DIRITTO PENALE
E UOMO
Criminal Law and Human Condition

Riflessione

Relazioni pericolose nel "terzo spazio"

The dangerous liaisons in the "third space"

di Vincenzo Scalia

Abstract. L'irrompere della cibernetica nelle interazioni sociali ha fatto sì che si creasse il cosiddetto "terzo spazio", ovvero il network *relazionale all'interno del* web. *In questo contesto, oltre all'opportunità di nuove forme di relazione, si sovrappone l'occasione di nuove forme di criminalità e di controllo sociale, che mettono a rischio lo spazio per l'esercizio delle libertà civili. Questa riflessione si prefigge di analizzare queste contraddizioni tra nuove opportunità interattive da un lato e controllo dall'altro.*

Abstract. As cybernetics break into social relation, the so-called "third space" is created. The opportunities for new forms of relation, within this domains, overlaps with new forms of crime and social control. Both of the latter are a threat to civil liberties. This work aims to both describe and discuss these contradictions between new interactive opportunities and social control.

1. Definire il "terzo spazio".

A partire dagli anni Ottanta, l'affermazione prorompente della rete telematica ha modificato i rapporti sociali, tanto che alcuni studiosi hanno iniziato a considerare l'esistenza di un «terzo spazio»[1]. Come l'ambiente naturale e sociale, la rete si connota come un contesto regolato da norme peculiari, attraversato da dinamiche specifiche, caratterizzato da conflitti peculiari, che sfociano nella produzione di rappresentazioni e identità del tutto inaspettate.

Se dovessimo volgere il nostro sguardo in direzione della criminalità, potremmo scorgere anche il lato oscuro del "terzo spazio". La rete infatti apre anche a nuove opportunità per la commissione di reati. Infatti, alle truffe online, come quelle della clonazione delle carte di credito e della violazione dei conti bancari, si sovrappongono la pedopornografia e il cosiddetto «cyberterrorismo». Inoltre, è grazie all'utilizzo del *Deep Web* che si creano le catene di comunicazione tra i pedofili ed è sempre grazie a questa sorte di rete parallela che le organizzazioni criminali, quale l'ISIS, riescono a reclutare e ad addestrare i propri membri eludendo ogni controllo superficiale.

In altre parole, l'utilizzo di internet, da un lato, aumenta e modifica le possibilità relazionali: si pensi all'obsolescenza delle cabine telefoniche e alla perdita di importanza della telefonia fissa di fronte all'irrompere delle *chat lines* e dei *social network* utilizzabili in tempo reale. Dall'altro lato, l'utilizzo della rete comporta anche che la fluidità, la volatilità delle relazioni virtuali, l'anonimità e l'impersonalità dello schermo, l'impossibilità di verificare l'identità dei nostri interlocutori al di là del video, sortiscano altresì l'effetto di generare nuovo panico morale.

Howard Becker e Stanley Cohen, tra criminologi contemporanei più importanti[2], sottolineano il ruolo dei nuovi imprenditori morali pronti ad agitare lo spauracchio di inedite minacce, da esorcizzare con l'implementazione di misure speciali, che finiscono il più delle volte per essere lesive nei confronti delle libertà civili. Le ricadute di questa deriva che potremmo definire "*cyber*-securitaria" finiscono per farsi sentire anche sul piano politico.

Il "terzo spazio" si struttura sin dall'inizio come un'arena pubblica, a cui hanno accesso una pluralità di attori individuali e collettivi. Al suo interno si producono due tipologie di lotte politiche. La prima è quella relativa all'utilizzo di internet per creare e diffondere pratiche politiche alternative. Non è casuale che molti dei movimenti recenti, come *Occupy Wall Street* e le primavere arabe[3], trovino nella rete un *habitat* fertile per diffondersi. L'utilizzo della rete ha permesso di aggirare la censura e la repressione esistenti nei paesi arabi facendo uso dei *social network*. Nel caso di *Occupy*, un uso

---

[1] D. Geer (a cura di), *Cybercrime. Digital Cops in a Network Environment*, New York University Press, 2015.
[2] H. Becker, *Outsiders,* Free Press, 1963; S. Cohen, *Folk Devils and Moral Panic,* Routledge, 1974.
[3] *Occupy Wall Street* fu un movimento che si sviluppò nella primavera del 2011 negli USA per protestare contro le crescenti disuguaglianze create dallo strapotere del capitale finanziario. Si veda in proposito D. Harvey, *Città Ribelli. I Movimenti Urbani dalla Comune di Parigi a* Occupy Wall Street, Il Saggiatore, 2011. La cosiddetta "Primavera araba" fu un susseguirsi di proteste che ebbero luogo in Algeria, Tunisia, Libia, Egitto, Siria nella primavera del 2011 contro i governi di questi paesi. Si veda in proposito D. Quirico, *Primavere Arabe. Le Rivoluzioni dall'Altra Parte del Mare,* Bollati Boringhieri, 2014.

analogo a quello arabo è servito per convocare le assemblee e le manifestazioni, oltre che per diffondere documenti politici, rivendicazioni e *slogan*.

La seconda tipologia di lotta politica riguarda la resistenza e l'insubordinazione nei confronti di un potere che si manifesta anche sotto forme cibernetiche. A questa tipologia vanno iscritti molti gruppi *hacker* o mediattivisti[4], o i casi di Julian Assange ed Edward Snowden.

Il primo è il giornalista australiano fondatore di *Wikileaks*, un gruppo di giornalisti che si avvale degli *hackers* per recuperare materiali dei servizi di sicurezza delle principali potenze. Le attività di *Wikileaks* sono state giudicate una minaccia per la sicurezza dei paesi occidentali[5], tanto che Assange, dopo essersi rifugiato per 7 anni presso l'ambasciata ecuadoriana a Londra, è stato arrestato nell'aprile 2019 e attende il processo di estradizione negli USA, dove rischia centinaia di anni di carcere.

Il secondo, ex-ingegnere elettronico di una ditta affidataria della *National Security Agency* (NSA), l'agenzia statunitense per la sicurezza interna, dopo avere svelato al *Guardian* la capillare rete di controllo dispiegata sui cittadini dei principali paesi di lingua inglese, è stato costretto a rifugiarsi a Mosca, dove gli è stata concessa la cittadinanza russa[6].

Si crea dunque un'ulteriore prospettiva sulla sicurezza in rete, dove le strategie di controllo e il panico morale si intrecciano direttamente con la prevenzione e la repressione della nascita di discorsi e pratiche alternative, sfociando in un vero e proprio securitarismo cibernetico.

1.1. Cybercrime *e* bazaar.

Quanto è reale la minaccia del *cybercrime*? Come si distingue dagli altri tipi di criminalità? Come si articola la dialettica tra libertà e sicurezza? I criminologi conservatori, come Peter Gottschalk, rispondono tracciando l'*identikit* del cybercriminale: si tratterebbe di un individuo dotato di abilità specifiche, geloso della propria identità illegale, che utilizza la rete per i propri scopi illeciti, e agisce all'interno di reti criminali: ne consegue la necessità di controllare e limitare l'uso della rete, attraverso la creazione di una cyberpolizia che si avvalga della tecnologia più sofisticata[7].

A questa interpretazione si contrappone quella proposta da James Treadwell, Goldsmith e Brewers. Questi autori si preoccupano di criticare l'impostazione che ritiene la rete un luogo di costanti pericoli e minacce, mettendone in rilievo i limiti.

---

[4] K. Steinmetz, *Hackers,* New York University Press, 2017.
[5] V., in proposito, A. Blake, *CIA 'working to take down' WikiLeaks threat, agency chief says,* in *The Washington Times*, 20 ottobre 2017.
[6] G. de Lagasnerie, *L'Arte della Rivolta. Snowden, Assange, Manning,* Stampa Alternativa, 2016.
[7] P. Gottschalk, *Policing Cybercrime,* Bookboon, 2010.

Il primo[8] sottolinea come la rete costituisca un vero e proprio *bazaar*: è possibile trovarvi gli attori più svariati, che operano in ambiti diversi. Internet, sostiene infatti Treadwell, si connota proprio per la sua fluidità: non soltanto è possibile adottare identità multiple, ma allo stesso tempo è possibile operare contemporaneamente nell'ambito di domini legali e illegali, approfittando della protezione fornita dell'anonimato.

La fluidità delle relazioni e delle interazioni vale anche per le attività illegali. I reati commessi su internet, come quelli che si verificano nello spazio reale, si connotano per essere per la maggior parte reati di lieve entità. I perpetratori, come mostra uno studio su alcuni operai dell'East End di Londra[9], non sono criminali abituali, né posseggono sofisticate abilità. Pianificano e commettono frodi di piccolo calibro quando si trovano in difficoltà economiche e in maniera intermittente, oltre che singolarmente.

La fluidità e l'occasionalità, ad un'accurata riflessione, non riguardano soltanto i cosiddetti *street crimes,* seppure trasposti in un'arena virtuale. Da molte parti, ad esempio, trapela l'allarme in relazione a nuovi tipi di reato commessi attraverso l'uso della rete e delle tecnologie, e che spesso risultano lesivi per la dignità delle donne o per la stabilità psicofisica dei minori. Ci riferiamo al *revenge porn* o al *cyberbullying*[10]. È recente, per esempio, il caso della maestra d'asilo torinese[11] licenziata in seguito a sue foto *sexy* e a un suo video pornografico diffusi dall'ex-fidanzato tra gli amici, che poi hanno mostrato questi materiali alle loro *partner*, una delle quali ha identificato l'insegnante e ha portato il materiale alla Preside.

Se da un lato ci troviamo in presenza di un vero e proprio *network* relazionale che si estende dagli amici dell'ex-fidanzato al corpo insegnante della scuola, dall'altro lato non si può certo affermare di trovarsi in presenza di una rete criminale. Addirittura, i soggetti coinvolti della vicenda mostrano di non avere contezza della gravità dei loro comportamenti, pensando di muoversi tra l'attività ludica e la richiesta di licenziamento da parte dei genitori degli studenti nei confronti di una giovane donna rea di vivere, al di fuori della propria sfera professionale, la propria sessualità in modo libero.

Il comportamento della Preside e dei genitori degli studenti coinvolti nella vicenda è cioè indicativo di un mancato riconoscimento dell'altrui diritto alla *privacy* e alle libertà individuali, probabilmente veicolata dalle forme di giustizialismo mediatico che vengono regolarmente elargite al pubblico attraverso trasmissioni televisive di largo consumo.

---

[8] J. Treadwell, *From the car boot to booting it up? eBay, online counterfeit crime and the transformation of the criminal marketplace*, in *Criminology & Criminal Justice*, 12, 2, 2012, pp. 175-194.
[9] *Ibidem.*
[10] Il *cyberbullying* consiste nella commissione di abusi nei confronti di un'altra persona all'interno dello spazio cibernetico. Gli insulti, le minacce, la diffamazione commesse in rete rappresentano i principali atti di *cyberbullying*. Il *revenge porn* è la diffusione di materiale erotico, quali foto o video, precedentemente fornito dalla vittima in modalità private e senza il consenso di quest'ultima.
[11] Per ragguagli si veda S. Lorenzetti, *La maestra d'asilo licenziata per un video* hard*: «Tradita dal mio ex: mi fidavo»*, in *Il Corriere della Sera*, 18 novembre 2018.

Goldsmith e Brewers si muovono sullo stesso solco di Treadwell, parlando dell'esistenza di una vera e propria «deriva digitale»[12]. I fruitori della Rete, secondo loro, perseguono una molteplicità di comportamenti, che attuano in modo non strutturato, e seguono finalità spesso strumentali. Ne consegue che i legami formatisi all'interno del *web* denotano un certo livello di caducità, in seguito alla quale diviene difficile teorizzare o dimostrare l'esistenza di *network* criminali.

Questo discorso vale anche nel caso di terrorismo e pedo-pornografia. In questi casi, spiegano gli autori, spesso ci troviamo di fronte o a individui isolati o a reti che hanno una durata temporale limitata, non sempre composte dalle stesse persone. Ad esempio, i cosiddetti VPN (*Virtual Private Network*), utilizzati dai pedo-pornografi, rischierebbero di attirare troppo l'attenzione, qualora la loro esistenza si prolungasse nel tempo. Per questa ragione, la loro durata e limitata nel tempo. In seguito si formano altri *network*, con altre modalità, e altri membri.

Queste due interpretazioni del *cybercrime*, per quanto importanti, tralasciano però due aspetti della criminalità informatica tanto cruciali quanto speculari al dibattito sulla criminalità che attraversa la sfera pubblica non virtuale:

1. Quanta sicurezza bisogna garantire ai fruitori della rete?
2. Chi deve garantirla?

Il tema non è affatto secondario, se si pensa quanto i discorsi sulla sicurezza, intesa come incolumità psicofisica protetta attraverso la mediazione degli apparati preventivi e repressivi, abbia egemonizzato l'agenda politica a partire dagli anni Novanta[13].

In particolare, per quanto riguarda la seconda delle domande proposte, la risposta si pone nel solco di una tendenza al progressivo ampliamento degli apparati di controllo e di repressione, tendenza che, nel tempo, ha finito per prevalere sulle ragioni di tutela delle garanzie individuali.

Infatti, sotto questo profilo, lo Stato, in quanto attore principe della prevenzione e della repressione della devianza e della criminalità, finisce per rientrare in gioco, mettendo sul piatto le tematiche relative al controllo sociale e al rapporto tra libertà e sicurezza. Da questi aspetti scaturiscono implicazioni direttamente politiche: come nel secondo spazio, ovvero lo spazio sociale[14], il discorso «securitario» ha catalizzato la repressione del dissenso, così, nel "terzo spazio", la minaccia cybercriminale può trasformarsi in un corpo contundente da brandire verso tipologie sempre più ampie di comportamenti non conformi al circuito intrattenimento-produzione-consumo. All'interno di questa dinamica, finiscono per essere penalizzati sempre sia gli individui che i gruppi sociali marginali o non-conformisti.

---

[12] A. Goldsmith, R. Brewer, *Digital drift and the criminal interaction order*, in *Theoretical Criminology, Theoretical Criminology*, 19, 1. 2015, pp. 112-128.
[13] M. Palma, S. Anastasia (a cura di), *La bilancia e la misura,* FrancoAngeli, 2002.
[14] Così definito da D. Geer (a cura di), *Cybercrime. Digital Cops*, cit.

Attivisti politici, minoranze etniche, gruppi di volta in volta individuati come "a rischio", rischiano di finire per rappresentare le nuove minacce contro le quali progettare e implementare misure repressive.

La regolamentazione statale della rete presenterebbe un problema qualitativamente rilevante, che Daniel Geer mette in relazione con la cosiddetta «fisica digitale»[15]. A differenza dello spazio materiale, il "terzo spazio" si caratterizza per la sua fluidità, volatilità ed imprevedibilità, nonché per l'anonimato legato alla tutela della *privacy*. Queste caratteristiche si incrociano con la tutela delle libertà civili e del libero mercato. Da questa sovrapposizione consegue la riottosità da parte degli individui e degli attori economici a fornire informazioni vitali per la loro esistenza e i loro interessi agli attori del controllo sociale, il che renderebbe problematico implementare ogni tipo di misure di sicurezza in rete.

In realtà, secondo quanto afferma Lee Tien[16], la lettura della rete come flusso libero e incontrollato di relazioni e informazioni si rivela, ad uno sguardo più accurato, limitata, nella misura in cui la rete funziona secondo il principio della regolamentazione architettonica. Come una casa orienta e determina i nostri movimenti secondo la sua conformazione, così la rete orienta i nostri percorsi digitali, creando le condizioni per un controllo *ex ante*, vale a dire imperniato sulla pre-determinazione della navigazione telematica. A differenza dell'ambiente fisico-sociale, dove le sanzioni vengono comminate *ex post*, il computer limita e dirige fin dall'inizio la nostra deriva nello spazio digitale.

Di conseguenza, volendo realizzare una riflessione più accurata, le possibilità che si formi e si radichi una cybercriminalità organizzata sono residue. Laddove nel secondo spazio le organizzazioni criminali riescono a fare leva sul controllo del territorio e sul loro potenziale militare, all'interno della rete debbono muoversi all'interno di spazi pre-determinati, con la possibilità da parte dei diversi attori di dotarsi di strumenti preventivi che ne annullano il potenziale militare. La regolazione architettonica, dunque, finisce per aumentare le possibilità di controllo da parte dello Stato, ma sotto nuove forme.

1.2. Pattugliare il web*:* cybercrimes *di Stato?*

Infatti, è proprio all'interno di questa cornice pre-regolamentata che si crea lo spazio per una nuova forma di sorveglianza: orizzontale, impercettibile, pervasiva; in altre parole, come la definisce lo studioso canadese David Lyon[17], «relazionale», che analizzeremo più in dettaglio nel prossimo paragrafo.

I social *network* all'interno dei quali interagiamo, le persone con cui chattiamo, i siti che visitiamo, vengono costantemente monitorati da sistemi digitali di controllo, che si avvalgono di una domanda di sicurezza a più ampio raggio per monitorare sia gli attori che le comunicazioni "a rischio". È questo il caso del progetto *Carnivore*, un programma di

[15] D. Geer (a cura di), *Cybercrime. Digital Cops*, cit., p. 72.
[16] L. Tien, *Architectural Regulation and the evolution of the social norms*, in D. Geer (a cura di), *Cybercrime. Digital Cops*, cit., pp. 37-58.
[17] D. Lyon, *Theorizing Surveillance: The Panopticon and Beyond*, Willan, 2006.

sorveglianza predisposto dall'FBI e approvato dal Congresso Usa all'indomani dell'11 settembre[18].

Le forze dell'ordine sono autorizzate a tenere sotto controllo, in seguito all'approvazione da parte della procura distrettuale, e per periodi di tempo limitati, quegli individui e quelle porzioni della rete sospettate di terrorismo. L'autorizzazione a proseguire con la sorveglianza può essere concessa qualora dalle indagini emergano degli indizi che inducano a ritenere fondati i sospetti, quindi a richiedere necessari ulteriori supplementi di indagine. Il progetto *Carnivore* nel corso degli anni è stato duramente contestato dalle organizzazioni attive nella difesa dei diritti civili, come la *American Civil Liberties Union* (ACLU), non soltanto perché la sua attuazione si traduce in una violazione della *privacy* e della libertà di espressione, ma anche perché l'attenzione degli inquirenti si rivolge soprattutto verso i cittadini americani di origine araba o di religione musulmana, favorendo la criminalizzazione a priori di interi strati della popolazione.

A fianco del progetto *Carnivore*, come ha svelato l'ingegnere elettronico americano Edward Snowden al *Guardian* nel 2013[19], esistono altri programmi di controllo della rete, elaborati ed implementati dalla NSA, che si connotano per essere molto più sofisticati e articolati. L'agenzia di sicurezza interna, infatti, rappresenta l'attore principale della sorveglianza relazionale, in quanto i suoi programmi di controllo non riguardano solo i presunti terroristi musulmani, bensì l'intera popolazione statunitense.

Il lavoro di sorveglianza che si svolge all'interno della rete si prefigge, dunque, di monitorare ogni forma di comunicazione, relazione e pratiche che vanno in senso contrario alla regolamentazione architettonica, quindi di monitorare le attività di gruppi non conformisti e reti alternative.

In questo contesto, figure del calibro di Snowden e Julian Assange, da un anno e mezzo detenuto in condizioni disumane nella prigione londinese di Belmarsh e a rischio di estradizione negli USA[20], risultano pericolose. Non soltanto, infatti, con la loro attività disvelano le filiere che sottostanno agli intrecci di potere correnti, ma dimostrano altresì la possibilità di ribaltare il flusso securitario attraverso un utilizzo della rete che si muove in direzione contraria a quello convenzionale, che vuole creare un utente docile, controllabile e addomesticabile.

Nello spazio materiale il panico morale attorno ad alcuni reati di piccola entità fornisce la sponda a coloro che mirano all'attuazione di misure repressive che passano attraverso la criminalizzazione di settori specifici della società. Nella rete, allo stesso modo, l'allarme sociale che si costruisce attorno ai *cybercrimes*, amplificato dalla paura del terrorismo, finisce per divenire il cavallo di Troia per l'implementazione di misure repressive e per la messa in atto di nuove forme di controllo sociale, nonché per la repressione di nuove forme del dissenso.

---

[18] H. Ventura, J. Mitchell, H. Deflem, *Governmentality and the War on Terror: FBI Project Carnivore and the Diffusion of Disciplinary Power*, in *Critical Criminology Journal*, 13, 2005, pp. 55-69.
[19] *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, in *The Guardian*, 9 giugno 2013.
[20] *Julian Assange 'has chronic lung condition'*, in *BBC News*, 29 novembre 2012.

Dall'altro lato, è la stessa fluidità della rete a permettere la produzione e la diffusione di saperi e pratiche dissenzienti, sia attraverso azioni individuali, come quelle di Snowden, sia attraverso la creazione di esperienze più strutturate, come *Wikileaks*. Sembrerebbe che ci troviamo di fronte alla formazione di un contro-potere telematico. In realtà, le contraddizioni della rete, come vedremo nel paragrafo successivo, fanno sì che si aprano nuovi spazi e nuove tipologie di sorveglianza.

2. Sorveglianza relazionale. Tra piattaforme ed auto-controllo.

La sorveglianza si connota per essere una delle attività cardinali del controllo sociale, ovvero di tutte quelle pratiche che ogni società implementa con lo scopo di convogliare i comportamenti dei suoi componenti verso aspettative, stili di vita e valori condivisi, secondo una tendenza ordinata, regolare e prevedibile. Osservare il comportamento degli individui, ci insegna Foucault[21], favorisce l'accumulazione di saperi da utilizzare per produrre nuovi dispositivi di potere.

Lo sviluppo e la diffusione di internet hanno permesso alle pratiche e ai saperi della sorveglianza di compiere un salto qualitativo in avanti. Alla sorveglianza verticale, esercitata a livello informale dalle agenzie di controllo sociale come famiglia, scuola, gruppo dei pari, classe, confessione religiosa, e a livello formale dagli apparati statuali, si è sovrapposta la sorveglianza orizzontale, quella che David Lyon definisce come di "tipo relazionale"[22], che utilizza le interazioni di ognuno all'interno della rete.

La sorveglianza relazionale si caratterizza per i suoi connotati di sorveglianza leggera, dal momento che non si avvale dell'utilizzo di mezzi di coercizione fisica. È invisibile, in quanto non è identificabile, come quella della polizia, attraverso segni come le divise, il presidio del territorio o il possesso di armi. Inoltre, si tratta di una sorveglianza di tipo partecipato: se nel contesto della sorveglianza verticale gli individui sopportano il controllo loro malgrado, nell'ambito della sorveglianza orizzontale di tipo relazionale siamo noi stessi partecipi e produttori delle strategie e delle pratiche di controllo[23].

Le rivelazioni di Edward Snowden, ex funzionario della NSA, in seguito ingegnere informatico della *Booz Allen Hamilton*, *contractor* del governo di Washington, che nel 2013 diffuse i segreti dell'apparato di sorveglianza della *National Security Agency*, hanno rappresentato uno spartiacque. L'ex funzionario americano, oggi rifugiato in Russia, ha spiegato il mutamento qualitativo registrato dalle pratiche di sorveglianza. In passato si dava la priorità alle pratiche di prevenzione e di repressione esterne, che vedevano contrapposti i cittadini da un lato e gli apparati statali dall'altro. Adesso il punto focale del controllo si è spostato nella rete, con miliardi di individui, attivisti, organizzazioni e attori governativi risucchiati in una pratica che diventa sempre più invasiva e minacciosa nei confronti delle libertà civili.

---

[21] M. Foucault, *Difendere la Società,* Ponte alle Grazie, 1996.
[22] D. Lyon, *Theorizing Surveillance*, cit.
[23] D. Lyon, *Surveillance after Snowden,* Polity Press, 2015; *Id., The Culture of Surveillance*, Polity Press, 2018.

Man mano che la matassa si dipana, si delinea l'esistenza di un sistema sempre più articolato e insidioso che coinvolge una pluralità di attori e che si espande fin negli interstizi più reconditi dell'individualità. Gli attori della sorveglianza si connotano per non essere un soggetto singolo, bensì una rete ibrida, all'interno della quale i confini tra pubblico e privato si fanno sempre più sfumati. Se da un lato NSA, CIA ed FBI rappresentano il punto nodale della sorveglianza relazionale, dall'altra parte non la portano a compimento in maniera diretta. Lo Stato, primo polo della sorveglianza relazionale, ne subappalta la messa in atto.

In un contesto socio-economico caratterizzato dal culmine del capitalismo post-fordista, a fornire i *software* necessari, a elaborare le strategie sono le ditte subappaltanti. Lo dimostra il caso dello stesso Snowden, che era un tecnico della *Booz Allen Hamilton*. I *contractors* rappresentano quindi il secondo polo della sorveglianza relazionale.

La terza polarità della rete del controllo è rappresentata dalle *corporations*: non soltanto quelle che operano all'interno del mercato informatico, ma anche ditte come *Amazon*.

Le imprese private hanno istaurato col governo statunitense un rapporto di mutualità, in seguito al quale la loro disponibilità a fornire dati relativi ai loro clienti le mette nelle condizioni di acquisire importanti fette di mercato. Questo discorso vale per le banche, ma, soprattutto, per i *social network*. *Facebook* e *Twitter*, fin dalla loro nascita, sono sorvegliati con il loro consenso dal programma *Prism*[24].

Questo aspetto rappresenta un passaggio fondamentale per entrare all'interno del secondo punto qualitativamente rilevante della sorveglianza relazionale. Si tratta della partecipazione attiva di tutti gli utenti del *web* alla sorveglianza. Aprirsi un *account* su *Facebook*, prenotare un volo, effettuare un pagamento online, twittare, rappresentano attività tutt'altro che neutrali, in quanto vengono immediatamente sottoposte a monitoraggio da parte degli apparati di sorveglianza.

Attraverso l'utilizzo dei *software* prodotti dalle principali ditte informatiche e dalle loro *sub*-appaltanti, come *Upstream*[25], che controlla i flussi cablati di informazioni, *XKeyscore*[26], che funge da *database*, e *Dishfire*[27], che intercetta gli sms di 200 milioni di cittadini, è possibile per le agenzie governative statunitensi appropriarsi dei metadati di milioni di persone, vale a dire di informazioni sensibili a largo raggio, che spaziano dal numero di conto in banca al luogo di residenza.

I dati acquisiti vengono poi condivisi con le agenzie governative (ovvero i servizi di sicurezza) dei paesi con cui gli USA hanno stipulato accordi di cooperazione in questo campo, come la britannica *Government Communications Headquarters* (GCHQ), la canadese *Canadian Securities Exchange* (CSE), l'australiana *Australian Signals Directorate*

[24] È il programma di sorveglianza utilizzato da agenzie di sicurezza statunitensi e britanniche, come la NSA e l'MI5 (sul tema, cfr. B. Gellman, L. Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, in *The Washington Post*, 7 giugno 2013).
[25] Per ulteriori informazioni, si veda questo articolo.
[26] Si veda, in proposito, quanto spiegato da Edward Snowden nell'intervista pubblicata a questo *link*.
[27] Ulteriori informazioni sono disponibili a questo indirizzo.

(ASD). La condivisione dei dati costituisce un passaggio cruciale del processo di sorveglianza, in quanto trasforma i metadati in *Big Data*, vista la mole delle informazioni accumulata. Dall'accumulo, si effettua poi il passaggio successivo della scrematura dei dati ottenuti, con lo scopo principale, dall'11 settembre in poi, di prevenire azioni terroristiche.

Ci troviamo così di fronte al livello preventivo della sorveglianza relazionale, che si articola in tre fasi distinte. La prima è quella dell'automazione, ovvero lo stadio durante il quale, attraverso l'uso di algoritmi e di altri apparati informatici, si creano i profili dei potenziali sovversivi, terroristi e oppositori, scandagliando meticolosamente la rete col fine di delineare l'*identikit* del terrorista medio: in questa fase, tutti gli oppositori delle politiche governative, dai *no-global* agli anti-abortisti, dai fondamentalisti musulmani ai gruppi femministi, vengono scandagliati. Nel caso del governo britannico, la legislazione *Prevent*[28], varata dall'esecutivo di David Cameron nel 2011, allarga le maglie della sorveglianza, nella misura in cui vengono catalogati dalla legge come estremisti tutti gli individui e i gruppi che si oppongono alla politica promossa dal governo in carica. Questo passaggio prepara la seconda fase, vale a dire quella dell'anticipo.

Approdiamo finalmente al secondo passaggio, ovvero l'aspetto qualitativamente più rilevante del nuovo tipo di sorveglianza.

Se prima le indagini venivano effettuate basandosi sui precedenti penali degli individui e dei gruppi da sorvegliare, adesso si lavora sulle potenzialità delle minacce, praticando una sorveglianza ossessiva e invadente nei confronti dei soggetti interessati. Tuttavia, prima di adottare misure di contrasto, si tenta una strategia di adattamento, cioè si filtrano le informazioni per stabilire le aree di intervento e i soggetti da monitorare. Come la criminologia attuariale, che ha importato il modello delle assicurazioni nelle strategie preventive, lavorando sulle aree «a rischio»[29], così l'*intelligence* opera una sorveglianza meticolosa e pervasiva su tutto il bacino dei potenziali sovversivi.

L'esito è quello della violazione delle libertà fondamentali, che porta a etichettare come potenziale minaccia tutti coloro che non si allineano al nuovo ordine mondiale, senza fare distinzioni, e finendo per produrre e diffondere panico morale.

Soprattutto, però, la sorveglianza relazionale, per quanto protetta dalla cornice legale del *Foreign Intelligence Surveillance Act*[30], che autorizza la sorveglianza senza il permesso della Corte, in particolare nella sezione 1802, produce nuovi errori giudiziari. Lo testimoniano le centinaia di casi che[31], dal 2001, hanno riguardato cittadini americani e

[28] V. *Prevent duty guidance for England, Scotland and Wales*, 12 marzo 2015.
[29] Branca della criminologia contemporanea, incentrata sulla riduzione del rischio di criminalità a partire dall'analisi delle probabilità che specifiche tipologie di individui o gruppi, sulla base di fattori come precedenti penali, fattori genetici, caratteristiche socio-culturali, condizioni economiche, siano coinvolti nella commissione di atti criminali. Si veda in proposito D. Robert, *Actuarial Justice,* In M. Bosworth (a cura di), *Encyclopedia of Prisons & Correctional Facilities,* vol. I, Sage, 2005, pp. 201-227.
[30] Cfr. il titolo 50 del Codice delle leggi federali degli Stati Uniti d'America, cap. 36, sub-cap. I, "*Electronic surveillance*".
[31] A. Worthington, *The Guantanamo Files,* Polity Press, 2007.

stranieri la cui unica colpa era quella di essere musulmani, che ha comportato lunghe detenzioni illecite in luoghi come Guantanamo.

Tuttavia, se si analizza l'aspetto partecipato della sorveglianza relazionale, è possibile scorgervi un aspetto che spiazza le interpretazioni tradizionali del controllo sociale. Non ci troviamo, infatti, in un contesto orwelliano, dal momento che, se la sorveglianza relazionale è possibile, lo è perché si basa su di una cultura della sorveglianza profondamente radicata. Non soltanto in riferimento al panico morale, ma, soprattutto, relativamente alle modalità con cui navighiamo sul *web*.

Innanzitutto, la disponibilità da parte degli utenti a fornire i propri metadati senza utilizzare troppe precauzioni li porta a favorire ogni sorta di controllo, anche in seguito alla convinzione ingenua di essere naturalmente protetti da truffe e da invasioni del proprio cyberspazio.

Inoltre, i sorvegliati sono loro stessi dei sorveglianti: quando si crea un *blog* o una pagina *web*, quando si agisce da *stakeholder* filtrando i commenti e i *post* sulla propria pagina di *Facebook*, quando si vanno a leggere i profili delle persone nei *social networks*, si svolge attività di sorveglianza. E non si tratta sempre di esercitare contro-sorveglianza, che pure, in una certa misura, è utile, come nel caso di *Wikileaks*. La via d'uscita, in questo contesto, probabilmente consiste nel prendere sul serio la sorveglianza relazionale. In altre parole, bisogna creare una sorta di auto-disciplina, che educhi gli utenti della rete ad usare il *web* criticamente. L'ambiguità della rete è un dato di fatto.

L'approccio binario del "vota chi vuoi eliminare" e del "sì o no", utilizzato dai *reality show* e riprodotto da piattaforme politiche come la piattaforma Rousseau, dietro la partecipazione diretta cela l'intento di catturare, elaborare e orientare la volontà individuale e collettiva. In periodi di populismo imperante, vero e presunto, è un rischio che, rispetto alle libertà civili, alla presunzione di innocenza, e alle criminalizzazioni individuali e di massa, non ci si può permettere di correre. Per questo l'auto-disciplina è importante.

Bibliografia.

H. Becker, *Outsiders*, Free Press, 1963.
S. Cohen, *Folk Devils and Moral Panic*, Routledge, 1974.
M. Foucault, *Difendere la Società*, Ponte alle Grazie, 1996.
D. Geer (a cura di), *Cybercrime. Digital Cops in a Network Environment,* New York University Press, 2015.
P. Gottschalk, *Policing Cybercrime*, Bookboon, 2010.
A. Goldsmith, R. Brewer, *Digital drift and the criminal interaction order*, in *Theoretical Criminology*, 19, 1. 2015, pp. 112-128.
G.de Lagasnerie, *L'Arte della Rivolta. Snowden, Assange, Manning*, Stampa Alternativa, 2016.
D. Harvey, *Città Ribelli. I Movimenti Urbani dalla Comune di Parigi a* Occupy Wall Street, Il Saggiatore, 2011.
S. Lorenzetti, *La maestra d'asilo licenziata per un video* hard*: «Tradita dal mio ex: mi fidavo»*, in *Corriere della Sera*, 18 novembre 2018.
D. Lyon, *Theorizing Surveillance: The Panopticon and Beyond*, Willan, 2006.

D. Lyon, *Surveillance after Snowden*, Polity Press, 2015.
D. Lyon, *The Culture of Surveillance*, Polity Press, 2018.
M. Palma, S. Anastasia (a cura di), *La bilancia e la misura*, FrancoAngeli, 2002.
D, Quirico, *Primavere Arabe. Le Rivoluzioni dall'Altra Parte del Mare*, Bollati Boringhieri, 2014.
D. Robert, *Actuarial Justice,* in M. Bosworth (a cura di), *Encyclopedia of Prisons & Correctional Facilities*, vol. I, Sage, 2005, pp. 201-227.
K. Steinmetz, *Hackers*, New York University Press, 2017.
L. Tien, *Architectural Regulation and the evolution of the social norms*, in D. Geer (a cura di), *Cybercrime. Digital Cops in a Network Environment*, 2015, pp. 37-58.
J. Treadwell, *From the car boot to booting it up? eBay, online counterfeit crime and the transformation of the criminal marketplace,* in *Criminology & Criminal Justice*, 12, 2, 2012, pp. 175-194.
H. Ventura, J. Mitchell, H. Deflem, *Governmentality and the War on Terror: FBI Project Carnivore and the Diffusion of Disciplinary Power,* in *Critical Criminology Journal*, 13, 2005, pp. 55-69.
A. Worthington, *The Guantanamo Files*, Polity Press, 2007.