NOMOS
Le attualità nel diritto

Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale

SORVEGLIANZA E CONTROLLO NELLA SOCIETÀ DELL'INFORMAZIONE. IL POSSIBILE CONTRIBUTO DELL'ETICA HACKER*

di Gianluigi Fioriglio **

SOMMARIO: 1. La società della sorveglianza e del controllo. – 2. Da "privacy e sicurezza" a "sorveglianza e sicurezza". – 3. La sorveglianza elettronica. – 4. Possibili evoluzioni e contributi dell'etica hacker.

1. La società della sorveglianza e del controllo.

La Società dell'informazione è sempre più una società della sorveglianza e del controllo, grazie alla concorrenza di molteplici e ben noti fattori e fenomeni, informatici e non. Fra essi possono qui ricordarsi la diffusione delle nuove tecnologie, la loro convergenza e pervasività, la globalizzazione, gli "allarmi sicurezza" a vario titolo, e così via. In tale quadro, qui solo brevemente accennato, sembrano trovare nuovo stimolo quei timori circa la tutela della "privacy informatica" che venivano paventati negli anni Settanta. Oggi, infatti, la persona non solo è sempre più trasparente ma anche sempre più digitalizzata e profilata.

Da un lato, strumenti informatici sempre più evoluti, ivi inclusi agenti software di elevata complessità, consentono di acquisire costantemente una notevole mole di dati personali, che, più specificatamente, vengono raccolti ed elaborati automaticamente per i fini più diversi, senza che gli interessati ne abbiano spesso contezza. Consentono, altresì, di bloccare, filtrare o comunque controllare contenuti ritenuti illeciti o contrari al regime politico dominante.

Dall'altro, bisogna considerare i rischi derivanti dall'evoluzione verso il web 2.0, prima, e il social web, poi, in cui il passaggio da una prospettiva *top-down* a una (seppur parziale) prospettiva *bottom-up* porta molti soggetti a perdere, più o meno volontariamente, il controllo di alcuni dati personali che li riguardano mediante la loro comunicazione a terze parti e la loro diffusione.

* Il presente saggio è una versione accresciuta della relazione presentata alla XXIX Conferenza Nazionale della Società Italiana di Filosofia del Diritto ("La filosofia del diritto fra storia delle idee e nuove tecnologie", workshop su "Nuove tecnologie e società"), Ravenna, 19 settembre 2014.

** Dottore di ricerca; Dipartimento di Scienze Politiche, "Sapienza" Università di Roma.

La problematica centrale al presente saggio ha tuttavia radici ben lontane, ove non si tenga presente esclusivamente la situazione contemporanea ingenerata dall'incessante incedere delle tecnologie ma piuttosto si prenda in seppur breve considerazione l'importanza concettuale e pratica della segretezza.

In tal senso, il punto di partenza non può che essere costituito dalla narrazione di Platone dell'anello di Gige e delle nefandezze che chiunque potrebbe compiere qualora avesse la certezza di non essere scoperto: "privatamente ogni uomo giudica assai più vantaggiosa l'ingiustizia che la giustizia"[1] e dunque ogni uomo si rivela nella sua essenza reale quando nessuno può vedere ciò che fa. La sorveglianza sociale è così un freno alle azioni dell'uomo e tale concetto è tuttora alla base di molte giustificazioni pratiche circa l'utilizzo di strumenti di sorveglianza e di controllo.

È evidente oltre che ben nota la correlazione con il concetto che sta alla base del modello di *Panopticon* teorizzato da Bentham: esso va ben oltre l'originaria matrice carceraria e rappresenta perfettamente il concetto di sorveglianza costante ancorché potenziale, va ad investire l'insieme delle relazioni sociali, da cui si può evincere che la sorveglianza è idonea a generare assetti nuovi dei poteri nonché a configurare la stessa costituzione del soggetto[2].

Come evidenziato da Foucault, "il dispositivo panoptico non è semplicemente una cerniera, un ingranaggio tra un meccanismo e una funzione; è un modo di far funzionare delle relazioni di potere entro una funzione, e una funzione per mezzo di queste relazioni di potere"[3].

Nel pensiero di Bentham, la sorveglianza consente di raggiungere diversi fini. Questi possono consistere in "punire i criminali incalliti, sorvegliare i pazzi, riformare i viziosi, isolare i sospetti, impiegare gli oziosi, mantenere gli indigenti, guarire i malati, istruire quelli che vogliono entrare nei vari settori dell'industria, o fornire l'istruzione alle future generazioni" e possono essere raggiunti mediante la costruzione dei relativi edifici "ove gli individui che devono essere controllati saranno il più assiduamente possibile sotto gli occhi delle persone che devono controllarli. L'ideale, se questo è lo scopo da raggiungere, esigerebbe che ogni individuo fosse in ogni istante in questa condizione. Essendo questo impossibile, il meglio che si possa auspicare è che in ogni istante, avendo motivo di credersi sorvegliato, e non avendo i mezzi di assicurarsi il contrario, *creda* di esserlo"[4]; è altresì importante "che per una porzione di tempo la più lunga possibile, ogni uomo *sia* realmente sotto sorveglianza"[5].

Per il filosofo inglese, i vantaggi del *Panopticon* sono di vario ordine e spaziano, in particolare, dalla onnipresenza potenziale del sorvegliante al fatto che tale metodologia di controllo si ripete in relazione all'intera scala gerarchica all'uopo in essere, per cui tutti saranno sorvegliati[6]. E, in risposta all'interrogativo circa il controllo dei controllori, propone di punire ogni mancanza con la massima severità: "È questo fatto che rende l'influsso del progetto

[1] Platone, *La Repubblica*, Roma-Bari, Laterza, 1994, (359-361) pp. 65-67..
[2] S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, Laterza, 2004, pp. 174-175.
[3] M. Foucault, *Sorvegliare e punire. Nascita della prigione*, tr. it., Torino, Einaudi, (ed. or. 1975) 2014, p. 225.
[4] J. Bentham, *Panopticon ovvero la casa d'ispezione*, tr. it., Venezia, Marsilio, 2009, p. 36.
[5] Ivi, p. 46.
[6] Ivi, p. 48.

non meno salutare a ciò che si chiama *libertà* che alla necessaria coercizione; non meno potente come controllo sul potere subordinato che come freno alla delinquenza; come schermo all'innocenza che come castigo per il crimine"[7].

La massima trasparenza, dunque, assurge ad elemento fondamentale e imprescindibile per il raggiungimento di scopi astrattamente condivisibili; e si può qui ricordare il sogno di Rousseau, come citato da Foucault nell'introdurre una edizione del *Panopticon* di Bentham, "di una società trasparente, al tempo stesso visibile e leggibile in ciascuna delle sue parti; che non ci siano più zone oscure, zone regolate da privilegi del potere reale o dalle prerogative di questo o di quel corpo, o ancora dal disordine; che ciascuno, dal punto di vista che occupa, possa vedere l'insieme della società; che i cuori comunichino gli uni con gli altri, che gli sguardi non incontrino più ostacoli, che regni l'opinione, l'opinione di tutti su tutti"[8],

Come evidenziato anche da Norberto Bobbio, non a caso la segretezza è in stretta connessione con il potere e il suo esercizio tanto da rendere rivoluzionario il principio della visibilità poiché esso contrasta la tendenza naturale di ogni forma di potere a nascondersi, il che può verificarsi o tacendo le proprie intenzioni o dichiarandole in forma menzognera[9].

Ma, oggi, tacere diviene sempre più difficile per qualsiasi potere (politico od economico, pubblico o privato), come dimostrano, in modo inequivocabile numerosi casi anche eclatanti come *WikiLeaks* e *NSAgate*, poiché i flussi informativi digitalizzati sono sempre più rapidi e incontrollabili così come le infrastrutture tecnologiche su cui viaggiano. Anche in virtù di ciò, come di seguito sarà più compiutamente esposto, diviene di estremo rilievo il controllo degli strati della Rete (infrastruttura, applicazioni, dati: v. *infra*).

Non bisogna tuttavia estremizzare la concettualizzazione e l'estremizzazione della trasparenza, che non è un bene di per sé, ma che indubbiamente lo è se correttamente pensata ed implementata; pertanto, si ripropone costantemente la problematica della liceità dei mezzi utilizzati per raggiungere i fini. Nel caso di specie, vi è il rischio che la trasparenza divenga il fine e non il mezzo (o uno dei mezzi) per raggiungerne una molteplicità: un esempio paradigmatico può ravvisarsi nel garantire l'imparzialità e il buon funzionamento della pubblica amministrazione. Uno scenario potenziale che estremizza gli effetti negativi di una società della sorveglianza e del controllo è sapientemente tratteggiato da George Orwell nel suo celebre "1984"[10], la cui visione distopica ha, com'è noto, influenzato gli ambiti più diversi, dai mass media agli studi accademici. Il "Grande fratello" è così assurto a simbolo metaforico di un controllo globale estremo e pervasivo, che non ha trovato riscontro nella Società dell'informazione in modo tanto palese ma, piuttosto, in modo più subdolo e sommerso. Anche in virtù della frammentazione di poteri, pubblici e privati, non si è infatti giunti ad un unico "Grande fratello" neanche in casi eclatanti come *Echelon* o *l'Information*

[7] Ivi, p. 49. E non vi sarebbe "nessun rischio che l'accrescimento di potere dovuto alla macchina panoptica possa degenerare in tirannia; il dispositivo disciplinare sarà controllato democraticamente, poiché sarà accessibile in ogni momento «al grande comitato del tribunale del mondo»" (M. Foucault, *Sorvegliare e punire*, op. cit., p. 226)..

[8] M. Foucault, *Introduzione*, in J. Bentham, *Panopticon ovvero la casa d'ispezione*, op. cit., p. 14.

[9] N. Bobbio, *Il futuro della democrazia*, Torino, Einaudi, 1995, pp. 215-216.

[10] G. Orwell, *1984*, tr. it., Milano, Mondadori, 2002.

Awareness Office[11], ma piuttosto ad una moltitudine di "Fratelli", grandi e piccoli[12]. Accanto a sistemi di controllo ed intercettazione più o meno globali, spesso gestiti dalle *intelligence* di vari stati, si accompagnano innumerevoli controlli effettuati da soggetti privati su scala più o meno ridotto a seconda dei casi[13].

La metafora del "Grande fratello", di per sé, esemplifica la perfetta negazione del *right to be let alone* così come teorizzato da Warren e Brandeis[14]: non si è mai soli, poiché si può essere sempre controllati, come in un Panopticon diffuso. Oggi, però, la concezione dei due giuristi statunitensi è ritenuta superata in favore di una più complessa concezione della privacy che pone al centro la facoltà dell'individuo di (tentare di) controllare i flussi informativi che lo riguardano[15]. In tal senso, la moltitudine dei "Fratelli" costituisce un attacco costante e sovente nascosto al diritto al controllo dei propri dati personali.

La metafora del "Grande fratello", seppur utile per esemplificare i rischi della sorveglianza globale dello Stato, non è dunque più adeguata a mostrare i rischi della Società della sorveglianza e del controllo.

In dottrina, così, è stato criticato il costante utilizzo della predetta metafora nonché il focalizzarsi sul modello della sorveglianza, poiché ciò distoglierebbe dagli aspetti più delicati connessi alla privacy informatica e, in particolare, circa gli innumerevoli database digitali. Il potere creato mediante essi sarebbe incontrollabile ed imperscrutabile, ponendo ciascuno di noi in una posizione di impossibilità di comprendere cosa realmente avviene, similmente a quanto accade ne "Il processo" di Kafka[16].

Il quadro, però, è più complesso e i dossier digitali sono solo una parte dei rischi della società contemporanea. Per delinearli compiutamente, appare necessario (ri)partire dalla considerazione che la persona è sempre più trasparente in una società in cui il controllo è tanto diffuso e pervasivo da permearla ed entrare in simbiosi con essa poiché l'acquisizione delle informazioni più diverse è tanto desiderabile, per il raggiungimento di diversi fini, da portare a una moltiplicazione dei sistemi di sorveglianza e controllo che va di pari passi con il fenomeno della moltiplicazione dei soggetti che acquisiscono e che esercitano diversi poteri.

---

[11] Sull'*Information Awareness Office* sia consentito rinviare a G. Fioriglio, *La privacy e i sistemi di controllo e di intercettazione globale: il caso dell'Information Awareness Office*, in *L'ircocervo*, 2003, 1.

[12] In altra prospettiva, Maria Rosaria Ferrarese ha evidenziato che, "paradossalmente, nelle società transnazionali, nonostante le accresciute e prodigiose potenzialità della tecnica, diventa difficile far funzionare un potenziale «panopticon» capace di controllare integralmente la vita dei soggetti, così come di far loro introiettare un determinato sistema di regole: sempre più, infatti, le regole sembrano «sfidate» da altre regole, potenziali o attuali in altri territori; e sempre più i soggetti possono sottrarre pezzi più o meno consistenti della propria vita all'osservanza di quelle regole, e scegliere di sottoporli ad altre" (M. R. Ferrarese, *Le istituzioni della globalizzazione. Diritto e diritti nella società transnazionale,* Bologna, Il Mulino, 2000, p. 47).

[13] Così, "diversamente dalle metafore del *Panopticon* e del *Grande Fratello*, il cui referente è un potere coercitivo centrale, tutto ora gira intorno al fatto che la sorveglianza prende forma in luoghi speciali, nei *non-luoghi informatici*, dove le informazioni di continuo introdotte diventano la contingente *misura di tutte le cose,* dove i dati automaticamente assemblati *vincolano* tutti e tutto, dove i risultati mutano involontariamente le entità, i significati e le vite su scala globale. Se le linee infatti di confine tra interno ed esterno sono problematiche, se il centro e la periferia si riorganizzano di continuo e casualmente, la *sorveglianza* non può non diventare *orizzontale*: sì da trasformare *tutti* (attori umani e non umani) in potenziali sorveglianti di qualcosa e di qualcuno" (A. C. Amato Mangiameli, *Diritto e cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Torino, Giappichelli, 2000, p. 22).

[14] S. D Warren – L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890, 5.

[15] L'evoluzione è ben tratteggiata da S. Rodotà (*Privacy e costruzione della sfera privata*, in *Politica del diritto*, 1991, ora in *Tecnologie e diritti*, Bologna, Il Mulino, 1995 p. 108).

[16] D. J. Solove, *The Digital Person. Technology and privacy in the information age*, New York, New York University Press, 2004, pp. 27-42.

Come sottolineato da Mario Losano, "lo sviluppo dell'informatica e delle reti di telecomunicazioni hanno reso ormai trasparente la società. Il cittadino si sente osservato senza possibilità di scampo, come un pesce rosso nella sua boccia di cristallo. Questo espressione è nata proprio nei paesi scandinavi, dove il controllo statale è assai forte e dove altrettanto forte è l'esigenza di una severa legge sulla tutela dei dati individuali"[17] E, del resto, "il terrorismo di Stato nel XX secolo è stato praticato dai Paesi a regime totalitario anche facendo ricorso a metodi di sorveglianza e repressione forniti di strumenti tecnologici moderni"[18].

L'evoluzione tecnologica facilita notevolmente il processo qui appena tratteggiato ed amplia lo spettro delle possibili attività che possono potenzialmente essere svolte. Prima di approfondire tali aspetti, appare opportuno ricordare quanto scritto, in linea più generale, da Vittorio Frosini: non dobbiamo dimenticare che "la tecnica di ieri e la tecnologia di oggi appartengono alla natura umana: è il mondo artificiale che l'uomo si è fabbricato, e che è molto più vicino alla sua umanità di quanto lo sia il mondo naturale, da cui l'uomo è stato generato nel corso dell'evoluzione cosmica"[19].

Dunque, non siamo dinanzi ad attività inconoscibili all'uomo per loro natura, bensì a tecnologie create dagli uomini per controllarne altri. Si ripropone, ancora una volta, "l'immagine di una tecnologia bifronte, come l'antico dio Giano. Di fronte a noi stanno «tecnologie della libertà» o «tecnologie del controllo»?"[20].

La società, dunque, si modifica. Non solo Società dell'informazione, ma anche Società della sorveglianza e del controllo, come si è detto. Se in Bentham e in Orwell vi era la possibilità di essere controllati, oggi quasi sussiste la certezza di esserlo senza tuttavia poterne anticipare le conseguenze anche a lungo termine in virtù del progresso tecnologico che prevedibilmente consentirà trattamenti incrociati di dati sempre più sofisticati, per cui anche il concetto di anonimato e di dato anonimo non possono che essere considerati in costante evoluzione. Difatti, anche se oggi non abbiamo strumenti tanto sofisticati da consentire un perfetto trattamento della enorme e sempre crescente mole di dati personali accumulata, bisogna pur considerare che l'evoluzione della tecnologia suggerisce che in un futuro non troppo remoto sarà possibile effettuare trattamenti incrociati di dati in modo più efficiente, che potrebbero così rendere varie le operazioni di anonimizzazione parziale potenzialmente effettuate sino ad oggi.

In linea più generale, si pone nuovamente il problema dei poteri di quello stesso Stato che non solo è sorvegliante ma che di fatto consente ai privati di sorvegliarne altri, e che sempre più spesso travalica i propri confini anche indipendentemente dal controllo della Rete. Il tutto deve essere bilanciato con i diritti fondamentali, individuali e collettivi; ossia, sia della

[17] M. G. Losano, *Il diritto pubblico dell'informatica. Corso di informatica giuridica*, Torino, Einaudi, 1986, pp. 14-15.
[18] V. Frosini, *La democrazia nel XXI secolo,* Macerata, Liberilibri, 2010 (1997), pp. 46-47.
[19] Ivi, p. 20.
[20] S. Rodotà, *Tecnopolitica*, op. cit., p. 27. In senso più ampio, come osservato da Carl Schmitt ed evidenziato da Bruno Montanari, "non è la tecnologia, come tale, ad essere divenuta un potere a sé stante, poiché la natura del potere è tale che può appartenere solo all'uomo e non ad una certa entità inanimata; essa, tuttavia, tiene in scacco l'uomo, perché si frappone alla relazione umana, impedendo agli uomini di guardarsi direttamente negli occhi, fino a rendere *inumano* il contesto umano" (B. Montanari, *La fragilità del potere. L'uomo, la vita, la morte*, Milano-Udine, Mimesis, 2013, p. 138).

singola persona che delle formazioni sociali dove si svolge la sua personalità (intese in senso lato).

In modo estremamente efficace, Stefano Rodotà evidenzia che non possiamo che convivere con la Società della sorveglianza, oramai divenuta un carattere della postmodernità, in cui una gabbia elettronica (al posto di quella d'acciaio di weberiana memoria) viene implacabilmente costruita intorno a ciascuna persona, che non può liberarsene con una negazione o una semplice ripulsa. Pertanto, è necessario operare la definizione di quelle condizioni che possano permettere di evitare che la società della sorveglianza "si risolva nel controllo autoritario, nella discriminazione, in vecchie e nuove stratificazioni sociali produttive di esclusione, nel dominio pieno di una logica di mercato che cerca una ulteriore legittimazione proprio nella tecnologia. Questo esige processi sociali, soluzioni istituzionali capaci di tener fermo il quadro della democrazia e dei diritti di libertà. È vano confidare nella sola autodifesa dei singoli: le speranze non possono essere affidate alle «strategie da bracconiere» che ciascuno di noi può cercare di praticare"[21].

Come rilevato da Teresa Serra, "La libertà non può più essere intesa come *libertà da* o *libertà di*, ma deve essere intesa come *libertà con* e deve essere collegata ad una definizione di uomo non riduttiva, e nella dialettica dominio-libertà, parallela peraltro alla dialettica politica-diritto, chiede di essere guardata nella sua accezione più ampia. Occorre, perciò, recuperare il ruolo del diritto e di una giusta correlazione tra morale, diritto, politica ed economica. E se il diritto non deve cedere il passo alla politica, quest'ultima non deve farsi dominare dall'economia. Quando si parla di diritto politica economia, ecc. si parla, dunque, di sistemi di libertà, ma anche di sistemi di potere e, all'interno di questi sistemi, è necessario riconoscere non solo il ruolo e l'importanza delle regole e delle figure astratte, ma anche dell'aderenza alla realtà che non è mai riducibile internamente a un modello"[22].

2. Da "privacy e sicurezza" a "sorveglianza e sicurezza".

Nella Società contemporanea il binomio "privacy e sicurezza" sembra cedere il passo a "sorveglianza e sicurezza": così la travagliata conquista del riconoscimento, da parte di numerosi stati, del diritto alla privacy quale diritto fondamentale[23] viene messa in discussione dai costanti ed innumerevoli allarmi-sicurezza. La segretezza torna quindi ad assumere una valenza negativa, mostrata quale anelito di quel rifugio tanto agognato da chi ha da celare le proprie attività illecite dietro lo scudo del diritto in generale e del diritto alla privacy in particolare.

Come evidenzia Stefano Rodotà, si viene così a delineare una società dell'integrale trasparenza che postula l'«uomo di vetro» argomentando che la sorveglianza continua e generalizzata, nonché la cancellazione d'ogni ragionevole brandello di *privacy*, potrebbero inquietare solo chi ha qualcosa da nascondere. Eppure l'«uomo di vetro» è metafora nazista

[21] S. Rodotà, *Tecnopolitica*, op. cit., p. 165.
[22] T. Serra, *L'uomo programmato*, Torino, Giappichelli, 2003, p. 65.
[23] Sul punto, sia consentito rinviare, *ex multis*, a G. Fioriglio, *Il diritto alla privacy. Nuove frontiere nell'era di Internet*, Bologna, Bononia University Press, 2008.

che legittima la pretesa dello Stato di chiedere e ottenere qualsiasi informazione e che implica la classificazione come «sospetto» e «cattivo cittadino», come «nemico dello Stato», di chiunque intenda mantenere spazi d'intimità, esercizio libero di diritti[24].

Proprio il diritto alla privacy, del resto, è un diritto che, per sua natura, confligge con altri e dunque il bilanciamento con gli stessi non è certo operazione nuova per il giurista che si trova dinanzi a fattispecie in cui esso ha rilievo centrale. Oggi, però, la questione rileva sotto diversi profili, di seguito esposti.

In primo luogo, se lo Stato stesso viene visto come Stato della prevenzione o se comunque la prevenzione viene vista come uno dei suoi caratteri fondamentali, allora, come evidenziato da Adalgiso Amendola sulla scorta della tesi di Erhard Denninger, non si può che sottolineare la "prevalente natura, non più reattiva, ma proattiva del sistema giuridico, implicita nei nuovi significati preventivi della sicurezza. La funzione di anticipazione e prevenzione dei rischi, che nello Stato di prevenzione finisce per prevalere sulle modalità classiche di regolamentazione dei conflitti, segna, infatti, una discontinuità netta anche con la concezione della personalità giuridica[25]. Nell'anticipazione e nella prevenzione dei rischi, la sorveglianza e il controllo dei cittadini hanno un ruolo fondamentale, poiché permettono di monitorare e studiare la realtà in ogni momento; tuttavia, dal momento che la società è sempre più globale, anche la sorveglianza ha confini sempre più evanescenti e dunque il controllo può essere effettuato altresì invadendo virtualmente gli spazi e le prerogative di altri stati e dei loro cittadini[26].

In secondo luogo, la delicata operazione del bilanciamento fra diritti diversi comporta una molteplicità di valutazioni per decidere quale sia il diritto che dovrà soccombere. In situazioni di emergenza, come in caso di guerra, è ben noto che possa verificarsi una compressione di determinati diritti, seppur con taluni limiti come si è visto da Norimberga in poi. Tuttavia, anche la guerra si trasforma e quella al terrorismo ne è un esempio tanto palese quanto foriero di cambiamenti nella tematica che ci occupa. Difatti, "in passato, la guerra era dichiarata, vi era un atto formale che la apriva ed uno che poneva ad essa termine: il «tempo di guerra», con la possibilità di limitare le garanzie costituzionali, era circoscritto con precisione. La guerra al terrorismo, invece, non solo non ha confini, ma soprattutto è senza tempo: per definizione di chi la conduce, è una «guerra infinita». Diventerà anch'essa infinita la limitazione di diritti e garanzie? La guerra al terrorismo, inoltre, è contro un nemico invisibile, e per ciò si fonda potentemente sulla creazione e sull'utilizzazione della paura. Significherà, questo, che tutti diventano potenzialmente, se non nemici, almeno sospetti, legittimando ogni forma di controllo di massa? Dobbiamo, dunque, rassegnarci a vedere modificato il concetto stesso di libertà? Queste domande non possono essere eluse, né di essere può essere proposta una versione riduttiva. Ci stiamo interrogando, infatti, intorno ai caratteri di un sistema democratico, ai rapporti di legittimità e proporzionalità tra mezzi e

[24] S. Rodotà, *Tecnopolitica*, op. cit., p. 175. Nello stesso senso, Id., *La vita e le regole. Tra diritto e non diritto*, Milano, Feltrinelli, 2006, p. 104.

[25] A. Amendola, *Persona e soggetto giuridico nello Stato di prevenzione*, in *Filosofia politica*, 2007, 3, p. 417.

[26] Secondo S. Rodotà, "La sorveglianza non vuole più conoscere confini, né ostacoli alla utilizzazione di qualsiasi tecnica. Si impadronisce dello spazio, fisico e virtuale, si appropria dei corpi, attribuendo un ruolo sempre più centrale alle tecniche biomediche" (*Tecnopolitica*, op. cit., p. 177).

fini"[27]. L'era emergenziale e della guerra sommersa ma costante, combattuta con metodi tradizionali e non, rappresenta dunque una sfida anche giusfilosofica che, condotta in difesa dei principi fondamentali dello Stato e dei diritti fondamentali dei cittadini, pone dei quesiti in ordine ad alcuni caratteri nodali degli stati contemporanei.

In terzo luogo, il *focus* sulla sorveglianza rafforza un potere segreto presente in ogni stato, quello delle *intelligence*. Esse possono sorvegliare senza essere di fatto sorvegliate e hanno un ambito di operatività vastissimo: basti pensare che, secondo Edward Snowden, nella NSA e nelle sue omologhe delle altre nazioni, qualsiasi analista o qualsiasi selezionatore, in qualsiasi momento, può decidere di controllare chiunque[28]. Anch'esse, però, non sono immuni dai rischi insiti nella digitalizzazione delle informazioni: proprio il caso di Snowden ne è un chiaro esempio, così come lo è quello di WikiLeaks, atteso che le informazioni digitali, per loro natura, si prestano a essere clonate e diffuse all'infinito e una volta uscite dalla sfera di controllo di chi le detiene diviene estremamente difficile, se non di fatto impossibile, bloccarne l'eventuale diffusione. Inoltre, il potere incontrollato in capo ai predetti sorveglianti, soprattutto ove unito alle possibilità di manipolazione della realtà consentite dalle moderne tecnologie, pone un primo quesito: come tutelarsi nelle ipotesi in cui la realtà sorvegliata venga interpretata erroneamente? Ad esempio, in riferimento alla videosorveglianza, autorevole dottrina ha osservato che essa non sempre «fa vedere» la realtà, ma che può invero oscurarla mostrandone una sola, distorta, dimensione, tradotta nella sola dimensione dell'ordine pubblico. Addirittura, ciò, attribuisce all'organizzazione pubblica i connotati di uno Stato di polizia e induce anche le organizzazioni private e i cittadini a divenire prigionieri della stessa logica[29]; in linea più generale, "Si manifesta una nuova dimensione della sorveglianza, che esalta il potere dello Stato di disporre di qualsiasi informazione personale, da chiunque raccolta e indipendentemente dalle finalità originarie della raccolta"[30]. Anche altre ipotesi di sorveglianza, comunque, presentano criticità: basti pensare all'intercettazione di testi, che avulsi dal loro contesto possono assumere significati diversi[31]. Un ulteriore quesito, poi, sorge in caso di falsificazione dolosa di eventuali registrazioni o intercettazioni, poiché fornire prova contraria potrebbe essere una *probatio diabolica* stante l'elevato grado di sofisticazione raggiunto dai moderni sistemi informatici che permettono di realizzare immagini e filmati già indistinguibili dalla realtà.

---

[27] Ivi, p. 178.

[28] E. Snowden, *Ecco perché ho parlato*, intervista di G. Greenwald rip. in S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, Laterza, 2014, p. 79.

[29] S. Rodotà, *Tecnopolitica*, op. cit., p. 180.

[30] Ivi, p. 176.

[31] Celebre il caso di una piccola società americana che operava nel settore dei giochi di ruolo cartacei, la *Steve Jackson Games Inc.*. Essa, suo malgrado, fu coinvolta nell'operazione *Sundevil*, posta in essere negli anni novanta negli Stati Uniti contro la criminalità informatica (ma molti innocenti furono erroneamente perseguiti). Questa società non produceva nulla in forma elettronica, ma nel suo ambito i computer venivano utilizzati sia a fini professionali che per gestire una *BBS* nella quale i fruitori dei giochi creati dalla stessa azienda potevano dialogare. In questa *BBS* non c'era nessuna informazione illegale, ma essa era frequentata anche da *hackers* e *crackers*, per cui le forze dell'ordine avevano iniziato a sorvegliare le attività della società ed i contenuti della *BBS*. Gli investigatori, però, non solo scambiarono le avventure fittizie create dalla *Steve Jackson Games* per materiale utilizzabile a fini criminosi, ma addirittura ritenerono che "GURPS Cyberpunk", un gioco di ruolo su cui la stessa azienda puntava molto, fosse, in realtà, un "manuale per il crimine informatico" (Cfr. B. Sterling, *Giro di vite contro gli hacker*, tr. it., Milano, Mondadori, 2004).

In quarto luogo, la sorveglianza non è solo effettuata da Stati (democratici e non): la persona digitale è sempre più tracciata e controllata per fini di lucro da privati che accumulano una mole enorme di dati personali, rendendo oltremodo illusoria la prospettiva di un loro effettivo controllo. Se "la tendenza alla privatizzazione della sicurezza, oltre che ad una responsabilizzazione delle potenziali vittime e ad una particolare declinazione della loro partecipazione al processo giudiziario, ha a che fare anche, e soprattutto, con la proliferazione di spazi pubblici gestiti privatamente", che "vengono altresì sorvegliati da polizie private" [32], anche la privatizzazione della sicurezza e della sorveglianza diventa informatica e contribuisce a definire lo scenario della sorveglianza globale. L'ambito privato del controllo, in particolare, è estremamente delicato. Innanzi tutto, vi sono le attività di sorveglianza poste in essere per ragioni di sicurezza: basti pensare alle numerosissime telecamere che scrutano quasi ogni angolo dei centri urbani, all'interno e all'esterno degli edifici. Al problema della privacy dei cittadini si aggiunge quello, ben noto, della sorveglianza e del controllo dei lavoratori, cui il diritto positivo tende a rispondere mediante l'imposizione di limitazioni specifiche. Inoltre, quando la sorveglianza privata è svolta nel mondo dei consumi e della logica di mercato, "non ha come obiettivo quello di impedire o scoraggiare determinati comportamenti [;…] l'interesse è abitualmente quello di far sì che i comportamenti di consumo vengano il più possibile ripetuti"[33], mentre "chi fa parte della società dei consumatori è a sua volta un prodotto di consumo"[34] e la sorveglianza privata tende verso la proliferazione degli utenti, che non visti come persone ma, per l'appunto, come consumatori.

Il quadro, in parte potenziale e in parte reale, qui delineato evidenzia una problematica di particolare delicatezza: si provocano danni potenzialmente gravissimi e irreparabili su larga scala poiché è noto che quando si verifica una violazione della privacy è di fatto impossibile ripristinare la situazione *quo ante*. La risposta del diritto positivo si concretizza normalmente in illusorie normative che lo burocratizzano con particolare riferimento al profilo della protezione dei dati personali, fatti salvi i richiami a solenni principi di rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

Tuttavia, come rileva David Lyon, "È facile interpretare la diffusione della sorveglianza come fenomeno tecnologico o come qualcosa che ha che fare con il «controllo sociale» e con il «Grande fratello». Ma questo scarica tutto il peso sugli strumenti e sui tiranni, e ignora lo spirito che anima la sorveglianza, le ideologie che la sospingono, gli eventi che le offrono un'opportunità e la gente comune che si adegua ad essa, l'esamina e decide che, se non può sconfiggerla, le conviene stare al gioco" [35]. La sorveglianza diffusa tranquillizza e deresponsabilizza, poiché spinge a concentrarsi verso gli effetti e non le cause. Una simile visione non può essere accolta dal punto di vista giusfilosofico, poiché ciò comporterebbe

[32] T. Pitch, *La demoralizzazione del controllo sociale. Come fare giustizia del diritto?*, in *Iride*, 2001, 32, p. 112.

[33] S. Rodotà, *Tecnopolitica*, op. cit., p. 138. Così, "nella prospettiva che si viene delineando, invece, l'idea di sorveglianza invade ogni momento della vita e si presenta come un connotato delle relazioni di mercato, la cui fluidità è posta direttamente in relazione con la possibilità di disporre liberamente di una massa crescente di informazioni" (ivi, p. 136).

[34] Z. Bauman, in D. Lyon – Z. Bauman, *Sesto potere. La sorveglianza nella modernità liquida*, tr. it., Roma-Bari, Laterza, (ed. or. 2013), 2014, p. 19.

[35] D. Lyon, *Introduzione*, in D. Lyon – Z. Bauman, *Sesto potere*, ivi, pp. xvii-xviii.

l'attribuzione di un ruolo meramente punitivo allo Stato, in contraddizione ai principi fondanti delle moderne democrazie[36]

Esse, però, sembrano spingere verso una normalizzazione della sorveglianza, soprattutto digitale. Deilbert e Rohozinski evidenziano quanto sia paradossale che le norme che la giustificano e che la impongono siano palesemente contrarie ai principi e alle libertà fondamentali propugnati, ma che ciò nonostante vengano emanate da molti di quegli stati che all'inizio del XXI secolo avevano guidato l'espansione globale dei principi liberali e democratici, anche in relazione al mercato[37].

La difesa della libertà informatica dinanzi all'assalto di poteri pubblici e privati può dunque essere considerata come un obiettivo da perseguire per il moderno uomo di vetro. Nella Società della sorveglianza supera quella forma ben tratteggiata da Vittorio Frosini in relazione alla privacy, ossia "la libertà di custodire la propria riservatezza informatica [che] è divenuta anche la libertà di comunicare ad altri le informazioni trasmissibili per via telematica, cioè la libertà di usufruire delle reti di trasmissione senza limitazioni di frontiere, una libertà di espressione della propria personalità valendosi dei sistemi di comunicazione automatizzata"[38]. Oggi, presumibilmente, diviene necessario ed imprescindibile estendere le garanzie della libertà personale (art. 13 Cost.) anche al «corpo elettronico», seguendo la traiettoria della rilettura dell'*habeas corpus* come *habeas data*[39].

3. La sorveglianza elettronica.

Se nei tempi antichi la lontananza spaziale era un antidoto alla sorveglianza e al controllo, oggi ciò non è più possibile, poiché nella Società dell'informazione lo spazio perde il suo significato tradizionale e la sorveglianza elettronica assume un ruolo centrale. Come osserva Agata Cecilia Amato Mangiameli, sarebbe errato ritenere che la sorveglianza elettronica sia una semplice ed ennesima riproposizione del rapporto moderno sorvegliante - sorvegliato, poiché il controllo è oramai continuo, automatico e involontario[40]; non a caso, Norberto Bobbio aveva da tempo evidenziato che "l'uso degli elaboratori elettronici, che si va estendendo e sempre più si estenderà, per la memorizzazione delle schede personali di tutti i

[36] Non può, in tal senso, concordarsi con la suggestiva ed estrema tesi di una società trasparente prospettata dallo scrittore David Brin (D. Brin, *The Transparent Society. Will Technology Force Us to Choose Between Privacy and Freedom?*, New York, Basic Books, 1999). Come osserva Mayer-Schönberger, la trasparenza totale non è sempre positiva. "Brin suggests that such social transparency will take away our anonimity and make us all feel like we are living again in a small village, in which we'll behave because we are watched: "in the village, it wasn't fear of the retribution, per se, that kept you from behaving callously toward your neighbors; it was the sure knowledge that someone would tell your mother, and bring shame to your family. Tomorrow, when any citizen has access to the universal database to come, our ' village' will include millions, and nobody's mom will be more than an e-email away". Brin's reference to one's parent as a person of (relative) power brings his benign sounding metaphor right back to the kind of social control mechanism that is at the heart of Bentham's panopticon, o fan oppressive architecture of surveillance. This is exactly why many are very reluctant to share their information with others" (V. Mayer-Schönberger, *delete. The Virtue of Forgetting in the Digital Age*, Princeton and Oxford, Princeton University Press, 2011, p. 165).

[37] R. Deilbert - R. Rohozinski, *Beyond Denial*, in R. Deilbert – J. Palfrey – R. Rohozinski – J. Zittrain (edited by), *Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge (MA, MIT Press, 2010, p. 11.

[38] V. Frosini, *La democrazia nel XXI secolo,* op. cit., p. 41.

[39] S. Rodotà, *Il mondo nella rete*, op. cit., p. 69.

[40] A. C. Amato Mangiameli, *Diritto e cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Torino, Giappichelli, 2000, p. 22.

cittadini, permette e sempre più permetterà ai detentori del potere di vedere il pubblico assai meglio che negli Stati del passato. Ciò che il novello Principe può venire a sapere dei propri soggetti è incomparabilmente superiore a ciò che poteva sapere dei suoi sudditi anche il monarca più assoluto del passato"[41]. Tutto ciò si riverbera sulla società nel suo complesso e "si immiserisce la figura del cittadino, mentre riemerge quella del suddito e si impone prepotentemente quella del consumatore. Non è soltanto lo spazio virtuale ad essere trasformato. Anche lo spazio reale, i tradizionali luoghi pubblici – strade, piazze, parchi, stazioni, aeroporti – vengono sempre più sottoposti ad un controllo capillare, scrutati implacabilmente, segnando così il passaggio da una sorveglianza mirata ad una generalizzata"[42].

La sorveglianza è sempre più sofisticata, del resto, e il trattamento informatizzato dei dati diviene la regola, indipendentemente dai freni che taluni legislatori cercano di imporre a tali attività. Ad esempio, non è facile accertarsi che effettivamente i dati personali siano conservati solo per il tempo prescritto dalla normativa applicabile a ciascun caso concreto. Si crea così una memoria digitale che, seppur frammentata in una molteplicità di database, rappresenta una versione ancora più terribile di un ipotetico *Panopticon* digitale: tutto ciò che facciamo e che faremo può essere memorizzato, i nostri atti e le nostre parole potranno essere sottoposte a innumerevoli giudizi sia oggi sia in un futuro indefinito ed indefinibile[43].

Come si è visto e com'è noto, la sorveglianza è del resto posta in essere da soggetti pubblici e privati con una molteplicità di strumenti sempre più sofisticati e sempre più interconnessi. Così, alla convergenza delle tecnologie in senso lato si accompagna altresì la convergenza degli strumenti materiali e immateriali di controllo, inseriti in dispositivi o servizi di uso quotidiano la cui facilità di utilizzo fa da contraltare alla loro complessità intrinseca. Il tracciamento dei movimenti è ormai effettuato da vari dispositivi; inoltre, a breve le tecnologie indossabili (*wearable computing*) inizieranno a diffondersi, per cui la persona non sarà mai *tecnologicamente* sola e l'*ubiquitous computing* troverà sempre maggiore realizzazione concreta; e qualora si ritenga che le tecnologie più importanti siano proprio quelle che si dissolvono nella vita quotidiana sino a renderle indistinguibili da essa[44], allora l'importanza di quelle di sorveglianza e di controllo è indubbia.

Se a partire dagli anni settanta gli interventi, più o meno riusciti, di vari legislatori di arginare gli assalti alla *privacy* informatica sono stati comunque importanti per la tutela dei diritti di libertà informatica, negli anni a venire il ruolo del diritto dovrebbe essere ancora più forte, al fine di guidare l'evoluzione tecnologica nel rispetto dei principi e delle libertà fondamentali.

---

[41] N. Bobbio, *Stato, governo, società. Frammenti di un dizionario politico*, Torino, Einaudi, 1985, p. 21.

[42] S. Rodotà, *Tecnopolitica*, op. cit., p. 172.

[43] V. Mayer-Schönberger, *delete*, op. cit., p. 11. "At the interface of power and time, permanent remembering creates the specter of a spatial and temporal panopticon, in which everybody may constantly be tempted to self-censor" (ivi, p. 127). Inoltre, la sorveglianza può ribadire le vecchie disuguaglianze e discriminazioni sociali, nonché crearne di nuove: "essere o non essere in possesso di strumenti che provano che siamo affidabili, potere o no venire assicurati contro certi rischi, essere o no assunti per un certo lavoro sono sempre più questioni che dipendono dalla raccolta o interpretazione di dati ottenuti per via informatica, o, peggio, genetica e biometrica, attraverso cui vengono ricostruiti i "profili" di rischio rappresentati da ciascuno" (T. Pitch, *La società della prevenzione,*Roma, Carocci, 2010, p. 142).

[44] In tal senso M. Weiser, in *Mobile Computing and Communications Review*, (reprinted from *The Computer for the 21st Century*, in *Scientific American*, 1991, 3, pp. 94-104), 1999, 3, p. 3.

E, "accanto all'opera di difesa della libertà in un mondo dominato dai possessori degli strumenti di informazione automatizzata – come sono quelli degli archivi magnetici dei dati personali, delle rilevazioni compiute dai satelliti artificiali, delle manipolazioni elettroniche e delle simulazioni e previsioni informatiche in diversi campi dell'economia e delle relazioni sociali – occorre, dunque, avanzare l'idea di una nuova forma di libertà inserita nel tessuto tecnologico della nuova società"[45].

Tuttavia, secondo Brin e in una prospettiva che taluni forse condividono, nella Società trasparente le leggi sulla privacy informatica sono e saranno comunque inutili, mentre i ricchi e i potenti, le forze dell'ordine e le *intelligence*, nonché le élite tecnologiche, avranno sempre un vantaggio[46]. Ragionare in questi termini vorrebbe tuttavia affermare l'impotenza dei vari Stati nel tutelare un diritto fondamentale della persona, quello alla privacy, nella sua accezione di diritto a difesa di quella libertà che oggi è presumibilmente riduttivo definire in termini di libertà informatica, atteso che la cesura tra realtà materiale e virtuale diviene sempre meno netta e che la dimensione digitale è vissuta da un sempre crescente numero di persone e nulla lascia pensare che nei decenni a venire possa registrarsi un'inversione di tendenza: tutt'altro.

Proprio la considerazione appena svolta spinge a denunciare la difficoltà a dimenticare, che giuridicamente si traduce nel diritto all'oblio, ma che la dottrina ha altresì visto quale modificazione di quella tendenza a dimenticare che è caratteristica comportamentale innata nell'essere umano[47].

L'uomo di vetro, però, nella Società della data-veglianza si trova a doversi costantemente difendersi dagli attacchi alla sua sfera privata; dal momento che diviene difficile controllare effettivamente ed efficacemente i propri dati personali, può forse ravvisarsi un'involuzione e un ritorno all'originaria configurazione del diritto alla privacy quale *right to be let alone*, poiché sembra che chiunque, più che controllare i propri dati, cerchi sempre più spesso di ritrovare quella sfera di riserbo oltremodo ridotta per una molteplicità di motivi[48].

Talvolta ciò è dovuto proprio a condotte incaute dell'uomo stesso, che sovente utilizza strumenti informatici senza avere consapevolezza non solo delle loro specificità, ma dei rischi connessi ai medesimi. Spesso, inoltre, l'uomo-consumatore sceglie di rinunciare a una porzione della propria privacy al fine di ricevere anche modesti vantaggi patrimoniali, come l'applicazione di uno sconto su determinati prodotti, o per noncuranza nella conclusione di contratti, anche gratuiti, per la prestazione di servizi o la vendita di beni. Come osserva

[45] V. Frosini, *La democrazia nel XXI secolo*, op. cit., pp. 76.

[46] In tal senso D. Brin, *The Transparent Society. Will Technology Force Us to Choose Between Privacy and Freedom?*, New York, Basic Books, 1999, p. 13. In dottrina si è altresì osservato quanto segue: "It is not hard to imagine that, in a future society, we will have little, or even, expectation of privacy in the public sphere, and may care very little, or even not at all, for this type of privacy" (S. Clarke, *Rights and computer ethics*, in L. Floridi (edited by), *The Cambridge Handbook of Information and Computer Ethics*, Cambridge (UK), Cambridge University Press, 2010, p. 246).

[47] V. Mayer-Schönberger, *delete*, op. cit., p. 92. "Since the beginning of time, for us humans, forgetting has been the norm and remembering the exception. Because of digital technology and global networks, however, this balance has shifted. Today, with the help of widespread technology, forgetting has become the exception, and remembering the default" (ivi, p. 2).

[48] Andando oltre il concetto stesso della sorveglianza, la stessa "istituzionalizzazione della vita umana ha raggiunto oggi livelli preoccupanti e le regole dettate dallo stato raggiungono i momenti più privati della vita del cittadino. Sulla base di questa considerazione occorrerà forse non trascurare anche la necessità di rivendicazione del diritto allo spazio della propria vita" (T. Serra, *La disobbedienza civile. Una risposta alla crisi della democrazia?*, Torino, Giappichelli, 2002, p. 30).

David Lyon, la sorveglianza tende a farsi liquida soprattutto nella sfera dei consumi e si diffonde in modi fino ad ora impensabili, reagendo alla liquidità e contribuendo contemporaneamente a riprodurla. Essa dilaga ovunque, pur senza un contenitore stabile, divisa fra le esigenze di «sicurezza» e sollecitata dal marketing insistente dei produttori di tecnologie[49], trovando terreno fecondo nella circostanza che, seppur con intensità variabile, le persone sono sempre più in rete per cui il confine fra la realtà virtuale e quella materiale diviene sempre più evanescente.

Bisogna però tener presente che la continua presenza in una dimensione "innervata dalle tecnologie trasforma la persona, può farla divenire il docile oggetto di poteri altrui, che non sono soltanto quelli delle diverse agenzie di sorveglianza, che esercitano un controllo su ogni comportamento classificato come appartenente a una delle tante, possibili forme di devianza. I nuovi poteri sono quelli che riducono la persona a oggetto, dal quale vengono costantemente estratte, con le tecniche più diverse, tutte le possibili informazioni, non solo per le tradizionali, anche se continuamente dilatate, forme di controllo, ma sempre più intensamente per costruire profili e identità, per stabilire nessi e relazioni, di cui ci si serve soprattutto per finalità economiche, per ritagliare dalla persona quel che interessa al mercato"[50]. Non a caso, le nuove prassi di sorveglianza, superando le previsioni di Foucalt, sono per lo più basate sull'elaborazione di informazione e consentono una nuova trasparenza in cui tutti sono costantemente controllati, osservati, messi alla prova, soppesati, valutati e giudicati – e tutto questo senza alcuna possibilità di reciprocità. Pertanto, mentre i dettagli della vita quotidiana dei sorvegliati diventano trasparenti per i sorveglianti, le loro attività sono sempre più difficili da riconoscere. Nel contesto fluido della modernità liquida il potere si sposta alla velocità dei segnali elettronici, mentre la trasparenza aumenta per alcuni e diminuisce per altri[51]. Si pone quindi la necessità di un ripensamento della vita collettiva ed individuale tenendo presente la nuova sorveglianza, così da limitare gli ambiti di operatività dell'occhio elettronico, definendo in particolare quegli spazi cui gli è precluso volgere lo sguardo, pena la mobilitazione di nuovi criteri di resistenza[52].

I database assumono, quindi, un ruolo sempre più importante, poiché costituiscono l'archivio di una molteplicità di informazioni, poi oggetto di trattamento. Essi, spingendo i principi panottici fuori dalla prigione, vanno a condurli nella società attuale giungendo così a una sorta di *Superpanopticon* e riconfigurando la costituzione del soggetto[53], per cui "tramonta il soggetto giuridicamente responsabile, centro di imputazione di diritti e doveri: alla persona

[49] D. Lyon, *Introduzione*, op. cit.,, pp. x-xi.

[50] S. Rodotà, *Il mondo nella rete*, op. cit., pp. 27-28. Come ricorda Lawrence Lessig, "there is a part of anyone's life that is *monitored*, and there is a part that can be *searched*. […] These two dimensions can interact, depending upon the technology in each. […] The same technologies that gather data now gather it in a way that makes it searchable. Thus, increasingly life becomes a village composed of parallel processors, accessible at any time to reconstruct events or track behavior" (L. Lessig, *Code. Version 2.0,* New York, Basic Book, 2006, pp. 202-203).

[51] D. Lyon, *Introduzione*, op. cit., p. xxii.

[52] In tal senso A. C. Amato Mangiameli, *Diritto e cyberspace*, op. cit., p. 18.

[53] D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, La Feltrinelli, 2002, pp. 160-161. Per la teorizzazione del *Synopticon*, quale superamento della teoria di Foucault Cfr. T. Mathiesen, *The viewer society. Michel Foucalt's 'Panopticon' revisited*, in *Theoretical Criminology*, 1997, 1(2), pp. 215-234.

quale «doppio» normativo dell'individuo naturalisticamente inteso si sostituisce ora il doppio, ibrido e virtuale, del soggetto fittizio, costruito attraverso i codici del controllo preventivo"[54].
Il tutto avviene sfruttando la rete Internet, dunque un *non-luogo* che costituisce la nuova frontiera della sorveglianza per molti stati. Essa è complessa e decentralizzata, com'è noto, e i tentativi di controllo sono posti in essere con molteplici modalità e sui suoi vari strati, qualora se ne schematizzi la visione seguendo la prospettazione di Yochai Benkler (o le successive varianti proposte dalla dottrina). In particolare, egli suddivide un sistema di comunicazione in tre "strati": fisico, logico, dei contenuti. Il primo identifica l'hardware, ivi incluse le infrastrutture di rete; il secondo consente il funzionamento dell'hardware, ivi inclusi i protocolli di rete; il terzo è relativo alle informazioni di qualsiasi tipologie che vengono trasmesse attraverso il sistema[55]. Lawrence Lessig evidenzia l'aspetto peculiare di Internet consistente nel mescolare libertà e controllo nei diversi strati, poiché il suo strato fisico è essenzialmente controllato da soggetti pubblici e privati e anche quello di contenuto è sostanzialmente, ma non esclusivamente, controllato; tuttavia, nello strato di codice il controllo è meno pervasivo. Nel complesso, comunque, Internet mescola al contempo sia strati liberi che controllati, non soltanto strati liberi[56].
In ambito informatico, però, la libertà può essere anche solo illusoria. Come più compiutamente esposto nel paragrafo successivo, nei meandri di codici informatici sempre più complessi possono trovarsi meccanismi di sorveglianza anche estremamente sofisticati; in altri casi, tali meccanismi sono addirittura accettati inconsapevolmente dagli utenti che acconsentono alla trasmissione di dati di varia tipologia. Ad ogni buon conto, dal momento che la Società dell'informazione è sempre più caratterizzata dall'interconnessione di innumerevoli dispositivi che possono identificare il relativo utilizzatore acquisendone dati personali, non v'è dubbio che il profilo della segretezza del codice assuma un ruolo centrale nella riflessione sulla sorveglianza elettronica.
Il sogno di una Rete incontrollata e incontrollabile è forse utopistico, ma altresì pericoloso. Una Rete al di fuori di qualsiasi ipotesi di controllo porrebbe a serio rischio, più di quanto non avvenga oggi, i diritti e le libertà fondamentali della persona. Non suscita stupore, dunque, che Internet e il Web siano filtrati e controllati[57], ma è necessario riflettere sulla definizione e sulla implementazione di modalità che possano bilanciare i diversi diritti ed interessi in gioco poiché Internet è oramai una componente essenziale della società contemporanea. Da una prospettiva umanistica, è stato così osservato che "Legitimate governmental and private interests are taking us into a world that is something like a strange

[54] A. Amendola, *Persona e soggetto giuridico nello Stato di prevenzione*, op. cit., p. 419.
[55] Y. Benkler, *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access,* in *Federal Communications Law Journal*, 2000, 3, *passim*.
[56] L. Lessig, *Il futuro delle idee*, tr. it. Milano, La Feltrinelli, (ed. or. 2001) 2006, p. 29.
[57] Di particolare interesse sono le informazioni raccolte e gli studi effettuata dalla *OpenNet Initiative*, disponibili sia sul proprio sito web (https://opennet.net) che in diverse pubblicazioni, fra cui si segnalano: R. Deilbert – J. Palfrey – R. Rohozinski – J. Zittrain (edited by), *Access Controlled*; op. cit.; R. Deilbert – J. Palfrey – R. Rohozinski – J. Zittrain (edited by), *Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge (MA), MIT Press, 2010; R. Deilbert – J. Palfrey – R. Rohozinski – J. Zittrain (edited by), *Access Contested. Security, Identity, and Resistance in Asian Cyberspace*, Cambridge (MA), MIT Press, 2011.

mix of Aldous Huxley's *Brave New World* and a well-run theme park"[58], sfruttando sia l'infrastruttura sia il Web, libero nella sua creazione e nel suo strato di codice grazie al suo creatore (Tim Berners-Lee)[59], ma *non-luogo* di contrasto fra privacy e controllo.

Il fatto che la gestione di un sistema e la sorveglianza dei suoi utilizzatori compongano un *unicum*, per cui l'apparato di sorveglianza si fa parte della struttura stessa del sistema e gli strumenti di controllo tendono addirittura ad impadronirsi dell'intero sistema e a connotarlo[60], trova ottima esplicazione in una moltitudine di esperienze Web: non a caso, la raccolta di dati degli utenti è prevista *ab origine* nella gran parte dei siti e servizi web. Inoltre, molti agenti software[61], per le finalità più diverse, scandagliano i contenuti accessibili in Rete ed effettuano automaticamente trattamenti di dati personali e non. L'identità di un soggetto può così essere ricostruita digitalmente in modo totalmente automatizzando, mediante software intelligenti che eseguono algoritmi sempre più complessi. Anche la reperibilità di una persona fisica o giuridica, nonché la consultabilità di uno o più profili o comunque di contenuti di qualsiasi tipologia, dipende oramai da algoritmi che decidono cosa può essere mostrato in seguito alle interrogazioni degli utenti. Come sottolineato in modo estremamente efficace da Stefano Rodotà, bisogna tuttavia "sottrarre la persona alla «dittatura dell'algoritmo», emblema di una società della spersonalizzazione, nella quale scompare la persona del decisore, sostituito appunto da procedure automatizzate; e scompare la persona in sé considerata, trasformata in oggetto di poteri incontrollabili. [...] Alle tecnologie dell'informazione e della comunicazione, infatti, è stata attribuita una virtù, quella di rendere la società più trasparente proprio per quanto riguarda la possibilità di controlli diffusi sul potere, su qualsiasi potere. Ma quando l'algoritmo diviene il fondamento stesso del potere esercitato da un soggetto, com'è nel caso assai enfatizzato di *Google*, e tutto ciò che lo riguarda è avvolto dalla massima segretezza, allora siamo davvero di fronte alla nuova versione degli *arcana imperii*, che non tutelano soltanto l'attività d'impresa, ma si impadroniscono, direttamente o indirettamente, della vita stessa delle persone[62].

Del resto, l'automazione estrema può portare a conseguenze negative; basti pensare alla censura algoritmica compiuta dai motori di ricerca web che, al fine di fornire risultati più pertinenti a chi li interroga, non opera in modo neutrale ma seleziona i risultati, fra l'altro, sulla base della sua collocazione geografica. In tal caso si decide, arbitrariamente, di reintrodurre quel concetto di spazio che proprio l'infrastruttura della Rete aveva permesso di superare, seppur nel ciberspazio.

Inoltre, la dittatura dell'algoritmo può verificare anche nella ricostruzione automatizzata dei profili delle persone svolta sulla base dei dati raccolti; in tal senso, assumono particolare rilevanza le attività dei prestatori di servizi che, per la natura degli stessi, acquisiscono ed

[58] J. Sullins, *Rights and computer ethics*, in L. Floridi (edited by), *The Cambridge Handbook of Information and Computer Ethics*, op. cit., p. 131.

[59] Cfr. T. Berners-Lee, *L'architettura del nuovo Web. Dall'inventore della Rete il progetto di una comunicazione democratica*, tr. it., Milano, La Feltrinelli, 2001.

[60] In senso S. Rodotà, *Tecnopolitica*, op. cit., p. 135.

[61] Gli agenti *software* "sono sistemi informatici in grado di agire con autonomia, senza il controllo diretto del loro utilizzatore" (G. Sartor, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in *Il diritto dell'informazione e dell'informatica*, 2003, 1, p. 55).

[62] S. Rodotà, *Il mondo nella rete*, op. cit., pp. 37-38.

elaborano dati personali, anche sensibili. Gli esempi costituiti dai servizi di social network, di motori di ricerca web e di posta elettronica sono più che sufficienti a far intuire la portata del fenomeno.

Come comportarsi nella Società della sorveglianza e del controllo? Pare opportuno citare V. Mayer-Schönberger e le sei proposte finalizzate a prevenire o mitigare le sfide del tempo e del potere poste dalla memoria digitale: astinenza digitale, diritto(i) alla privacy informatica, infrastruttura digitale per i diritti alla privacy (sulla falsariga dei sistemi di *Digital Rights Management*), adattamento cognitivo (alla società che cambia), *information ecology* ("deliberate regulatory constraint of what information can be collected, stored, and thus remembered, by whom and for how long"), contestualizzazione perfetta (raccolta continua di informazioni, società trasparente come prospettata da Brin); come osserva egli stesso, tutte presentano delle problematiche e comunque le prime tre appaiono migliori delle ultime tre, ferma restando la sua proposta di una "data di scadenza" per le informazioni: "one possible way we can mimic human forgetting in the digital realm is by associating information we store in digital memory with expiration dates that users set"[63].

Tuttavia, come evidenziato da Lawrence Lessig in relazione alla rete Internet, non vi è un'unica soluzione alle problematiche di *policy*, ma ogni soluzione richiede quanto meno due modalità[64]. Nel paragrafo che segue verranno delineate talune possibili evoluzioni e prospettato il potenziale contributo che può dare l'etica hacker per mitigare, più che risolvere, le problematiche principali conseguenti all'avvento della Società dell'informazione o della sorveglianza o, come alcuni preferiscono, della dataveglianza.

4. Possibili evoluzioni e contributi dell'etica hacker.

Si è sin qui esposto e ribadito che oggi la privacy viene messa a rischio sotto più fronti, cui si aggiunge quello forse più pericoloso: la sorveglianza globale, giustificata, oramai da diversi anni, da motivi di sicurezza in alcuni stati e comunque imposta in altri. Un dibattito mai sopito, che nell'ultimo periodo ha trovato rinnovato vigore grazie a diversi casi, con particolare ma non esclusivo riferimento a quello originato dalle già citate rivelazioni di Edward Snowden[65]. Il recente passato mostra come da *Echelon all'Information Awareness Office*

[63] V. Mayer-Schönberger, *delete*, op. cit., p. 128-171. Jonathan Zittrain, invece, osserva quanto segue: "For privacy, peer-leveraging technologies might make for a much more constrained world rather than the more chaotic one they have wrought for intellectual property. More precisely, a world where bits can be recorded, manipulated, and transmitted without limitation means, in copyright, a free-for-all for the public and constraint upon firms (and perhaps upstream artists) with content to protect. For privacy, the public is variously creator, beneficiary, and victim of the free-for-all. The constraints – in the form of privacy invasion that Jeffrey Rosene crystallizes as "unwanted gaze" – now come not only from the well-organized governments or firms of Privacy 1.0, but from a few people generatively drawing upon the labors of many to greatly impact rights otherwise guaranteed by a legal system" (J. Zittrain, *The Future of the Internet and How to Stop It*, New Haven & London, Yale University Press, 2008, p. 216).

[64] L. Lessig, *Code*, op. cit., p. 223.

[65] La più grande paura per Edward Snowden è, tuttavia, che dopo le sue rivelazioni non cambi nulla; "la gente verrà a sapere dai media tutte queste rivelazioni, saprà che il governo si appropria del potere e che è davvero capace di tenere sotto controllo la società americana e la società globale, nel vero senso della parola. Ma non sarà disposta a correre il rischio necessario ad alzarsi in piedi compatta e a lottare per cambiare le cose, a costringere i suoi rappresentanti a prendere effettivamente una posizione nel suo interesse, quello del popolo. E nei prossimi mesi, nei prossimi anni, le cose non potranno che peggiorare, finché alla fine, un giorno, verrà il momento in cui la politica dovrà cambiare. Perché l'unica cosa

(IAO) statunitense la sorveglianza non sia unicamente prerogativa di regimi autoritari, ma venga altresì esercitata in stati democratici in violazione di diritti e libertà fondamentali, esasperando altresì una problematica di particolare delicatezza: come tutelarsi? Come far sì che le persone riescano a far sentire la propria voce? Il caso dello IAO è emblematico: finalizzato all'implementazione del progetto "Total Information Awareness", fu "smembrato" in seguito alle proteste e portato avanti in modo meno palese, come rilevato dallo stesso Snowden. In altri termini, le proteste dei cittadini sono state aggirate rendendo ancor più segreta l'attività di sorveglianza, il che dovrebbe sollecitare ulteriori riflessioni sulla reale motivazione che spinge alla effettuazione di attività tanto delicate quanto lesive della sfera intima di ciascun essere umano. In linea generale, la persona viene sorvegliata e spiata perché se ne presume la potenzialità delinquenziale o perché incapace di difendersi dai propri simili. Ma "da lungo tempo gli hacker hanno sottolineato che nell'era elettronica la preservazione della privacy non è affatto scontata, ma richiede una maggiore consapevole protezione"[66].

Secondo Stefano Rodotà, in questo momento storico, il termine privacy sintetizza un insieme di poteri che, a partire dal "right to be let alone", hanno avuto un'evoluzione e una diffusione nella società proprio al fine di rendere disponibili forme di controllo sui diversi soggetti che effettuano attività di sorveglianza. Questo contropotere diffuso, pertanto, concorre all'esclusione della piena legittimazione sociale ed istituzionale dei sorveglianti[67].

Tuttavia, in mancanza di una sufficiente opera dei vari Stati che ponga rimedio alle problematiche sin qui accennate, il recupero dei principi dell'etica hacker può costituire un'altra tipologia di contropotere diffuso e contribuire a un mutamento di prospettiva che de-burocratizzi il diritto alla privacy e aiuti a tutelarlo efficacemente, nonché a proteggere la libertà di informazione (e, mediante essa, anche altri diritti fondamentali) grazie alle competenze tecnologiche degli hackers che possono consentire di aggirare i moderni strumenti di censura digitale.

Del resto, "la pretesa dell'identificazione totale spinge verso la ricerca di vie per sottrarsi al diktat della rivelazione integrale e in ogni caso dei dati identificativi. Questo si traduce in scelte individuali o nella creazione di soggetti collettivi, di gruppi di persone senza nome che, come *Anonymous*, aggirano con «strategie da bracconiere», con una vera guerriglia tecnologica, gli ostacoli imposti e aprono strade adeguate all'effettività dei diritti in rete"[68].

---

che vincola e pone limiti alle attività di sorveglianza della popolazione è la politica" (E. Snowden, op. cit., p. 84). E, si potrebbe aggiungere, "È il caso, però, che l'individuo contemporaneo, che è il vero protagonista della storia, continui sempre a dispiegare, di fronte alle trasformazioni del suo tempo, di fronte alle rivoluzioni più o meno eclatanti, la sua capacità di critica e di riflessione per evitare che si realizzi il proposito, coltivato spesso dai detentori del potere, di renderlo un essere superfluo, secondo l'ammonimento sempre attuale, oggi più che mai attuale, di Hannah Arendt" (M. Sirimarco, *Ancora su apocalittici e integrati: ovvero tra Hermes e Narciso*, in Id (a cura di), *Informatica, diritto, filosofia,* Roma, Aracne, 2007, p. 290).

[66] P. Himanen, *L'etica hacker e lo spirito dell'età dell'informazione*, tr. it., Milano, La Feltrinelli, (ed. or. 2001) 2007, p. 82.

[67] S. Rodotà, *Tecnopolitica*, op. cit., p. 169. Oltretutto, "Despite repression in dozens of countries that censor the Internet, the digital environment is, in most cases, serving as a locus of reform efforts. Smart technologists and digital activists have devised ways around every censorship and surveillance program in place in the world today. The Internet has become a major battleground between those who seek to consolidate power and those who wish to see it more broadly distributed. The global crew of Digital Natives is a far better bet than the dictators in the long run" (J. Palfrey – U. Gasser, *Born Digital. Understanding the first generation of digital natives*, New York, Basic Books, 2008, p. 270).

[68] S. Rodotà, *Il mondo nella rete*, op. cit., p. 26.

Ad ogni buon conto, l'etica hacker, intesa nel suo significato più profondo che supera l'interpretazione negativa che di essa ha la visione comune, sviluppata negli anni Sessanta e ben esemplificata da Steven Levy negli anni Ottanta[69], è basata su principi il cui rispetto viene spesso solo proclamato da soggetti pubblici e privati, ma effettivamente garantito solo dagli stessi hackers. Ne esistono diverse varianti, ma è generalmente basata sul rispetto dei principi di libertà dell'informazione, condivisione della conoscenza, non discriminazione e valorizzazione del merito. Il rispetto dei principi che ispirano tale etica, in particolare, consente di distingue fra i veri hackers e i c.d. *cracker*, ossia i pirati o criminali informatici (nonostante il sensazionalismo mediatico abbia portato a una diffusa confusione fra tali figure)[70].

In particolare, dovrebbero essere garantiti sia il libero, completo e illimitato accesso ai computer e "a tutto ciò che potrebbe insegnare come funziona il mondo", sia la libertà dell'informazione (ovunque in catene, come ricorda Wark McKenzie[71]. Eric Raymond evidenzia, in particolare, che il principio basilare e universalmente riconosciuto dagli hackers è la convinzione che la condivisione delle informazioni sia un bene di formidabile efficacia e che essi debbano condividere le loro competenze scrivendo codice libero e facilitando l'accesso all'informazione e alle risorse tecnologiche ove possibile[72]. La loro effettiva implementazione in ambito informatico-giuridico consentirebbe di lottare effettivamente contro le sempre più sofisticate tecnologie di controllo, atteso che sarebbe possibile comprendere il funzionamento degli strumenti tecnologici oggi utilizzati e sapere se nei meandri dei codici informatici sono presenti tecniche e metodologie che violano i principi fondamentali a tutela della persona. In altri termini, sarebbe possibile sorvegliare e controllare gli strumenti utilizzati dai sorveglianti. Nel *Panopticon*, ad ogni buon conto, Bentham aveva previsto una sorta di meccanismo, comunque non infallibile, per cui i sorveglianti erano potenzialmente sorvegliati a loro volta; ma nella Società della sorveglianza digitale i sorveglianti sono protetti dalla segretezza, fatti salvi i casi in cui il diritto positivo prevede dei meccanismi di tutela concretamente attivabili. Del resto, "a immagine e somiglianza del «Dio nascosto» il sovrano assoluto, l'autocrate, è tanto più potente quanto meglio riesce a vedere quello che fanno i suoi sudditi senza farsi vedere. L'ideale del sovrano equiparato a Dio in terra è quello di essere, al pari del Dio celeste, l'onniveggente invisibile"[73]. E, in una società permeata e pervasa da codici e programmi informatici, la loro segretezza talvolta in ordine alla loro stessa esistenza consente di coadiuvare i soggetti che cercano di essere onniveggenti invisibili.

Inoltre, si consideri che garantire l'accesso libero, completo e illimitato alle tecnologie fondamentali può essere visto quale obbligo, in capo a ciascuno Stato, di combattere efficacemente il c.d. *digital divide*. Nella sua accezione più generale, con questa espressione si fa riferimento al gap che separa chi ha accesso alle moderne tecnologie e chi, invece, ne è

[69] S. Levy, *Hackers. Gli eroi della rivoluzione informatica*, tr. it., Milano, Shake, 2002.
[70] Per la trattazione della tematica sia consentito rinviare a G. FIORIGLIO, *Hackers*, Roma, Nuova Cultura, 2010.
[71] W. Mckenzie, *Un Manifesto Hacker. Lavoratori immateriali di tutto il mondo unitevi!*, tr. it., Milano, La Feltrinelli, 2005, p. 58.
[72] E. S. Raymond (compiled by), *The New hacker's dictionary*, Cambridge (MA), MIT Press, 1999, p. 234.
[73] N. Bobbio, *Il potere invisibile*, in M. Revelli (a cura di), *Democrazia e segreto*, Torino, Einaudi, 2011, p. 5.

privo. Vi sono, poi, diverse specificazioni del fenomeno, per cui si può avere accesso ai computer, ma essere svantaggiati nell'accesso ad Internet per velocità, disponibilità e/o costo della connessione; ancora, si può essere costretti ad utilizzare strumenti ormai obsoleti; e così via. Quale pre-requisito, ciascuno Stato dovrebbe altresì contribuire efficacemente alla formazione informatica dei propri cittadini, mediante iniziative organiche e capillari. Se quanto qui esposto venisse realizzato adeguatamente, la condotta digitale dei cittadini non potrebbe che essere più cauta, con intuitivi effetti benefici.

Come si è accennato, è poi assolutamente necessario garantire realmente la libertà dell'informazione e di tutti i relativi processi; ma tale principio, però, si scontra con le normative in materia di proprietà intellettuale, per cui talune operazioni svolte su codici informatici divengono illegali (nonostante alcune aperture giurisprudenziali). Sarebbe dunque opportuno modificare talune normative per dare concreta realizzazione a quello spirito di condivisione della conoscenza posto a base di tante comunità hacker. Esse, auto-organizzate in modo informale (come evidenziato da Manuel Castells), talvolta perseguono finalità di critica politica di fronte alle degenerazioni della democrazia, per quanto le loro azioni sono maggiormente legate a degenerazioni od eventi che colpiscono le loro comunità [74], soprattutto in relazione a questioni connesse alla proprietà intellettuale e alla privacy. In modo molto suggestivo, Wark McKenzie contrappone la classe hacker a quella vettoriale ("la classe dominante emergente del nostro tempo"); per quest'ultima, "la politica è finalizzata al controllo assoluto sulla proprietà intellettuale attraverso strategie di comunicazione, controllo e comando di tipo militare", per cui gli hackers si ritrovano espropriati sia come individui sia come classe e, dal momento che la classe vettoriale consolida progressivamente il proprio monopolio sui mezzi per realizzare il valore della proprietà intellettuale, la classe hacker ne è la classe antagonista[75].

La classe hacker, dunque, si trova a lottare per tutelare direttamente il proprio diritto a utilizzare una risorsa immateriale artificiosamente, e giuridicamente, limitata; indirettamente, tutela la libertà informatica della collettività. Non a caso, le esperienze di collaborazione fra hackers, nonostante le spinte egoistiche e individualistiche, sono numerose e proficue. In ambito informatico, in particolare, trovano compiuta realizzazione soprattutto nei software a sorgente aperto, che possono essere studiati e modificati da chiunque[76]. Lo strumento

[74] Le comunità hacker, inoltre, sono comunità collegate in rete; come altri movimenti, esse possono essere reti di reti, ed esse "because they are a network of networks, they can afford not to have an identifiable centre, and yet ensure coordination functions, as well as deliberation, by interaction betwen mutiple nodes. Thus, they do not need a formal leadership, command and control centre, or a vertical organization to distribute information or instructions. This decentered structure maximizes chances of participation in the moviment, given that these are open-ended networks without defined boundaries, always reconfiguring themselves according to the level of involvement of the population at large. It also reduces the vulnerability of the movement to the threat of repression, since there are few specific targets to repress, except for the occupied sites, and the network can reform itself as long as there are enough participants in the movement, loosely connected by their common goals and shared values. Networking as the movement's way of life protects the movement both against its adversaries and against its own internal dangers of bureaucratization and manipulation" (M. Castells, *Networks of outrage and hope*, Cambridge, UK , Polity Press, 2012, p. 221-222).

[75] W. Mckenzie, *Un Manifesto Hacker*, op. cit., p. 17.

[76] Sulla cooperazione in prospettiva *bottom-up* cfr. i numerosi esempi in G. Reynolds, *An Army of Davids. How markets and technology empower ordinary people to beat big media, big government and other goliaths*, Nashville, Nelson Current, 2006; C. R. Sunstein, *Infotopia. How many minds produce knowledge*, New York, Oxford University Press, 2006; D. Tapscott – A. D. Williams, *Wikinomics. How Mass Collaboration Changes Everything*, London, Penguin Books, 2010.

giuridico che lo consente è quello della licenza d'uso; ne esistono varie tipologie, più o meno restrittive, ma comunque consentono di garantire la libertà del codice e dunque garantiscono un importante aspetto della libertà informatica.

Nella Società della sorveglianza e del controllo, infatti, vi è un problema molto delicato, connesso sia ai software proprietari che ai servizi informatici: come si è anticipato e prospettato alla luce di diverse prospettive, la trasparenza è molto rara e mentre l'interazione con gli strumenti tecnologici si semplifica, internamente i medesimi sono sempre più oscuri e complessi, al di fuori della portata dell'uomo medio, che anche da questo punto di vista è sempre più "di vetro". Sarebbe dunque auspicabile una maggiore possibilità di controllo circa quanto accade negli strumenti comunemente diffusi, anche se è noto che solo una piccola parte delle persone potrebbe avere le conoscenze e le capacità per comprendere compiutamente ciò che accade nelle stesse. Ma è necessario legittimare, dal punto di vista giuridico, taluni strumenti di autodifesa, per evitare che la tecnologia, di consumo e non, divenga il "cavallo di Troia" privilegiato per la sorveglianza globale, ad esempio mediante la costante inclusione delle c.d. *backdoors* (letteralmente porte di servizio), che consentono l'ingresso in un sistema informatico più o meno complesso, in una molteplicità di dispositivi: il che acquisirà ancora maggior rilievo nella c.d. *Internet of things*, in cui l'interconnessione di reti ed oggetti sarà ancora più pervasiva e le informazioni saranno generate e trasmesse sempre più in modo automatico dagli stessi dispositivi "intelligenti".

Un parallelismo può aiutare a comprendere il paradosso dell'involuzione nella prospettiva sin qui delineata: in epoca antica, la legge scritta aveva notoriamente consentito una maggior tutela a chiunque fosse sottoposto alla stessa. Oggi il numero di leggi in vigore è spropositato e sono sempre più facilmente reperibili, anche se la loro interpretazione, in sistemi giuridici stratificati e complessi, è compito oltremodo arduo. In epoca moderna, il codice informatico è sempre più segreto, di pari passo con l'involuzione della Società, nonostante lo stesso sia alla base del funzionamento di molti suoi settori, pubblici e privati. Dinanzi a tecnologie sempre più sofisticate e invasive, l'apporto degli hackers e della loro etica nonché delle loro capacità tecnologiche può essere fondamentale per garantire la sussistenza di spazi (informatici e non) di libertà, oltreché per tenere vivo lo spirito critico nell'uomo del nuovo millennio nei confronti di tecnologie pervasive ed ubique; in ultima analisi, per tentare di ridurre quel dominio dell'uomo sull'uomo che sembra ormai connaturato all'odierna società globale.