Cybercrime: Hacking e criminalità informatica

**** M. Lilli***

Secondo un lancio Ansa del 5 luglio scorso, sembra che nell'ultimo quinquennio, nel nostro Paese, il *cybercrime* – altrimenti detto crimine la quale condotta è correlata alla violazione di un sistema informatico o telematico – sia aumentato notevolmente. Mentre, è del 26 luglio la notizia rimbalzata su diversi media secondo cui il sistema informatico di un noto istituto bancario internazionale sarebbe stato violato, carpendo fraudolentemente migliaia di dati riferiti ad altrettanti clienti.

Tuttavia, a parte questa sorta di allarme lanciato dai media, più o meno periodicamente e con la medesima enfasi, sono in pochi ad occuparsi dei motivi sociali e psicologici che determinano questi fenomeni e condotte delittuose, vale a dire quali strategie preventive si dovrebbero adottare sia nei confronti di chi agisce, al fine di distoglierli dall'attuarli, sia nei confronti delle potenziali vittime quale processo educativo nei loro confronti tale da tenerle in qualche maniera distanti dal rischio, o comunque al fine da renderle pienamente consapevoli del fenomeno e dei suoi effetti negativi.

Ebbene, da questo ultimo inciso, quello del rischio, credo preliminare una precisazione. Vale a dire comprendere e far comprendere soprattutto ai diversamente esperti la differenza che corre tra il concetto di pericolo (quale fatto generico) e quello di rischio (potenzialmente calcolabile). Definizioni apparentemente decontestualizzate dall'ambito criminologico ma che, viceversa, dal mio punto di vista, ne sono parte piena proprio con specifico riguardo al processo di prevenzione e dunque contrasto del crimine stesso.

Ora, a parte la qualità criminale di chi agisce nell'ambito del *cybercrime*, cioè delle attitudini e preparazione tecnica dei soggetti operanti, credo che gran parte dei risultati dai medesimi ottenuti sia da ricercare nella scarsa educazione all'uso delle nuove tecnologie, che tradotto significa approccio superficiale alla conoscenza e utilizzo delle strumentazioni informatiche e telematiche. Peggio ancora quando tale superficialità investe i cosiddetti addetti ai lavori, cioè tecnici o definitisi tali che si adoperano a tutela della tecnologia *hardware* e *software*, sia di grandi imprese, sia del singolo internauta, che comunque anch'egli ha interesse – e per certi versi costretto – ad utilizzare, per esempio, i nuovi sistemi di transazione economica.

Su queste premesse, quello che dal mio punto di osservazione scarseggia specie nel nostro sistema Paese è la cosiddetta *cultura della sicurezza*, verso la quale la criminologia – brevemente, la

scienza che studia il crimine nel suo più ampio insieme di significati – deve avere una parte ancora più attiva proprio all'indirizzo di percorsi pedagogici mirati. Intendo dire che il risultato dell'analisi dei fenomeni criminali complessi sarà tanto più positivo quanto essa, l'analisi, sia in grado di prevenire, piuttosto che solo reprimere, la consumazione del reato.

Diciamo pure che, citando Durkheim (1858-1917), è preliminarmente essenziale analizzare la corrispondenza che si determina tra il fenomeno in esame e i relativi bisogni generali del cosiddetto *organismo sociale*, cioè, come spiegava l'autore nell'opera *Le regole del metodo sociologico* (1895): «Quando ci si accinge a spiegare un fenomeno sociale, bisogna cercare separatamente la causa efficiente che lo produce e la funzione che esso assolve» (cfr. cit. Crespi, 2002, pp. 23-24).

Ancora una volta, come ho affermato in precedenti pubblicazioni (2015), sono convinto che bisogna ampliare l'ambito cognitivo del concetto di *sicurezza sociale*, ad oggi noto e ricordato solo quale riferimento alla previdenza e assistenza attraverso l'intervento pubblico. Infatti, è mio punto di vista che la vera essenza del significato di *sicurezza sociale* nel suo complesso insieme la si coglie proprio facendo l'esegesi della definizione del concetto stesso, dunque i fini cui è rivolta tale sicurezza, cioè il benessere della persona, che dunque chiama in causa anche quel diritto inalienabile sancito dall'articolo 32 della Costituzione che riguarda giustappunto la salute; definita dall'Organizzazione Mondiale di Sanità (1948): «uno stato di completo benessere fisico, mentale e sociale», no quindi solo assenza di malattia o infermità. Vivere perciò una condizione di solo benessere fisico non significa, *de plano*, star bene anche dal punto di vista psicosociale più in generale.

Ed allora ecco che, per quanto più riguarda il presente contributo, la *sicurezza sociale* può essere anche intesa come quell'insieme di provvedimenti finalizzati ad assicurare a tutti ogni mezzo che risulti sufficiente e necessario al fine di soddisfare i bisogni della vita in ogni momento dell'esistenza, e garantire quindi la difesa contro particolari tipologie di rischio in grado di danneggiare anche la propria sfera economica, i quali effetti si riversano inevitabilmente, investendola con conseguenze devastanti, su quella psichica individuale.

Sicurezza sociale e prevenzione del crimine, da intendere perciò come analisi delle condizioni che definiscono il rischio della devianza e i modelli decisionali che utilizzano paradigmi di difesa adeguati ad ogni circostanza. Ma si parla anche di meccanismi autoregolativi, cioè a dire di modalità che permettono alla persona di gestire le diverse variabili e i termini di utilizzo nel contesto di vita. Una sorta di autotutela basata sulla conoscenza e sulla consapevolezza, concetti ormai acclarati anche all'interno dei paradigmi criminologici.

Pertanto, il concetto di sicurezza soggettivamente percepita si riferisce alla capacità che ognuno si riconosce nel poter controllare e prevenire gli eventi, ciò al fine di assicurare la propria stabilità, ma vista la realistica impossibilità di perseguire pienamente questo fine, vengono messi in moto meccanismi difensivi volti ad isolare quanto percepito come minaccioso, un po' così come avviene con i processi di etichettamento, cioè allontanare da se quelle persone che assumono un comportamento non conforme, altrimenti detto deviante, rispetto al modello di riferimento socialmente accettato e condiviso.

E il tema che occupa questo contributo, il fenomeno legato ai crimini informatici, credo possa intendersi come esempio emblematico. Fra tutti il cosiddetto furto di identità, reato strettamente legato alla sottrazione dei propri dati personali – come per esempio quelli relativi alla carta di credito piuttosto che al numero di conto corrente bancario – carpiti con artifizio e raggiro attraverso una telefonata, una email, uno Short Message Service, una chat (*phishing*), oppure attraverso l'intrusione diretta da parte del malintenzionato all'interno dei dispositivi – personali o di terze parti – di archiviazione dati (*hacking*).

Per esempio, si è stimato «che nel 2004, circa 57 milioni di persone sono state bersaglio del phishing. Soltanto nel giugno 2004 ci sono stati 1422 attacchi phishing. Il numero degli attacchi nel 2004 è aumentato rispetto a quelli del 2003 con una stima del 1,126%. Circa il 19% dei destinatari ha aperto l'e-mail e cliccato sul link. Circa il 3-5% dei riceventi ha divulgato le proprie informazioni finanziarie» (cfr. Picozzi, 2008, p. 434).

Non è dunque un caso se, per certi versi paradossalmente, il *phishing* risulti ancorché oggi più pericoloso dell'*hacking*, in quanto rappresenta l'anello più vulnerabile datosi che è l'utente finale ad "abboccare" a messaggi/email esca, cliccandoci sopra ed essere così inconsapevolmente diretto verso l'irreparabile. Pertanto, il problema non è dato tanto dalla vulnerabilità dei *server* contenenti e custodi dei dati, e questo proprio perché sono ingenti gli investimenti di natura economica – in termini di sicurezza – da parte delle aziende interessate, al punto da poter definire gli stessi, *server*, ragionevolmente sicuri.

E sempre dal punto di vista della ricerca criminologica, è da me condivisibile la tesi per cui la stessa ricerca «è da sempre stata fin troppo impegnata nella spiegazione delle cause che spingono un soggetto a commettere un reato, e, al contrario, fin troppo poco volta allo studio dei metodi e degli strumenti adatti a ridurre la criminalità e a diminuire il senso di insicurezza sociale» (cfr. Curti, 2013, in Federici, p. 82).

Principio, quello appena richiamato, che ancora una volta riconduce a percorsi di studio più che altro indirizzati verso una anamnesi del fenomeno qui in esame che abbia come fine privilegiato

quello che si potrebbe ragionevolmente definire dell'educazione informatica, detta anche reale conoscenza e uso delle nuove tecnologie con annessi rischi di utilizzo. Rischi, dal punto di vista della repressione del reato, oramai ben contemplati nel nostro ordinamento penale soprattutto a seguito dell'entrata in vigore della Legge 18 marzo 2008, n. 48, in tema di criminalità informatica, che ha ratificato la Convenzione del Consiglio d'Europa (Budapest, 23.11.2001).

La Convenzione, di fatto, dopo avere definito il concetto di dato informatico, disciplina anche le misure da adottare ai fini del contrasto a tale fenomeno delittuoso, che devono includere il potere da parte delle autorità preposte di: «a) sequestrare o acquisire in modo simile un sistema informatico o parte di esso o un supporto per la conservazione di dati informatici; b) fare e trattenere una copia di quei dati informatici; c) mantenere l'integrità dei relativi dati informatici immagazzinati; d) rendere inaccessibile o rimuovere quei dati dal sistema informatico analizzato». Assimilando perciò, con tali indicazioni, il dato informatico ad un bene (cosa) materiale (cfr. Corte di Cassazione, Sezioni Unite Penali, Presidente Santacroce, Sentenza n. 31022/15, del 29 gennaio 2015).

Concludo questo breve intervento citando, come spesso mi capita di fare (2016), un giurista, illustre maestro, di quella che egli definiva *cultura dei limiti*, Severino Santiapichi (1926-2016); vale a dire, aggiungo, quella consapevolezza che ognuno dovrebbe avere e portare seco in ogni momento del proprio agire quotidiano, specie se rivolto verso l'interesse collettivo.

Concetto, quello di limite, che dal mio punto di vista investe lo stesso principio di *norma giuridica*, nel senso che, ho già scritto (2017): «considerate le innumerevoli componenti umane e sociali più in generale che determinano spesso repentini mutamenti del tessuto sociale di riferimento […] una ipotesi di compiuta normazione tale da poter soddisfare ogni settore e comportamento dell'essere umano, il più delle volte imprevedibile, sia un qualcosa di assolutamente improponibile proprio dal punto di vista oggettivo, forse, financo utopico».

Anche perché, parafrasando Calamandrei (1889-1956), non basta leggere e coordinare le regole scritte nel codice, tanto che i codici regolano solo quello che si vede, cioè la forma, ignorando i procedimenti psicologici che invece si compiono nel segreto delle singole coscienze. ***ML***

° ° ° ° °

Riferimenti bibliografici

Calamandrei P. (1959-2013) *Elogio dei giudici*, Milano, Salani.

Crespi F. (2002) *Il pensiero sociologico*, Bologna, il Mulino.

Durkheim E. (1895-2008) *Le regole del metodo sociologico*, Torino, Einaudi.

Federici M.C. (2013) (a cura di) *La sicurezza umana: un paradigma sociologico*, Milano, Angeli.

Lilli M. (2017) *La norma giuridica*, in *Sociologia Contemporanea* (ISSN 2421-5872), n. 14A17 del 06.06.2017.

Lilli M. (2016) *La verità dei giudici. Riflessioni sociologiche*, in *Sociologia Contemporanea* (ISSN 2421-5872), n. 14A16 del 24.10.2016.

Lilli M. (2015) *Aspetti della sicurezza sociale*, in *Sociologia Contemporanea* (ISSN 2421-5872), n. 19A15 del 10.12.2015.

Picozzi M. (2008) (a cura di) *Crime Classification Manual*, Torino, CSE.

° ° ° ° °

Pubblicato in *Sociologia Contemporanea*, 19A17 del 06/09/2017