Il diritto penale della Globalizzazione
Pacini Giuridica

Diritto e spazio cibernetico

di Pierpaolo Rivello – 03.04.2018

1. Le minacce cibernetiche

Lo spazio cibernetico può essere definito come l'insieme delle infrastrutture informatiche interconnesse; al riguardo, come noto, l'art. 1 della Convenzione europea di Budapest del 23 novembre 2001 ha chiarito, a sua volta, che deve essere considerato "sistema informatico" ‹‹qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati››.

Tale settore è esposto al rischio, purtroppo estremamente elevato, di minacce ed attacchi che possono assumere, come è stato autorevolmente sottolineato, caratteri particolarmente sofisticati e svolgersi tramite l'uso di vere e proprie "armi cibernetiche", quali *malware* appositamente sviluppati ‹‹che si esplicano attraverso modalità cosiddette asimmetriche›› [1].

Varie sono le tipologie di tali minacce, e correlativamente diversificate devono essere le "risposte" da parte del mondo del diritto.

Il dato maggiormente conosciuto presso l'opinione pubblica è quello concernente il *cyber-crime*, che può configurarsi in varie fattispecie, dalla truffa telematica al furto d'identità, dall'alterazione di informazioni alla violazione dei diritti di proprietà individuale [2].

In relazione a detto ambito ogni Nazione ha cercato di riadattare la propria normativa penalistica, al fine di delineare nuove ipotesi criminose calibrate a questa nuova "realtà virtuale", ed anche il nostro Paese è intervenuto reiteratamente sul punto [3], provvedendo al contempo, anche dal punto di vista procedimentale, a tener conto di questi mutati scenari, soprattutto in relazione alla fase investigativa [4].

Non va peraltro dimenticato che, accanto a nuove tipologie di reato, si assiste alla verificazione di reati "comuni" commessi avvalendosi di metodologie informatiche.

È stato infatti acutamente sottolineato che ‹‹alcune fattispecie di reato tradizionali, come furti di informazioni, spionaggio, frodi, gioco d'azzardo, prostituzione, traffici vari, molestie, minacce, pedofilia, pornografia, criminalità organizzata […], hanno subìto una un'evoluzione e sono in grado di articolarsi in prevalenza all'interno dei nuovi sistemi di comunicazione digitale (*cyberpedofilia*, […], *cyberstalking*,

---

[1] M. MENSI, *Sicurezza cibernetica e tutela dei diritti*, in M. MENSI – P. FALLETTA (a cura di), *Il diritto del web*, Wolters Kluwer, Cedam, Milanofiori Assago, 2015, p. 290.

[2] L. CUOMO – R. RAZZANTE, *La nuova disciplina dei reati informatici*, Giappichelli, Torino, 2009, p. 1 ss.; L. CUOMO – R. RAZZANTE, *La disciplina dei reati informatici*, Giappichelli, Torino, 2007, p. 1 ss.; M. MENSI, *Sicurezza cibernetica e tutela dei diritti*, cit., p. 290 e 291; L. PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. ec.*, 2011, n. 4, p. 827 ss.

[3] Cfr., per un approfondimento sul punto v., in particolare, M.M. ALMA – C. PERRONI, *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici, in Dir,. pen. proc., 1997, p. 504 ss.*; M F. MUCCIARELLI, *Commento alla L. 23 dicembre 1993 n. 547-Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, in Legisl. pen.,* 1996, p. 57 ss.; L. STILO, *Crimini informatici : dalle ‹‹liste nere›› al codice penale italiano*, in *Nuovo dir.*, 2002, p. 62 ss.

[4] Cfr., per tutti, L. LUPARIA – G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali,* Giuffrè, Milano, 2007.

hacking, diffusione di virus informatici, frodi telematiche, *spamming*, *netstrike*, diffusione di informazioni illegali *on-line*›› [5].
Oltre a dette ipotesi, possono infine essere delineate forme di spionaggio cibernetico e di *cyber-terrorism*, prodromico ad uno scenario di vera e propria *cyber-warfare*.

2. Le misure a tutela della *cybersecurity*.

Da tempo la NATO ha provveduto alla creazione della *Cyber Defence Management Authority* (CDMA), avente il compito di coordinare la difesa informatica e gestita dal *Cyber Defence Management Board*, di cui fanno parte tutti i responsabili degli uffici militari, operativi e tecnici che si occupano di difesa informatica, e che costituisce il principale organo di consulenza del Consiglio Atlantico in materia di difesa informatica.
In effetti, l'ambito afferente alla tutela delle informazioni assume sempre più un valore strategico, proprio in conseguenza dell'enorme "valore" delle informazioni immagazzinate, tanto che, non infondatamente, è stato osservato come ormai, in una scala di importanza, esse rivestano non di rado una valenza perfino superiore a quella attribuibile al possesso di determinate materie prime, potendo essere considerate alla stregua del nuovo "oro nero" [6].
Per quanto specificamente concerne l'Europa, dal punto di vista normativo abbiamo già ricordato la Convenzione di Budapest sul *cybercrime* del 23 novembre 2001, elaborata dal Consiglio d'Europa ed entrata in vigore il primo luglio del 2004.
Occorre aggiungere che l'Unione Europea fin dal 2004 ha provveduto alla creazione *dell'European Network and Information Security Agency* (ENISA), e cioè l'Agenzia Europea per la sicurezza delle reti e dell'informazione. L'UE nell'agosto del 2013 ha emanato la Direttiva 2013/40/UE, volta a sostituire la precedente Decisione Quadro 2005/222/GAI del Consiglio, ed avente l'obiettivo di armonizzare il diritto penale degli Stati membri per quanto concerne la tematica degli attacchi contro i sistemi informatici, nella consapevolezza del fatto che solo così risulta possibile agevolare la cooperazione interstatuale nella lotta a tali forme di criminalità.

3. Il bilanciamento tra tutela della sicurezza e garanzia della *privacy*.

Talvolta la focalizzazione, da parte di vari Governi, sull'esigenza di un'efficace contrasto alle attività terroristiche ha indotto a sottovalutare la non meno essenziale necessità di tutela dei diritti fondamentali degli individui.
Sotto più di un aspetto l'esperienza degli U.S.A. appare emblematica al riguardo. A seguito dell'attentato alle Torri Gemelle dell'11 settembre si è assistito ad un'imponente attività di raccolta di dati personali, resa possibile dal c.d "*Patriot Act*", una legge federale del 2001 che, al fine di tutelare la sicurezza nazionale contro il pericolo del terrorismo, ha operato forti compressioni alle garanzie dei cittadini.

[5] L. CUOMO – R. RAZZANTE, *La nuova disciplina dei reati informatici*, cit., p. 2.
[6] V. al riguardo l'approfondita disamina di F. VITALI, *L'oro nero dei dati*, in *Limes*, 2014, n. 7, p. 29 ss.

In particolare, per quanto concerne l'oggetto della nostra disamina, la Sezione 215 del *Patriot Act* ha modificato numerose disposizioni del "*Foreign Intelligence Surveillance Act*" del 1978, volte a disciplinare la sorveglianza elettronica, ampliando l'ambito delle possibilità di acquisizione di dati ricavati da intercettazioni di colloqui telefonici o di messaggi.

Va rilevato come l'opinione pubblica americana non abbia, almeno in maggioranza, mostrato di voler contrastare tale soluzione, ritenendo probabilmente che la lotta al terrorismi giustifichi tali limitazioni ai diritti individuali. Sono stati semmai gli scandali successivi, quali il caso *Wikileaks* del 2010, a incrinare la fiducia e a far sorgere nuovi interrogativi [7].

D'altro canto, nello stesso contesto temporale e quasi paradossalmente si è però pure assistito ad un fenomeno di segno opposto, rappresentato da una nuova sensibilità, in larga parte del mondo, verso la *privacy* e la "sfera privata", con conseguente diffidenza al riguardo nei confronti delle intromissioni giustificate dall'interesse pubblico.

Sotto questo aspetto, peraltro, «l'impostazione statunitense e quella dell'Unione europea non sono perfettamente allineate. In sostanza, mentre la prima pone l'accento sul valore economico e negoziale dei dati personali, che possono pertanto essere liberamente ceduti dagli utenti, l'approccio europeo muove dalla centralità della persona e dal diritto in capo a quest'ultima di intervenire per tutelarne il corretto trattamento» [8].

Non è questa la sede per un'approfondita disamina in tema di normativa *privacy* e del Regolamento europeo del 2016.

Possiamo limitarci ad osservare che, se in relazione ad alcune tematiche ad essa correlate, quale ad esempio quella dei *data breaches*, appare difficile negare la positività di un approccio caratterizzato da una sempre più marcata accentuazione della rilevanza di eventuali "perdite" di dati e della consapevolezza della necessità di rendere immediatamente edotti di tale circostanza gli individui coinvolti, in altri casi si assiste ad uno "scontro" interno fra contrapposte esigenze, che richiederebbe, forse, non solo un più ampio dibattito in sede dottrinale ma anche un maggior coinvolgimento "sociale", al fine di pervenire in maniera davvero condivisa all'individuazione della soluzione da considerare "preferibile".

Alludiamo in particolare a quello che viene comunemente definito come "diritto all'oblio"[9], e che è, in realtà, il diritto ad essere rappresentati e valutati in modo corrispondente alla propria attuale condizione personale e sociale, senza il "retaggio" derivante dalla perdurante menzione di episodi del passato ormai privi di concreta rilevanza, ma idonei, qualora ancora riportati, a lasciare una macchia fortemente negativa.

Il problema, come noto, è particolarmente rilevante in caso di consultazione dei risultati dei motori di ricerca, volti a riportare dati non più rappresentativi dell'attuale *status* personale. Si fronteggia in tal caso il diritto all'informazione con quello, vantato dal singolo cittadino, di non essere più "perseguitato" dall'ombra dei fatti di un passato ormai remoto.

---

[7] V. sul punto M. FENSTER, *Disclosure 's effects: WikiLeaks and transparency*, in Iowa Law Review 97.3, 2012, p. 753 ss.; P. BELLIA, *WikiLeaks and the institutional framework for national security disclosures*, in *Yale Law Journal*, 121.1448, 2012, p. 12 ss.

[8] M. MENSI, *Sicurezza cibernetica e tutela dei diritti*, cit., p. 328.

[9] Cfr. V. MAYER-SCHÖNBERGER – C. FORMENTI, *Delete:il diritto all'oblio nell'era digitale,* Milano, 2010; M. MEZZANOTTE, *Il diritto all'oblio: contributo allo studio della privacy storica*, Napoli, 2009; S. Niger, *Il diritto all'oblio. Diritto all'anonimato: anonimato, nome e identità personale*, Padova, 2008.

È probabilmente a tutti ben noto quello che rappresentò l'episodio paradigmatico al riguardo, e che condusse ad una fondamentale decisione pregiudiziale della Corte di Giustizia UE.
Si era in presenza di un reclamo mosso da un cittadino spagnolo, Mario Costeja Gonzales, contro *La Vanguardia Ediciones SL, nonché contro Google Spain* e *Google Inc.*, in quanto, a distanza di anni, operando una ricerca su Google al nome di tale soggetto si continuava a vedere, in posizione preminente, la menzione di una vendita all'asta di immobili a seguito di un pignoramento effettuato nei suoi confronti.
Non interessa ai nostri fini soffermarci su uno degli aspetti principali della vicenda, e cioè l'interrogativo circa l'assoggettamento di Google Inc., avente sede legale negli Stati Uniti , alla legge europea sulla *privacy*, all'epoca rappresentata dalla Direttiva 95/46/EC, nota come "Direttiva madre" ; importa invece sottolineare come, in questo come in tanti altri casi similari, si fosse in presenza di un imprenditore che, pur avendo ripreso una florida attività, era vittima, dal punto di vista della cronaca, del ricordo di fatti lontani che finivano inevitabilmente col "bollarlo" negativamente.
Assolutamente lineare e condivisibile appare al riguardo una pronuncia della Cassazione, con cui venne lucidamente sottolineato come occorra evitare che mediante la diffusione, a livello *web*, di fatti non più attuali venga leso il diritto all'oblio.
Fu osservato che tale diritto «salvaguarda la proiezione sociale dell'identità personale, l'esigenza di un soggetto di essere tutelato dalla divulgazione di informazioni (potenzialmente) lesive in ragione della perdita […] di attualità delle stesse, sicché il relativo trattamento viene a risultare non più giustificato ed anzi suscettibile di ostacolare il soggetto nell'esplicazione e nel godimento della propria personalità»[10].
Si aggiunse che «esiste un diritto giuridicamente tutelato dell'interessato a una proiezione genuina e attuale della propria identità, che il Web non può ignorare […] se l'interesse pubblico sotteso al diritto all'informazione (art. 21 Cost.) costituisce un limite al diritto fondamentale alla riservatezza al soggetto cui i dati appartengono è correlativamente attribuito il diritto all'oblio e cioè a che non vengano ulteriormente divulgate notizie che per il trascorrere del tempo risultino ormai dimenticate o ignote alla generalità dei consociati»[11].

[10] Cass. civ., sez. III, 5 aprile 2012, n. 5525, in *CED Cass*., n. 622169.
[11] Cass. civ., sez. III, 5 aprile 2012, n. 5525, *cit.*