DOPPIOZERO

Lo spionaggio e la rete

Adele Bianco

26 Marzo 2016

A completamento di quanto illustrato da Joy Marino e Paolo Giaccaria circa l'impatto delle nuove tecnologie sulla nostra vita, in questo contributo ci occuperemo della rete, in particolare del suo lato occulto. La diffusione di Internet e la digitalizzazione di molte attività che regolano distribuzione e fornitura di informazioni, beni e servizi è una caratteristica peculiare delle società contemporanee (Kshetri 2010). La progressiva informatizzazione da un lato è uno strumento che agevola la nostra quotidianità, dall'altro comporta il problema della gestione delle reti e della custodia delle banche dati. Data la crescente rilevanza di queste tecnologie, la questione della sicurezza dell'intero complesso costituisce un problema specifico. Essa riguarda infatti una materia assai delicata come i dati personali, anche sensibili, della popolazione; c'è quindi il rischio che quei dati possano essere utilizzati in maniera impropria (Rodotà 2014).

La tutela della sfera privata che noi oggi chiamiamo *privacy* era già ben chiara a Georg Simmel come problema legato alla modalità e alla qualità delle relazioni sociali di un soggetto. Nel suo saggio su *Il Segreto e la società segreta*, egli afferma che questa dimensione esiste come «proprietà privata spirituale» del soggetto (p. 302). Simmel esplicita che «ciò che non viene rivelato non si può sapere [perché] […] intorno ad ogni uomo vi [è] una sfera ideale di grandezza variabile in direzioni diverse […] nella quale non si può penetrare senza distruggere il valore di personalità dell'individuo», (p. 301. Al riguardo cfr. anche quanto scrive Marco Belpoliti. Nel caso in cui il controllo avvenga da parte dei servizi di sicurezza degli Stati, si ricorderà che a lungo si è parlato della rete Echelon (Campbell 2003; O'Neill 2005; Radden Keefe 2006; Mainoldi, 2007; Loader, Douglas 2010). Echelon è il sistema mondiale d'intercettazione delle comunicazioni private e pubbliche. Echelon si basa sul fatto che ciascuno di noi lascia quotidianamente dietro di sé una scia di tracce elettroniche (transazioni commerciali, scambi di informazioni). Di nuovo sovviene quanto scrive Simmel nell'*Excursus sui rapporti epistolari* (ivi, pp. 326-328), quasi a mettere in guardia il popolo dei cibernetici: «la forma scritta […] comporta una "pubblicità" […]

potenziale», questione di cui di recente si è dibattuto a proposito del c.d. “diritto all’oblio”. Tutte le informazioni sono convogliate in sistemi che le elaborano e che mettono in relazione elementi apparentemente casuali in maniera da far emergere, da una massa non organizzata di dati, informazioni utili ai servizi di sicurezza. In tal modo essi riescono a conoscere e a controllare in tutto il mondo le attività di individui e organizzazioni potenzialmente pericolosi e delle loro eventuali relazioni. L’analisi di flussi di dati a fini di controllo, spionaggio — soprattutto in funzione antiguerriglia e antiterrorismo — non è una novità; la rete ha ulteriormente perfezionato le modalità di ricerca e di elaborazione dei dati, reso possibile ampliare le indagini e potenziare la capacità informativa degli elaboratori.

Fin dagli anni ’70 – come illustra un film dell’epoca di Sidney Pollack, *I tre giorni del Condor*, 1975 – i calcolatori fungevano da banche dati e svolgevano una prima scrematura delle informazioni da vagliare. I pionieri in questo campo di attività – raccolta di informazioni, loro selezione e analisi allo scopo di profilare specifiche tipologie di soggetti – sono le società commerciali. Per veicolare in maniera mirata la pubblicità esse raccolgono dati su gusti, abitudini di acquisto, modalità di consumo della clientela e li associano con altre variabili strutturali. In tal modo i clienti vengono distinti in categorie per personalizzare le offerte commerciali. Il TIA (Total Information Awareness) è un “sistema di sistemi” in grado di raccogliere informazioni sia da fonti aperte, come Internet, sia da banche dati pubbliche e private. I dati raccolti vengono esaminati per prevenire eventuali attentati e venire a conoscenza di attività sospette e di potenziali minacce. L’applicazione e lo sviluppo di sistemi di controllo dell’informazione hanno subito un particolare impulso dopo l’attentato alle Torri Gemelle nel 2001. Questi sistemi, finanziati con milioni di dollari, sono capaci di scandagliare dati personali sensibili, elemento che pone la questione della tutela della *privacy* dei cittadini. Da più parti e ripetutamente si è osservato che con la giustificazione della lotta al terrorismo si sia creata una sorta di “Grande Fratello” planetario. In proposito le obiezioni sono due: la prima è relativa alla sua utilità nella prevenzione di atti terroristici: quanto più aumenta la massa di informazioni, tanto più risulta difficile selezionarla e utilizzarla in maniera proficua. La seconda obiezione riguarda il rischio che questo “Grande Fratello” diventi a livello globale uno strumento di controllo dei movimenti di opinione internazionali (ad es. quello no-global), utile pure a fini di spionaggio economico e strategico.

Parallelamente allo sviluppo della digitalizzazione, si sono affermate nuove forme di criminalità legate all’ambito informatico, se non esclusiva espressione di esso. Il loro impatto è rilevante, fino a rappresentare una minaccia per la sicurezza

collettiva. I crimini informatici presentano delle caratteristiche proprie, perché si manifestano in un ambito tecnologico del tutto nuovo per il quale sono necessarie professionalità e conoscenze sofisticate, non alla portata di tutti. I crimini informatici sono dunque strutturalmente differenti da quelli tradizionali (Colombo, Barbagli, Savona 2011) ed è quindi necessario distinguerne i diversi tipi. Come osservano Holt e Bossler (2016), la nozione di computer crime si presenta fin dai primi anni ‘70 ed è utilizzata per lo più con riferimento al cattivo uso delle banche dati (computer misuse). Con la diffusione e anche la maggiore semplicità di accesso ai sistemi informatici, dalla fine degli anni ‘90 si iniziò ad indicare con la nozione di cybercrimes i crimini commessi on line, anche se alcuni continuavano ad utilizzare la vecchia definizione di computer crime (Wall 2007). Tra le due nozioni c’è una differenza sotto il profilo tecnico. Cybercrime si riferisce a crimini commessi da chi ha una particolare conoscenza del cyberspazio, mentre chi compie computer crimes dispone anzitutto di particolari competenze informatiche. Oltre ai crimini informatici in senso lato, Giacomello (2014) indica, ancorché come possibilità remote, il Cyberterrorismo e il Cyberwarfare. Benché si tratti di tipi di attacchi diversi – il primo organizzato da gruppi terroristi, il secondo un vero e proprio atto di guerra tra Stati – loro bersaglio sono delle infrastrutture strategiche (cfr. al riguardo l'articolo di Matteo Vegetti).

Lo scopo è creare disagi alla popolazione e arrecare danno alle reti di comunicazioni, in particolare quelle militari. Al momento si tratta di due forme che non si manifestano in tutta la loro potenziale gravità. Largamente praticato è invece lo spionaggio in rete volto a controllare scambi di informazioni e dati, anche di tipo militare. Un aspetto importante dei crimini informatici e che li differenzia dalle forme tradizionali di criminalità, è che, come poc’anzi osservato, essi richiedono raffinate conoscenze tecniche, in genere un vantaggio non indifferente nei confronti delle vittime. Altri fattori che caratterizzano i crimini informatici sono *in primis* la loro novità e in secondo luogo il fatto che avvengono (anche: sono realizzati) in uno spazio e su scala globale. La localizzazione dei crimini informatici è diversa da quella tradizionale perché dal punto di vista spaziale, vittima e criminale possono essere anche molto distanti. Molto spesso gli attacchi provengono da lontano, anche da altri Stati. Questo fatto facilita l’attività criminale e mette chi la esercita al riparo da eventuali tentativi di repressione e punizione da parte delle autorità. Entrambi questi elementi aggirano il tradizionale apparato repressivo e sanzionatorio, ancora concepito e organizzato su base statal-nazionale. La cooperazione tra Stati stenta a decollare. In relazione ai crimini informatici vanno pertanto sviluppate nuove norme giuridiche (Cuniberti et al. 2009); e realizzate specifiche misure preventive.Venendo ora ad una tipologia di crimini informatici, è opportuno

distinguere tra atti offensivi che hanno nella rete il loro terreno naturale e reati comuni, che avvengono anche fuori dalla rete, ma che la rete potenzia o agevola (Wall 2007). Tra i primi vanno menzionate le violazioni negli accessi commesse dagli hacker allo scopo di neutralizzare i sistemi o di modificarne anche temporaneamente il funzionamento. Si pensi agli interventi del gruppo Anonymous contro i terroristi jihaidisti (Frediani, 2012 e qui). Altri tipi di crimini sono rappresentati dalla propagazione di virus, ovvero dall'invio di programmi volti a penetrare nei sistemi e a danneggiarli; dalle violazioni negli accessi per ottenere informazioni, sottrarre dati o cancellarli. I criminali informatici penetrano nei sistemi informatici delle proprie vittime sfruttandone la buona fede, la poca prontezza e l'ingenuità e carpendo così informazioni.

Un'altra strada per penetrare i sistemi informatici è sfruttare gli errori del software, i cosiddetti bachi, per raccogliere informazioni su dati sensibili ed eventualmente modificarli.La seconda categoria di crimini informatici è il cyber-deception/theft, ossia il furto o la sottrazione indebita di materiali e informazioni. Rientra in questa categoria la pirateria di quanto è attinente alla proprietà intellettuale: l'acquisizione illegale di materiali come i contenuti video, i file musicali nonché gli stessi software, scambiati in rete senza il rispetto del copyright. Questo fenomeno rappresenta per le aziende del settore una perdita all'anno di miliardi; per tale ragione esso è particolarmente studiato (Holt & Bossler 2014). La repressione del cyber-deception/theft è difficile perché le vittime non denunciano spesso quanto subiscono e non collaborano con gli investigatori. Preferiscono far fronte da sole ai furti. Le aziende non denunciano l'accaduto perché temono una perdita di immagine riguardo alla propria affidabilità e preferiscono risolvere in proprio anche giungendo ad accordi con gli stessi criminali. Come si vede, si tratta di reati comuni che trovano nella rete nuovo terreno fertile: merci e contenuti illegali. materiale pedo-pornografico. traffico d'armi e di stupefacenti, fino a quello di esseri umani o di organi di esseri umani (Izzi 2011).