Sicurezza e fiducia nell'età della tecnologia

Massimo Durante

Sicurezza e fiducia nell'età della tecnologia

Bernardo: *Who is there?*
Francisco: *Nay, answer me: stand, and unfold yourself.*

(Shakespeare, *The Tragedy of Hamlet*, Act I, Scene I)

1. L'idea di sicurezza e la sua centralità per la politica

Nella riflessione moderna sulla politica così come nell'esercizio della sua pratica concreta l'idea di sicurezza ha sempre esercitato un ruolo centrale. Un ruolo intorno al quale si è definito di volta in volta il senso stesso della politica e, più in particolare, della forza politica. La forza politica si nutre dell'idea di sicurezza come di una linfa vitale, poiché tale idea possiede una propria forza politica che le deriva dalle condizioni di possibilità in cui affonda le radici. La forza politica dell'idea di sicurezza risiede, infatti, nel suo duplice radicamento: antropologico e filosofico-politico.

Dal punto di vista antropologico, la pretesa di sicurezza si radica nelle più intime paure[1] dell'essere umano, che toccano o, meglio, strutturano la sua dimensione evolutiva di meccanismo programmato per mettere al sicuro la propria capacità di sopravvivere ed evolvere. La sicurezza è fin dal principio insicurezza: condizione negativa e scrittura in filigrana del carattere difettivo dell'essere umano. Nella modernità al modello cartesiano del Soggetto che trova in sé le proprie certezze si contrappone il modello scettico shakespeariano inaugurato nell'Amleto. Nel primo verso della tragedia, la sentinella Bernardo, chiamato a sorvegliare sulla città e a garantire in tal modo la sicurezza dei propri consociati, rivolgendosi alla sentinella Francisco, cui deve dare il cambio ma che non riconosce nel buio della notte, indirizza la seguente domanda: "Chi è là?". A tale domanda Francisco replica in modo parimenti evocativo: "No, rispondi tu: fatti avanti e mostra chi sei".

[1] Sul tema della paura nel discorso politico-pubblico v. M. Durante, "Perché l'attuale discorso politico-pubblico fa leva sulla paura?", in *Filosofia politica*, num. monografico "Paura", curato da M.-L. Lanzillo, a. XXIV, numero 1, aprile 2010, pp. 49-70.

E' qui che ha inizio la modernità o, più precisamente, quel processo di germinazione delle minacce costitutive della società che trova origine nella modernità ma si manifesta appieno, sotto tale profilo, solo con la postmodernità, in cui a essere minacciata non è la vita in quanto tale ma l'identità degli individui[2]. Non essendo più sicura di chi stia davanti e fuori di sé, la coscienza non è neppure più certa di se stessa. La soggettività (umana e quindi politica) è messa in questione: acquista lo statuto di una domanda aperta, non più autoreferenziale ma sistematicamente attraversata dal dubbio e caratterizzata ormai da una insicurezza di fondo, che fa il suo ingresso nella storia della politica moderna come questione essenziale, cui ogni epoca dà risposta puntuale e concreta[3].

Dal punto di vista filosofico-politico, l'idea di sicurezza si radica in quella di libertà. Ciò accade in un duplice senso. Da un primo e più tradizionale punto di vista, perché non vi sarebbe libertà se non vi fosse dapprima sicurezza, per cui l'idea di sicurezza si radica nell'esigenza di garantire la libertà degli individui. Individui costantemente minacciati non potrebbero dirsi liberi e non sarebbero in grado di esercitare i diritti che la libertà riconosce e assicura loro. Ciò porta con sé un secondo e meno tradizionale punto di vista, non sempre messo in evidenza con sufficiente chiarezza in tutte le sue implicazioni. La libertà, per essere garantita, ha bisogno di consegnarsi all'esterno[4], di mettersi al sicuro, di fare affidamento su forme istituzionalizzate di protezione delle libertà.

Questo meccanismo di istituzionalizzazione delle forme fiduciarie di protezione (l'insieme di processi o dispositivi cui viene in concreto affidato la realizzazione di quel regime di sicurezza, che si intende porre a garanzia della nostra libertà) investe l'idea di fiducia e costituisce una premessa di fondo, di regola inesplorata, del discorso sulla sicurezza. Tale premessa porta a considerare più da vicino il nesso complesso e problematico tra sicurezza e fiducia.

2. La relazione tra sicurezza e fiducia

La sicurezza è, perciò, centrale al progetto politico della modernità, che si presenta come un processo di relativa immunizzazione dal rischio di insicurezza (in

---

[2] Vedi in tal senso A. Giddens, *Le conseguenze della modernità. Fiducia e rischio, sicurezza e pericolo*, introduzione di A. Bagnasco, Bologna, il Mulino, 1994, p. 96 e ss.

[3] Risposta che differisce, ad esempio, nel passaggio dalle culture premoderne a quelle moderne, e poi in seno a quelle moderne, come osserva Anthony Giddens, *Le conseguenze della modernità*, op. cit., in particolare pp. 102-112.

[4] In tale prospettiva v. E. Lévinas, *Liberté et commandement*, Montpellier, Fata Morgana, 1994, in particolare p. 33, dove osserva che la libertà, per proteggersi, è chiamata "à instituer hors de soi un ordre de raison; à confier le raisonnable à l'écrit, à recourir à une institution. La liberté, dans sa crainte de la tyrannie, aboutit à l'institution, à un engagement de la liberté au nom de la liberté". E inoltre p. 34: "L'oeuvre suprême de la liberté consiste à garantir la liberté".

realtà si tratta soltanto di una gestione del rischio, rispetto al quale non c'è mai completa immunità) sotto due profili: come 1) bene (integrità di vita e del proprio progetto di vita), che spetta a ciascun individuo, *uti cives*; e come 2) condizione per il godimento di beni, vale a dire per la messa in pratica dei progetti di vita (con conseguente riduzione del concetto stesso di progetto di vita a quello di sicurezza economica), che attiene di regola alla collettività o quantomeno si determina con riferimento alla società complessivamente intesa. Nel primo caso la sicurezza è un obiettivo della politica; nel secondo è un trascendentale della politica (condizione di possibilità).

Tale distinzione tende a perdersi nell'uso univoco del termine sicurezza, ma può rintracciarsi nella distinzione, propria della lingua inglese, tra *safety* e *security*. La *safety* si riferisce alla sicurezza come tutela dell'integrità della vita rispetto alla minaccia di un pericolo più o meno imminente. Tale idea ha una connotazione temporale che s'iscrive nell'immediatezza, nell'ambito di rapporti immediati (*e.g.* quella dimensione violenta della temporalità che per Locke non ci lascia il tempo di delegare le nostre decisioni all'autorità di un terzo[5]). La *security* fa soprattutto riferimento alla sicurezza come tutela delle condizioni per il godimento di beni (integrità del progetto di vita) rispetto alla minaccia di pericoli o rischi che possono formare oggetto di più attenta previsione e calcolo: ha una connotazione intertemporale che si colloca nella mediatezza, in rapporti mediati (*e.g.* quella dimensione della temporalità sottesa alla razionalità strumentale e calcolante).

Il discorso politico-pubblico tende a oscillare tra queste due forme di sicurezza, che prevedono una diversa gestione del rischio. Nella modernità, la politica si serve del potere di differire il rischio, per legittimarsi, e tale potere è eminentemente politico nella misura in cui crea le condizioni di possibilità del suo stesso esercizio (in quanto evoca e contribuisce a creare il senso stesso di insicurezza). La fine della modernità o la post-modernità mostra l'esistenza di questo velo di differimento (la struttura fiduciaria della sicurezza). La contemporaneità gioca con questo velo e a sua volta lo rivela (nel duplice senso di infittire o rimuovere il velo secondo le opportunità delle circostanze politiche): fa retrocedere la *security* a *safety*, mostrando l'urgenza di una minaccia non ulteriormente rinviabile.

---

[5]J. Locke, *Due trattati sul governo* [1690], Torino, Utet, 2010, 3.19: "[…] l'aggressore non ci lascia tempo per appellarci al nostro giudice comune, né alla decisione della legge, per riparare un crimine che potrebbe essere irreparabile".

Tale differimento del rischio (che è una presa in carico della *safety*) apre lo spazio del governo del rischio e fa affidamento su forme intertemporali e fiduciarie di gestione della sicurezza (*security*). Questo è il tratto caratterizzante del progetto politico moderno costruito sulla sicurezza, che prosegue nella postmodernità (che lo svela) e nella contemporaneità (che lo rivela e radicalizza). La sicurezza è sostanzialmente sempre affidata: non è gestita in proprio. La modernità politico-giuridica si caratterizza per il processo di istituzionalizzazione sistematica e tecnica di forme intertemporali e fiduciarie di gestione della sicurezza[6].

Vediamo in sintesi in cosa consiste questo processo di istituzionalizzazione delle forme della gestione della sicurezza, concentrando l'attenzione sulla dimensione fiduciaria. La gestione della sicurezza avviene, nella modernità, secondo tre direzioni possibili, che si intersecano tra loro, tramite: 1) la creazione di relazioni fiduciarie (rapporti tra attori [*e.g.* contratto sociale]); 2) l'incorporazione della delegazione di fiducia in dispositivi (giuridici o tecnologici [*e.g.* documenti di identità; raccolta di dati; norme giuridiche o tecnologiche]); 3) l'incorporazione della delegazione di fiducia in organizzazioni miste (costituite da attori e dispositivi [*e.g.* fisco, come prelievo di risorse, in base alla raccolta di dati personali, per organizzare la sicurezza sul territorio]).

Mentre la modernità è caratterizzata dall'istituzionalizzazione delle forme della gestione della sicurezza secondo le direzioni indicate, e la postmodernità è connotata dallo svelamento (se non dalla denuncia) di tale processo di delegazione (e per tale via di riappropriazione) della gestione del rischio, la contemporaneità è caratterizzata da una radicalizzazione di tale processo. In quest'ottica, la nostra tesi consiste nel dire che il processo di istituzionalizzazione della forme della gestione della sicurezza si iscrive oggi nel quadro di un più generale e profondo (e pertanto radicale) mutamento del soggetto della politica, che abbiamo segnalato altrove in relazione al tema della paura[7]: il passaggio dalla dialettica governanti/governati alla dialettica governabile/ingovernabile in quanto nodo intorno a cui si costruisce il discorso politico-pubblico nel presente. Nell'ambito del discorso sulla sicurezza (e in rapporto al tema della fiducia), ciò avviene se-

---

[6] Cfr. sul punto, nel quadro di una diversa riflessione, A. Giddens, *Le conseguenze della modernità. Fiducia e rischio, sicurezza e pericolo*, op. cit., p. 31: "La separazione del tempo e dello spazio e il loro costituirsi in dimensione standardizzate e 'vuote' ha reciso i legami tra l'attività sociale e la sua 'aggregazione' nelle particolarità dei contesti di esperienza. Le istituzioni disaggregate estendono notevolmente la portata della distanzi azione spazio-temporale e, per avere questo effetto, dipendono dalla coordinazione nel tempo e nello spazio"; p. 36: "Tutti i meccanismi di disaggregazione, siano essi emblemi simbolici o sistemi esperti, riposano sulla *fiducia*. La fiducia gioca quindi un ruolo fondamentale nelle istituzioni della modernità".

[7] Sul punto cfr. M. Durante, "Perché l'attuale discorso politico-pubblico fa leva sulla paura?", *op. cit.*, in particolare pp. 68-70.

condo due modalità principali, che analizzeremo nel proseguo del presente saggio, ma di cui possiamo delineare fin d'ora i tratti essenziali.

Da una parte, vi è un'evoluzione del processo di delegazione delle forme di gestione della sicurezza in direzione di una loro progressiva incorporazione entro dispositivi tecnologici automatizzati, in base al funzionamento di algoritmi che sfuggono, in parte, al diretto controllo umano. Ciò solleva un tema destinato a rivestire un ruolo crescente: quello del governo degli algoritmi[8], la cui operatività automatizzata e impersonale s'iscrive nel plesso governabile/ingovernabile piuttosto che nel plesso governanti/governati. Ad esempio, algoritmi controllano il funzionamento di sistemi complessi, come il mercato degli scambi nella finanza internazionale[9] o il meccanismo d'indicizzazione dei risultati del più rilevante motore di ricerca secondo la regola del più popolare[10]. Un algoritmo siede nel consiglio d'amministrazione di una società giapponese[11].

---

[8] Sul punto v. l'interessante lezione di Jonathan Zittrain: "Love the Processor, Hate the Process: The Temptations of Clever Algorithms and When to Resist Them", accessibile online al seguente indirizzo: https://cyber.law.harvard.edu/events/2015/04/Zittrain.

[9] Come ha notato bene Andrea Curiat (http://money.wired.it/finanza/2013/05/08/mit-privacy-trasparenza-5728752.html), "le criticità della finanza internazionale, infatti, sono più evidenti proprio quando si inseriscono nel quadro di operazioni automatizzate di compravendita titoli via computer. Gli errori dei software di *trading* possono propagarsi rapidamente nel sistema con ripercussioni potenzialmente catastrofiche. È quello che è successo nel 2010, l'anno del famoso "Flash Crash": gli algoritmi utilizzati dagli *high-frequency* trader, operatori che sfruttano la velocità di calcolo dei computer per operare sui mercati finanziari in intervalli di tempo misurabili in frazioni di secondo, hanno interpretato male le condizioni della Borsa statunitense. Un piccolo errore di calcolo originario si è tramutato in una spirale negativa di compravendite che ha bruciato miliardi di dollari di capitalizzazione nel giro di poche ore".

[10] Il sistema di Google d'indicizzazione delle pagine web si basa sulla regola del più popolare, cioè su un algoritmo d'analisi ("PageRank") che assegna un peso numerico (misurabile e quindi monetizzabile) a un sito in base ai suoi collegamenti (link) e permette così di calcolarne il grado di popolarità, conferendogli un valore d'ordine più elevato all'interno del sistema di ricerca: più collegamenti possiede un sito, più alto è il suo numero di PageRank, e maggiore la probabilità di essere visitato. Sul punto v. S. Brin e L. Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine", in *Seventh International World-Wide-Web Conference*, April 14-18, 1998, Brisbane-Australia, accessibile online all'indirizzo: *http://ILPubs.stanford.edu:8090/361/*. Per una critica della regola del più popolare in ambito politico v. L.-M. Bartels, "Is the 'Popular Rule' Possible? Polls, Political Psychology, and Democracy", in *The Brookings Review*, vol. 21, n. 3, 2003, pp. 12-15.

[11] Vital (acronimo di *Validating investment tool for advancing life sciences*) è il primo robot manager che siede nel consiglio di amministrazione della *Deep knowledge ventures* (Dkv), una società giapponese specializzata in biotecnologia. In alcune interviste, Dmitry Kaminskiy, a.d. di Dkv, ha detto che "Vital è un membro paritario del consiglio di amministrazione perché la sua opinione (che in realtà è il risultato del suo algoritmo di analisi) sarà considerata come la più importante". Ha inoltre detto che tutte "le decisioni sugli investimenti saranno prese solo dopo che Vital ne avrà elaborato i dati". E' di rilievo la nota con cui la Dkv ha giustificato la sua adozione: "Gli uomini sono emotivi e soggettivi. Possono fare degli errori. Le macchine, invece,

D'altra parte, il processo di delegazione delle forme di gestione della sicurezza si realizza nel presente in un quadro mutato della concezione (descrittiva e normativa[12]) della politica, per cui la politica non è più intesa solo come una forma di controllo sul territorio, ma piuttosto come una forma di controllo sulla "public mind"[13] o, per dirlo altrimenti, sul ciclo di vita delle informazioni[14]. Le informazioni costituiscono sempre più le risorse in base a cui ci rappresentiamo il mondo e decidiamo[15]. Esse sono rilevanti, se non cruciali sul piano normativo, per costruire quegli standard con cui mediamo il nostro rapporto con il reale[16]. Ciò solleva un ulteriore aspetto critico nella questione del potere contemporaneo: quella del governo degli standard[17], che si somma (talora saldandosi, talora contrapponendosi) a quella vista del governo degli algoritmi. Il conflitto o la saldatura tra algoritmi (con il loro dominio dell'efficienza automatizzata e impersonale) e standard (con il loro dominio delle valutazioni incorporate in pro-

---

possono scegliere il cammino giusto in base all'intuizione e alla logica. Sommando questo all'esperienza degli investitori dell'impresa, sarà possibile minimizzare i rischi". Sul punto v. l'articolo di R. Miranda accessibile online: http://www.formiche.net/2014/05/27/chi-che-dmitry-kaminskiy-la-mente-dietro-al-primorobot-consigliere-damministrazione/.

[12] Sul tema mi permetto di rinviare ai miei "E-democracy as the Frame of Networked Public Discourse. Information, Consensus and Complexity", in P. Mindus, A. Greppi, M. Cuono (eds.), *Legitimacy 2.0. E-Democracy and Public Opinion in the Digital Age*, Paper Series - 25th IVR World Congress: Law, Science and Technology, Frankfurt, Goethe University Press, pp. 1-28; "Informazione e regolazione. Internet come problema democratico", in *Teoria Politica*, Nuova Serie, Annali II, 2013, pp. 39-65.

[13] Come osserva M. Castells, *Comunicazione e potere*, Milano, Egea, 2009, p. 56: "La *public mind* – ossia l'insieme di valori e cornici interpretative che hanno ampia esposizione nella società – è in ultima analisi ciò che influenza il comportamento collettivo".

[14] Per tale nozione v. L. Floridi, *La rivoluzione dell'informazione*, introduzione di J.-C. De Martin, Torino, Codice Editore, 2012.

[15] In tal senso v. Benkler, *La ricchezza della rete. La produzione sociale trasforma il mercato e aumenta le libertà*, introduzione di F. Cardini, Egea Università Bocconi Editore, Milano, 2007, p. 1: "L'informazione, la cultura e la conoscenza sono ingredienti fondamentali della libertà e dello sviluppo umano. Il modo in cui esse vengono prodotte e scambiate all'interno della società influenza fortemente la percezione del mondo com'è e di come dovrebbe essere, e di come noi in quanto società o comunità politica determiniamo ciò che si può o si dovrebbe fare".

[16] Sul tema v. ampiamente L. Bush, *Standards. Recipes for reality*, Cambridge Mass., The MIT Press, 2011, in particolare p. 13: "Standards are means by which we construct realities. They are means of *partially* ordering people and things so as to produce outcomes desired by someone. As such, they are part of the technical, political, social, economic, and ethical infrastructure that constitutes human societies".

[17] Aspetto centrale nell'analisi di L. Bush, *Standards*, op. cit., che osserva, p. 28: "What is central for the analysis in this book is the intimate connection between standards and power. However much standards appear to be neutral, benign, merely technical, obscure, and removed from daily life, they are, I argue, largely an unrecognized but extremely important and growing source of social, political, and economic relations of power. Indeed, in our modern world standards are arguably the most important manifestation of power relations".

cessi o dispositivi prodotti in serie) sono destinati a occupare la scena del dibattito politico-pubblico negli anni a venire.

In entrambi i casi, tali modalità di governo e, più in particolare, di delegazione della gestione del rischio sono tributarie della pervasiva dimensione tecnologica delle società dell'informazione. Il mutamento del quadro della politica si coniuga infatti strettamente con la crescente dipendenza delle società dalle tecnologie dell'informazione e comunicazione[18] e dalla graduale convergenza tra offline e online[19]. Poiché la mappa delle nostre dipendenze traccia anche la mappa delle nostre fragilità, ciò esige di esaminare il rapporto tra sicurezza e fiducia nella prospettiva appena delineata.

3. Sicurezza e fiducia nell'età contemporanea

Oggi, la gestione della sicurezza è sempre più implementata in termini di *security*, sebbene sia invocata in misura crescente come *safety*. La sicurezza come *security* implica una dilazione della minaccia che la sicurezza come *safety* non pare consentire. Allorché infatti la minaccia di un male sia percepita o rappresentata come potenzialmente immediata non vi è più spazio per la mediazione della sicurezza delegata: la *security* retrocede a *safety*, e ciò esige un supplemento di direzione o controllo, che mette in crisi la gestione fiduciaria della sicurezza. Se invece la minaccia di un male è percepita o rappresentata come mediata, la gestione del rischio è delegata in maniera crescente a dispositivi tecnologici (automatizzati e standardizzati) ovvero a sistemi misti (in cui la previsione intertemporale di un mezzo di sicurezza [es. airbag] è relativo alla possibilità di prevenire un male improvviso). Ad esempio, la sicurezza informatica[20] tiene conto del fatto che chi intende violare un sistema e creare insicurezza tende in primo luogo a sfruttare le strutture cognitive della fiducia degli utenti nonché la dilazione temporale delle risposte con cui le loro vulnerabilità sono percepite, pub-

[18] Sul punto v. U. Pagallo, *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Giappichelli Editore, Torino, 2014, pp. 1-8 e pp. 30-32.

[19] In tema v. di recente L. Floridi (ed.), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Dordrecht, Springer, 2015.

[20] Sul punto v. uno dei principali documenti in materia di sicurezza informatica, l'*Internet Security Threat Report*, redatto dalla Symantec Corporation, in particolare il vol. 19, 2014, che punta l'attenzione sui fenomeni di *social engineering* e *zero-days vulnerabilities*. Vi è inoltre un progetto di un sistema di sicurezza "trustless" (che non riposa sulla fiducia: salvo convenire sul senso del termine) avanzato dall'IBM in più contesti (dai bitcoin all'Internet delle cose), fondato su un dispositivo detto "blockchain", una sorta di libro mastro generale che tiene traccia di tutte le interazioni tra determinati agenti in rete. La sicurezza risiede nel fatto che di ogni interazione resti una traccia accessibile. Sul punto v. il report prodotto dall'IBM, evocativamente intitolato: *Device democracy. Saving the future of the Internet of Things*, accessibile online: http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF.

blicate e aggiustate. Oggi, si assiste, perciò, a questo apparente paradosso, per cui la sicurezza è spesso invocata come *safety* (cosa che garantisce maggiori poteri di direzione e controllo), ma è di regola praticata come *security*, in particolare con mezzi tecnologici. Da tale punto di vista, la contemporaneità è connotata da un triplice profilo problematico: 1) dal rapporto circolare, virtuoso e vizioso, di fiducia e sicurezza; 2) dalla graduale incorporazione della gestione del rischio in processi e dispositivi tecnologici; 3) dal rapporto sempre più stringente tra informazione, fiducia e sicurezza.

3.1. *Il duplice rapporto circolare tra fiducia e sicurezza*

Nel graduale passaggio da una gestione fiduciaria basata in prevalenza su rapporti umani a una tecnologicamente mediata può rilevarsi un duplice rapporto circolare tra fiducia e sicurezza: virtuoso e vizioso.

A) Consideriamo, prima, il caso di una *circolarità virtuosa*, in cui i due elementi della relazione si rafforzano reciprocamente:

1) il senso di sicurezza è rafforzato dal senso di fiducia: ciò avviene, ad esempio, nel caso in cui nutriamo fiducia in coloro ai quali è demandata la gestione della sicurezza. La crisi del rapporto governanti/governanti ha minato alla base questo rapporto fiduciario e con esso il rapporto di delegazione della gestione della sicurezza, che si è perciò indirizzato verso forme d'incorporazione della sicurezza in organizzazioni miste o meglio in dispositivi tecnologici automatizzati, che tendono a mutare la fiducia in affidamento[21] e a rendere tale gestione (in apparenza) più prevedibile, affidabile e dunque controllabile, ma anche più asettica, impersonale e anonima.

2) Il senso di fiducia è rafforzato dal senso di sicurezza, perché il senso di sicurezza ci permette di esporci maggiormente e di sviluppare rapporti fiduciari dotati di una certa stabilità. Ciò era vero nei rapporti fiduciari interpersonali ma resta vero nel caso di rapporti incardinati su dispositivi tecnologici automatizzati, il cui funzionamento (relativamente) prevedibile e standardizzato si caratterizza, almeno in linea di principio, per un elevato grado di stabilità. Nella radicalizzazione attuale della gestione della sicurezza, ciò non riguarda più tanto quella *machina machinarum* che è lo stato moderno ma il *macchinale* stesso elevato a processo: l'incorporazione di tale gestione in dispositivi e processi automatizzati, impersonali e anonimi, sempre più capillari, la cui diffusione tende a creare un generale senso di fiducia in tutti gli ambiti di applicazione. In tal senso, nell'età tecnologica, la fiducia non è più prestata puntualmente ma, per così

[21] Su tale distinzione v. ad es. P. Pettit, "Trust, Reliance and the Internet, in *Analise & Kritik*, 26/2004, pp. 108-121. Sull'ammissibilità teorica della fiducia verso agenti autonomi artificiali, v. M. Durante, "What Is the Model of Trust for Multi-agent Systems? Whether or Not E-Trust Applies to Autonomous Agents", in *Knowledge, Technology & Policy*, 23/2010, pp. 347-366.

dire, all'ingrosso[22] e spesso al di là di una specifica capacità tecnica di controllo sul processo di delegazione, incorporazione e funzionamento di processi e dispositivi tecnologici.

B) Consideriamo il caso opposto, frutto sia della radicale dipendenza tecnologica della nostra età che della radicalizzazione del passaggio dalla dialettica politica basata sul plesso governanti/governati a quella basata sul plesso governabile/ingovernabile. Si tratta di una *circolarità viziosa*, in cui i due elementi della relazione si indeboliscono reciprocamente:
1) la fiducia è più facilmente tradita là dove ci sentiamo più al sicuro, nella sfera delle nostre sicurezze: in tal caso, il senso di sicurezza rende più vulnerabile la fiducia. Ciò è sempre stato vero nei rapporti interpersonali, come ha osservato Helen Nissenbaum[23], ma resta vero per i rapporti tecnologicamente mediati, in cui l'affidamento su processi e dispositivi standardizzati e automatizzati pare garanzia di un funzionamento più sicuro, efficiente ed efficace, al prezzo però di una reale capacità di controllo diretto sulle modalità di tale funzionamento (demandare a un passaporto biometrico il controllo sulla circolazione delle persone sembra sollevare, ad esempio, dalla necessità di ulteriori indagini).
2) La sicurezza è più facilmente messa a repentaglio là dove nutriamo maggiore fiducia (o un eccesso di fiducia) su coloro o su ciò a cui è demandata la gestione della sicurezza. Tale aspetto è forse il più spinoso, perché nella gestione basata su relazioni interpersonali un certo grado di affidamento era correlato a un certo grado di confronto e di assunzione di responsabilità, che segnava o avrebbe dovuto segnare la dialettica tra governanti e governati. Nell'incorporazione di fiducia in processi e dispositivi tecnologicamente mediati, il passaggio alla dialettica governabile/ingovernabile tende a elidere un necessario spazio di confronto, interpretazione e discussione pubblica, nella cui sfera di riflessività sottoporre a scrutinio e valutazione i risultati di tale gestione, e ad allentare il senso di responsabilità politica che sfuma in amministrazione dell'(in)governabile. Tale aspetto ci invita a considerare più da vicino il carattere problematico (dal punto di vista della legittimità politica e democratica) dell'incorporazione della gestione della sicurezza in processi e dispositivi tecnologici più o meno standardizzati e automatizzati.

---

[22] Sul punto cfr. M. Durante, "E-democracy as the Frame of Networked Public Discourse. Information, Consensus and Complexity", *op. cit.*, p. 8.
[23] In tal senso cfr. H. Nissenbaum, "Will Security Enhance Trust Online, or Supplant It?", in R. Kramer & K. Cook (eds.) *Trust and Distrust Within Organizations: Emerging Perspectives, Enduring Questions*, Russell Sage Publications, New York NY, 2004, pp. 155-188, in particolare p. 169: "Homicide statistics, however, tell a curious story: when the relationship of the killer to victim is known, we find that only 22 percent of killers are strangers – the proverbial outsiders. Seventy-eight percent are spouses, friends, and acquaintances. Betrayal comes from those who are allowed within our spheres of safety, within our safe zones".

3.2. *L'incorporazione della gestione della sicurezza in processi e dispositivi tecnologici*

La crescente incorporazione della gestione della sicurezza in processi e dispositivi tecnologici è una caratteristica dell'età tecnologica. Per quanto tale incorporazione presenti indubbi aspetti positivi derivanti dal processo di automazione e standardizzazione, in termini di efficienza, prevedibilità, uniformità ed affidabilità, solleva parimenti alcuni nodi problematici.

Come ricordato, la sicurezza implica necessariamente un certo grado di neutralizzazione del rischio[24]. Tuttavia, la gestione della sicurezza non è mai completa immunizzazione dal rischio, che è sempre incorporato nel sistema fiduciario di gestione della sicurezza, poiché la fiducia o l'affidamento implicano sempre un certo grado di esposizione al rischio[25]. La sicurezza è piuttosto un modo di gestione del rischio attraverso la sua ripartizione tra soggetti, meccanismi e tempi differenti. Essere al sicuro non è un modo per eliminare rischi quanto piuttosto per ridistribuirne il peso e il tempo tra diversi attori, processi o dispositivi.

L'incorporazione di fiducia in un processo o dispositivo tecnologico avviene oggi nei modi più disparati. Pensiamo, ad esempio, a un airbag o a un sofisticato sistema di frenatura in un'auto che si guida da sola: l'affidamento su dispositivi tecnologici implica un certo grado di sfiducia su altri sistemi di controllo (come quello umano). Ogni processo di delegazione della gestione del rischio costituisce un'articolazione più o meno visibile di fiducia e sfiducia.

L'incorporazione di standard (*e.g.* una particolare taratura dei freni) segue di regola l'incorporazione di fiducia in un dato dispositivo tecnologico ma può verificarsi il caso opposto. Pensiamo al caso, già ricordato, del passaporto biometrico. Il passaporto genericamente inteso è una forma mista d'incorporazione di fiducia: permette a taluni operatori di verificare certe qualità del soggetto con un meccanismo di controllo relativamente semplice. Il passaporto biometrico implica l'incorporazione di uno standard ulteriore, che finisce per rendere desueto, in determinati contesti, il passaporto genericamente inteso (come se un soggetto si trovasse a dover giustificare la propria incapacità di conformarsi ad un dato standard)[26]. L'incorporazione di fiducia in processi e dispositivi tecno-

---

[24] Sulla retorica e ideologia di tale processo di neutralizzazione del rischio cfr. U. Beck, "La società (mondiale) del rischio e le insicurezze fabbricate", in *Iride*, a. XXI, n. 55, sett.-dic., 2008, pp. 511-520.

[25] In tal senso cfr. N. Luhmann, *La fiducia* (1968), Bologna, Il Mulino, 2002.

[26] Sul tema v. D. Lyon, *Identifying Citizens: ID Cards as Surveillance*, Cambridge, Polity, 2009. Vedi inoltre quanto osserva David Lyon, in D. Lyon – Z. Bauman, *Sesto potere. La sorveglianza nella modernità liquida*, Roma-Bari, Laterza, 2014, p. 126: "In molte situazioni di sorveglianza essi vengono ridotti a dati, come si coglie con particolare evidenza nell'uso della biometria al passaggio delle frontiere. In questo caso esemplare, però, la prospettiva è quella di verificare l'identità corporea, ossia della persona, per consentirle (o impedirle) di varcare un confine. La

logici e l'adozione di standard sono scelte attinenti alla gestione della sicurezza che hanno un carattere *normativo*, dal momento che fissano modalità e requisiti di tale gestione, e pertanto non sono neutrali. La pretesa di maggiore sicurezza, precipitata in un dispositivo tecnico apparentemente neutrale e fabbricato in serie (*e.g.* il passaporto biometrico), traccia il quadro normativo delle richieste che nel tempo diviene consueto (cioè standard nel duplice senso di uniforme ma anche di portatore di qualità[27]) avanzare per consentire l'accesso di determinati soggetti in determinati contesti. Nel caso considerato, è proprio l'elemento della sua producibilità in serie, della sua serialità, a far sì che lo standard incorporato nel dispositivo funga non solo da strumento uniforme e apparentemente neutrale di riconoscimento ma anche e soprattutto da garante di qualità. Tale esempio e molti altri, che attengono in particolare all'ambito della sorveglianza elettronica[28], ci ricordano i tre principali nodi problematici che l'incorporazione della gestione della sicurezza in processi e dispositivi tecnologici standardizzati e automatizzati solleva.

3.2.1. *L'invisibilità delle tecnologie basate sul computer*

In primo luogo, è opportuno ricordare che una delle caratteristiche salienti delle tecnologie basate sul computer è la loro relativa *invisibilità*: "la maggior parte delle volte e sotto numerose condizioni le operazioni del computer sono invisibili"[29]. Da un lato, l'invisibilità delle operazioni del computer rappresenta un fattore di estrema efficienza, perché contraddistingue la complessità dei calcoli del computer e non richiede l'intervento o il controllo dell'utente; dall'altro, costituisce un fattore problematico poiché tale invisibilità ci rende vulnerabili rispetto a rischi e imprevisti che l'utente non è sempre in condizione di percepire e padroneggiare. Ciò determina conseguenze problematiche derivanti dalle modalità con cui si configura il fattore d'invisibilità. È possibile fare riferimento a tre classi principali[30] entro cui ricondurre la previsione di tali conseguenze: 1) la classe dei casi di *abuso invisibile*; 2) la classe dei casi di *valori di programma invisibili*; e infine 3) la classe dei casi di *complessità di calcolo invisibile*.

Nella prima classe possiamo ricondurre quei casi in cui l'uso intenzionale di una operazione invisibile è volta a realizzare un'azione illecita: è il caso della violazione della privacy o della proprietà o di operazioni bancarie illecite o di sorve-

---

conclusione obbligata è che l'informazione *riguardante* quel corpo viene trattata come se avesse un ruolo decisivo nel determinare l'*identità* della persona".

[27] Su questa duplice accezione di standard v. L. Bush, *Standards*, op. cit., pp. 18-20.

[28] In tema v. D. Lyon *Surveillance Studies: An Overview*, Cambridge, Polity, 2007; D. Lyon, K. Ball, K. Haggerty (eds.), *Routledge Handbook of Surveillance Studies*, London, Routledge, 2012. Ed inoltre D. Lyon – Z. Bauman, *Sesto potere. La sorveglianza nella modernità liquida*, op. cit.

[29] Cfr. J. Moor, "What is computer ethics?", in T. Ward Bynum (ed.), *Computers & Ethics*, Blackwell Publisher, Malden Mass., 1985, pp. 266-275, cit. p. 273 (traduzione nostra).

[30] J. Moor, "What is computer ethics?", *op. cit.*, p. 265 e ss.

glianza non autorizzata, ecc. Nella seconda classe possiamo ricordare i casi in cui in un dato programma sono implementati valori invisibili, che si traducono in giudizi di valore relativi a scelte implicite, che non appaiono nel prodotto di un'operazione realizzata con il computer: è il caso, ad esempio, di un programma di ricerca che indirizzi l'utente verso talune compagnie o società somministratrici di un dato servizio piuttosto che altre. Talora l'implementazione di valori risulta invisibile allo stesso programmatore che non è in condizione di calcolare le conseguenze non previste derivanti dall'applicazione di scelte operate in sede di programmazione. Nella terza classe possiamo ricondurre quei casi in cui l'enorme complessità di calcolo, la cui verifica richiede un procedimento altamente complesso e non economico, può determinare una serie di conseguenze non interamente calcolabili e prevedibili: è il caso in cui un'attività mette in bilancio l'affidabilità delle operazioni basate su un calcolo più efficiente di quello umano dal punto di vista probabilistico e la fallibilità del computer determinata dalla impossibilità di un controllo e di una verifica diretta sulle operazioni.
In questa prospettiva, l'incorporazione della gestione della sicurezza in processi e dispositivi tecnologici può correlativamente: 1) dare luogo ad *abusi invisibili*, come nel caso in cui un'asserita esigenza di sorveglianza si traduca in un'illecita intrusione nella privacy con l'acquisizione incontrollata di una smisurata mole di dati personali; 2) veicolare in modo più o meno surrettizio valori impliciti nel *design*[31] di tali processi e dispositivi tecnologici, traducendosi in malcelate forme di paternalismo[32], che circoscrivono lo spazio delle scelte personali e tendono a modellare le condotte sociali con decisioni sottratte, in tutto o in parte, alla comprensione, discussione e valutazione pubblica; 3) creare conseguenze socialmente rilevanti, di cui sia arduo tracciare i termini della responsabilità (politica, giuridica ecc.), a causa di una pretesa difficoltà nella gestione della *complessità* del reale (quel plesso di governabile/ingovernabile, che in modo sempre più sottolineato assurge a soggetto della politica contemporanea).

3.2.2. *L'assenza di mediazione: comprensione, discussione e valutazione pubblica*
In secondo luogo, il meccanismo d'incorporazione della gestione della sicurezza in processi e dispositivi tecnologici tende a elidere o quantomeno a circoscrivere la sfera di comprensione, discussione e valutazione pubblica che funge da interfaccia tra l'istituzionalizzazione delle forme fiduciarie di sicurezza e la loro ap-

[31] Sul tema v. U. Pagallo, *Il diritto nell'età dell'informazione*, op. cit., pp. 129-164. Sulla questione cfr. inoltre P. Brey, *Values in technology and disclosive computer ethics*, in Floridi L. (ed.), *Information and Computer Ethics*, Cambridge, Cambridge University Press, 2010.
[32] Sul punto v. R.-H. Thaler – C.-R. Sunstein, *Nudge. La spinta gentile. La nuova strategia per migliorare le nostre decisioni sul denaro, salute, felicità*, Milano, Feltrinelli, 2009. Vedi anche U. Pagallo, *Il diritto nell'età dell'informazione*, op. cit., pp. 147-150.

plicazione[33]. Tale interfaccia non solo svolge un ruolo cruciale nel processo di legittimazione politica e democratica della gestione della sicurezza ma può anche ristabilire un certo grado di accettazione sociale, là dove tale gestione produca risultati controversi in contesti normativi caratterizzati da disaccordo su valori, norme e principi, come può accadere nelle società pluralistiche. In linea di principio, quanto più elevato è il grado di coesione sociale (di condivisione di valori, norme e principi fondamentali) in un dato contesto, tanto maggiore sarà il grado di accettabilità sociale del rischio insito nel processo di delegazione della gestione della sicurezza. Tuttavia, proprio i caratteri di automazione e standardizzazione tendono a elidere o a circoscrivere quella sfera pubblica di dibattito, interpretazione e valutazione, essenziale alla formazione di un grado sufficientemente informato, consapevole e responsabile, di accettazione sociale. Vi è una conseguenza ulteriore. Il difetto di mediazione tra l'istituzionalizzazione delle forme fiduciarie di sicurezza e la loro applicazione tende, in modo surrettizio, a far regredire la sicurezza intesa come *security* verso la sicurezza come *safety*, con la conseguente richiesta di maggiori poteri di controllo, direzione ed eccezione che la messa a repentaglio della vita tende a giustificare. Forse, non è stato sufficientemente rimarcato come, nell'età della sicurezza generalizzata, la pretesa minaccia permanente di pericoli improvvisi, diffusi e imprevedibili, stia alla base dell'incorporazione della gestione del rischio in processi e dispositivi tecnologici sempre più standardizzati e automatizzati, in una sorta di contraddizione o cortocircuito per cui il contingente presiede, oggi, alla fabbricazione del seriale e dell'automatico. Ad esempio, la sbandierata esigenza di prevenire crimini, cyber-attacchi o altre forme di terrorismo, ha avallato nel tempo e in più contesti l'attivazione di sistemi di filtraggio automatico e capillare per la raccolta di informazioni e dati personali, che ha dato luogo allo scandalo del progetto Prisma dell'Agenzia nordamericana per la sicurezza nazionale (NSA) e i cosiddetti file GCHQ britannici[34] ed è stato severamente giudicato, in Europa, dalla Corte Europea di Giustizia illegittimo perché indiscriminato (C-360/10, §§ 50)[35].

---

[33] Tale problematica è, ad esempio, efficacemente sottolineata da Jonathan Zittrain per ciò che concerne più specificatamente l'ambito del diritto e dell'automazione giuridica, il quale pone in evidenza che ad essere messa a rischio è proprio "the public understanding of law with its application eliminating a useful interface between the law's terms and its application". Sul punto v. J. Zittrain, "Perfect Enforcement on Tomorrow's Internet", in R. Brownsword – K. Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, London, Hart, 2007, pp. 125-156.

[34] Vedi sul punto l'articolo di John Lancaster, *The Snowden files: why the British public should be worried about GCHQ*, in "The Guardian", 3 ottobre 2013, accessibile online al seguente indirizzo: *http://www.theguardian.com/world/2013/oct/03/edward-swonden-files-john-lancaster*.

[35] Per una dettagliata analisi del tema v. U. Pagallo, *Il diritto nell'età dell'informazione*, op. cit., in particolare pp. 174-183.

3.2.3. *La natura abilitante dei processi e dispositivi tecnologici*

In terzo luogo, occorre considerare la natura *abilitante* dei processi e dispositivi tecnologici. La tecnologia crea possibilità che alterano l'ambiente in cui l'uomo agisce e sono suscettibili di rendere obsoleto il diritto esistente e mutare la realtà sociale e politica. Tali possibilità rilevano, inoltre, sotto un aspetto cruciale: quello del potere. Infatti, se implementate, esse assegnano nuovi poteri o modificano la struttura dei poteri esistenti, allocando o ridistribuendo il potere secondo logiche differenti da quelle che organizzano o regolamentano un dato sistema[36]. È in ragione di tale redistribuzione del potere che la tecnologia interessa la politica, il diritto e l'economia, e obbliga a ripensare le condizioni e i modi in cui tale potere è creato, allocato, ridistribuito. Da tale redistribuzione dipende, in larga misura, la riconfigurazione di una società o di un dato sistema politico, giuridico ed economico[37].

La redistribuzione del potere, frutto dell'evoluzione tecnologica, non è necessariamente né legittimata politicamente (tramite una qualche forma di sanzione democratica) né ratificata giuridicamente (*ex ante* da un parlamento o *ex post* dalle corti). Questo punto è stato rilevato, in altro ambito, da Lawrence Lessig, che ha sostenuto l'idea che, nelle società tecnologicamente avanzate, la regolazione delle condotte sociali non è più avocata esclusivamente o prevalentemente al diritto ma è sempre più l'esito dell'interazione o della competizione tra diversi sistemi regolativi (diritto, economia, architettura, norme sociali, tecnologia), in cui "il codice è la legge"[38], la regolazione avviene con l'incorporazione di norme nella tecnologia: "Questo è il futuro della legge sul copyright: più che di *legge*, si tratta di *codice* sul copyright. I controlli sull'accesso ai contenuti non saranno ratificati dai tribunali; saranno controlli inseriti dai programmatori tramite il codice. E, mentre i controlli introdotti per legge sono sempre verifi-

---

[36] Su questa dinamica cfr. M. Durante, *Il futuro del web: etica, diritto, decentramento. Dalla sussidiarietà digitale all'economia dell'informazione in rete*, Collana Digitalica, Torino, Giappichelli, 2007, in particolare pp. 284-289.

[37] In tal senso v. ad esempio Y. Benkler, *La ricchezza della rete. La produzione sociale trasforma il mercato e aumenta lelibertà*, op. cit., p. 39: "La tecnologia da sola tuttavia, non può determinare una struttura sociale. […] La tecnologia non è però nemmeno del tutto irrilevante. […] La tecnologia apre nuovi, possibili spazi alle pratiche sociali. In base a determinate condizioni tecnologiche, alcune cose possono diventare più semplici ed economiche, altre possono diventare più complesse ed onerose. Le caratteristiche di un determinato periodo storico dipendono dall'interazione tra gli spazi di fattibilità tecno-economica e le risposte sociali a tali cambiamenti – sia in termini di risposte istituzionali, come leggi e regolamenti, sia di cambiamenti nelle pratiche sociali".

[38] L. Lessig, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999, e dello stesso autore, *Code: Version 2.0*, New York, Basic Books, 2006.

cati da un giudice, quelli inseriti nella tecnologia sono sprovvisti di analoghi riscontri"[39].

Tale redistribuzione del potere è suscettibile di mutare, in modo più o meno visibile, determinati assetti istituzionali e la distribuzione del potere tra gli attori politici[40]. Come è intuibile, ciò coinvolge anche l'incorporazione della gestione della sicurezza in processi e dispositivi tecnologici e, dunque, l'affidamento sul processo di standardizzazione e automazione di tali processi e dispositivi. Occorre ribadire un punto già rimarcato nel corso del saggio. Nelle relazioni interpersonali la fiducia è prestata di norma in termini puntuali e condizionali ed è sottoposta nel tempo a qualche forma di verifica: anche la fiducia politica, pur avendo un carattere sistemico e non strettamente puntuale e condizionale, possiede però una certa ciclicità e temperatura, che fanno sì che la sua concessione non sia mai piena e incondizionata ma anzi accompagnata da riserve, riscontri e ripensamenti. Non si può dire lo stesso della fiducia riposta nello strumento tecnico. Se la fiducia implica la decisione di dipendere[41] dal comportamento altrui per realizzare dati obiettivi, allora dipendenza tecnologica e diffusione delle attività basate su computer implicano che la prestazione di fiducia nei confronti dei processi e dispositivi tecnologici sia data all'ingrosso[42] e abbia un carattere sistematico. Ciò assicura a chi governa tramite l'istituzionalizzazione di forme di gestione della sicurezza affidata a processi e dispositivi tecnologici di beneficiare spesso di prestazioni fiduciarie che o risultano sostanzialmente indiscriminate e dispensate da verifica o, allorché la fiducia sia tradita, deflagrano in scandali.

La successione di scandali che ha accompagnato le attuali politiche della sicurezza – per cui si potrebbe dire che le politiche della sicurezza sono innanzitutto politiche dello scandalo – è rivelatrice non solo della particolare riallocazione del potere che la tecnologia ha permesso, talora senza una reale legittimazione politica e democratica, ma anche dell'asimmetria informativa che circonda tale riallocazione del potere e rappresenta per certi aspetti il tratto costitutivo del potere politico nelle società dell'informazione. Occorre, dunque, puntare la nostra attenzione su tale aspetto problematico, che investe la relazione tra informazione, fiducia e sicurezza.

3.3. *Il rapporto tra informazione, fiducia e sicurezza*

---

[39] L. Lessig, *Cultura libera. Un equilibrio fra anarchia e controllo, contro l'estremismo della proprietà intellettuale* [2004], Milano, Apogeo, 2005, p. 143.

[40] Sul punto v. M. Durante, *Il futuro del web*, op. cit., pp. 284-287; e inoltre U. Pagallo, *Il diritto nell'età dell'informazione*, op. cit., pp. 168-183.

[41] In tal senso cfr. M. Taddeo, "Fiducia o*n-line*: rischi e vantaggi", in M. Durante – U. Pagallo (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, Utet, 2012, pp. 419-435.

[42] Sul punto v. M. Durante, *Il futuro del web*, op. cit., p. 29.

Le tecnologie dell'informazione e della comunicazione stanno reontologizzando la realtà, vale a dire costruendo un mondo fatto da informazioni: un "habitat informazionale"[43] o, per dirlo con Luciano Floridi, "un'infosfera"[44], che supera la dicotomia offline/online[45]. Secondo tale visione, le informazioni sono il presupposto sulla cui base ci rappresentiamo il mondo, l'interpretiamo, prendiamo decisioni e agiamo conformemente ad aspettative, conoscenze e cultura che elaboriamo con le risorse informative a disposizione. In questa ottica, la politica non può più essere intesa unicamente come arte di governo o come sfera delle decisioni collettive sovrane (normativamente) né come ambizione al monopolio legittimo dell'uso della forza o al controllo su un territorio (descrittivamente). Essa deve, piuttosto, essere intesa come forma di gestione e controllo sul ciclo di vita dell'informazione (produzione, emissione, circolazione, distribuzione, immagazzinamento, ridistribuzione e cancellazione dei dati[46]), che condiziona la formazione della public mind, la prestazione del consenso, l'elaborazione dei processi decisionali e la legittimazione dell'esercizio del potere politico. Tale concezione della politica, elaborata nel quadro delle società dell'informazione tecnologicamente avanzate, investe anche le politiche della sicurezza e, in particolare, l'istituzionalizzazione delle forme fiduciarie di gestione della sicurezza. Ciò richiede di considerare la relazione che sicurezza e fiducia intrattengono con le informazioni nel quadro fin qui delineato.

Il controllo sulle informazioni è vitale per qualunque progetto o politica della sicurezza. La sicurezza di *x* non dipende solo dalla quantità di informazioni che *x* detiene ma anche e soprattutto dalla sua capacità di modellare l'accesso che altri hanno a tali informazioni. La sicurezza di *x* può dipendere, infatti, sia dal sottrarre ad altri un'informazione (dove ho nascosto la refurtiva) sia dal fornire loro un'informazione (il mio gruppo sanguigno). La sicurezza dipende dal controllo sulle informazioni (*rectius*: sul ciclo di vita delle informazioni): il loro con-

---

[43] Per tale espressione v. Y. Kallinikos, *The Consequences of Information. Institutional Implications of Technological Change*, Cheltenham, Edward Elgar, 2006. Sul punto v. anche dello stesso autore, *Governing through technology. Information Artefacts and Social Practice*, Basingstoke, Palgrave MacMillan; e con N. Tempini, *Post-material Meditations: on Data Tokens, Knowledge and Behavior*, 2012, accessible online all'indirizzo: *www.tigair.info/docs/kalltemp_egos11.pdf*.

[44] Per tale nozione v. Floridi, *Infosfera. Etica e filosofia dell'informazione*, traduzione di M. Durante, introduzione di T.-W. Bynum, Collana Digitalica, Torino, Giappichelli, 2009.

[45] In tal senso osserva bene L. Floridi, *La rivoluzione dell'informazione*, op. cit., p. 14: "Stiamo assistendo, dunque, a una migrazione epocale e senza precedenti dell'umanità dal suo habitat consueto all'infosfera stessa, e ciò anche in ragione del fatto che quest'ultima sta assorbendo il primo. [...] Quando gli immigranti digitali come noi saranno sostituiti da nativi digitali come i nostri figli, il corso dell'e-migrazione sarà completato e le future generazioni si sentiranno sempre più deprivate, escluse, svantaggiate o povere, ogni qualvolta si troveranno disconnesse dall'infosfera, come pesci fuor d'acqua".

[46] Sul tema v. diffusamente Floridi, *La rivoluzione dell'informazione*, op. cit.

trollo è un modo per gestire la sicurezza. Tuttavia, come recenti esperienze insegnano in modo tragico (si pensi a molti attentati terroristici), il controllo sulle informazioni (in quanto presupposto della sicurezza) dipende a sua volta dalla capacità di un sistema di avere accesso a informazioni rilevanti e attendibili. Chi stabilisce quali siano le informazioni rilevanti, cui prestare attenzione? E quali siano quelle attendibili, vale a dire degne di fiducia?

Anche la fiducia intrattiene un rapporto vitale con le informazioni, da cui sono escluse due situazioni limite: quella della completezza delle informazioni, dato che la certezza non esige prestazione fiduciaria; e quella della totale incompletezza delle informazioni, poiché l'ignoranza richiede una prestazione fiduciaria cieca. La fiducia ha sempre rapporto con informazioni incomplete: dipende cioè dall'incompletezza delle informazioni o, meglio, è un modo per gestire la loro incompletezza. Da questo punto di vista, fiducia e sicurezza hanno un rapporto diverso con le informazioni. La fiducia è relativa a un certo livello di informazioni: troppe informazioni o troppo poche tendono a escludere le circostanze in cui importa prestare fiducia. La sicurezza ha piuttosto un rapporto scalare con le informazioni. Maggiori informazioni e maggiore controllo sulle informazioni producono maggiore sicurezza, con un limite significativo però: quello segnato dall'esigenza di fare fronte al sovraccarico informativo[47] che rende più difficile l'accesso alle informazioni rilevanti e attendibili. Si potrebbe sostenere, perciò, che si ha tanta più sicurezza quanto maggiore è il controllo di cui si dispone su maggiori informazioni rilevanti e attendibili. Ciò solleva una serie di interrogativi destinati a strutturare le politiche della sicurezza e dell'informazione[48] nelle società dell'informazione: 1) chi ha accesso a quali informazioni (ciò pone il problema della disponibilità di informazioni)? 2) Chi è il custode delle informazioni rilevanti e attendibili (ciò pone il problema del controllo sulle informazioni)? 3) Chi può sollevare domande circa la gestione dei flussi di informazioni rilevanti e attendibili (ciò pone il problema della gestione delle condizioni di insicurezza o incertezza)?

Non è possibile rispondere a tali interrogativi in questa sede. Dobbiamo limitarci a osservare che le politiche della sicurezza sono destinate a costruirsi come

---

[47] Tale espressione fa riferimento alla situazione parossistica in cui la sovrabbondanza di informazioni (*information overload*) impedisce ad un sistema (o utente) di gestire e decodificare le informazioni che provengono dall'ambiente, fino a paralizzare il flusso informativo, realizzando un paradosso tipico della società dell'informazione. Per un'introduzione a questi problemi, dal punto di vista della teoria dell'informazione, v. L. Floridi (ed.), *The Cambridge Handbook of Information and Computer*, Cambridge, Cambridge University Press, 2010, e dello stesso autore, *La rivoluzione dell'informazione*, op. cit.

[48] Dobbiamo la seguente tripartizione alla riflessione di Luciano Floridi che la pone al centro di un'indagine tuttora in corso sulle politiche dell'informazione nell'età contemporanea.

processo di istituzionalizzazione di forme fiduciarie nella gestione dell'accesso, controllo e decodificazione delle informazioni. Possiamo, però, fare una considerazione di carattere generale, per segnalare una discontinuità con il passato più recente della società della sorveglianza. Non si tratta tanto di acquisire informazioni, sottraendole al loro legittimo possessore, quanto piuttosto di inferire informazioni dalla grande mole di dati (*Big Data*)[49] che molti sono spinti a rivelare spontaneamente nella società dell'"autocomunicazione di massa"[50], per riprendere una celebre formula. Ciò tende a produrre una più penetrante forma di sorveglianza, in cui non si acquisiscono informazioni che appartenevano alla sfera di riservatezza delle persone ma informazioni che gli individui rilasciano volontariamente [51] o informazioni nuove che neppure il singolo conosceva su di sé[52]. Con la generalizzazione del racconto di sé, da cui s'inferiscono profili, pattern e tipologie, la nuova sorveglianza non controlla gli individui: *li produce in serie*. Non si tratta, dunque, solo di bilanciare sicurezza o sorveglianza con la privacy intesa come riservatezza, ma con quella privacy decisionale e informazionale[53], in cui consiste il diritto degli individui a costruire liberamente la loro

[49] Sul tema v. di recente A.-G. Ferguson, "Big Data and Predictive Reasonable Suspicion", in *University of Pennsylvania Law Review*, 163/2, 2015, pp. 329-410, accessibile online al seguente indirizzo: http://ssrn.com/abstract=2394683. Nella prospettiva di un contemperamento tra sicurezza e privacy v. N.-M. Richards – J.-H. King, "Big Data and the Future for Privacy", Ottobre 2014, accessibile online all'indirizzo: http://ssrn.com/abstract=2512069.

[50] M. Castells, *Comunicazione e potere*, op. cit, p. 60: "Con la diffusione di Internet, però, è emersa una nuova forma di comunicazione interattiva, caratterizzata dalla possibilità di inviare messaggi *many-to-many*, in tempo reale o in un momento stabilito, e con la possibilità di usare la comunicazione *point-to-point*, in narrowcasting o broadcasting, a seconda dello scopo e delle caratteristiche della pratica comunicativa prescelta. Chiamo *autocomunicazione di massa* questa forma storicamente nuova di comunicazione".

[51] Sul punto vedi quanto sostiene David Lyon (in D. Lyon – Z. Bauman, *Sesto potere. La sorveglianza nella modernità liquida*, op. cit.), p. 8: "Io credo che la caratteristica più saliente della versione contemporanea della sorveglianza sia il fatto che è riuscita in qualche modo a costringere e persuadere gli opposti a lavorare all'unisono, a metterli al servizio della stessa realtà. Da una parte, il vecchio stratagemma panottico (…) viene implementato, gradualmente ma in modo coerente e apparentemente inarrestabile, su scala pressoché universale. Dall'altra parte, ora che il vecchio incubo panottico di 'non essere mai più soli' (abbandonati, ignorati e negletti, bocciati ed esclusi) è venuto meno, la gioia di essere notati ha la meglio sulla paura di essere svelati".

[52] Su questo aspetto della nuova sorveglianza v. U. Pagallo, *Il diritto nell'età dell'informazione*, op. cit., pp. 179-183.

[53] Sull'evoluzione dell'idea di privacy v. H. Tavani, "Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy", in *Metaphilosophy*, 38/1, pp. 1-22. Sui diversi concetti e modelli di privacy v. U. Pagallo, *La tutela della privacy negli Stati Uniti d'America e in Europa. Modelli giuridici a confronto*, Milano, Giuffré, 2008.

personalità insieme con la loro autodeterminazione informativa[54]. La sicurezza ha come limite politico e giuridico con cui confrontarsi l'integrità dell'identità individuale e la dignità della persona, concepite come quella libera e autonoma costruzione del sé non interamente negoziabile e scambiabile.

4. Conclusioni

La sicurezza ha un ruolo sempre più centrale nella politica contemporanea. Sia essa intesa come *safety* o *security*, la sicurezza costituisce una leva politica cruciale, che consente a un governo di dotarsi di maggiori poteri di direzione e controllo con la promessa di un'immunizzazione della società dai rischi o pericoli che ne minacciano l'integrità. Tuttavia, tale immunizzazione è sempre relativa, non solo perché non si può immaginare un'esistenza posta al riparo da qualsiasi minaccia, ma per una ragione più essenziale, non sempre indagata a fondo, che investe la relazione complessa e problematica tra sicurezza e fiducia.

La sicurezza è invero sempre affidata. Di norma, essa non è gestita o assicurata in proprio ma delegata a forme fiduciarie che istituzionalizzano e prendono in carico la gestione del rischio. La sicurezza esige, dunque, fiducia e affidamento. Tuttavia, dove vi sono fiducia e affidamento, vi è rischio. Quel rischio, da cui la società pretende essere in tutto o in parte immunizzata con le politiche della sicurezza, riappare sotto mutate spoglie nelle forme fiduciarie di gestione del rischio. Il processo di delegazione della gestione della sicurezza è, infatti, suscettibile di produrre una riallocazione del potere tra gli attori politici e una riconfigurazione degli assetti istituzionali. Nel presente, tale processo di delegazione tende a saldarsi con la dipendenza tecnologica delle società odierne e, pertanto, ad affidare la gestione della sicurezza a processi e dispositivi tecnologici sempre più automatizzati e standardizzati.

Il carattere impersonale, anonimo, apparentemente neutrale e benigno dei processi e dispositivi tecnologici fanno sì che la riallocazione del potere e la riconfigurazione degli assetti istituzionali non sempre passino al vaglio di uno scrutinio pubblico che ne assicuri la legittimità politica e democratica, insieme a una discussione più aperta e consapevole sui modi in cui sono controllati e regolati l'accesso, la raccolta e l'acquisizione dei dati. Tale fenomeno si iscrive nel quadro di un progressivo mutamento del soggetto della politica: il plesso governanti/governati cede il passo alla centralità del plesso governabile/ingovernabile[55].

---

[54] Sul tema v. A. Glorioso, "Un nuovo concetto di 'auto-determinazione informazionale' come bussola concettuale per navigare il nuovo mondo digitale", in M. Durante – U. Pagallo (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, op. cit., pp. 383-394.

[55] Sul rischio di un *presente ingovernabile* (per riprendere un'espressione di David Bidussa) cfr. W. Sofsky, *Rischio e sicurezza*, Einaudi, Torino, 2005. Con un eccesso di enfasi e di pessimismo, Zygmunt Bauman segnala (in D. Lyon – Z. Bauman, *Sesto potere. La sorveglianza nella modernità liquida*, op. cit., rispettivamente p. 101 e p. 74) "il divorzio incombente tra il potere (la possibilità di fare) e la politica (la possibilità di scegliere cosa fare", che si iscriverebbe nel qua-

Alla luce di tale mutamento la delegazione della gestione del rischio a processi e dispositivi tecnologici da parte delle politiche della sicurezza è raffigurata come un carattere *emergente* della complessità delle società contemporanee, suscettibile di comportare tuttavia, nella sua opacità, un allentamento dei diritti e un affievolimento delle forme di responsabilità politica.
Nel presente si assiste, perciò, a un apparente paradosso, per cui la sicurezza è sovente invocata come *safety* (cosa che garantisce maggiori poteri di direzione e controllo), ma più spesso praticata come *security*, in particolare con il ricorso alle risorse messe a disposizione dalla tecnologia in termini di processi e dispositivi automatizzati e standardizzati. Ciò dà luogo, o può dare luogo, a una sorta di contraddizione o cortocircuito democratico, in cui si mostra quella radicalizzazione dell'età contemporanea, rispetto al moderno e al postmoderno, per cui il contingente presiede, oggi, alla fabbricazione del seriale e dell'automatico, in cui illividisce e trascolora il progetto moderno di costruzione dell'identità individuale.

---

dro di un progressivo processo di "adiaforizzazione" (Z. Bauman, *Le sfide dell'etica*, Milano, Feltrinelli, 1996), per cui sistemi e processi sarebbero portati a sganciarsi da qualsiasi considerazione morale. Secondo Bauman, tale processo toccherebbe anche taluni aspetti della tecnologia, per cui "l'effetto più degno di nota dei progressi della tecnologia che ci permette di operare 'a distanza', con distacco, automaticamente, è *l'emancipazione progressiva e forse inarrestabile delle nostre azioni dai vincoli morali*".