Archivio Penale
settembre–dicembre 2013 fascicolo 3 anno LXV
ISBN 978-88-548-6177-0
DOI 10.4399/97888548617702
pag. 765–769

Le ragioni di un confronto di idee

Donatella Curtotti

1. Il compito del diritto è mettere in ordine la società; aiutare a dare a ciascuno ciò che non ha ma deve avere. Il compito del diritto e del processo penale è ancora più alto; la pena deve saper trasformare il *malum* in *bonum passionis*, insegnando all'uomo e alla società ad essere ciò che non è ma deve essere (Carnelutti).

Per perseguire tale funzione, le norme penali (sia le fattispecie incriminatrici che quelle relative all'accertamento penale) dovrebbero essere costruite in rapporto ai fenomeni che turbano l'ordine sociale, all'evoluzione che questi subiscono col passare del tempo e col modificarsi delle esigenze della società, così da individuare al meglio le condotte che meritano una punizione ed il modo più giusto per applicarle.

Ebbene, si sa che negli ultimi venti anni la società è stata travolta dall'*Information and Communications Technology* (ICT), cioè dalla c.d. tecnologia informatica, con cambiamenti epocali in ogni settore della vita umana (sociale, economico, culturale) che hanno alterato completamente il tradizionale modo di comunicare, lavorare ed interagire. La rivoluzione tecnologica ha dato vita ad una società informatica, immersa in un mondo virtuale (*cyberspace*), privo di fisicità e di contestualità, alterato nello spazio e nel tempo e connotato da impersonalità.

Come questo abbia prodotto automaticamente un nuovo tipo di criminalità (quella, appunto, informatica) è inutile dirlo. Così come è pacifico che la novità non sta tanto nel fatto che le nuove tecnologie ed Internet costituiscono l'obiettivo delle attività criminali, quanto che i computer e le nuove forme di comunicazione interattiva rappresentano solo nuove forme strumentali per commettere o preparare reati di tipo tradizionale; tanto da far dire ad una nota studiosa americana che la categoria dei *cybercrimes* rappresenta una sorta di *"old wine in new bottles"* (Brenner), cioè un "vecchio" fenomeno realizzato con un "nuovo" strumento . Altrettanto evidente è come tutto questo abbia prodotto un nuovo modo di indagare e valutare l'esistenza dei fatti di reato. Non solo quelli di matrice informatica. Gli strumenti informatici (*computer*, *mobile*, *ipad*) costituiscono ormai *tools* imprescindibili di accertamento di qualsivoglia ipotesi di reato rappresentando elementi (e, quindi, fonti di prova) di cui ogni individuo fa uso nella vita quotidiana.

In tutto questo, però, non c'è nulla di originale sotto il profilo scientifico. Al pari del rapporto "società/criminalità", quello "criminalità/ricerca scientifica" presenta un andamento simbiotico. Il tema in esame non costituisce un'eccezione. La dottrina penale studia il tema della criminalità informatica sin da quando la criminalità informatica è diventata oggetto d'interesse del legislatore italiano producendo riflessioni sulle norme e soluzioni *de iure condendo*, senza riserve. A partire dall'intervento del 1993 che, su impulso della Raccomandazione sulla criminalità informatica, adottata dal Comitato dei Ministri del Consiglio d'Europa, il 13 settembre 1989, ha introdotto con l. 23 dicembre 1993, n. 547, alcuni reati c.d. informatici nonché una prima forma peculiare di raccolta della prova digitale, la c.d. captazione telematica, di cui all'art. 266–*bis* c.p.p. Gli studi hanno, poi, seguito le tre stagioni riformatrici nel settore, come quella della normativa repressiva della pedopornografia *on line* (l. 15 febbraio 1996, n. 66; l. 3 agosto 1998, n. 269; l. 6 febbraio 2006, n. 38), quella successiva all'attentato terroristico alle torri gemelle (l. 15 dicembre 2001, n. 438; d.l. 27 luglio 2005, n. 144) coeva a quella del codice *privacy* e alle sue modificazioni (d.lgs. 30 giugno 2003, n. 196; l. 26 febbraio 2004, n. 45; l. 31 luglio 2005, n. 155 e d.lgs. 30 maggio 2008, n. 109), e soprattutto quella più sistematica contenuta nella l. 18 marzo 2008, n. 48, in adesione alla Convenzione di Budapest del 2001, costituente nuove fattispecie penali e nuove attività investigative.

Non avrebbe avuto senso un confronto di idee che fosse motivato solo da questo. Sarebbe risultato ripetitivo e sterile. In realtà, qualcosa di nuovo all'orizzonte c'è. Lo dice a chiare lettere la Comunicazione congiunta a Parlamento europeo, Consiglio, Comitato economico e sociale europeo e Comitato delle Regioni del 7 febbraio 2013 che, nell'elaborare la strategia dell'Unione europea sulla Cybersicurezza, individua come strategia prioritaria la riduzione drastica del crimine informatico.

È noto che con l'entrata in vigore del Trattato di Lisbona la criminalità informatica è stata inserita nell'art. 83 TFUE fra i fenomeni delittuosi di natura grave e transazionale su cui l'UE ha competenza penale. Con l'ultima direttiva *in subiecta materia*, l'interesse a livello europeo è determinato dall'incremento esponenziale di tale tipologia di crimine, annessa ai già noti problemi legati al suo accertamento, come la galoppante sofisticatezza degli strumenti impiegati, la facile condizione di anonimato dietro cui si celano i rei, la transnazionalità dell'attività illecita.

Drastically reducing cybercrime (2.2. della Comunicazione congiunta):

The more we live in a digital word, the more opportunities for cyber criminals to exploit. Cybercrime is one of the fastest growing forms of crime, with more than one million people worldwide becoming victims each day. Cybercriminals and cybercrime networks are becoming increasingly sophisticated and we need to have the right operational tools and capabilities to tackle them. Cybercrimes are high–profit and low–risk, and criminals often exploit the anonymity of website domains. Cybercrime knows no border — the global reach

of the Internet means that law enforcement must adopt a coordinated and collaborative cross–border approach to respond to this growing threat.

A questo punto, è inevitabile una riflessione di natura statistica. L'Eurobarometro della Commissione europea, nell'ultimo sondaggio sull'impatto della criminalità informatica del 22 novembre 2013 che ha interessato oltre 27000 persone, stima che il 12% degli intervistati ha subito una violazione del proprio profilo su un social network o della propria casella di posta elettronica da parte di *hackers* e che il 7% è stato vittima di frodi bancarie o con carta di credito *on line*. L'ultimo rapporto Clusit 2013 relativo alla sicurezza ICT in Italia al 2012, documenta che rispetto al 2011 c'è un tratto di forte crescita (+ 245% complessivamente) delle minacce informatiche essendo aumentate, in parallelo, sia la numerosità degli attacchi e la loro sofisticazione sia, di conseguenza, la severità dei danni subiti dalle vittime. Tra le tipologie di attacco (tra cui anche quelle di matrice attivista e lo spionaggio), il *cybercrime* è statisticamente il maggiore con un incremento del 372,35% rispetto al 2011 (633 crimini nel 2012, 170 nell'anno precedente).

Un ulteriore elemento di novità viene messo in luce ancora una volta dall'Unione europea, con la Direttiva 2013/40/UE, del 12 agosto 2013, relativa agli "Attacchi contro i sistemi di informazione". La necessità della direttiva è legata alla rapida evoluzione degli *hardware* e *software* che producono strumenti informatici nuovi e nuove forme di aggressione (§ 16). Non a caso, pur affermando che il quadro giuridico di riferimento per la lotta alla criminalità informatica rimane la Convenzione del 2001 (§ 15), la direttiva si riferisce in particolare agli attacchi "particolarmente gravi" per i quali mira a: *a)* avvicinare il diritto penale degli Stati membri; *b)* inasprire le sanzioni penali e prevedere nuove circostanze aggravanti; *c)* favorire la cooperazione di polizia e giudiziaria. Sono ritenuti attacchi particolarmente gravi: quelli su "larga scala" (es. i botner, ossia una rete di computer, infettata con *software* maligni per mezzo di attacchi informatici mirati, che può essere attivata all'insaputa degli utenti). Particolare gravità è riconosciuta agli attacchi ad infrastrutture critiche, vitali per il mantenimento delle funzioni essenziali della società, della salute, del benessere economico o sociale delle persone, come reti di trasporto, impianti energetici, reti governative. Infine, gravi sono ritenuti anche il "furto d'identità" e altri reati connessi all'identità.

È fatto un particolare richiamo agli Stati membri nel "affrontare le indagini penali e nel ripartire le competenze tra le competenti autorità nazionali" (§ 28).

2. A questo punto, può dirsi che il profilo di novità che giustifica un confronto di idee sul tema della criminalità informatica non è dato, perlomeno a primo acchito, da una nuova dimensione giuridica del problema, quanto da una diversa prospettiva fenomenica dello stesso. Di per sé, il *cyberspace*

costituisce uno spazio virtuale in continua evoluzione; negli ultimi anni, però, dopo l'implementazione di Internet, ha segnato il passaggio da una dimensione privata degli apparati informatici ad una pubblica o collettiva, basata sull'interconnettività globale. Basti pensare alla nuova dimensione del *cloud* e della struttura stessa del *web*. Il solo termine anglosassone di *cloud computing* (in italiano, nuvola informatica) induce anche il giurista meno esperto a pensare ad apparecchiature molto avanzate ed integrate, allocate in postazione remote e difficilmente individuabili, con immense potenzialità di calcolo, conservazione ed elaborazione di dati, nonché condivisione e circolazione degli stessi, che paradossalmente possono essere raggiunte in pochi istanti ed indipendentemente dal posto in cui l'utente si trova.

Tutto questo genera una doppia conseguenza, con annessi profili d'interesse per il giurista. Per un verso, modifica drasticamente la dimensione del fenomeno criminale in esame, ampliandola sia nella "quantità" di illeciti perpetrati che nella "qualità" degli stessi (agendo su larga scala o su interessi e beni non solo privati). Di qui, la necessità di capire se alcune delle norme entrate in vigore *ex* l. n. 48 del 2008, ed allora giustificate da una dimensione più contenuta del fenomeno, siano ancora opportune come l'art. 51 c.p.p. che assegna al p.m. distrettuale la competenza in materia di *computer crimes*. Altrettanto importante diventa capire cosa siano le investigazioni sul *cloud*, se le norme relative alle perquisizioni, ispezioni e sequestri siano applicabili e quale sia la giurisdizione competente posta la transnazionalità o addirittura a–territorialità dei sistemi. Di qui, la necessità di ricorrere anche ad una voce scientifica di diritto internazionale.

Per altro verso, l'aumento dei reati informatici acuisce le problematiche giuridiche già legate alle metodologie delinquenziali di matrice informatica di più "vecchia" memoria. Anche lo studioso meno avvezzo a queste tematiche, purtroppo altamente specialistiche e anche complesse, sa che la dottrina e la giurisprudenza si sono sempre poste due domande: se sia possibile applicare ai reati informatici i principi, le norme e la produzione ermeneutica di cui si avvale comunemente sia il diritto penale che il diritto processuale penale; quale sia il giusto bilanciamento di interessi tra la tutela delle libertà civili e la difesa sociale in questo campo. In altri termini, il rischio paventato da tutti è che i diritti del singolo — protetti dal tradizionale "armamentario" normativo — si affievoliscano per l'esigenza di adoperare differenti modalità di approccio ai reati informatici rispetto ai reati e agli accertamenti più tradizionali.

Viene facile pensare, sotto il profilo del diritto penale, alle problematiche legate alla determinazione dei confini della condotta che, nel *modus operandi* di tipo informatico, è difficile identificare con quella caratterizzata da fisicità e materialità. Nel campo del diritto processuale penale, il *leit motiv* del problema è il *vulnus* della posizione difensiva dell'imputato al cospetto di una prova (c.d. digitale) preformata rispetto al dibattimento il cui elemento

caratterizzante è la facile modificabilità del contenuto. Meritano attenzione, quindi, i profili legati alla natura ripetibile od irripetibile delle operazioni d'indagine informatica così come quelli sulla natura sanzionatoria dell'inadempimento delle procedure operative (*best practices* o *Sops*) impiegate dagli organi di p.g. nelle attività investigative che, differentemente da altre forme di indagini tecnico–scientifiche, sono state immesse nel tessuto codicistico come forme peculiari di ispezioni o perquisizioni.