1952: un manoscritto da giovane dottorato, un tentativo di scavare una nicchia fuori da un mondo, quello informatico, dominato da grandissimi nomi[24] e all'interno di un mondo accademico fortemente segnato dalla dicotomia tra strutturalisti e teorici del conflitto. Portare il concetto di «informazione» fuori dal campo delle scienze dure significava per Garfinkel gettarvi uno sguardo «husserliano», privarlo dell'ontologia[25] netta di cui era stato vestito nel territorio d'origine per infine accoglierlo, attraverso la porta *fenomenologica*, nel seno delle scienze sociali. In tutto ciò il tentativo di preservare la potenza del concetto di informazione, pur nella sua declinazione culturale, storica, situazionale. Tra le varie definizioni di *informazione*, variamente trasportabili in ambito sociale riportate da Garfinkel, scegliamo qui l'elegante formulazione di *Karl Deutsch*:

> l'ingegneria delle comunicazioni trasferisce informazione [...] [che è] relazione secondo pattern (*patterned*) tra eventi[26]

La brevità di questa definizione di origine quasi intuitiva è un ottimo punto di partenza. È necessario aggiungervi però qualcosa che adatti tale concetto di informazione ai presupposti antropologici assunti fino ad ora. Si tratta dunque di prendere in prestito un concetto ingegneristico, informatico, fisico per adattarlo all'idea che

> l'informazione è costituita - e non solo interpretata o rappresentata simbolicamente e scambiata - ma realmente costituita come tale dagli aspetti (cooperativamente ordinati) dell'ordine sociale situato nel quale essa si trova[27]

Senza dilungarci nell'analisi della costruzione concettuale affrontata da Garfinkel, si pone immediatamente il problema relativo all'*interesse* specifico posto da un

[22]Goffman 1966, pp. 35, 39.
[23]Ibid., p.14.
[24]Aho 2010, p. 118.
[25]Ibid., p.118.
[26]Garfinkel 2008, p. 107.
[27]Ibid., p. 13.

tale concetto di *informazione*. Questa parte lascia in sospeso la questione, che verrà però ripresa in entrambe le sezioni successive.

Si nota da una parte il pieno inserimento in una linea di studi etnografici che fanno del *self* l'oggetto di un sistema semiotico e al tempo stesso il soggetto[28] interagente[29] di tale sistema, e dall'altra il netto rifiuto dell'assunto teorico individualistico[30]. All'elemento oggettivo, esterno, fondamentalmente *cosale* dell'**informazione** è possibile dunque aggiungere anche un elemento situazionale, mutabile, culturalmente collocato[31]. Il concetto di informazione porta logicamente con sé quello di *entropia*, che possiamo indicativamente accogliere come *misura del grado di disordine di un sistema*: l'applicazione di tale idea a livello sociale è meno surreale di quanto non sembri a prima vista, e verrà affrontato in particolare nel capitolo «La Rincorsa ai Dati».

Riservatezza oltre il diritto

Se da una parte l'assunto geografico, da cui è discesa la possibilità di appropriarci di una nozione di spazialità o regionalità[32] da tracciare attorno al soggetto, permette di indossare un certo tipo di lenti per osservare la realtà sociale, dall'altra parte il concetto di informazione appena delineato completa la cassetta degli attrezzi concettuali necessari per scolpire finalmente una definizione *sociologica* di «riservatezza». Si può già provare a indossare questi occhiali concettuali per provare a distinguere alcune situazioni interessanti: cos'è, ad esempio, la visita di un sito *web*? Ci si potrebbe chiedere in che misura questa attività possa essere assimilata dal punto di vista concettuale a quella di recarsi in banca per effettuare alcune operazioni sul proprio conto corrente. In quest'ultimo, tradizionale, caso si può immaginare che il cliente che si dirige verso la banca accetti l'idea di *emettere* informazione **relativa** alla propria attività, come la direzione intrapresa o gli abiti indossati; una volta all'interno della banca però, si può prevedere che incrementerà il controllo sulle proprie informazioni cercando di individuare uno **spazio**, come potrebbe essere un ufficio, per conversare con l'agente della banca: in tal caso l'informazione non sarà solo emessa intenzionalmente[33], ma diretta a

[28] Singer 1980, p. 495.
[29] Vedi *supra* sulla «capacità» di agire dell'individuo.
[30] Aho 2010, p. 120.
[31] Cavanagh 2015.
[32] Goffman 1956, p. 66.
[33] Sebbene ci siano elementi di volontarietà/involontarietà legati al problema dell'informazione incarnata e disincarnata, sarebbe impreciso definire in termini di intenzionalità tale distinzione. Paradossalmente sembrerebbe più adeguato distinguere i due tipi di informazione non a partire dal soggetto che la emette, ma da chi la raccoglie: è egli impegnato in un'attività di mera «ricezione» oppure in un'analisi lirica e complessa del flusso di informazioni che sta ricevendo?

uno specifico interlocutore, l'agente, e **protetta**[34] da eventuali ascoltatori esterni. Analogamente, per quanto riguarda la visita del sito *web*, nulla vieta di distinguere, come nel caso della banca, il momento in cui ci si *reca* nel luogo e il momento in cui vi si compie qualcosa: che l'utente accetti l'idea di *disseminare* informazioni *relative al fatto che*[35] sta scambiando informazioni con un *web server*, ad esempio, non implica in alcuna maniera che egli non voglia escludere terzi dal **contenuto** di tale informazioni. È dunque sufficiente distinguere i vari tipi di informazione e le varie spazialità coinvolte per scomporre alcuni problemi complessi in parti semplici.

Nello spazio teorico di Georg Simmel è la **menzogna** a essere una «forma molto rude», talvolta non ancora cosciente[36], di emergenza di alcune necessità relazionali legate al problema della «conoscenza» dell'altro. È importante non lasciarsi confondere dal significato moralmente negativo del «mentire» nel valutare la sua «diretta *significatività* sociologica positiva»[37]: il mantenimento di un riserbo è significativo in quanto preservazione di informazione nell'ambito del conoscimento dell'altro. Il problema del «segreto», di ciò che viene *riservato*, risiede nella banale considerazione che, se a mentire è un'alterità che si trova lontana dal «centro della nostra personalità», allora è evidentemente facile aggiustare la nostra attitudine pratica rispetto a tale mancanza di integrità, mentre al contrario, se a mentire sono le poche persone del nostro ambiente più stretto, allora «la vita si fa intollerabile»[38]. E ancora Simmel ricorda in *Brücke und Tür*: «direttamente o simbolicamente, con il corpo o con la mente, continuiamo a separare i nostri

Cfr. sui concetti introduttivi di informazione Goffman 1966, pp. 14-17. Eloquente in tal senso è l'approccio antropologico assunto da Michael Whatson e Edward Hall, i quali riportano, nelle parole stesse di Goffman, tale aspetto di forte liricità della disponibilità informazionale in ogni contesto «prossematico», ossia problematico dal punto di vista prossemico: «una moltitudine di parole, gesti, atti ed eventi secondari si rende disponibile, che ciò sia voluto o meno, attraverso la quale una persona presente [all'interazione] può, intenzionalmente o no, simbolizzare il proprio carattere e le proprie attitudini»(Watson e Hall 1969, p. 223).

[34]È importante che sia l'**informazione** ad essere protetta. Adottare un approccio incentrato sulla «visibilità» potrebbe sembrare a prima vista più comodo e immediato, ma porterebbe ad una indistinguibilità di situazioni, risultando evidentemente più povero dal punto di vista euristico: non sarebbe in questo caso distinguibile la circostanza in cui una telecamera sta riprendendo le azioni del soggetto, operando dunque una registrazione dettagliata dell'*informazione disseminata* dal cliente che si sta dirigendo verso la sua banca. È questo il problema che starebbe alla base dell'«afasia» del diritto americano di fronte all'*esposizione*(Cohen 2008, p. 184) di sé che costituisce la sostanza dei *social network*.

[35]Una potente quanto ardua distinzione viene operata da Simmel tra conoscenza del *che* e del *cosa*: mentre la prima è relativa a «caratteristiche esterne», la seconda è una conoscenza che potremmo dire «di merito» rispetto all'oggetto. *Cfr.* su questo Simmel 1906b, p. 452.

[36]Ibid., p. 449.

[37]Ibid., p. 448, grassetto aggiunto.

[38]Ibid., pp. 444-445.

legami e a riallacciare le nostre separazioni»[39], ad ogni interazione corrisponde un qualche *ritiro*.

Diventa ora possibile procedere alla traduzione della «sensazione» di riservatezza, in quanto «reazione» rispetto all'intrusione non voluta, sia essa reale o potenziale, di qualcuno; è importante non trascurare il fatto che tale sensazione vive dei diversi contesti situazionali, ossia è «porzione strutturata del campo fenomenologico totale di una persona»[40]. Tutto questo può essere ampiamente coperto e abbracciato dall'armamentario concettuale della «spazialità». Riprendendo dunque anche l'idea di riservatezza come *claim*, pretesa *reattiva* relativa alle informazioni relative a qualcuno o qualcosa in termini di possibilità di controllo, raccogliamo tutti gli elementi necessari per procedere alla definizione centrale del lavoro. Definiamo quindi *riservatezza* come:

> *Reazione* consistente in una pretesa (*claim*) relativa all'**informazione** emessa [disseminata o disincarnata] dal soggetto in termini di *controllo* su di essa e dunque esclusione di altri dall'accesso, nella **regione** identificabile di spazio in cui questa è definita e si muove.

A titolo di prova, si può confrontare questa definizione con l'importante osservazione di Simmel sulla *discrezione*, che altro non è che «il senso di giustizia (*justice*) relativo alla sfera dei contenuti intimi della vita»[41]. È importante mettere in evidenza dunque un altro elemento strettamente legato alla nozione di **reattività** accolta, ossia quello di giustizia: in questo ordine di idee l'individuo percepisce la propria reazione come giusta, sensata. Tuttavia non è qui ignorato il fatto che tale aspetto trascini con sé tutto un insieme di problematicità più o meno evidenti che saranno trattate più avanti.

Come ultima riflessione, è interessante notare come nel tentativo di estrazione di un concetto comune a tutti i «diritti» alla *privacy* Jeffrey Reiman metta in evidenza che il contenuto dell'intimità non è tanto la rivelazione o la preservazione in sé delle informazioni, ma il fatto di curarsi dell'altro che le riceve e della nostra relazione con questi anche sulla base delle informazioni condivise: è tale idea di *cura* a permettere delle distinzioni nel nostro modo di relazionarci con gli altri, costituendo il presupposto stesso di tale possibilità relazionale; *privacy* costituisce dunque «un aspetto essenziale della complessa pratica sociale per mezzo della quale il gruppo sociale riconosce - e comunica all'individuo - che la sua esistenza è tale. E ciò costituisce una precondizione della **personalità**»[42].

[39] Citato in Schwartz 1968, p. 741
[40] Bates 1964, p. 430.
[41] Simmel 1906b, p. 454.
[42] Reiman 1976, pp. 35-39, grassetto aggiunto.

Spazialità cifrate

Il capitolo precedente delinea i concetti di spazialità, controllo dell'informazione, riservatezza; è possibile ora farli entrare nel vivo della questione, ossia il loro legame con la *crittografia*. Gli ultimi vent'anni hanno visto un mondo occidentale vivere in maniera sempre più tormentata[43] il rapporto con la *privacy*. Se questa prima era un lusso, un vero e proprio indicatore di status sociale, con il tempo è apparsa sempre più come uno scudo, uno strumento di difesa basilare. Ciò che probabilmente ha cambiato le cose è stata la possibilità, inedita, di accesso alle tecnologie di protezione della propria riservatezza a un costo praticamente azzerato. Si tratta, in sostanza, di comprendere come *crittografia* e riservatezza siano giunte a trovarsi strettamente legate.

Il lusso della *privacy*

La letteratura sociologico-politica in quello che potremmo considerare il **campo** qui occupato dalla *riservatezza* si è concentrata sull'aspetto del controllo[44], discorrendo ampiamente delle variabili di potere che si proiettano dai sempre più ampi e complessi dispositivi di controllo[45] orchestrati da governi di tutto il mondo. *Privacy* è un termine che, storicamente, è stato probabilmente relegato ad un certo ambito di classe, quello dominato dall'esigenza liberal-borghese di un «**diritto** a essere lasciati in pace»[46], il monumento supremo alla libertà negativa[47]. L'assenza di coercizione ricama un confine e definisce tale area di libertà. Tutto ciò appare

[43] *Cfr.* su questo lo studio di Nasu sulla riabilitazione della sfera privata nelle scienze sociali accompagnata da una proposta di «teoria della privatizzazione», Nasu 1992, pp. 77, 78, 81.

[44] Particolare riferimento è qui fatto a *Surveiller et Punir*(Foucault 1975). Come viene notato in Hull 2014, pp. 1-2, se si guarda all'aspetto etico o legale del discorso sulla *privacy*, Michel Foucault è completamente assente dalla discussione.

[45] Agamben 2006, pp. 19-20.

[46] Vagle 2015, p. 136.

[47] Nella sua celebre lezione tenuta a Oxford il 31 ottobre 1958, *Isaiah Berlin* riconduce la definizione del concetto di libertà negativa alla formulazione classica del *not being interfered with by orhers*. Il problema pratico della convivenza di individui che pur auspichino alla massima estensione della propria *libertà naturale* è ricongiunto all'idea di certi *libertarians* come John Locke, John Stuart Mill, Benjamin Constant, Alexis de Tocqueville che debba «esserci una certa area minima di libertà personale che non può in alcun caso essere violata», che «né lo Stato, né qualsiasi altra autorità possano essere autorizzate a invadere»(Berlin 1999, pp. 156-157). Tuttavia Berlin riprende anche una nozione di libertà negativa costruita da Mill e articolata su due linee(ibid., p. 159):

1. Ogni coercizione è un male di per sé (concezione libertaria classica);
2. Gli uomini dovrebbero cercare di scoprire la verità, o sviluppare un certo tipo di carattere (realizzazione di sé).

Per una lettura critica dell'*opportunity-concept* incarnato nella nozione di libertà negativa di Berlin vedi Taylor 1997, *passim*.

chiaro nell'opera iniziale di Michel Foucault, dove l'altra faccia della borghesia è quella della sorveglianza e della disciplina, della punizione corrisposta agli illegalismi della proprietà ma non agli illegalismi dei diritti: una punizione che dispiega i suoi effetti lungo linee storiche che abbandonano lo splendore dei supplizi per approdare alle moderne tecnologie carcerarie, illuminate dalla prospettiva *panottica*. Guardare alla *privacy* come lusso è un problema concreto che non manca di fondamenta, e andrebbe considerato come un importante punto di riferimento. La *privacy*, così come i suoi antecedenti concettuali, ha definito ed è stata definita da *status* sociali[48], ha strutturato costumi, distinto la classe dominante dai ceti poveri, l'alto ufficiale dal soldato semplice[49].

Ma ciò che davvero sembra poter aspirare a far scricchiolare tale logica è la possibilità, inedita, per tutti di poter accedere, semplificando, all'incirca alle stesse tecnologie crittografiche cui può accedere il «borghese» più ricco della terra. Il segreto di questa rivoluzione dei mezzi e delle possibilità risiede chiaramente nella semplice considerazione che, nell'era digitale, il costo marginale di produzione del prodotto intellettuale tende a zero: si tratta del medesimo ragionamento a fondamento di molte discussioni sull'*open-access* in ambito scientifico. E il problema non si esaurisce qui se si considera anche il fatto che, ancora oggi, l'uso di software e tecniche computazionali di crittografia autonome per cifrare *e-mail* o messaggi, è ancora poco diffuso a causa dell'ostacolo di «competenza» talvolta presentato dalla complessità di tali tecniche. Tuttavia, sono sempre più numerosi i *software* che grazie alla loro semplicità permettono, anche a un utente con competenze minime, di utilizzare tecniche di cifratura autonome per comunicare[50].

Si può dire che, parallelamente a una crescita di attenzione[51] rispetto all'idea di *privacy*, sicuramente legata anche alle vicende di Edward Snowden[52] o alle rivelazioni sul programma *PRISM* della *National Security Agency* statunitense[53], è corrisposta una sempre maggiore diffusione di software di crittografia di facile utilizzo. Al tempo stesso si osserva però anche un'evoluzione del mercato della *privacy*, che marcherebbe una parallela direzione inversa segnando un'affermazione di un mercato «lussuoso» della privacy. Per il momento non mi sembra scorretto affermare che, pur essendo reale quest'ultima tendenza, moltissimo software di

[48]Grossklags e Barradale 2014, p. 13.

[49]Schwartz 1968, p. 743.

[50]È questo tipo di considerazioni che ha portato *Phil Zimmerman*, attivista politico e padre di *PGP*, al tentativo - evidentemente riuscito - di dare a tutti la possibilità di utilizzare le tecniche di cifratura più avanzate per i propri dati e per la propria comunicazione(Singh 2001, pp. 223-224).

[51]Kasper 2005, pp. 84 e *ss.*

[52]Epstein, Roth e Baumer 2014, p. 144.

[53]Vagle 2015, p.102.

crittografia di alta qualità è open-source e ad accesso libero[54], dunque disponibile potenzialmente per chiunque lo voglia utilizzare.

Tecnologie di rifugio

Comprendere quali *software* siano realmente coinvolti, sia nella designazione dello spazio di *riservatezza* che nel processo di criminalizzazione trattato in questo lavoro, significa operare una selezione all'interno della fitta nebulosa di programmi che implementano funzioni crittografiche e che siano generalmente orientati alla *sicurezza* informatica. Per definizione data, *riservatezza* è tale solo quando sono soddisfatte le condizioni di:

- *spazialità*: è possibile individuare la regione di **spazio** (in cui l'informazione è definita e si muove) interessata dalla pretesa specifica;
- *controllo*: su tale regione è possibile esercitare un controllo reale che **escluda** soggetti indesiderati dall'accesso all'informazione che in essa si muove.

Sebbene a prima vista queste due condizioni possano dare l'impressione di delineare in modo netto il nostro oggetto, nella realtà le cose si fanno più complesse[55], e appare opportuno compiere un processo inverso, che consiste nella domanda: il software e le implementazioni specifiche delle tecnologie poste sotto un'attenzione (attuale o potenziale) dall'azione penale, soddisfano queste condizioni e sono utilizzati perché tali condizioni, poste come obiettivo specifico, siano attese? Se la risposta è affermativa, allora il percorso logico strutturato segue i tre macro-concetti: riservatezza, crittografia (specifica), criminalizzazione. Questa

[54] Senza poter trattare qui tale questione nel dettaglio, è importante notare che software come *PGP* (*Pretty Good Privacy*), *OpenSSL* (che è implementato, a titolo di esempio significativo, per dare vita al protocollo *HTTPS*), *dm-crypt/LUKS* (per la cifratura di volumi fisici) o il protocollo «a cipolla» *Tor* (per l'«anonimizzazione» del traffico in rete) sono soggetti a licenze che prevedono la pubblicazione del sorgente, caratteristica che rende possibile un controllo diffuso sulla qualità, i contenuti, le funzioni e la sicurezza del *software* stesso. In più si tratta, in tali casi, di quello che chiamiamo generalmente *software libero*, con riferimento alla sua possibilità di circolazione.

[55] Giusto a titolo di esempio, per riprendere il discorso della nota precedente: un *software* di sicurezza che non renda pubblico il proprio codice sorgente, adempie davvero a queste condizioni? Dalla possibilità che tale *software* includa delle funzioni, potenzialmente malevoli, conosciute solo dal programmatore, uscirebbe indebolito in primo luogo il secondo elemento, dal momento che ci sarebbe un indebolimento delle possibilità di controllo sull'accesso all'informazione, e di conseguenza anche il primo, dal momento che non si potrebbe più identificare con un apprezzabile grado di certezza quale sia lo spazio davvero interessato dal flusso di informazioni. Tuttavia estremizzando tale dilemma, saremmo portati a dubitare praticamente di tutto il software attualmente esistente, dal momento che tutto ciò che viene coinvolto nel suo funzionamento deve essere conosciuto (almeno in potenza) alla perfezione: il compilatore specifico del linguaggio scelto, il compilatore con cui è stato compilato il compilatore, e così via fino ad arrivare alle funzioni specifiche del processore e dunque al livello di *hardware*.

operazione richiede però una maggiore precisione concettuale rispetto al termine *crittografia*, e immediatamente una precisazione: se il termine «crittografia» indica, in senso ampio, l'insieme delle conoscenze relative alla «sicurezza» della comunicazione[56], più preciso risulta il termine «cifratura» o «crittazione», ossia la tecnica attraverso la quale un messaggio viene reso inintelligibile[57], assicurandosi dunque, che nessun ascoltatore o lettore indesiderato possa accedervi[58].

Pochi lavori giuridici si occupano nel dettaglio di **quali** specifiche tecnologie crittografiche costituiscono oggetto della legislazione penale. Tuttavia un recentissimo lavoro di *Jeffrey Vagle* pone, a partire da una punto di vista giuridico, una domanda significativamente sociologica: cosa succede quando il tuo utilizzo di tecniche di cifratura è automaticamente etichettato da parte dei governi come un comportamento *sospetto*?[59]. Vagle offre una chiarissima visione d'insieme dello stato dell'arte della legislazione americana su questo aspetto, che ha le sue radici da una parte nella sezione 702 del *Foreign Intelligence Surveillance Act* del 1978 (*FISA*), che autorizza la *National Security Agency* a collezionare e archiviare informazioni raccolte nel corso di comunicazioni, semplicemente per il fatto che siano cifrate, per il tempo necessario alla loro decrittazione[60], e dall'altra nelle

[56]È bene notare che la sicurezza della comunicazione riguarda un ampio spettro di esigenze. Accogliendo qui a titolo meramente illustrativo una classificazione riportata in Stallings 1998, p. 5, sintetizziamo i servizi di sicurezza informatica nelle seguenti aree:

- *Segretezza*: assicura che l'informazione archiviata o trasmessa sia accessibile solo da parti autorizzate.
- *Autenticazione*: assicura che l'origine del messaggio o del documento elettronico siano correttamente identificate, dunque che il messaggio non sia falso
- *Integrità*: assicura che solo le parti autorizzate possano modificare un certo messaggio
- *Non-rifiuto*: richiede che né il mittente, né il destinatario siano in grado di negare la trasmissione
- *Controllo dell'accesso*: richiede che l'acceso alle risorse informative possa essere controllato da e per il sistema in oggetto
- *Disponibilità*: richiede che le risorse del sistema di un computer siano disponibili quando richiesto dalle parti autorizzate

. Un'elencazione meno tecnica è riportata da Vagle 2015, p. 117. L'accento ricade nella trattazione di questo lavoro sugli aspetti generali della *segretezza* e dell'*autenticazione*.

[57]Con il termine semplice ma non esatto di «inintelligibile» si intende il risultato dell'applicazione di un algoritmo di cifratura, con dei blocchi di informazioni detti *chiavi* come parametri, a un testo detto *in chiaro*, tale per la diretta accessibilità del messaggio in esso contenuto, per ottenerne un testo detto *cifrato*, il cui messaggio originario diventa accessibile idealmente soltanto attraverso un'analoga applicazione dell'associato algoritmo di decrittazione(Goldreich 2004, p. 374). È chiaro qui il legame tecnico tra cifratura e funzione di *segretezza*.

[58]Petras 2001, p. 689.

[59]Vagle 2015, p. 104.

[60]Il senso specifico di questa disposizione risiede nel fatto che i *tempi attesi* per la decrittazione con metodi di «*brute force*» di un messaggio cifrato di cui non conosciamo la chiave per la decrittazione sono strettamente legati alla scoperta di possibili falle negli algoritmi di cifratura

International Traffic in Arms Regulations previste dall'*Arms Export Act* del 1978, che includono nell'elenco delle armi sottoposte a disciplina la crittografia. Ci sono disposizioni di sistemi penali come quello indiano, inglese, francese o sudafricano che attualmente puniscono penalmente chi rifiuti di consegnare *password* e chiavi di cifratura[61] quando richiesto dalle autorità[62]. Limitazioni sono state poste da varie legislazioni alla *lunghezza* delle chiavi di sessione utilizzate, soprattutto in Francia[63], fino a che, nel 2004 l'utilizzazione dei «mezzi di crittologia» viene definita «libera», abrogando le precedenti disposizioni restrittive[64].

Senza alcuna intenzione di esaurire qui un discorso giuridico che già vive problematicamente gli ambiti accademici del diritto, è possibile concludere che, in larga misura, i *software* basati su algoritmi di cifratura asimmetrica[65] utilizzati per la cifratura e la firma di mail, messaggi o contenuti, quelli utilizzati per la protezione di dati personali e cifratura simmetrica di supporti fisici[66] o finalizzati alla «anonimizzazione» della navigazione in rete[67], o che in generale forniscono una possibilità di cifratura *end-to-end*[68], sono tutti attualmente, potenzialmente o storicamente stati interessati da legislazioni penali e da disposizioni relative alla «sicurezza nazionale». Il motivo dichiarato per cui queste tecniche sono oggetto

---

o nelle sorgenti di entropia per la generazione di dati casuali e alla progressiva crescita della potenza di calcolo delle macchine impiegate. La ricerca in tale ambito riguarda la possibilità di comprendere quanto siano *difficili* da «rompere» le protezioni di sicurezza. In tal senso è interessante la *RSA Factoring Challenge*, ora non più attiva, basata sul principio alla base del sistema cifratura asimmetrica *RSA*, sviluppato al *MIT* nel 1977, ossia sulla difficoltà computazionale di fattorizzare un prodotto dato di due numeri primi molto grandi. Per un discorso più ampio su questo e sulle modalità di attacco, vedi Singh 2001, pp. 209-210 e Koblitz e Menezes 2004, pp. 603-607.

[61] Disposizione presente nel *Regulation of Investigatory Powers Act 2000* del Parlamento del Regno Unito.

[62] Price 2014.

[63] Il *décret n 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable* limitava la lunghezza delle chiavi di sessione al valore 128 bit.

[64] *Loi n 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.*

[65] Con l'esempio illustre di *PGP/GPG*(O'Connor 1996), basato sull'algoritmo *RSA*.

[66] *TrueCrypt* era un software *open source* molto utilizzato per la cifratura di volumi fisici. È stato investito in pieno dalle varie *Key Disclosure Laws* che hanno reso obbligatoria, in diversi paesi, la rivelazione delle *password* o la fornitura delle chiavi di cifratura alle autorità.

[67] *Tor* ha costituito l'oggetto di numerosi interessi in tal senso, giusto a titolo di esempio, nel luglio 2014 Putin ha pubblicato la possibilità di un premio da 110 mila dollari(Khrennikov 2014) per chi riuscisse a rompere il famoso sistema di sicurezza basato sul metodo di «routing a cipolla».

[68] La libreria crittografica *OpenSSL* è alla base del protocollo *HTTPS* (in cui «S» sta per *secure*), risultato dell'implementazione di *SSL/TLS* in *Hypertext Transfer Protocol*, grazie al quale vengono rese sicure e private le comunicazioni con un web server. Per maggiori dettagli sulle condizioni date dal sistema di *certificazione* delle chiavi utilizzate, vedi Koblitz e Menezes 2004, p. 607. Nell'aprile 2014, al momento della scoperta del *bug* di *OpenSSL Heartbleed*, scesero dei sospetti sul fatto che l'*NSA* sarebbe stata a conoscenza della vulnerabilità già da 9 mesi, nel corso dei quali l'avrebbe sfruttata per mettere in atto attacchi specifici(Riley 2014).

di considerazioni giuridiche è la loro capacità di nascondere in maniera *efficace*[69] a chiunque non sia voluto, e in particolare alle autorità governative, delle informazioni specifiche volute dall'utente, al punto che l'*unica possibilità* per le autorità di accedere a tali contenuti è quella di farsi consegnare le chiavi di cifratura, come visto cone le *Key Disclosure Laws*.

Da questa considerazione si raccolgono i due elementi posti in evidenza all'inizio del paragrafo: quello della *spazialità*, che si definisce sull'area di messaggio trasformata in *testo cifrato*, e quello del *controllo* su di essa, che è continuamente richiamato dalla gestione delle chiavi di accesso ai contenuti cifrati. Più difficile risulta invece capire **quanto** questo legame tra crittografia e riservatezza sia stretto. È appunto tale allineamento che costituisce l'oggetto del contendere in tutte le disposizioni, talvolta altalenanti nel tempo, sulla regolamentazione delle risorse crittografiche. Sembrerebbe rischiarare il problema l'adozione di una prospettiva che guardi all'esistenza di tale legame come subordinata a dei riconoscimenti «societali» della *riservatezza*[70]; malgrado la formulazione non immediata, si tratta semplicemente di capire se parti della società, quali e in che misura, riconoscono una forma di protezione della *riservatezza* nell'utilizzo di tecniche crittografiche: si è visto come *Phil Zimmerman*[71] ha pensato esattamente questo, quando ha rischiato un'incriminazione al momento della pubblicazione del codice di *PGP*, mentre un *David Cameron* in campagna elettorale è pronto a disconoscere tale dignità alle medesime tecniche[72].

Nulla da nascondere

Nel corso del suo intervento all'edizione del 2010 dei *Crunchy Awards* di *San Francisco*, il fondatore di *Facebook* Mark Zukerberg dichiara che la *privacy* non è più una «norma sociale», e che proprio questo ha finalmente permesso il decollo di tutti «quei servizi che le persone ricevono condividendo tutta questa informazione [tramite il *blogging*]»[73]. Oltre a essere un ottimo esempio della validità del significato sociale di *informazione*[74] in questo ambito, la dichiarazione del giovane imprenditore statunitense è una campana a morto dell'idea tradizionale di *privacy* nel *web 2.0*. Questo aspetto è però solo una faccia del problema della *riservatezza*, ed è molto più legato all'economia di mercato dei grandi servizi *internet*, che

[69] Sull'efficacia di tali tecniche, vedi *supra*, su *RSA*, e Stallings 1998, pp. 173 e ss.
[70] Bates 1964, p. 431.
[71] Vedi *supra*, nel paragrafo «Il lusso della *privacy*».
[72] Dredge 2015.
[73] Barnett 2010.
[74] Vedi *supra*, «Informazione ed entropia».

alla vera e dura idea *politica* del «nulla da nascondere»; è quest'ultima che, pur essendo apparentata alla sempre meno straniante conoscenza dei servizi utilizzati, rivela in realtà la presenza dello *Stato* nelle logiche comunemente adottate ad un livello che potremmo dire di *habitus*.

Web 2.0

Esattamente undici anni prima dell'intervento di Mark Zukerberg ai *Crunchy Awards*, il *CEO* di *Sun Microsystems*, *Scott McNealy*, fu investito da una tempesta di critiche e attacchi, suscitando sbigottimento e incredulità ad ogni livello per aver dichiarato: « *You have zero privacy anyway. Get over it.*»[75]. Se a quella dichiarazione, percepita come pretestuosamente normativa, fece seguito una levata di scudi pressoché unanime, con una rinnovata mobilitazione del dibattito sulla *privacy*, l'intervento di Zuckerberg, apparso come francamente descrittivo, ha invece affondato il colpo nel ventre molle dell'incerto e talvolta afasico dibattito accademico sulla *privacy*[76], ormai già violentemente strattonato e spossato dai profondi cambiamenti del *World Wide Web*. Cosa è successo, esattamente, in questi dieci anni? Innanzi tutto, i «guardiani» della *privacy* hanno vissuto un periodo di crisi concettuale, probabilmente legato al paradigma della «visibilità». Come nota la studiosa americana *Julie E. Cohen*, il mondo occidentale si è ritrovato intrappolato in una terminologia *visuale*[77], che ha finito per investire inevitabilmente anche lo stesso armamentario concettuale giuridico sulla *privacy*[78], mentre la soluzione del gioco starebbe nel percorrere fino in fondo la strada foucaultiana, attraversando la sorveglianza «radicalmente decentralizzata» per superare la *disciplina* dei corpi e delle menti in un'autentica *seduzione*[79]. Dall'altra parte, il mondo di *internet* è cambiato profondamente, ed effettivamente, quello che sembrava «solamente» un potente e incredibilmente semplice strumento di accesso a contenuti e informazioni, il *web*, si è trasformato in un ancora più semplice,

[75]Pronunciata nel corso di una conferenza stampa per il lancio del sistema di rete *Jini*, la frase di McNealy era riferita in particolare alla decisione di *Intel* di disabilitare delle funzioni di autenticazione a livello di processore per l'allora appena uscito *Pentium III*(Sprenger 1999).

[76]Vedi *e.g.* Kasper 2005, pp. 72-75

[77]La definizione di Cohen si spinge fino ad individuare la natura del problema nella definizione giudaico-cristiana di Dio come «dio che tutto vede». Per quanto riguarda la *privacy*, applicare il concetto di «visibilità» come parametro di valutazione diventa un problema evidente quando non c'è alcun *Big Brother* cui puntare il dito(Cohen 2008, p. 185). Ed è proprio *Big Brother* ad essere diventato, secondo Daniel Solove, uno straordinario esempio di quelle potenti e latenti *metaphors we live by*, «esperienza di qualcosa nei termini di un'altra»(Lakoff e Johnson 1980 in Solove 2004, p. 28). In qualche modo, come già accennato *supra*, si registra un calo di capacità euristica che rende indistinguibili situazioni in cui c'è manifestamente un problema di *riservatezza*.

[78]Cohen 2008, p. 185.

[79]Ibid., p. 187.

intuitivo e potente strumento di accesso, pubblicazione e continua rielaborazione di contenuti, informazioni, *design*, servizi, identità. Le grandi aziende di *internet* hanno definito un oligopolio fondato sugli stessi dati forniti dagli utenti nell'utilizzo stesso dei servizi. *Blog*, pagine *web* personali, siti di opinioni ed enciclopedie collettive raccolgono flussi di informazioni inserite ed elaborate da utenti (*user-generated content*) per riversarle nuovamente nel *web 2.0*. Sono ormai paleolitici i dibattiti sulla possibilità di poter accomunare lo spazio dei *forum* a quello fisico[80]; è ora la nostra modalità di vivere la tecnologia ad aver subito profondi cambiamenti, articolandosi su nuove **metafore** e identità definite principalmente sui *social network*, sull'utilizzo di applicazioni sempre nuove su dispositivi sempre più portabili. Sembra adeguato parlare di dispositivi[81] che, a decine e sofisticatissimi, penetrano le nostre abitudini, si rinnovano, si scambiano tra loro e mutano; sia sufficiente per ciò pensare alle migliaia di *app*(licazioni) disponibili in pochissimi secondi su quasi ogni *smartphone*. E non sarebbe ancora un errore parlare di dispositivi, nella consapevolezza che ognuno di essi sì intermedia una relazione tra noi e qualcosa o qualcuno, ma al tempo stesso **ci** intermedia, ordinando, strutturando e rielaborando le *informazioni* che noi stessi forniamo con il nostro utilizzo[82].

Radiografia di un sillogismo

Se qualcosa è cambiato profondamente in quegli anni *duemila* che separano le due dichiarazioni di scomparsa della privacy, la prima senza trovare credibilità, la seconda quasi trasformandosi in un certificato di morte, va ricercato in primo luogo a livello logico. Si tratta in parte di una vera e propria adozione di una prospettiva di «psicanalisi sociale», nel tentativo di districarsi nel ginepraio di interconnessioni logiche che reggono esteticamente il *sensus communis*[83] degli uomini. Il terzo millennio ha fatto il suo ingresso sulla scena del mondo occidentale con l'attentato alle *Twin Towers* dell'11 settembre 2001, calpestando spietata-

[80]Cohen 2008, p. 195.

[81]Per il significato della parola *dispositivo* mi rifaccio completamente a quello chiarificato da Giorgio Agamben, riprendendo il percorso *Hegel*, *Hyppolite*, *Foucault* per arrivare ad indagare l'evoluzione del concetto di «positività» come termine ultimo, storico, di cristallizzazione delle relazioni di potere(Agamben 2006, pp. 10-13).

[82]È esattamente questa la direzione intrapresa dalle grandi aziende del *web*: rendere ogni contenuto un servizio, ogni archivio di dati una *cloud* decentralizzata. Questo cambiamento spinge ad un'iniezione di quantità di dati sempre più enormi nella rete *internet*, dunque un transito sempre più massiccio per i *server* di analisi dei dati di un'azienda come Google(Jackson 2015).

[83]Riprendendo il *Kant* della *Critica del Giudizio*, la teorica politica *Hannah Arendt* offre una critica del gusto estetico come parte del *sensus communis*, dal quale dipende ogni comunicazione, il discorso umano in sé(Arendt 1982, p. 70).

mente qualsiasi idea di «fine della storia» e segnando una rinnovata dinamica della mobilitazione occidentale nella guerra al terrore. Negli anni immediatamente successivi all'attentato di *Manhattan* comincia a scorrere fuori dagli uffici di Governo e Congresso statunitensi un fiume di misure che, in nome della *sicurezza nazionale*, ha cacciato dalla storia più recente alcune basilari condizioni *garantiste*; sulla punta della spada, il sillogismo che affermerebbe l'inconsistenza di qualsiasi problema di *privacy* nel caso in cui nessuno avesse «nulla da nascondere»[84](per semplicità riportato in seguito come «Argomento *NTH*», *Nothing To Hide*). Ciò che diventa davvero interessante in tutto questo, è che l'argomento *if you've got nothing to hide, you've got nothing to fear* è diventato estremamente comune ad ogni livello[85], al punto da essere diventato, secondo *Bruce Schneier*, la più comune forma di attacco argomentativo contro i legali che si occupano di *privacy*[86]. In fondo, come nota Schneier, l'anello ultimo che regge la **ragionevolezza** del *NTH* è il presupposto, questo sì davvero nascosto, che il «nascondere» sia un'attività che si riferisca necessariamente a qualcosa di sbagliato[87] e che, per tale motivo, la riservatezza debba essere necessariamente anch'essa sbagliata[88].

Con l'identificazione del *secretum* con lo sbagliato, si ritorna al problema lasciato in sospeso con Simmel sul *giusto* che risiede nell'attitudine individuale al riserbo. È evidente che tale idea di «giusto» utilizzata da Simmel, così come quella di «diritto» inserita da Goffman nelle sue definizioni[89], non ha alcun presupposto di tipo legalistico, statalista o giusnaturalistico. Ciò che questi autori indicano è la semplice idea che è l'**individuo** a considerare giusta la propria condotta o la propria aspettativa[90], ossia *giustificata*, e, con Raymond Boudon potremmo dire, *razionale*[91]. Accogliere la semplice idea di «ragionevolezza» della *riservatezza* è un presupposto metodologico fondamentale, da cui è possibile partire per spiegare come si possa affermare anche l'idea opposta, di coerenza dell'argomento *NTH*. La quasi banale intuizione, ricevibile all'interno di un discorso improntato

[84]Solove 2007, p. 746.
[85]Ibid., p. 748-749.
[86]Solove 2011.
[87]Schneier 2006.
[88]Risulta chiaro come ci sia tutto un insieme di problemi legato all'ipotesi che risiede nell'identificazione del giusto con il legale e che, tuttavia, verrà per il momento accantonato.
[89]Vedi *supra*, nelle definizioni di *Informational* e *Conversational Preserve*.
[90]Kirsten Martin mette in evidenza quali siano le diverse aspettative di *privacy* che l'utente tende ad avere nell'utilizzo di determinate tecnologie(Martin 2012, *passim*).
[91]Nel significato del termine «razionale» utilizzato da Raymond Boudon, in linea con un individualismo metodologico già accolto in Max Weber, è l'idea del «relativamente razionale» a rendere possibile una rivoluzione copernicana nella lettura del sociale(Boudon 1986, pp. 96-97).

a un approccio weberiano di teoria dell'azione[92], che tale *razionalità* risieda in una questione di prospettive[93], si traduce metodologicamente nella necessità di trasformare ogni quesito del tipo «*è razionale X?*» in «*secondo quale prospettiva X è (ir)razionale?*»[94]; e talvolta la risposta non è immediata, dal momento che potrebbero dover intercorrere delle conoscenze tecniche che permettano di strutturare la catena di ragionamento per la valutazione del comportamento o della condotta.

Da tali premesse segue che sarebbe un grave errore logico confondere i due interrogativi, entrambi importanti, sul carattere di «giustezza» assegnato agli individui alla riservatezza e sull'«attenzione» da essi dedicata per proteggerla[95]. Ma tutto questo restituisce in realtà *due* domande distinte. La prima riguarda il carattere di *giustezza* relativo alla riservatezza: secondo quale prospettiva considerare la riservatezza giusta ovvero ingiusta è ragionevole? La seconda invece riguarda l'attitudine concreta alla preservazione della riservatezza: la scarsa attenzione alla riservatezza è dovuta a un'interiorizzazione dell'argomento del tipo *NTH*, dunque all'idea radicata che nascondere qualcosa è sbagliato, oppure (anche) a qualcos'altro? La risposta alla prima domanda è già parzialmente emersa, in quanto va ricercata proprio nell'anello a tenuta di tutta la catena dell'argomento *NTH*: l'equazione tra *qualcosa da nascondere* e *ciò che non ha diritto ad essere nascosto*[96], oltre a negare logicamente la possibilità che possa esistere qualcosa che l'individuo possa nascondere, è evidentemente tutta da dimostrare[97], e rimane per

[92]In proposito, la «banalità» del discorso weberiano è rappresentata con un'efficacia quasi spietata da James Coleman con il suo diagramma divenuto noto come *Coleman's boat*.

[93]Cohen 2012, pp. 247-249.

[94]Il problema dei «punti di vista» si fa ben più politico nel pensiero di *Pierre Bourdieu*: un effetto di *divinizzazione* fa prevalere un punto di vista sugli altri, e in particolare è il capitale simbolico dello Stato a renderlo capace di aspirare al ruolo di «punto di vista di tutti i punti di vista»(Bourdieu 2012b, p. 53).

[95]L'affiancamento logicamente fallace delle due questioni costituisce quello che Gordon Hull considera un «*privacy paradox*»(Hull 2014, p. 1).

[96]Raymond Boudon parla di «presupposto tacito» rispetto alle ipotesi nascoste che reggono ragionamenti con forte potere esplicativo. In più si può accogliere l'idea di un «effetto epistemologico attivo» sul concetto(Boudon 1986, pp. 208 e ss.) stesso del *nascondere* alla base dell'argomento NTH presso i giuristi, che si ripercuote successivamente in un insieme di «effetti di comunicazione» che investono circolarmente pubblico e mondo accademico(ibid., p. 135).

[97]Il duello argomentativo contro l'argomento *NTH* viene portato avanti di Daniel Solove in un articolo del 2008, in cui vengono efficacemente messe in evidenza le fallacie che minano alla sostenibilità dell'argomento stesso. È importante tenere in conto come questo argomento si presenta in realtà sotto diverse forme, e che il sorpasso argomentativo è immediato solo nelle forme estreme: si è appena visto come un'interpretazione oltranzista del *NTH* arriva a negare la possibilità stessa che qualcosa possa essere nascosto. Ma è nelle sue varianti meno estreme, che il gioco si farebbe più duro; per arrivare a dimostrare l'insostenibilità dell'idea che un'analisi sistematica delle informazioni da parte di macchine, con rilevazione di *pattern* legati ad attività illegali, non invada la *privacy* (*then you've got nothing to fear*) Solove passa per una tassonomia delle invasioni della *privacy*, così strutturata(Solove 2007, p. 758):

il resto un'ipotesi nascosta. La risposta alla seconda sembra richiedere alcuni passaggi aggiuntivi che diventeranno più chiari nell'appendice sugli «apparati privati di sicurezza».

- Information Collection (Surveillance, Interrogation)
- Information Processing (Aggregation, Identification, Insecurity, Secondary Use, Exclusion)
- Information Dissemination (Breach of Confidentiality, Disclosure, Exposure, Increased Accessibility, Blackmail, Appropriation, Distortion)
- Invasion (Intrusion, Decisional Interference)

Anche qui si può notare che, come osservato *supra*, è la prospettiva di *chi riceve* l'informazione, anziché quella di chi la *emette*, a risultare più interessante dal punto di vista euristico per riconoscere alcune situazioni altrimenti indistinguibili.

Lo Stato tra sapere e potere

Parlare di criminalizzazione significa parlare dell'ingresso e della fuoriuscita di determinate condotte dal campo di interesse penale, dunque anche necessariamente parlare di Stato. Il quesito di fondo è: cosa significa criminalizzare, in generale, per lo Stato, e criminalizzare la crittografia, in particolare? Si è già visto come il termine crittografia debba essere specificato, individuando che cosa, in questo lavoro, esattamente significa, e ciò è stato fatto nella parte precedente. Riordinato il campo empirico di riferimento, si può quindi concentrare l'attenzione sull'attività di criminalizzazione, e sulle condizioni che la rendono possibile. Adottando una chiave di lettura dello stato *à la Bourdieu*, ritrovata a partire dalla celebre definizione di Max Weber di stato[98], emerge il problema della giunzione tra la criminalizzazione in sé e l'argomento *nothing to hide* che può essere ritrovata nei termini di una ricomposizione logica tra il piano individuale e quello statale.

Stato, istituzionalizzazioni e logiche

Il 7 gennaio 2015, un attentato alla sede di Parigi del settimanale *Charlie Hebdo* scuote di violenza la Francia e l'Europa. L'11 gennaio, dopo tre giorni «di sirene, elicotteri nel cielo, notizie convulse», la *république* scende in piazza per sanzionare il proprio 11 settembre[99]: un milione e mezzo di francesi si riversa nel corteo che, aperto da un cordone di capi di Stato, risuona della semplice parola d'ordine della «libertà di espressione», condensata nel motto *Je suis Charlie*, sono *Charlie*. Se è vero che è proprio la *république* a scendere in primo luogo in piazza[100], a richiamare il popolo-nazione[101] attorno una traiettoria discorsiva ben precisa, è altrettanto vero che l'eloquenza giocata in quelle giornate e nelle settimane a seguire è essa stessa della *république*, dello Stato; lo Stato è il presupposto logico di «Je suis Charlie», tanto quanto la *libertà di espressione*, come ogni altro diritto soggettivo moderno, presuppone logicamente uno Stato che la protegga. È dunque qui necessaria un'ontologia precisa dello Stato, non solo istituzione ma anche fondatore simbolico di istituzioni, concetti, categorie.

[98] Weber 2008, p. 156.

[99] Chomsky 2015.

[100] Fin dalla loro organizzazione, le marce del 10 e 11 gennaio in Francia sono state definite *marches républicaines*(Ministère de l'Intérieur 2015a).

[101] Nel pensiero di Thomas Mann l'espressione *we the people* (talvolta esplicita, come nel caso della Costituzione degli Stati Uniti d'America) è alla base delle diverse idee di popolo *stratificato* ovvero *organico*; la confusione concettuale della parola «popolo» tra le due specie *ethnos* e *demos* può trasformare questo concetto in un potente elemento di mobilitazione, soprattutto in un discorso in nome del popolo «intero»(Mann 2005).

Alla ricerca dello Stato

Tracciare un'ontologia dello Stato non presuppone necessariamente un approccio genetico, tanto che numerose sono le teorie dell'ipotetico contratto originario[102] nel pensiero filosofico politico contemporaneo; potremmo far rientrare in questo gruppo anche l'approccio kantiano alla base dell'idea moderna di *stato minimo*[103]. Ciò che sembra caratterizzare queste visioni è una visione fondamentalmente **normativa**. È opportuno dunque distinguere un tentativo più descrittivo, che sembrerebbe tuttavia imporre uno studio genetico[104], prospettiva che ha fatto colare altrettanti fiumi d'inchiostro e che trova un punto significativo nella definizione elaborata da Max Weber di Stato come

> comunità umana che, entro un territorio definito [...] reclama per sé con successo il monopolio della forza legittima[105]

Pur potente nell'esplicitare i due concetti di *territorio* e *legittimità*, la definizione di Weber rimane troppo ancorata all'idea di forza, sia essa economica o politica, ma in ultima istanza sempre fisica, militare; è questa una visione tutt'altro che lontana dalla realtà, se si pensa che si ritrova pressoché intatta nella forma del «principio di effettività»[106] nel diritto internazionale. Un'ontologia dello Stato sembrerebbe però richiedere un qualcosa in più, e precisamente l'idea di **potere simbolico**[107], che restituisca finalmente uno Stato capace di fondare concetti e, a traverso di essi, fondarsi, rendersi in sostanza immaginabile. La definizione

[102] L'idea di contratto sociale affonda profondamente le proprie radici nella storia più remota del pensiero politico. Tuttavia è sufficiente qui richiamare Thomas Hobbes o John Locke, i quali distinguono all'interno del contratto sociale un *pactum unionis* e un *pactum subjectionis*, pur supportando tesi completamente differenti. Jean-Jacques Rousseau adotta invece un'altra prospettiva, rifiutando l'idea di cessione dei propri diritti allo Stato, e introducendo quella di una libertà ritrovata nella «sottomissione» di ognuno alla volontà generale; e ancora non sarebbe chiaro il discorso se non si comprendesse in Rousseau l'elemento dell'*amour propre*, che Charles Taylor individua come fondazione post-cartesiana dell'ideale di *autenticità*(Taylor 1994, pp. 29-30).

[103] È la distinzione, in campo morale, tra etica e dottrina del diritto, parallela a quella tra felicità e diritto, che permette a Immanuel Kant di elaborare una nozione di *Rechtstaat* ben distinta da quella di *Wohlfartstaat*, fondando l'idea moderna di di «stato di diritto»(Marini 2007, p. 78).

[104] Celebre è il lavoro di Charles Tilly; anche Pierre Bourdieu esplicita un approccio pienamente genetico(Bourdieu 2012b, pp. 203 e ss.).

[105] Weber 2008, p. 156.

[106] L'idea di esercizio con successo del monopolio della forza legittima si ritrova in diritto internazionale nella forma di capacità di controllo effettivo del territorio. Questa nozione, originariamente ancorata all'ambito militare, potrebbe lasciare degli spazi per la considerazione di responsabilità originanti da forme di potere e coercizione economica, dunque rendendo l'intero armamentario materiale un fatto giuridico. Si trova un esempio significativo su questo nel commento ufficiale agli articoli 1 e 19 della Quarta Convenzione di Ginevra del 12 agosto 1949(Uhler e Coursier 1958, p. 308).

[107] Borghini 2009, p. 74.

di Max Weber deve subire una correzione, per arrivare a tracciare un'idea di stato come «X», incognita, che esercita un «monopolio della violenza simbolica legittima»[108]. L'idea di violenza simbolica lancia molto oltre il concetto di stato, fino a restituirlo come *punto di vista dei punti di vista*, quello che Bourdieu, citando Leibniz, definisce il «piano geometrale di tutte le prospettive»[109]. Tale potere simbolico, che è intimamente potere di «costruire il dato»[110], fa dello Stato al tempo stesso una *natura naturans* e una *natura naturata*[111], e non può esercitarsi che diffusamente[112], penetrando dinamiche di riproduzione e controllo sociale, a un tempo controllo e autocontrollo[113].

Istituzionalizzazioni

Risulta a questo punto necessario indagare più a fondo l'idea di potere simbolico appena adottata. L'idea genealogica adottato da Bourdieu rileva un processo di centralizzazione degli strumenti di legittimazione, parallelo allo «sviluppo di un apparato simbolico» attorno al sovrano[114]; lo Stato accede storicamente al monopolio del potere universale di «nominazione», imponendosi come fonte delle autentiche categorie adottabili nel giudizio. All'interminabile catena di interrogativi sul *chi stabilisca cosa*, lo Stato è riuscito a piazzarsi esattamente nel punto di convergenza di ogni catena di domande, definendo il punto dove *ananke stenai*, è necessario arrestarsi[115], diventando per l'appunto quel piano geometrale di tutte le prospettive. Il capitale simbolico, in quanto **metacapitale**, rende così possibile la *definizione* di concetti e identità sociali[116]. A questo punto l'interrogativo cui bisogna rispondere è quello che riguarda la possibilità e le modalità concrete attraverso le quali un potere simbolico viene esercitato: Bourdieu risponde che lo Stato costruisce, attraverso l'amministrazione pubblica e i suoi rappresentanti, categorie e «problemi sociali» che il mondo accademico si limita principalmente a ratificare. Ciò che la storia ci ha consegnato è un «capitale statuale», che passa

[108]Pierre Bourdieu considera lo Stato come un oggetto impensabile(Bourdieu 2012b, pp. 13-14).
[109]Ibid., p. 53.
[110]Borghini 2009, p. 76.
[111]Bourdieu 2012b, p. 197.
[112]L'idea di esercizio diffuso del potere rinvia alla riflessione affrontata *supra* su *Big Brother* come metafora distorsiva legata al paradigma della visibilità .
[113]Lo stato costituisce un campo, in perfetta analogia a un campo da gioco, con le proprie regole, le proprie logiche e il proprio linguaggio, riuscendo a ottenere, da coloro ce vi entrano, una sottomissione a vincoli, censure oggettive e incorporate, cui essi non riescono neanche ad accorgersi(Bourdieu 2012b, p. 151).
[114]Bourdieu 2012a, p. 113.
[115]Ibid., p. 115.
[116]Borghini 2012, p. 189.

per l'accumulazione di tutte le forme di capitale, da quello fisico-coercitivo a quello propriamente simbolico; tale capitale «complesso» definisce un campo di regole e potere entro il quale i soggetti lottano per acquisire il potere sullo Stato[117]. Il potere simbolico si esercita dunque attraverso una capacità di istituzionalizzazione che conduce a pensare a condotte e categorie come naturali e, tra esse, in primo luogo lo Stato stesso[118].

Fissati gli elementi centrali della questione, è necessario allontanarsi leggermente dall'idea dello stato come detentore di un «monopolio», per concentrare maggiormente l'attenzione sul fatto che tale prospettiva coinvolge la società nel suo complesso, e che molteplici attori concorrono dinamicamente nella sua strutturazione, pur potendo individuarne alcuni che siano preminenti rispetto ad altri[119].Ciò che a questo punto rileva ai fini del lavoro è che un tale approccio permette di considerare la non univocità delle logiche in gioco nel sociale: se è vero infatti che lo spazio sociale si struttura tramite logiche, ed esiste un potere di *nominazione*, ossia di produzione categoriale, che può essere addirittura «monopolizzato», allora le logiche che abitano il sociale utilizzano categorie ben lontane dall'essere fissità date, dunque soggette a mutazioni e inserite in contesti simbolici che le rendono necessariamente situate. Ci si avvicina così all'idea che gli attori sociali agiscono e, potremmo dire con Boudon danno ragione di ciò che fanno[120], attraverso logiche «morbide, fluide»[121].

Le istituzionalizzazioni, possibili attraverso una continua costruzione del dato, riguardano dunque anche le logiche stesse utilizzate dagli attori sociali. Si esplicita inoltre l'ipotesi che tali logiche siano necessarie all'attore sociale per giustificare, ossia spiegarsi ragionevolmente, delle norme sociali; si accoglie inoltre una definizione classica di norma sociale come «un insieme di regole relative a come una persona dovrebbe comportarsi - o è obbligata a farlo - in determinate circostanze»[122]. Nell'ambito della distinzione presentata da William Graham Sumner tra *folkways* e *mores*, ciò su cui deve essere concentrata l'attenzione sono i secondi:

[117]Bourdieu 1995, p. 96.
[118]Borghini 2012, p. 187.
[119]In tal senso la visione di Bourdieu è uno strumento di lettura dell'intero sociale, sebbene alcuni attori, quali lo Stato, la famiglia o la scuola contribuiscano in maniera significativamente più rilevante nella definizione dei modi di riproduzione e nella strutturazione del sociale(Bourdieu 1995, p. 33).
[120]Vedi su questo *supra*, nel paragrafo «Radiografia di un sillogismo».
[121]Bourdieu 1995, p. 149.
[122]Questa definizione è inclusa nel lavoro di Theodore Mills, che a sua volta fa esplicito riferimento a George Homans(Mills 1959, p. 672). È importante notare il semplice fatto che una norma sociale non è necessariamente giuridica, e la sanzione che può conseguirne può essere anche semplicemente morale(Toscano 2006, p. 456).

consapevoli e orientati[123], i *mores* sono strettamente connessi con la necessità di astrarre le abitudini adottate in un insieme in sé coerente[124] e non esplicitamente contraddittorio di principi.

Criminalizzazioni

L'espressione «criminalizzazione della crittografia» è evidentemente composta da due concetti, ossia la criminalizzazione, quale fenomeno sociologico, e la crittografia, quale suo oggetto. Se sul versante di ciò che è oggetto di criminalizzazione è stata già affrontata un'analisi al tempo stesso empirica e teorica per rilevare un forte legame tra crittografia oggetto di criminalizzazione e riservatezza[125], per quanto riguarda la criminalizzazione è necessario assumere la prospettiva dello Stato. Criminalizzazione è una dinamica delle norme sociali, sintetizzata nell'ingresso di alcuni comportamenti sociali nel campo della sanzione penale; tuttavia questa dinamica è in sé problematica, dal momento che richiede un interrogativo specifico sulle modalità e le condizioni in cui questo avvenga. Il punto di partenza di questo passaggio è che non è sufficiente la volontà politica di legiferare perché una criminalizzazione sia tale: ci sono vincoli di risposta e adeguatezza sociale che automaticamente si impongono e sui quali è necessario interrogarsi; è importante prendere in considerazione anche come questi «ostacoli» possano essere superati, e si suppone sia possibile in una condizione di mutamento di quelle logiche «morbide» del sociale trovate nella prospettiva bourdieusiana. Resta infine opportuno interrogarsi se l'argomento «nothing to hide» sottenda una logica di questo tipo, cosa che, nel caso affermativo, permetterebbe la delineazione di collegamento diretto tra piano individuale e piano socio-statale.

Vincoli morali

Il recentissimo dibattito negli Stati Uniti sulla raccolta massiccia di dati *internet* e telefonici da parte dell'amministrazione Obama, che ha condotto alla riforma del *Patrioct Act* attraverso un *Freedom Act* che disciplinasse nuovamente alcune pratiche per la *National Security Agency*, è stato ampiamente caratterizzato da un concreto conflitto sulla designazione dell'attività dell'*NSA* rispetto alla *privacy* e al controllo dei cittadini[126]. Il forte ancoraggio delle critiche ad un immaginario

[123]Sumner 1906, p. 38.
[124]Ibid., p. 49.
[125]Vedi *supra*, nel paragrafo «Tecnologie di rifugio»
[126]Opinione pubblica e classe politica sono state entrambe coinvolte in un aspro dibattito, al punto di rivolgere all Governo la domanda su quale sia il nesso tra la sorveglianza e le grandi promesse elettorali relative ai matrimoni *gay* o alla tutela sanitaria(Huffington Post 2015).

orwelliano[127] ha parzialmente strutturato il campo della discussione all'idea di quale attività di controllo governativo possa essere definita come *Big Brother*; è importante notare come tale critica sia stata già affrontata dall'Amministrazione USA, mettendo in campo il carattere di **selettività**[128] e di decentralizzazione del controllo sostanziale[129] dei dati[130]. Analogamente, il dibattito che ha attraversato la Francia a partire dal 19 marzo 2015, giorno di presentazione da parte del Presidente del Consiglio Manuel Valls del *Projet de loi sur le renseignement*[131], è stato caratterizzato da un forte scontro, pur agitato prevalentemente da giornalisti e gruppi di attivisti dei diritti in rete[132], nel seno dell'opinione pubblica. Da queste considerazioni risulta necessario tenere in conto due aspetti: il primo è il dato di fatto di una certa *conflittualità* o mancanza di un *consensus* tanto esteso da poter appiattire il dibattito; il secondo aspetto riguarda la questione su **chi** concretamente prenda in mano l'opposizione a tali progetti di legge, se si tratta di «addetti ai lavori» o di fasce di opinione che tagliano trasversalmente la cittadinanza.

Si possono sintetizzare le traiettorie seguite dalle condotte criminali secondo quattro linee di criminalizzazione/decriminalizzazione ed emersione/nascondimento: tra queste è di specifico interesse la prima, che riguarda il passaggio di condotte «da un'area di normalità o devianza sociale a una di criminalità sanzionata penalmente»[133]. L'ingresso di una condotta nella normazione penale può essere accompagnato da un consenso ovvero dissenso più o meno ampio, che pone degli specifici problemi riguardo la condivisione del giudizio estetico-morale sotteso dalla norma; è questa un'idea già compresa nei lavori di Émile Durkheim e Max Weber, dove è possibile trovare una distinzione concettuale tra diritto e morale,

[127] Vedi *supra*, sul ruolo di *Big Brother* come *metaphor we live by*.

[128] La selettività consiste nell'idea che, se il controllo dei *metadati* può virtualmente riguardare tutti, il controllo attivo e dedicato dei contenuti è effettuato solamente nei casi sospetti, chiamando in primo luogo in causa l'obiettivo di colpire i terroristi. La questione della selettività è più problematica di quanto non sembri a prima vista, e viene affrontata da Daniel Solove nel già citato lavoro sul *Nothing to Hide Argument*(Solove 2007, p. 752).

[129] Questo tipo di attività, che ha conosciuto un impiego sempre più esteso dopo l'11 settembre 2001, è detta *data mining*, e consiste nell'analisi dei dati personali «alla ricerca di *patterns* di comportamenti sospetti»(ibid., pp. 745-746)

[130] Fox News 2013.

[131] Ministère de l'Intérieur 2015b.

[132] Gli attivisti de *La Quadrature du Net* hanno condotto una forte opposizione al progetto di legge, appellandosi ai principi di difesa della *privacy* e dei dati personali e di libertà dalla censura in rete. Gli stessi attivisti hanno aperto una pagina *web* dedicata per informare e sensibilizzare l'opinione pubblica. Numerosi giornalisti hanno aperto campagne di opposizione al progetto di legge, in particolare nell'ambito della redazione di *Liberation*(Alonso, Léchenet e Kristianadjaja 2015).

[133] Vidoni Guidoni 2004 citato in Procaccini 2012, p. 24.

tuttavia nell'ambito di una fondamentale continuità sociologica[134]. A partire da queste considerazioni, si può ricucire l'idea di **conflitto** introdotta empiricamente nei termini di condizione in cui comportamenti e mentalità non sono oggetto di un accordo diffuso e trasversale, ma sono «legati più estesamente e con maggior forza alle appartenenze di *status groups*»[135]; in questa definizione, il concetto di *status* ha un preciso significato che affonda le radici nell'ambito estetico-morale in senso ampio in quanto, secondo gli stessi autori, specifico insieme di «attitudini morali, valori e norme»[136] che rende distinguibile quello specifico gruppo nell'ambito della situazione sociale conflittuale. Si ritrovano i medesimi elementi, pur in altri termini, in tutt'altra visione, in particolare nei *cultural goals*, le mete culturali, che ogni società fisserebbe davanti a sé secondo Robert King Merton[137]: sebbene qui l'accento sia posto su una visione direzionale della società, ciò che rileva è che tali contenuti finalizzanti abbiano una certa vocazione al coinvolgimento di tutti i membri della società[138], descrivendo un linguaggio valoriale comune di preferibilità per la descrizione delle norme sociali[139]. Affondando le mani in due visioni sociologiche così differenti si estrae criticamente un comune denominatore che, guardando indietro alla tipologia dell'adattamento individuale di Merton[140], concepisca la devianza come «un processo di azione motivata di un soggetto che [...] tende a deviare dalle aspettative che gli altri si sono fatti rispetto al suo ruolo»[141]. Tali aspettative e valori riguardano una questione di *gusto*[142] rispetto al giusto e allo sbagliato, che descrive un *continuum* nell'ambito della norma sociale che spazia «da un'idea di diversità culturale alla devianza sociale per giungere alla criminalità»[143]: il pedale continuo di quest'insieme di visioni così diverse è la sempiterna necessità nell'attività di criminalizzazione di ricondurre l'illegale

[134]Toscano 2006, pp. 429-430.
[135]Hagan, Silva e Simpson 1977, p. 322.
[136]Ibid., p. 323.
[137]Merton 1968, p. 197 e ss.
[138]Toscano 2006, p. 458.
[139]Si trova anche nella teoria di Talcott Parsons l'idea di *sistema di valori societario*, concepito da Alessandro Dal Lago come «l'insieme di mete culturali che orienta il comportamento degli attori sociali e **da cui discendono le norme** dell'azione sociale(Dal Lago 1981, p. 40, grassetto aggiunto)
[140]Tale tipologia è data da due dimensioni: la prima riguarda le mete culturali, mentre la seconda riguarda i mezzi istituzionali, in termini di condivisione, rifiuto o la sostituzione positiva. Ed è sintetizzabile(Toscano 2006, p. 459) nei comportamenti di conformità, innovazione, ritualismo, rinuncia, ribellione.
[141]Dal Lago 1981, p. 41.
[142]Si presenta qui un profondo parallelismo con i concetti di *common sense*, **comunicabilità**, gusto, *judgement* e *thinking* presentati da Hannah Arendt nella sua interpretazione della Critica del Giudizio di Kant(Arendt 1982, p. 63 e *passim*)
[143]Procaccini 2012, p. 23.

all'ingiusto e viceversa[144].

L'eccezione e le vittime

In seguito all'attacco alla sede del settimanale *Charlie Hebdo*, il governo francese ha fatto scattare il livello massimo di allerta del piano statale antiterrorismo, il *Plan Vigipirate*. Introdotto nel 1978 sotto la presidenza di Valéry Giscard D'Estaing, il piano è interamente concepito per far fronte alle minacce terroristiche all'interno del Paese e prevede, nell'ambito di una stretta collaborazione tra i ministeri, l'impiego di forze militari in vari contesti civili quali trasporti pubblici, monumenti, luoghi di culto, istituzioni pubbliche, sorveglianza nelle strade[145]. Ciò che rende eccezionale l'attivazione del livello *alerte attentat* a partire da gennaio 2015 è l'incremento massiccio di organico impiegato nell'attività di controllo: se la norma prevede un impiego di circa 1500-2500 militari, a partire da marzo 2015 François Hollande ha deciso di mantenere l'impiego di circa 10 mila militari sul suolo nazionale **a sostegno** delle forze del Ministero degli Interni[146]. Le modalità della militarizzazione del territorio sono esplicitamente affiancate all'idea della ricerca del nemico interno, il terrorista che può annidarsi in ogni luogo, ma rievocherebbero anche alcune dinamiche di «guerra civile» che hanno caratterizzato la guerra di liberazione algerina[147]. Tale specifica configurazione di riduzione del nemico globale interno sarebbe apparsa in Francia per la prima volta tra il 1993 e il 1994, inscrivendo nella vita urbana una logica di «securizzazione» delle strade e dei territori che richiamasse una volta per tutte «la sicurezza come la prima delle libertà»[148]. Del resto, la guerra al terrore è concepita come una prosecuzione sul piano esterno di dinamiche di polizia: il cittadino diventa vittima non sono della criminalità di strada, ma anche del nemico del suo stato, che si è fatto sempre più atomizzato e onnipresente, la cui ricerca può essere condotta soltanto attraverso l'intensificazione e l'estensione di pratiche di *screening* del tessuto sociale[149]. Il risultato è stato la giustificazione dell'indistinguibilità relativa del militare e del poliziotto, accompagnata dalla privatizzazione dei controlli previsti all'interno del piano antiterrorismo[150].

Tale «indistinzione» è rievocata nell'idea di «stato di eccezione» come para-

[144]Turk 1966, p. 347.
[145]Ministère de la Défense 2014.
[146]Sin dal 21 gennaio 2015 il numero di militari impiegati era stato innalzato a 7500(Le Monde 2015).
[147]Rigouste 2007, pp. 159-163.
[148]Mathiot 2013.
[149]Simon 2008, pp. 360-361.
[150]Rigouste 2007, p. 173.

digma di governo situato in una «frangia ambigua e incerta, all'intersezione fra il giuridico e il politico»[151]; stato di eccezione è dunque la condizione in cui uno Stato produce provvedimenti eccezionali, frutto di **crisi politica**, che si trovino nella «paradossale situazione di provvedimenti giuridici che non possono essere compresi sul piano del diritto»[152]. Un altro parallelismo tra criminalizzazione ed eccezione può essere individuato nell'adozione come risultato pratico da parte del primo di ciò che è invece obiettivo teorico nel secondo: il risultato finale dell'eliminazione fisica di intere categorie di cittadini[153] trova la sua realizzazione nella prospettiva dell'imprigionamento di massa[154]. L'ingresso del militare nel pieno sociale delle città, ossia il ritorno del **politico**, nel senso schmittiano del termine, nel civile, segna un passaggio chiaramente interessante nella strutturazione delle modalità di governo delle democrazie occidentali; pur non trattando in questa sede il complesso problema dell'eccezione in quanto caratteristica sempre più dominante della democrazia, ciò che questo insieme di riflessioni suggerisce è la possibilità di grossi cambiamenti in campo normativo nei periodi di crisi politica. Ogni momento di rinnovato bisogno di assicurare cura, controllo e uso della nuda vita[155] esposta al pericolo, impone la questione della riorganizzazione nella forma di governo più adeguata a fronteggiare il pericolo[156].

Riprendendo l'ipotesi della vocazione al continuo affiancamento del legale al morale, ripresa in Weber e Durkheim, è possibile riallacciare l'aspetto emergenziale della guerra globale al terrore e quello normativo della criminalizzazione della crittografia[157] all'idea di morbidità delle logiche sociali introdotta a partire dal lavoro di Bourdieu[158]. La legislazione di urgenza che ha storicamente fatto seguito a forti eventi traumatici sembra aver goduto di una situazione di aumentata morbidità delle logiche, a partire dal *Patriot Act* del 26 ottobre 2001[159], che sembrerebbe

[151]Fontana 1999, p. 16, citato in Agamben 2003, p. 9.
[152]Ibid., pp. 9-10.
[153]Ibid., p. 11.
[154]Garland 2001, pp. 179-181.
[155]Il concetto di *nuda vita* è ripreso da Agamben attraverso un approccio storico-etimologico della distinzione semantica e morfologica dei termini *zoé*, ossia il «semplice fatto di vivere comune a tutti i viventi», e *bios*, ossia «la forma o maniera di vivere propria di un singolo o di un gruppo». La nozione biopolitica sorge dal momento in cui il potere politico si fondi sulla separazione della nuda vita (originariamente *zoé*, poi storicamente indicato dal prefisso «bio») dal contesto delle forme di vita(Agamben 1996, pp. 13-14).
[156]Ek 2006, p. 368.
[157]Si ricorda qui l'esplicito riferimento, nell'ambito di tale dibattito, agli attentati di Parigi del gennaio 2015(Zezima e Jaffe 2015).
[158]Il lavoro di Edwin Sutherland sull'origine delle *Sexual Psychopath Laws* metteva in evidenza il forte ruolo giocato dalla «manipolazione dell'opinione pubblica da parte della stampa e dall'influenza degli esperti nel processo legislativo»(Jenness 2004, pp. 147-148).
[159]Jonathan Simon riporta che è stato ampiamente riconosciuto come il testo della legge non sia stato letto «dalla grande maggioranza dei membri del Congresso che lo hanno votato, se non

essere determinata da quella condizione di «vittimizzazione» che avrebbe avvolto progressivamente, secondo Jonathan Simon, gran parte delle soggettività sociali, arrivando infine a configurarsi come una politica di riconoscimento[160]; ed è infine lo stesso Simon a sostenere che le vittime, con il loro carico di **vulnerabilità** e bisogni, delineino «le condizioni ideali per l'intervento del governo»[161].

Presunzioni di Colpevolezza

Ricostruito il campo concettuale di esistenza sociale dello Stato attraverso una specifica ontologia dello stesso, introdotto l'approccio teorico della criminalizzazione e la sua necessità di confrontarsi con delle logiche concrete e individuabili, il discorso può chiudersi sulla ricerca di queste logiche. Questo capitolo cerca inoltre di trovare l'incontro, nello stesso punto di intersezione, non solo del filo delle modalità di azione statale con l'elemento logico dell'argomento *Nothing to Hide*, ma anche con il piano individuale, arrivando ad individuare nell'argomento *NTH* un'autentica cinghia di trasmissione concettuale sul piano sociale tra individuo e stato. Ritrovare un tutto coerente a partire dalle due riflessioni inizialmente distinte sulla riservatezza dell'individuo e sull'attività di criminalizzazione da parte dello Stato permette infine di chiudere sui significati sociali in senso ampio che quest'ultima porta con sé, delineando una «presunzione di colpevolezza» in un rapporto assolutamente particolare con l'idea di affidamento all'attività di controllo.

Questione di logiche

Nel riprendere la questione sulle condizioni valoriali che contornano l'attività di criminalizzazione, si introduce automaticamente una concezione del comportamento deviante che debba escludere il carattere di «irrazionalità»: in questa idea si inscrive la critica di Alessandro Dal Lago alle teorie storiche della devianza, che vede per l'appunto un abbattimento impietoso di alcune concezioni che guardino alle devianze come a semplici prodotti dell'irrazionalità e della mancanza di educazione, ritrovandovi invece una «capacità di prefigurare nuovi rapporti socia-

tutti»; frutto questo di un senso di trauma che spiegherebbe anche quella mancanza di interesse di popolo americano e Congresso verso gli scandali di Abu Ghraib e Guantánamo(Simon 2008, pp. 354-355).

[160]Charles Taylor affronta il problema identitario in termini di riconoscimento da parte del tutto sociale che circonda l'individuo(Taylor 1994, *passim*). Pur nella distanza in termini accademici e metodologici, Simon non sembra discostarsi troppo dall'idea di Taylor nel definire esplicitamente la «vittima» come un'identità specifica e ben determinata(Simon 2008, p. 98).

[161]Ibid., p. 98.

li»[162]. Quest'idea deve valere *a fortiori* per dei soggetti che, trovandosi in una situazione deviante, giustificano apertamente[163] le ragioni della propria condotta nella sfera pubblica[164]. Allo stesso tempo è necessario escludere il carattere di irrazionalità dell'azione statale di criminalizzazione: il bisogno, per un sistema di controllo, di legittimarsi continuamente richiede un'apposita discorsività non riferita al controllo di fatto esercitato dall'autorità, bensì rivolta al sistema di norme sociali in cui esso opera; l'oggetto della norma penale deve incontrare «immagini, convinzioni e spiegazioni accettate»[165], pena il deterioramento del *range* di controllo[166] o l'inefficacia del discorso elettorale stesso. Dunque, ammesso da una parte il rapporto stretto tra concezioni morali, condotta deviante e criminalizzazione[167], introdotta inoltre l'idea di «logiche morbide» che abitano il sociale[168], si riallacciano i fili del discorso sul problema delle logiche che sottendano un certo intento di criminalizzazione. Secondo tali premesse, l'argomento *NTH* porta con sé una logica esplicita che offre uno specifico punto di appoggio argomentativo per la legislazione sul controllo e sull'*intelligence*, dunque anche per il caso più specifico della crittografia.

È stato già anticipato[169] come l'argomento «*if you've got nothing to hide, you've got nothing to fear*» sia stato presentato come un vero e proprio sostegno di carattere logico-argomentativo ai provvedimenti presi in seguito ai tragici eventi dell'11 settembre 2001. A questo punto diventa inoltre chiaro come l'argomento *NTH* sia strettamente legato al meccanismo di logiche morbide e norme sociali individuato nel corso di questa sezione, rivelandosi dunque incastonato nel discorso sociale sulla criminalizzazione. Esso costituisce un'autentica cinghia lo-

[162]In tal proposito, la critica di Dal Lago è principalmente rivolta alla capacità delle teorie sociologiche della devianza di spiegare i fenomeni delle bande e della criminalità di quartiere, soltanto parzialmente inclusi dall'approccio di Merton. Alla devianza deve essere restituita una dignità positiva proprio in risposta ai tentativi di esorcizzazione seguiti dai positivismi degli anni '50 e '60(Dal Lago 1981, p. 62).

[163]Potremmo attribuire a questa categoria più specifica l'idea di «political crime», in quanto la devianza è strutturata attorno a un conflitto «tra coloro che cercano di mantenere una data struttura di autorità e coloro che cercano di modificarla o distruggerla»(Turk 1966, p. 339), considerando all'interno dell'idea di «struttura di autorità» anche il campo di estensione della stessa. In generale si potrebbe sostenere che è necessario ammettere la possibilità di restituire una spiegazione e un significato della condotta deviante come presupposto epistemico-metodologico per lo studio della devianza(Hagan 1986, p. 432).

[164]Vedi *supra*, sugli ambiti di opposizione al Progetto di Legge sull'*Intelligence* in Francia.

[165]Mills 1959, p. 676.

[166]L'aspetto dell'intima convinzione della giustezza della norma è considerato elemento fondamentale perché essa sia applicata nell'insieme dei livelli sociali oggetto di controllo(Turk 1966, p. 349).

[167]Vedi *supra*, nel paragrafo «Vincoli morali».

[168]Vedi *supra*, nel paragrafo «Istituzionalizzazioni».

[169]Vedi *supra*, nel paragrafo «Radiografia di un sillogismo».

gica di trasmissione tra livello individuale e statale proprio grazie ad un ulteriore elemento di forza argomentativa che rende più chiara la sua ampia diffusione: il bilanciamento, come tecnica giuridicamente accettata nei nostri ordinamenti di risoluzione del conflitto tra due diritti. Nello spazio giuridico è possibile individuare immediatamente i due termini in giustapposizione, diritto individuale alla *privacy* e diritto collettivo alla sicurezza sono i termini che incorrono nel dibattito indicato[170]. È proprio in sede di bilanciamento di diritti che l'argomento *NTH* arriva a rendere irrilevante il diritto alla *privacy*, prefigurando per il diritto collettivo alla **sicurezza** una facile vittoria[171]. Del resto è difficile resistere alla forza del «bilanciamento dei diritti» e, probabilmente, l'unico modo per portare il discorso altrove consiste nell'evadere il campo giuridico. Dal Lago nota come abbiamo assistito ad un processo di «de-eticizzazione» nelle società contemporanee, dove la giustizia in quanto istituzione ha acquisito sempre più la pretesa di una validità intrinseca: il **consenso** ricercato è dunque prodotto in fase procedurale formale[172].

Introdurre nuovi concetti, in particolare quello di *riservatezza*, che siano autonomi rispetto allo spazio simbolico giuridico, sembra permettere l'abbandono del campo giuridico come sede del discorso, aprendo la possibilità di guardare dall'esterno le dinamiche stesse del dibattito giuridico: *nothing to hide* diventa così una logica relativa al rapporto tra riservatezza e criminalizzazione non univoca e non necessaria, probabilmente destinata a vincere all'interno del campo giuridico proprio in quanto tale campo si struttura per diritti, anteponendo logicamente il fatto che essi siano protetti da parte di uno Stato; in questo senso l'argomento *NTH* potrebbe essere considerato un esempio di *pensiero di Stato*, nel senso dato da Bourdieu, possibile attraverso lo Stato e, ad un tempo, produttivo del concetto stesso di Stato[173].

Fiducia e affidamento

Un'ultima riflessione sull'attività di criminalizzazione riguarda i concetti sociali extra-giuridici che questa porta con sé. Leggere nei nuovi termini introdotti la penalizzazione dell'uso di tecniche crittografiche significa, in conclusione, vedere in tale attività legislativa la sanzione della possibilità per lo stato di penetrare le

[170]Il bilanciamento tra libertà e sicurezza è l'arma giuridica adottata in materia di *privacy* e antiterrorismo dall'Autorità garante per il diritto alla *privacy* in Italia(Garante per la Protezione dei Dati Personali 2014).

[171]Solove 2007, p. 747.

[172]Dal Lago 1981, p. 68.

[173]Bourdieu nota come, in tali dinamiche, «il nostro pensiero, essendo in gran parte il prodotto del suo oggetto, non riesce più a percepirne l'essenziale e, in particolare, tale relazione di appartenenza del soggetto all'oggetto»(Bourdieu 2012a, p. 149).

spazialità che, potenzialmente, gli individui potrebbero o vorrebbero conservare. Ciò che è stato introdotto, di nuovo, fino a questo punto è che, in questa lettura, non si tratta più di rilevare quali diritti vengano astrattamente lesi, ma di individuare che certi bisogni possono essere compressi, limitati, o impediti dall'attività statale; la possibilità inedita di fronteggiare efficacemente la possibilità di controllo dei messaggi e delle informazioni da parte del cittadino è al tempo stesso possibilità reale di ricostruzione di spazialità individuali di riservatezza che, in questi termini, viene penalizzata. In termini espliciti, si afferma che l'attività di criminalizzazione non comporta semplicemente la compressione di un diritto formalmente e storicamente definito, ma un'attività basilare di «ritrazione»[174] trovata a partire da considerazioni antropologiche[175]. Il risultato atteso è stato dunque quello di una «riabilitazione del valore sociale della *privacy*»[176], quel valore sociale probabilmente caduto nel confronto con il sempre più permeante potere legittimante del diritto[177].

La logica sottesa al *NTH*, in rapporto dialettico con lo sforzo di «criminalizzazione» sembra infine risolversi in una fondamentale «presunzione di colpevolezza» già facilmente individuabile in alcuni significativi precedenti legislativi, primo tra tutti il *Foreign Intelligence Surveillance Act* del 1978, che autorizza la *NSA* a conservare i messaggi e, in generale, i dati cifrati intercettati per tutto il tempo necessario a decrittarli, ossia illimitatamente[178]; questo significa semplicemente che un messaggio cifrato intercettato dall'*NSA* può essere salvato sui server dell'Agenzia soltanto per il fatto che è cifrato: dalla forma cifrata si estrae dunque un sospetto sulla liceità del contenuto, cosa possibile solo e solamente a partire dal presupposto logico di equazione totale tra il *secretum* e lo sbagliato[179] presupposto dall'argomento *NTH*.

Tutto questo insieme di condizioni porterebbe, secondo Jeffrey Vagle, alla lesione di un fondamentale rapporto di mutua *fiducia* tra governo e cittadini; rapporto che costituirebbe un principio fondamentale dell'ordinamento, tale da fare da guida per l'interpretazione stessa del disposto costituzionale[180]. Alcuni difen-

[174]Si riprende qui la diade interazione-ritiro di Simmel presentata *supra*, nella prima sezione.
[175]La potenza del concetto di riservatezza costruito appare in questo momento in cui, forte della sua derivazione concettuale da forme ben evidenti e largamente riconosciute delle modalità dell'interazione sociale, può sfuggire l'ambito di discussione giuridico ed inserirsi in pieno in un dibattito fino a questo momento dominato dal concetto giuridico di *privacy*.
[176]Questo è il titolo di un *paper* di Valerie Steeve, che prende in analisi il tentativo di Alan Westin alla luce di alcune riflessioni nell'opera di George Herbert Mead(Steeves 2009, *passim*).
[177]Dal Lago 1981, p. 68.
[178]Vagle 2015, p. 104.
[179]Vedi, su questo, *supra*, nel paragrafo «Riservatezza oltre il diritto».
[180]Vagle 2015, p. 124.

sori della *privacy* nel dibattito sulla criminalizzazione e la penalizzazione delle pratiche crittografiche, così come sul controllo e la sorveglianza, stanno facendo di questo aspetto un punto forte di ancoraggio del discorso; tuttavia sembra problematico riuscire a fare del concetto a due facce della «mutua fiducia» una vera arma concettuale, proprio per la sua bilateralità e, in campo giuridico, plasticità continua nell'ambito dell'attività di bilanciamento dei diritti. Infine, se è vero che numerose sentenze della Corte Suprema hanno sancito questo principio come fondamentale «per ogni società democratica», la storia stessa della Corte Suprema sembrerebbe insegnare come sia possibile osservare dei cambiamenti e delle evoluzioni talvolta più che significative dei principi e delle gerarchie in cui essi stessi sono collocati.

Appendice: Apparati privati di sicurezza

Lo spazio sociale sino ad ora disegnato vede però un altro attore significativamente attento alla questione sulla riservatezza e la gestione di dati: le grandi aziende private dei servizi *internet*. In questa breve appendice si cerca così di tracciare i termini essenziali della questione, in particolare per comprendere se, e in che modo, gli interessi di grandi aziende come *Google*, *Facebook* o *Yahoo* possano entrare in conflitto con le dinamiche di criminalizzazione delle tecniche crittografiche. L'utilizzo e l'analisi dei dati degli utenti in rete è un elemento fondamentale del *business* strutturatosi negli ultimi anni attorno ai servizi in rete. *Account* di posta elettronica, motori di ricerca, *social network*, notizie, *chat*, pagine *web* personali, sistemi operativi per *smartphone*[181], sono messi a disposizione da aziende come *Google* e *Facebook* senza alcun costo da sostenere da parte dell'utente. Il prezzo da pagare è, paradossalmente, l'utilizzo stesso di tali strumenti: in questo modo le informazioni che emettiamo, altrimenti caoticamente disperse in rete, possono essere canalizzate, analizzate, fatte fruttare. Da tale fondamentale dinamica derivano alcuni problemi in ambito di protezione della *privacy* degli utenti, a tal punto che le stesse aziende hanno cominciato ancor più paradossalmente a fornire servizi di gestione sicura dei dati degli utenti: la sicurezza e la *privacy* diventano così un servizio. Questo secondo momento sembrerebbe rivelare però una contraddizione rispetto alla dinamica di criminalizzazione della crittografia, la cui risoluzione può essere solo debolmente ipotizzata.

La rincorsa ai dati

La maggior parte dei servizi *internet* utilizzati dall'utente medio, una volta concluso un contratto con un fornitore di servizio per l'accesso alla rete *internet*, sono in sé gratuiti: le grandi multinazionali della rete internet assicurano perlopiù servizi di qualità discreta, intuitivi ed efficienti, in modo totalmente o parzialmente gratuito. La maggior parte dei guadagni di queste aziende deriva in realtà dalle pubblicità[182] inserite nelle pagine web con le quali si interfacciano gli utenti[183].

[181] Google Inc. 2015c.

[182] I servizi di pubblicità costituiscono il 90% dei profitti di Google: per il 2015 questi hanno configurato un guadagno netto di $59.624 mln su di un ammontare delle entrate totali di $66.001 mln(Google Inc. 2015a).

[183] Il colosso dei *social network* Facebook Inc. realizza attraverso le pubblicità una porzione che va dal 90% al 95% del bilancio totale(Facebook Inc. 2015). Quando nel 2011 ha introdotto un proprio sistema di pagamenti attraverso una propria valuta, *Facebook Credits*, l'azienda ha puntato sull'abbassamento della percentuale di guadagni derivati da pubblicità(Womack 2011); tuttavia, tale prospettiva ha visto soltanto la fine del servizio di valuta interna, con la chiusura totale del servizio di pagamenti(Cohen 2013).

Il contenuto pubblicitario è personalizzato attraverso l'analisi delle informazioni che essi lasciano su di loro proprio mentre navigano o scambiano *mail*. Ciò porta a tre *conseguenze* principali: la prima è che la progressiva personalizzazione di servizi come, ad esempio, un motore di ricerca, porta alla chiusura dell'utente in una «bolla», al di fuori della quale ci sono tutte le informazioni che il suo servizio internet reputa non interessanti per lui; la seconda riguarda l'interesse radicale nell'accesso ai dati da parte dei nuovi grandi colossi di *internet*, cosa che implica anche i principali problemi a livello di privacy; la terza riguarda invece lo *sforzo tecnologico* compiuto da queste aziende, alla continua ricerca di metodi computazionali che permettano loro di abbassare il grado di entropia dell'enorme mole di informazioni pescate dal massiccio e continuo flusso di pacchetti leggibili attraverso i loro server.

Personalizzazione e *Filter Bubble*

Come già anticipato, bisogna tenere in considerazione il fatto che parlare di pubblicità in questo ambito significa fare riferimento a qualcosa di radicalmente diverso rispetto alla concezione tradizionale delle pubblicità della televisione o dei grandi cartelloni nelle città; si parla prevalentemente di *targeted advertising*, ossia l'utilizzo di specifici vettori mediatici che consentano al produttore di indirizzare la pubblicità verso specifici segmenti del mercato, in una condizione di migliore conoscenza delle preferenze dei consumatori attraverso i segmenti stessi[184]. Il *targeting* è un obiettivo concreto per le agenzie pubblicitarie, dal momento che permette di abbattere i costi di esposizione della pubblicità restituendo un incremento notevole dei suoi tassi di successo[185].

Un altro aspetto molto importante riguarda l'evoluzione dei motori di ricerca nel *world wide web*: l'esplosione di *Google* ha segnato un'evoluzione storica nell'ambito, con un passaggio alla seconda generazione dei motori di ricerca. I risultati restituiti dalle ricerche su Google, ad esempio, tendono a variare da utente a utente, sulla base delle sue caratteristiche desunte dalla cronologia, dalle ricerche precedenti, e ogni altro tipo di informazione utile a disposizione del motore stesso. Si tratta di un fenomeno di progressiva personalizzazione[186] dei risultati restituiti dallo strumento, ad oggi vero e proprio punto di forza e parametro di valutazione dell'efficienza dello stesso.

[184]Iyer, Soberman e VIllas-Boas 2005, p. 466.

[185]In tal senso si parla anche di *behavioral targeting*, ossia di indirizzamento verso categorie comportamentali di individui che siano potenzialmente più interessati a quello specifico prodotto: è la possibilità di rendere reale questa semplice dinamica ad incrementare i tassi di successo della pubblicità(Beales 2010, p. 7).

[186]Carpineto e Romano 2005, p. 28.

La **personalizzazione** è dunque qualcosa che caratterizza sempre più la presenza degli utenti in rete, sia nell'aspetto dei servizi forniti, che in quello pubblicitario. Una conseguenza di tale processo è la creazione di *filter bubbles*, bolle all'interno delle quali si trova ciò che un qualche algoritmo valuta per noi utile e interessante, mentre al di fuori si trova ciò che sembra meno utile al nostro profilo[187]: si tratta dunque di un problema di selezione ma al tempo stesso limitazione delle possibilità di accesso ad alcuni contenuti in rete[188]. Sorgono inoltre degli evidenti problemi relativi alle possibilità di nascondimento di alcune tematiche specifiche, come nota Eli Pariser, l'attivista e studioso che ha coniato l'espressione «*filter bubble*»[189]. Altra considerazione è che ogni attività di personalizzazione implica la necessità di analizzare grosse moli di dati per procedere principalmente ad operazioni di *profiling*, senza escludere i contenuti delle comunicazioni, alla ricerca di parole chiave ed elementi significativi che permettano di collocare un certo utente all'interno del giusto segmento di mercato. È proprio questa dinamica di *data mining*, analisi approfondita dei contenuti dei dati, che introduce ai problemi principali per quanto riguarda la *riservatezza*[190]; il *profiling* è per questo motivo il principale obiettivo degli avvocati e studiosi che si occupano di *privacy* nell'ambito dei servizi in rete[191].

Computazioni

Questo processo di continua personalizzazione dei contenuti richiede una grandissima capacità di computazione per l'analisi dei dati utili alle profilazioni. I grandi colossi dei servizi *internet* hanno intrapreso dei progetti enormi in campo informatico, che sembrerebbe possibile sintetizzare in due tipi di problemi: da una parte la necessità di estendere in termini di potenza delle attività essenzialmente umane[192], dall'altra quella di ridurre la complessità di problemi matematici molto difficili[193]. Sembrerebbero delinearsi due strade di sviluppo tecnologico, la prima attraverso lo sviluppo di tecnologie computazionali basate sul concetto di «reti neurali», la seconda attraverso la ricerca nell'ambito della computazione quantistica.

[187] Lazar 2011.
[188] Kamin 2011.
[189] Pariser 2012.
[190] Gould 2014.
[191] Worley 2010.
[192] Il *profiling* è solo uno, per quanto significativo, di questo tipo di problemi, che riguarda l'estrazione di caratteristiche ed elementi relativi alla personalità dell'utente a partire dal flusso lirico dei dati che questo lascia «dietro di sé» mentre naviga in rete.
[193] Un esempio significativo è, per l'appunto, la fattorizzazione di numeri primi, che permetterebbe di risalire alle chiavi private utilizzate per la cifratura dei dati con algoritmo RSA.

Per quanto riguarda la via delle *reti neurali*, si parla di *machine learning*, la capacità di tali macchine di apprendere «categorie» a partire dal flusso disordinato dei dati in ingresso[194]: come il cervello umano, riescono a simulare la possibilità di «riordinare» il mondo, restituendo dati ad un livello di entropia più basso rispetto a quelli in ingresso. Il tipo di operazioni ricercato sembra del tutto analogo a quello che sta alla base del *crowdwork*, lavoro della folla, un insieme di progetti lanciati da alcune aziende, tra cui *Amazon*, che vedono come lavoratore praticamente chiunque voglia creare un *account*: ciò che viene richiesto è di effettuare *Human Intelligence Task*, ossa piccole operazioni banali che, tuttavia, sono molto difficili per delle macchine, come l'inserimento di commenti verosimili, valutazione di risultati dei motori di ricerca, ricerca di duplicati, valutazione degli stati d'animo, classificazione o valutazione di immagini e fotografie complesse[195]. La classificazione e l'analisi di grandi moli di dati ad alto livello di entropia sembra così essere l'obiettivo dei grandi studi per l'utilizzo di macchine che usino tecniche di «deep learning», apprendimento profondo[196].

La via della computazione quantistica[197] invece riguarda tutt'altro tipo di problemi: non si tratta di costruire macchine in grado di apprendere, ma strumenti computazionali in grado di risolvere problemi molto complessi. Teoricamente, la computazione quantistica permette di ridurre il numero di operazioni necessarie per risolvere alcuni problemi matematici come, ad esempio, la fattorizzazione dei numeri primi, di un ordine 2^n, con n numero di atomi utilizzati in una computazione che sfrutti le loro proprietà quantistiche[198]. Come già scritto *supra*, il problema alla base dell'algoritmo di cifratura RSA è di questo tipo.

Entrambe queste tecnologie rilevano fortemente del nostro concetto di riservatezza. Le reti neurali permettono un'estrazione dell'**informazione**[199] da un flusso discontinuo e altamente entropico di dati e pacchetti: si tratta di un caso in cui la nozione di «controllo» sull'informazione emessa delineata nella prima parte risulta coinvolta in pieno, proprio per l'attenzione posta dal lato di chi osserva, anziché

[194]Smith 2003.
[195]Wikipedia 2015.
[196]A titolo di esempio, il progetto *Google Brain* punta a diventare una vera e propria intelligenza artificiale, in grado di compiere operazioni fino a pochi anni fa ritenute quasi impossibili per una macchina(Markoff 2012).
[197]Simonite 2014.
[198]Barenco 1998, pp. 144-151.
[199]Sebbene il concetto di informazione venisse da Garfinkel applicato a casi davvero corporei: per esempio «quando un suicida è tale?», non è difficile immaginare che negli anni tale idea ha fatto molta strada anche in altri ambiti. Le aziende con la possibilità di gestire enormi moli di dati di rete sanno bene che questi sono tali in quanto interpretati, cioè in quanto ordinati, categorizzati a partire dall'informazione disponibile.

su quello di chi la emette[200].

La dolce tutela

Il momento in cui una discorsività completamente nuova sulla privacy e sulla sorveglianza comincia a investire tanto i governi quanto aziende come Google, può essere collocato nel 2009. Quell'anno, un ufficiale dell'*intelligence* dell'esercito statunitense, Chelsea Manning, invia a Julian Assange, che dal 2006 dirige il progetto *Wikileaks*, centinaia di documenti estratti dagli archivi militari USA, in particolare sul bombardamento aereo di Baghdad nel 2007, sulle guerre in Afghanistan e Iraq o sulla gestione di *Guantànamo Bay*. A partire da questo momento, la questione della gestione dei dati si interseca con quella sui segreti di stato ed emerge un **parallelismo** tra possesso delle informazioni e possibilità di sapere, controllare, sorvegliare: nell'occhio del ciclone delle successive rivelazioni di Edward Snowden si trova la collaborazione di Facebook, Google e altre compagnie con la *National Security Agency* statunitense[201]. La risposta dei colossi del *web* è consistita, di fronte alle accuse di violazione della privacy, nell'avvio di progetti che fanno della protezione dei dati degli utenti un obiettivo esplicito: la sicurezza diventa così un servizio, la protezione dei dati gettati nella *cloud* è affidata a mani esperte. Il risultato sarebbe confusamente contraddittorio se si ignorasse che la protezione dei dati non è affidata all'utente, ma all'azienda stessa che, limitandosi ad escludere efficacemente ogni altro osservatore, può continuare a godere dell'accesso di cui ha bisogno. Si delinea un conflitto così tra la protezione dei dati, diventata ora un vero e proprio servizio, e la criminalizzazione stessa della crittografia.

La sicurezza come servizio

Non è facile dipanare la spessa coltre di nebbia che avvolge quelle grandi aziende private che si trovano, in qualche modo, a gestire grandissime moli di dati personali. Con l'esempio significativo, nonché più importante, di Google, risulta difficile capire se, e in quali termini, l'azienda abbia rapporti con la *National Security Agency* statunitense, in quali modi acconsenta alle richieste dei governi di accesso ai dati personali o ai contenuti delle conversazioni degli utenti; la maggior parte

[200] Vedi *supra*, un'analogia può darsi con il caso dell'uomo che si reca in banca: così come diventano distinguibili le situazioni in cui questi è potenzialmente visto, nel tragitto, da tutti coloro che si trovano lungo il percorso, e quella in cui entra nello spazio di registrazione di telecamere, allo stesso modo si distingue la situazione in cui le informazioni sono semplicemente trasmesse in chiaro e quella in cui queste, nella medesima forma, transitino per delle macchine che operino *de facto* su di esse un'analisi lirica e complessa per estrarne dati ad un basso livello di entropia.

[201] Tréguer 2015.

delle ipotesi si perdono nell'ardua difficoltà della dimostrazione di rapporti così complessi. Ciò che è possibile sapere è che un'azienda come Google ha intrapreso un'impegnativa attività di *lobbying* sul congresso statunitense, senza però poter concludere su quali siano i contenuti sostanziali di questa attività di pressione[202].

Nel 2009, di fronte alle accuse di lesione del diritto alla *privacy* dei propri utenti, in particolare per quanto riguarda il servizio di posta elettronica, l'amministratore delegato di Google, Eric Schmidt, rigetta le accuse dichiarando che «se hai qualcosa che non vuoi che nessuno conosca, forse non dovresti farla, in primo luogo», riprendendo la medesima logica dell'argomento *Nothing to Hide*, analizzato *supra* in questo lavoro; in più, lo stesso Schmidt ammette che ci sono casi in cui l'azienda è forzata a **rilasciare** dati personali[203]. Ma di fronte a questo scenario, si può vedere come Google ha lanciato tutto un insieme di contenuti di *marketing* esplicitamente improntati al problema della sicurezza: la possibilità di mantenere un sistema di *cloud* estremamente sicuro e protetto dagli attacchi esterni[204], permette a questa azienda di fare della gestione dei dati un autentico servizio[205]. Il servizio di sicurezza è interessantissimo dal punto di vista tecnologico[206], ma ancora di più lo è da quello politico: non è mai l'utente a cifrare i propri dati, che vengono consegnati a Google in chiaro, ma sarà l'azienda a preoccuparsi della loro protezione, tenendo verosimilmente ben ferma la possibilità di accedervi. Dello stesso tenore sembra essere tutto un insieme di implementazioni di funzioni di *privacy* e sicurezza in Facebook, così come studi che cercano di trovare una convergenza tra utilità e *privacy* nell'ambito dei *social network*[207].

Conflitto e conciliazione

Si delinea così una conflittualità debole attorno alla questione della sicurezza; la domanda che si pone immediatamente riguarda la possibilità per l'attività di protezione dei dati, di conciliarsi con l'esigenza, per le autorità governative, di poter leggere contenuti e messaggi scambiati. Questo problema, qui irrisolto, consente di aggiungere un altro tassello all'analisi affrontata nelle parti precedenti di questo

[202] Consistente in una spesa di circa 15 milioni di dollari l'anno, il *lobbying* di Google è finalizzato, secondo quanto dichiarato dall'azienda stessa in un suo *disclosure document*, a spingere per «*legislative efforts to clamp down on aggressive patent litigation, a push to allow skilled immigrants to more easily stay in the United States, net neutrality, tax reform and broadband deployment, the company said in its disclosure statement*»; tuttavia una grande sfida dell'azienda sembra essere quella di evitare di dover fronteggiare le forti sfide in materia di *antitrust* che sta affrontando in Unione Europea(Bartz 2015).

[203] Metz 2009.

[204] Rowinski 2011.

[205] Google Inc. 2015b.

[206] Buffington 2015.

[207] Vedi, ad esempio, Guo e Chen 2012.

lavoro: si è visto come la criminalizzazione abbia come oggetto tutto un insieme di tecniche utilizzate a livello **autonomo** per la protezione dei propri messaggi e dei propri dati, ma qualcosa sembra cambiare nel momento in cui la responsabilità di metterli al sicuro viene delegata a qualcun altro. È ampiamente riconosciuto e dibattuto il fatto che numerose autorità governative inviino a compagnie di tecnologia e informazione richieste[208] relative ai dati personali degli utenti: Google dichiara di aver ricevuto, nella seconda metà del 2014 più di 30.138 richieste riguardanti più di 50.585 account, delle quali il 63% è risultato nel rilascio di qualche dato personale[209].

Nella sua battaglia di immaginario alla crittografia, David Cameron ha dichiarato che non dovrebbe esistere alcun mezzo di comunicazione che le autorità governative non possano intercettare per leggerne i contenuti: la soluzione sarebbe così l'introduzione di «*back-doors* nei programmi utilizzati per la cifratura che permetta un accesso «laterale» da parte degli inquirenti o delle autorità governative. Il problema emerge chiaramente rispetto a due aspetti principali: il primo è che l'inserimento di queste *back-doors* comporta essenzialmente delle falle di sicurezza nel codice sorgente che vanificherebbero l'utilizzo stesso del programma; il secondo è che tale disposizione richiederebbe ad ogni *software*, per adempiere ai criteri di legge, di avere un codice sorgente inaccessibile, in modo tale da non poter individuare la *back-door*. Sembra chiaro come a prima vista queste dichiarazioni da campagna elettorale non possano concretamente applicarsi[210]; tuttavia sembrerebbe possibile immaginare queste *back-doors* come **reali** porte sul retro. L'idea che potrebbe dischiudersi dall'intera dinamica qui descritta proverrebbe

[208]Le richieste possono essere di vari tipi: ordini di tribunale, richieste di emergenza, tabulati e metadati relativi agli utenti, intercettazioni, mandati di perquisizione, mandati di comparizione, richieste di conservazione dati(Google Inc. 2015d). L'ONG statunitense *Electronic Frontier Foundation* stende ogni anno un rapporto sulle pratiche di *privacy* e trasparenza adottate dalle aziende riguardo all'accesso dei governi ai dati dei loro utenti; EFF prende in considerazione cinque aspetti principali(Cardozo et al. 2014, pp. 5-6) per la valutazione delle pratiche dell'azienda:

1. Necessità di un mandato emesso da un giudice per acconsentire all'accesso dei contenuti delle comunicazioni;
2. Informazione degli utenti sulle richieste ricevute dalle autorità governative;
3. Pubblicazione periodica di rapporti di trasparenza;
4. Pubblicazione di linee guida sulle risposte da fornire alle autorità governative che presentino richieste;
5. Azioni delle compagnie in sede giudiziaria a favore della *privacy* dei propri utenti;
6. Pubblica opposizione alla sorveglianza di massa.

[209]Google Inc. 2015d.
[210]Doctorov 2015.

così dal processo stesso di «privatizzazione» della sicurezza[211], consistente in un affidamento cieco dei dati in chiaro alle grandi *cloud* degli specialisti della sicurezza i quali, a loro volta, possono diventare un canale diretto per le autorità governative ai dati personali degli utenti[212]. Tale dinamica di *alienazione* dei dati, e ancor più quella dei rapporti possibili tra governo e azienda, se reale è ancora in fase di affermazione, una suggestione che sgorga dall'impianto logico adottato in questo lavoro. Rimane la necessità di attendere la pubblicazione di ulteriori notizie, nonché approfondire e affinare gli strumenti sociologici di analisi per una sempre maggiore comprensione del campo sociologico strutturato attorno alla crittografia e alla sua criminalizzazione. Tuttavia, successivamente agli attentati di Parigi sembra essere avvenuto un processo di catalizzazione di questa dinamica: il ministro degli Interni francese Bernard Cazeneuve ha annunciato il 20 aprile di aver concluso un accordo con Microsoft, Google, Facebook, Apple, Twitter e i principali fornitori di servizio *internet* francesi sulla rimozione rapida dei contenuti propagandistici segnalati dal ministero attraverso un «gruppo di contatto permanente tra ministero e operatori»[213]; si registra poi nei medesimi accordi una pressione crescente dei governi, in particolare quelli di Regno Unito, Francia e Belgio, operata al fine di costringere questi attori privati a retrocedere sull'idea di implementare tecniche di cifratura *end to end* nei loro servizi[214].

[211] Un'analogia interessante può essere trovata nel lavoro di Jonathan Simon, con l'affermazione progressiva di una mentalità della fortificazione(Simon 2008, pp. 366-367), seppur qui ritrovata in modalità del tutto peculiari.

[212] Sarebbe dunque sensato raccogliere la considerazione di Julian Assange rispetto a Google come «problema politico»(Keane 2015).

[213] Cassini 2015.

[214] In particolare l'attacco è stato rivolto a *Whatsapp*, che ha annunciato di voler rendere cifrare le *chat* dei propri utenti(Tréguer 2015), proprio qualche mese dopo l'annuncio del superamento della quantità dei messaggi globalmente inviati attraverso il programma rispetto a quelli scambiati via SMS(Sparkes 2015).

Conclusioni

Questo lavoro ha avuto come obiettivo quello di studiare un fatto sociale, la possibilità di criminalizzazione della crittografia, con metodologia e strumentazione concettuale sociologiche; questo significa che sono state ricercate e adottate quelle nozioni che sembrassero più adeguate a leggere in maniera ricca e significativa il fenomeno. A tal proposito il lavoro è stato principalmente tagliato su due piani: quello individuale e quello collettivo. Per quanto riguarda il piano individuale, si è cercato di dimostrare come l'utilizzo autonomo di tecnologie crittografiche sia strettamente legato alla possibilità di difendere le proprie informazioni personali in modo efficace: tuttavia si è reso necessario un articolato percorso di costruzione teorica del concetto di *riservatezza*, data la carenza in letteratura sociologica di un concetto parallelo a quello di *privacy*. Le caratteristiche sul ruolo dello Stato sono state invece estratte da una lettura che affondasse le proprie radici da una parte nella concezione bourdieusiana e, dall'altra, nel filone della sociologia della devianza e nella criminologia di Jonathan Simon. Il risultato è stato quello di poter far convergere le riflessioni sull'argomento *NTH*: questo si presenta infatti come il luogo dove Stato e individuo riallineano vere e proprie logiche; esso costituisce, dunque, una cinghia di trasmissione concettuale che fa girare il meccanismo stesso di criminalizzazione.

Molteplici obiettivi si sono imposti nel corso del lavoro: il più significativo è sicuramente la ricostruzione dell'idea di riservatezza, e il suo rapporto con la crittografia. Si è visto che l'assenza, in letteratura sociologica, di formulazioni consolidate del concetto di riservatezza ha imposto un'operazione di edificazione del concetto stesso in questa sede. A tale scopo è stato preso primariamente in considerazione un filone di studi etnometodologico e, in particolare, un'insieme di concetti presentati nei lavori di Erving Goffman e Harold Garfinkel: a partire dalla nozione di *territory of the self* di Goffman, è stata elaborata una nozione di «spazialità», regione di spazio, anche concettuale, riguardante l'individuo. A questa, è stato necessario associare il concetto di informazione introdotto in ambito sociale da Harold Garfinkel e le idee di «reazione» e *segreto* adottate da Georg Simmel, per arrivare così alla formulazione di un concetto di riservatezza: *reazione* consistente in una pretesa relativa all'informazione emessa [disseminata o disincarnata] dal soggetto in termini di *controllo* su di essa nella regione identificabile di spazio in cui questa è definita e si muove. A questo punto è stato necessario un lavoro di inversione empirica per comprendere che rapporto leghi da una parte crittografia e riservatezza e, dall'altra, criminalizzazione e riservatezza: si è proceduto dunque ad una selezione delle tecnologie effettivamente coinvolte dal-

l'attività di criminalizzazione per poi comprendere come queste giochino un ruolo significativo nella protezione della riservatezza così come è stata definita. Se tutto il percorso di definizione del concetto di riservatezza risulta convincente, allora si è ricollegata l'idea che soggiace al concetto di *privacy* ad un insieme evocativo di dinamiche non complesse dell'interazione sociale: in qualche modo si stabilisce una continuità tra l'idea, ad esempio, di nascondere degli effetti personali in un cassetto e quella di proteggere delle informazioni personali con un algoritmo di cifratura.

Sebbene sia possibile ricostruire un quadro in sé coerente dell'intera dinamica presa in oggetto limitandosi ai due piani dello Stato e dell'individuo, questo sarebbe davvero incompleto se non si considerasse la presenza di un terzo attore: i grandi colossi dei servizi *internet*. L'ultima parte costituisce così il campo di prova e, al tempo stesso, di arricchimento dell'insieme concettuale elaborato nella parte precedente del lavoro. È questo però un campo che rapidamente si trasforma in mare aperto, dove è necessario ancora costruire le coordinate per navigarlo. Appare però una dinamica particolarmente rilevante: quella della trasformazione della sicurezza in un servizio. Ciò sembrerebbe produrre un autentico conflitto con la pressione di criminalizzazione della crittografia presa in esame, conflitto il cui superamento potrebbe risiedere nell'idea di vere e proprie «porte sul retro» per l'accesso ai dati personali: l'ipotesi lanciata è quella dell'acquisizione, da parte di queste grandi aziende, di un ruolo di *gate-keepers* dell'informazione protetta.

Riferimenti bibliografici

Testi e Articoli

Agamben, Giorgio (1996). *Mezzi senza Fine*. Torino: Bollati Boringhieri.

— (2003). *Stato di Eccezione*. Torino: Bollati Boringhieri.

— (2006). *Che Cos'è un dispositivo?* Roma: nottetempo.

Aho, James (2010). «Harold Garfinkel: Toward A Sociological Theory of Information.» In: *Human Studies* 33.1, pp. 117–121.

Arendt, Hannah (1982). *Lectures on Kant's Political Philosophy*. A cura di Ronald Beiner. Chicago: The University of Chicago Press.

Attewell, Paul (1974). «Ethnomethodology since Garfinkel». In: *Theory and Society* 1.2, 179–210.

Barenco, Adriano (1998). «Quantum Computation: an Introduction». In: *Introduction tu Quantum Computation and Information*. A cura di Hoi-Kwong Lo, Sandu Popescu e Tim Spiller. Singapore: World Scientific.

Bates, Alan (1964). «Privacy: a Useful Concept?» In: *Social Forces* 42.4, 429–434.

Berlin, Isaiah (1999). ««Two Concepts of Liberty»». In: *Arguments for Freedom: Philosophy and the Human Situation*. A cura di Nigel Warburton. Open University Press. Cap. I, pp. 155–165.

Borghini, Andrea (2009). *Potere simbolico e immaginario sociale: Lo Stato nella vita quotidiana*. Trieste: Asterios Editore.

— (2012). «Stato». In: *Il Mondo Contemporaneo: un lessico sociologico*. Ipermedium.

Boudon, Raymond (1986). *L'Idéologie, Ou l'Origine des Idées Reçues*. Fayard.

Bourdieu, Pierre (1995). *Ragioni Pratiche*. Bologna: Il Mulino.

— (2012a). *Sullo Stato: Corso al Collège de France. Volume I (1989-1990)*. Milano: Feltrinelli.

— (2012b). *Sur l'État: cours au Collège de France (1989-1992)*. Paris: Seuil.

Callero, Peter (2003). «The Sociology of the Self». In: *Annual Review of Sociology* 29, 115–133.

Cardozo, Nate et al. (2014). *Wha has your back? Protecting Your Data from Government Requests*. Rapp. tecn. Electronic Frontier Foundation. URL: `https://www.eff.org/files/2014/05/15/who-has-your-back-2014-govt-data-requests.pdf`.

Carpineto, Claudio e Giovanni Romano (2005). «Verso i Motori di Ricerca di prossima Generazione». In: *Mondo Digitale* 1.2, pp. 19–31.

Cohen, Julie (2012). «Irrational Privacy?» In: *Journal on Telecommunications and High Technology Law* 10.2, pp. 241–250.

Dal Lago, Alessandro (1981). *La Produzione della Devianza: Teoria sociale e Meccanismi di Controllo*. Milano: Feltrinelli.

Davis, Murray (1973). «Georg Simmel and the Aesthetics of Social Reality». In: *Social Forces* 51.3, pp. 320–329.

Ek, Richard (2006). «Giorgio Agamben and the Spatialities of the Camp: An Introduction». In: *Geografiska Annaler. Series B, Human Geography* 88.4, 363–386.

Epstein, Dmitry, Merrill C. Roth e Eric P.S. Baumer (2014). «It's the Definition, Stupid! Framing of Online Privacy in the Internet Governance Forum Debates». In: *Journal of Information Policy* 4.1, pp. 144–172.

Fontana, Alessandro (1999). «Du droit de résistance au devoir d'insurrection». In: *Le Droit de résistance*. A cura di Jean-Claude Zancarini. Paris: ENS éditions.

Foucault, Michel (1975). *Surveiller et Punir: naissance de la Prison*. Paris: Gallimard.

Garfinkel, Harold (1967). *Studies in Ethnomethodology*. Prentice-Hall, New Jersey.

— (2008). *Toward a Sociological Theory of Information*. A cura di Anne Warfield Rawls. Boulder, London.

Garland, David (2001). «The new iron cage». In: *Mass Imprisonment: Social Causes and Consequences*. London: Sage Publications, pp. 179–181.

Goffman, Erving (1956). *The Presentation of Self in Everyday Life*. Edinburgh: University of Edinburgh.

— (1966). *Behavior in Public Places: Notes on the Social Organization of Gatherings*. The Free Press, New York.

— (1971). *Relations in Public*. Basuc Books, New York.

Goldreich, Oded (2004). *Foundations of Cryptography II: Basic Applications*. Cambridge: Cambridge University Press.

Guo, Shumin e Keke Chen (2012). *Mining Privacy Settings to Find Optimal Privacy-Utility Tradeoffs for Social Network Services*. 2012 ASE/IEEE International Conference on Social Computing and 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust.

Hagan, John (1986). «Toward a Structural Criminology: Method and Theory in Criminological Research». In: *Annual Review of Sociology* 12, pp. 431–449.

Hagan, John, Edward T. Silva e John H. Simpson (1977). «Conlict and Consensus in the Designation of Deviance». In: *Social Forces* 56.2, 320–340.

Hall, Edward T. et al. (1968). «Proxemics [and Comments and Replies]». In: *Current Anthropology* 9.2/3, pp. 83–108.

Iyer, Ganesh, David Soberman e J. Miguel VIllas-Boas (2005). «The Targeting of Advertising». In: *Marketing Science* 24.3, pp. 461–476.

Jenness, Valerie (2004). «Explaining Criminalization: From Demography and Status Politics to Globalization and Modernization». In: *Annual Review of Sociology* 30, 147–171.

Kasper, Debbie V. S. (2005). «The Evolution (Or Devolution) of Privacy». In: *Sociological Forum* 20.1, 69–92.

Koblitz, Neal e Alfred J. Menezes (2004). «A Survey of Public-Key Cryptosystems». In: *SIAM Review* 46.4, pp. 599–634.

Lakoff, George e Mark Johnson (1980). *Metaphors we live by*. Chicago: University of Chicago Press.

Mann, Michael (2005). *The Dark Side of Democracy*. New York: Cambridge University Press.

Marini, Giuliano (2007). *La Filosofia Cosmopolitica di Kant*. Bari: Laterza.

Martin, Kirsten (2012). «Information Technology and Privacy: conceptual Muddles or Privacy Vacuums?» In: *Ethics and Information Technology* 14.4, pp. 267–284. URL: `http://dx.doi.org/10.1007/s10676-012-9300-3`.

Merton, Robert King (1968). *Social Theory and Social Structure*. New York: The Free Press.

Mills, Theodore M. (1959). «Equilibrium and the Processes of Deviance of Control». In: *American Sociological Review* 24.5, 671–679.

Nasu, Hisashi (1992). «For the Restoration of the Private Sphere: Thoughts on Privatization Theory». In: *Human Studies* 15.1, pp. 77–93.

Petras, Richard T. (2001). «Privacy for the Twenty-First Century: Cryptography». In: *The Mathematics Teacher* 94.8, pp. 689–691.

Procaccini, Andrea (2012). «Devianza». In: *Il Mondo Contemporaneo: un lessico sociologico*. Ipermedium.

Reiman, Jeffrey H. (1976). «Privacy, Intimacy and Personhood». In: *Philosophy and Public Affairs* 6.1, pp. 26–44.

Rigouste, Mathieu (2007). «L'ennemi Intérieur, de la guerre coloniale au contrôle sécuritaire». In: *Cultures & Conflits*.67, pp. 157–174.

Sassen, Saskia (2002). «Towards a Sociology of Information Technology». In: *Current Sociology* 50.3, 365–388.

Schwartz, Barry (1968). «The Social Psychology of Privacy». In: *American Journal of Sociology* 73.6, pp. 741–752.

Simmel, Georg (1906a). *Sociology*. A cura di Kurt H. Wolff. The Free Press.

— (1906b). «The Sociology of Secrecy and of Secret Societies». In: *American Journal of Sociology* 11.4, pp. 441–498.

Simon, Jonathan (2008). *Il governo della paura: Guerra alla criminalità e democrazia in America*. A cura di Alessandro De Giorgi. Milano: Raffaello Cortina Editore.

Singer, Milton (1980). «Signs of the Self: An Exploration in Semiotic Anthropology». In: *American Anthropologist* 82.3, 485–507.

Singh, Simon (2001). *The Code Book: How to Make it, Break it, Hack it, Crack it*. New York: Delacorte Press.

Solove, Daniel J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.

Stallings, William (1998). *Cryptography and Network Security: Principles and Practice*. New Jersey: Prentice Hall.

Steeves, Valerie (2009). «Reclaiming the Social Value of Privacy». In: *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. A cura di Kerr, Lucock e Steeves. Oxford University Press. Cap. 11, pp. 191–208.

Sumner, William Graham (1906). *Folkways: a Study of the sociological Importance of Usage, Manners, Customs, Mores, and Morals*. Boston: Ginn e Company.

Taylor, Charles (1994). *Multiculturalism: examining the politics of recognition*. A cura di Amy Gutman. Princeton: Princeton University Press.

— (1997). «What's Wrong with Negative Liberty?» In: *Contemporary Political Philosophy: An Anthology*. A cura di Robert E. Goodin e Philip Pettit. Australian National University. Cap. 25, pp. 418–428.

Toscano, Mario Aldo (2006). *Introduzione alla Sociologia*. Milano: FrancoAngeli.

Tréguer, Félix (2015). «Stato e Imprese all'Assalto». In: *Le Monde diplomatique (il manifesto)*, p. 4.

Turk, Austin T. (1966). «Conflict and Criminality». In: *American Sociological Review* 31.3, 338–352.

Uhler, Oscar M. e Henri Coursier (1958). *Commentary: IV Geneva Convention on the Protection of Civilian Persons in Time of War*. A cura di Jean S. Pictet. International Committee of the Red Cross.

Vagle, Jeffrey L. (2015). «Furtive Encryption: Power, Trust and the Constitutional Cost of Collective Surveillance». In: *Indiana Law Journal* 90.1, 101–150.

Vidoni Guidoni, Odillo (2004). *La Criminalità*. Roma: Carocci.

Watson, Michael e Edward T. Hall (1969). «On Proxemic Research». In: *Current Anthropology* 10.2/3, pp. 222–224.

Weber, Max (2008). *Max Weber's Complete Writings on Academic and Political Vocations*. A cura di John Dreijmanis. New York: Algora Publishing.

Risorse elettroniche[215]

Alonso, Pierre, Alexandre Léchenet e Gurvan Kristianadjaja (2015). *Loi sur le renseignement: pourriez-vous être espionné ?* URL: http://www.liberation.fr/apps/2015/04/quiz-loi/.

Barnett, Emma (2010). *Facebook's Mark Zuckerberg says privacy is no longer a 'social norm'*. URL: http://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html.

Bartz, Diane (2015). *Google lobbying spending reached new high in early 2015*. URL: http://www.reuters.com/article/2015/04/21/us-google-lobbying-idUSKBN0NC1UO20150421.

Beales, Howard (2010). *The Value of Behavior Targeting*. URL: https://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

Buffington, Jason (2015). *Why Google Cloud Storage Nearline is Super Interesting for Data Protection*. URL: http://www.esg-global.com/blogs/why-google-cloud-storage-nearline-is-super-interesting-for-data-protection/.

Cassini, Sandrine (2015). *Terrorisme : accord entre la France et les géants du Net*. URL: http://www.lesechos.fr/journal20150423/lec2_high_tech_et_medias/02124922454-terrorisme-accord-entre-la-france-et-les-geants-du-net-1113723.php.

Cavanagh, Allison (2015). *Issue Six: Research Methodology Online. Behaviour in Public? : Ethics in Online Ethnography*. URL: http://www.cybersociology.com/files/6_2_ethicsinonlineethnog.html.

Chomsky, Noam (2015). *We Are All - Fill in the Blank*. URL: http://www.telesurtv.net/english/opinion/We-Are-All---Fill-in-the-Blank-20150110-0021.html.

Cohen, David (2013). *Farewell, Facebook Credits*. URL: http://www.adweek.com/socialtimes/farewell-facebook-credits/428240.

Cohen, Julie (2007). *Cyberspace As/And Space*. URL: http://scholarship.law.georgetown.edu/facpub/807.

— (2008). *Privacy, Visibility, Transparency, and Exposure*. URL: http://scholarship.law.georgetown.edu/facpub/805.

Doctorov, Cory (2015). *What David Cameron just proposed would endanger every Briton and destroy the IT industry*. URL: http://boingboing.net/2015/01/13/what-david-cameron-just-propos.html.

[215]Quando possibile, è stato preferito l'indirizzo con protocollo https rispetto a http.

Dredge, Stuart (2015). *Tech pioneer Phil Zimmermann calls Cameron's anti-encryption plans 'absurd'*. URL: http://www.theguardian.com/technology/2015/feb/02/encryption-phil-zimmermann-david-cameron.

Facebook Inc. (2015). *Investor Relations: earnings slides. First Quarter 2015*. URL: http://investor.fb.com/results.cfm.

Fox News (2013). *Obama: Phone, Internet data collection not 'Big Brother'*. URL: http://www.foxnews.com/politics/2013/06/07/obama-phone-internet-data-collection-not-big-brother/.

Garante per la Protezione dei Dati Personali (2014). *Privacy e sicurezza. Soro risponde a Tricarico*. URL: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3479404.

Google Inc. (2015a). *2015 Financial Tables: Full year financial tables with quarterly data*. URL: https://investor.google.com/financial/tables.html.

— (2015b). *Google Apps Help: Your security and privacy*. URL: https://support.google.com/a/answer/60762?hl=en.

— (2015c). *Google Products*. URL: https://www.google.com/about/products/.

— (2015d). *Transparency Report: Requests for user information*. URL: https://www.google.com/transparencyreport/userdatarequests/.

Gould, Jeff (2014). *The Natural History of Gmail Data Mining*. URL: https://medium.com/@jeffgould/the-natural-history-of-gmail-data-mining-be115d196b10.

Grossklags, Jens e Nigel Barradale (2014). *Social Status and the Demand for Security and Privacy*. URL: https://www.petsymposium.org/2014/papers/Grossklags.pdf.

Huffington Post (2015). *Big Brother Bodyshamed By Congress, Will Slim Down*. URL: http://www.huffingtonpost.com/2015/06/02/huffpost-hill_n_7497228.html.

Hull, Gordon (2014). *Successful Failure: what Foucault can teach us about self-management in a world of Facebook and big data*. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2533057.

Jackson, Joab (2015). *Google takes on real-time big data analysis with new cloud services*. URL: http://www.pcworld.com/article/2911112/google-takes-on-realtime-big-data-analysis-with-new-cloud-services.html.

Kamin, Julia (2011). *The future of personalization is here*. URL: http://www.thefilterbubble.com/the-future-of-personalization-is-here.

Keane, John (2015). *Why Google is a political Matter: a Conversation with Julian Assange*. URL: http://www.themonthly.com.au/issue/2015/june/1433080800/john-keane/why-google-political-matter.

Khrennikov, Ilya (2014). *Putin Sets 110,000 Dollars Bounty for Cracking Tor as Anonymous Internet Usage in Russia Surges*. URL: http://bloom.bg/1ECBrwa.

Lazar, Shira (2011). *Algorithms and the Filter Bubble Ruining Your Online Experience?* URL: http://www.huffingtonpost.com/shira-lazar/algorithms-and-the-filter_b_869473.html.

Le Monde (2015). *Vigipirate : les armées vont adapter leurs effectifs*. URL: http://www.lemonde.fr/actualite-medias/article/2015/03/11/vigipirate-les-armees-vont-adapter-leurs-effectifs_4591267_3236.html.

Leib, Robert (2013). *Spaces of the Self: Foucault and Goffman on the Micro-Physics of Discipline*. URL: https://www.academia.edu/4191231/Spaces_of_the_Self_Foucault_and_Goffman_on_the_Micro-Physics_of_Discipline.

Markoff, John (2012). *How Many Computers to Identify a Cat? 16,000*. URL: http://www.nytimes.com/2012/06/26/technology/in-a-big-network-of-computers-evidence-of-machine-learning.html?pagewanted=all.

Mathiot, Cédric (2013). *La sécurité, première des libertés ? Histoire d'une formule*. URL: http://www.liberation.fr/politiques/2013/09/24/la-securite-premiere-des-libertes-histoire-d-une-formule_934227.

Metz, Cade (2009). *Google chief: Only miscreants worry about net privacy*. URL: http://www.theregister.co.uk/2009/12/07/schmidt_on_privacy/.

Ministère de la Défense (2014). *Vigipirate [dossier]*. URL: http://www.defense.gouv.fr/operations/france/vigipirate-pps/dossier-de-reference/vigipirate.

Ministère de l'Intérieur (2015a). *Marche républicaine silencieuse à Paris dimanche 11 janvier : organisation, recommandations et dispositif de sécurité*. URL: http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Marche-republicaine-silencieuse-a-Paris-dimanche-11-janvier.

— (2015b). *Projet de loi sur le renseignement*. URL: http://www.interieur.gouv.fr/Actualites/Dossiers/Projet-de-loi-sur-le-renseignement.

O'Connor, Tim (1996). *Is It Legal to Use PGP?* URL: http://www.roughdraft.org/pgplegal.html.

Pariser, Eli (2012). *Filter bubbles, meet Upworthy*. URL: http://www.thefilterbubble.com/filter-bubbles-meet-upworthy.

Price, Rob (2014). *Can police force you to surrender your password?* URL: http://kernelmag.dailydot.com/issue-sections/features-issue-sections/11071/police-force-password-cellphone/.

— (2015). *David Cameron Wants To Ban Encryption.* URL: http://uk.businessinsider.com/david-cameron-encryption-apple-pgp-2015-1?op=1?r=US.

Riley, Michael A (2014). *NSA Said to Have Used Heartbleed Bug, Exposing Consumers.* URL: http://www.bloomberg.com/news/articles/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.

Rowinski, Dan (2011). *How does Google protect your Data in the Cloud?* URL: http://readwrite.com/2011/07/22/how_does_google_protect_your_data_in_the_cloud.

Schneier, Bruce (2006). *The Eternal Value of Privacy.* URL: http://archive.wired.com/politics/security/commentary/securitymatters/2006/05/70886.

Sheppard, Mike (1996). *Proxemics.* URL: https://www.cs.unm.edu/~sheppard/proxemics.htm.

Simonite, Tom (2014). *Google Launches Effort to Build Its Own Quantum Computer.* URL: http://www.technologyreview.com/news/530516/google-launches-effort-to-build-its-own-quantum-computer/.

Smith, Leslie (2003). *An Introduction to Neural Networks.* URL: http://www.cs.stir.ac.uk/~lss/NNIntro/InvSlides.html.

Solove, Daniel J. (2007). *«I've got Nothing to Hide» and Other Misunderstandings of Privacy.* URL: http://ssrn.com/abstract=998565.

— (2011). *Why Privacy Matters Even if You Have 'Nothing to Hide'.* URL: https://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/.

Sparkes, Matthew (2015). *WhatsApp overtakes text messages.* URL: http://www.telegraph.co.uk/technology/news/11340321/WhatsApp-overtakes-text-messages.html.

Sprenger, Polly (1999). *Sun on Privacy: 'Get Over It'.* URL: http://archive.wired.com/politics/law/news/1999/01/17538.

Wikipedia (2015). *Amazon Mechanical Turk: Cases of uses.* URL: https://en.wikipedia.org/wiki/Amazon_Mechanical_Turk#Cases_of_uses.

Womack, Brian (2011). *Facebook Revenue Will Reach $4.27 Billion, E-Marketer Says.* URL: http://www.bloomberg.com/news/articles/2011-09-20/facebook-revenue-will-reach-4-27-billion-emarketer-says-1-.

Worley, Becky (2010). *Cyberspace Wild West ? Advocates Want Limits on Online Personal Info Profiling.* URL: http://abcnews.go.com/GMA/ConsumerNews/restrictions-sought-internet-data-profiling/story?id=10389313.

Zezima, Katie e Greg Jaffe (2015). *Obama, Cameron to discuss encryption of online services*. URL: http://www.washingtonpost.com/politics/obama-cameron-to-discuss-encryption-of-online-services/2015/01/15/e215effe-9ceb-11e4-96cc-e858eba91ced_story.html.

> /dev/null