Rivista elettronica di Diritto, Economia, Management

Numero 3 - 2013

La criminalità informatica

a cura di Paolo Galdieri, con il patrocinio dell'ANDIG (Associazione Nazionale Docenti di Informatica Giuridica e diritto dell'informatica)

Peer Review

FONDATA E DIRETTA DA
DONATO A. LIMONE

CLIOEDU®

Direzione e redazione
Via Antonio Canal, 7
00136 Roma
donato.limone@gmail.com

Gli articoli pubblicati nella rivista sono sottoposti ad una procedura di valutazione anonima. Gli articoli sottoposti alla rivista vanno spediti alla sede della redazione e saranno dati in lettura ai referees dei relativi settori scientifico disciplinari.

Anno IV, n. 3, dicembre 2013
ISSN 2039-4926
Autorizzazione del Tribunale civile di Roma N. 329/2010 del 5 agosto 2010
Editor ClioEdu
Roma - Lecce

INDICE

Editoriale

Questo numero della Rivista è dedicato alla "criminalità informatica" ed è curato da Paolo Galdieri, docente di informatica giuridica, segretario generale dell'ANDIG (Associazione Nazionale Docenti di Informatica Giuridica e diritto dell'informatica), che ringrazio per avere progettato e realizzato un numero di alto profilo e contenuto scientifico.

1. Il contributo introduttivo è di Giovanni Floris che rileva come nella cosiddetta società dell'informazione le tecnologie assumono un ruolo centrale modificando i rapporti sociali ed individuali, con ripercussioni nell'ambito della politica, dell'economia e della vita di tutti i giorni. La stessa attività giornalistica non può prescindere dall'uso di nuovi mezzi anche se ciò non deve e non può modificare il modo di pensare del giornalista quanto al suo *modus operandi*. La società dell'informazione, tuttavia, non si caratterizza tanto e solo per gli aspetti positivi, registrandosi, inevitabilmente, quale rovescio della medaglia in negativo il fenomeno della criminalità informatica, fenomeno complesso che mette tra l'altro in ballo discussioni intorno alle contrapposte esigenze di sicurezza da un lato e libertà della rete da un'altra.

2. Paolo Galdieri fa un'analisi della criminalità informatica e dell'evoluzione della legislazione penale. Restano numerose questioni aperte, dopo la legge 547/93 e le successive modifiche, soprattutto legate all'interpretazione delle nuove disposizioni, delle tecnologie che ad esse si riferiscono, dei contesti all'interno dei quali le norme vanno applicate. Sul piano del diritto positivo le maggiori questioni attengono al fatto che, per la prima volta, all'interno dell'ordinamento giuridico, vengono inseriti termini tecnici che possono prestarsi ad interpretazioni eterogenee. Vi sono poi problemi interpretativi legati al mezzo impiegato per commettere il reato, ad esempio la rete, quali quelli relativi all'accertamento del reato, del suo autore e dell'individuazione del luogo in cui il delitto è stato commesso. Questioni peculiari attengono, infine, alla delicata fase dell'acquisizione della prova informatica, essendo ancora incerti i requisiti che la stessa debba avere per "resistere" nel corso del dibattimento.

3. Al tema dei furti di identità in rete è dedicato lo scritto di Marco Schipani; il numero di tali furti negli ultimi anni è cresciuto in modo esponenziale. Nel momento in cui è divenuto più difficile attaccare i *server* centrali di grandi aziende o istituzioni, i "cyber criminali" hanno deciso di spostare la loro "attenzione" sul punto più debole della catena della sicurezza sulla rete: i singoli internauti. Ciò è in larga parte dovuto al fatto che in rete è sempre più semplice riuscire a sostituirsi all'identità digitale di altri per porre in essere condotte delittuose, evitandone le conseguenze penali. In questo contesto opera il *phishing,* che è una tecnica di ingegneria sociale volta a carpire informazioni personali altrui da poter utilizzare sulla rete con svariate modalità. Contrastare tale fenomeno è apparso, sin da subito, alquanto problematico, dal momento che nel nostro ordinamento giuridico non esiste una norma che punisca il *phishing* tout court. Dottrina e Giurisprudenza sono tuttavia concordi nel ritenere che le singole condotte in cui può essere scomposto un *phishing attack* spesso possono essere fatte rientrare nell'alveo di norme quali quelle che puniscono la sostituzione di

persona, il trattamento illecito di dati, l'accesso abusivo ad un sistema informatico o telematico, la frode informatica. Il legislatore è ultimamente intervenuto in materia con l'art. 9 del D.L n. 93 del 14 agosto 2013. Attraverso tale norma si è tentato di combattere il fenomeno del *phishing* con l'introduzione del reato di frode informatica commessa con sostituzione d'identità digitale.

4. Isabella De Vivo si occupa di pornografia virtuale. Alla legge n. 269/1998 si deve l'introduzione nel codice penale delle fattispecie di cui agli artt. 600 *ter* e 600 *quater*, norme che consentono di punire la "distribuzione" e la "cessione" di materiale pedopornografico in internet, nonché la condotta di mera "detenzione" .Con la successiva modifica , introdotta con la legge 38 /2006, il raggio d'incriminazione viene esteso fino a comprendere le condotte aventi ad oggetto immagini c.d. "pseudo-pornografiche". Sono tali ai sensi dell'art. 600 *quater*, le immagini realizzate attraverso mere elaborazioni grafiche e che pertanto prescindono da un effettivo sfruttamento sessuale di soggetti minori. La disposizione è tuttora oggetto di forti rilievi critici . Controversa è infatti, la natura del bene giuridico sotteso alla tutela penale, da cui le difficoltà di fornire una chiave di lettura che renda il dettato normativo compatibile con il principio costituzionale di necessaria offensività del reato.

5. Nell'ambito dell'e-commerce, sostiene Francesco Buffa nel suo contributo, particolare rilevanza assumono, anche per la loro diffusione, varie forme di truffa. A protezione degli utenti sono applicabili alcune norme civilistiche, ma queste sono in diversi casi insufficienti, non disponendo il singolo consumatore di strumenti effettivi di ricerca dell'autore della frode e di tutela nei suoi confronti, mentre l'applicazione delle norme penali assicura risultati più proficui nella scoperta e repressione delle frodi. Le norme penali rilevanti sono diverse, a seconda delle modalità di perpetrazione del reato e dell'oggetto della condotta.

6. L'attuazione della Convenzione di Budapest sul Cybercrime attraverso la legge 48 del 2008 (Giuseppe Corasaniti) ha lasciato aperta una incertezza interpretativa di fondo in relazione ai limiti della intervenuta integrale ratifica delle disposizioni riguardanti i reati contro la proprietà intellettuale commessi via web. L'attuazione della Convenzione comporta, infatti, secondo Giuseppe Corasaniti, non solo la doverosa cooperazione internazionale per il contrasto alla criminalità nel settore, ma, soprattutto l'accettazione dei principi di fondo che la Convenzione fissa, limitandosi a tali atti commessi deliberatamente, su scala commerciale e attraverso l'utilizzo di un sistema informatico. Ne consegue perciò un impatto interpretativo di ordine generale sulle disposizioni penali della legge n. 633 del 1941 più volte modificate ed integrate che deve tener conto anche delle più recenti posizioni europee della Corte di giustizia.

7. Alla luce del ruolo, sempre più pervasivo, assunto da Internet nelle società moderne, è indispensabile stabilire come operino le norme penali rispetto a tale Fenomeno (Rocco Lotierzo). E, stabilire se, e in quali termini, gli Internet Service Providers - che consentono il funzionamento della Rete delle reti per come la conosciamo - possano incorrere in responsabilità penali, è una delle questioni di maggior attualità. Essa coinvolge non solo l'osservanza di precetti garantistici, che trovano base fondativa nella Costituzione; bensì anche la salvaguardia della complessiva gamma di valori che nella Rete possono trovare una risorsa o una minaccia.

8. La prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio di proventi illeciti e di finanziamento del terrorismo è un serio e forte impegno di tutti gli Stati componenti l'Unione europea (Fulvio Berghella). Gli obblighi prescritti dalle normative sono molti e complessi, essi richiedono il trattamento di una grande mole di dati e informazioni da effettuare con l'ausilio di sofisticate e dedicate procedure informatiche che devono coniugare i principi delle normative con le esigenze di analisi, sicurezza e segretezza. La soluzione italiana è all'avanguardia.

9. Luigi Montuori esamina la questione dei reati informatici, considerati dal peculiare angolo visuale della protezione dei dati personali, anche alla luce di recenti novelle legislative e interventi del Garante, evidenziando le norme e le tutele del Codice (d.lgs. n. 196/2003) di cui si possono giovare le vittime di reati informatici, nonché i rapporti tra l'apparato sanzionatorio amministrativo e quello penale all'interno del Codice privacy. Inoltre, si sofferma sui particolari profili della *data retention*, del trattamento illecito di dati (in particolare mediante lo *spamming*) e del nuovo istituto della "violazione di dati personali". L'Autore propone alcune riflessioni sul possibile impatto sull'attuale sistema giuridico e, più in concreto, sulle imprese, dell'estensione ai delitti del Codice del campo applicativo della responsabilità penale degli enti, come disposta dal recente decreto legge del 14 agosto 2013, ma non confermata in sede di conversione. Infine, si evidenziano i recenti sviluppi relativi alla necessità di assicurare il rigoroso rispetto dei principi di protezione dei dati personali e trasparenza nell'utilizzo dei nuovi strumenti quali le *app*.

10. Una delle principali caratteristiche della criminalità informatica è la sua dimensione transnazionale (Eugenio Albamonte). Ciò impone che, per un adeguato contrasto, gli Stati si dotino di uno strumentario di diritto penale sostanziale e processuale che, oltre ad essere adeguato alla qualificazione giuridica delle condotte ed allo svolgimento efficace delle indagini, sia il più possibile uniforme. Infatti l'omogeneità delle norme è il primo fondamento di una proficua cooperazione giudiziaria tra gli Stati. Ma oltre ad una disciplina normativa comune è necessario che si addivenga ad una interpretazione quanto più condivisa delle norme, soprattutto quando l'operazione dell'interprete consiste nel dare una qualificazione giuridica a condotte criminali sempre mutevoli e connotate da una elevata tecnicità. Questo è l'ambito in cui opera il Cybercrime Convention Committee (T-CY) istituito dalla Convenzione di Budapest presso il Consiglio d'Europa, dal quale pervengono linee guida particolarmente utili a chi, nel nostro Paese, è impegnato nello studio delle nuove forme di criminalità informatica.

11. Il "Digital forensics" ha alterato il concetto stesso di fonte di prova portandolo, negli ultimi anni, ad un livello di astrazione tale che lo rende difficilmente gestibile dal Codice di Procedura Penale (Marco Mattiucci). In questo lavoro si dettagliano proprio i vari livelli intermedi di oggetto virtuale che possono essere incontrati in una indagine tecnica di Polizia Giudiziaria con le relative influenze ai concetti di sopralluogo e sequestro nonché all'analisi forense.

12. La presa di coscienza delle gravi minacce derivanti dall'utilizzo illegale delle nuove tecnologie ha evidenziato la necessità di rafforzare il contrasto a conseguenti fenomenologie criminali in continua evoluzione (Alberto Reda). Tali fenomenologie interessano soprattutto le reti telematiche, in particolare la rete mondiale *Internet*, da cui l'economia nazionale ed europea dipendono fortemente

e sulle quali sono compiuti illeciti il cui contrasto rientra a pieno diritto nella missione istituzionale della Guardia di Finanza quale polizia economica e finanziaria. Il Corpo interviene nel comparto attraverso due direttrici che, in linea con l'approccio unitario e trasversale che caratterizza l'azione del Corpo, sono in continuo contatto funzionale tra loro. Vi è la rete dei reparti territorialmente distribuiti sul territorio nazionale, con il compito di assicurare nei rispettivi ambiti, l'efficiente tutela degli interessi economici e finanziari; vi è poi quella dei Reparti Speciali, che si affiancano ai primi e che, istituiti per le investigazioni in specifiche materie, sono incaricati di realizzare direttamente, ovvero con azioni di supporto alle unità operative, moduli investigativi connotati da elevati *standards* qualitativi per i reparti territoriali.

13. La polizia postale e delle comunicazioni è un reparto specialistico della Polizia di Stato che opera in prima linea nella prevenzione e nel contrasto della criminalità informatica (Antonio Apruzzese e Emanuela Napoli). Tra le sue attività istituzionali vi è tra l'altro quella del contrasto della pedopornografia online, dei crimini informatici, della tutela delle infrastrutture critiche. Attualmente diversi sono i nuovi scenari operativi con i quali la Polizia postale e delle comunicazioni si confronta quotidianamente. Tra questi particolare attenzione merita il fenomeno delle nuove organizzazioni di criminali informatici e quello dei nuovi reati di odio sovente perpetrati attraverso la rete. Per ottenere risultati sempre più concreti in questo settore occorre che accanto all'attività delle Forze di Polizia si diffonda una cultura della legalità in rete, che può essere favorita anche attraverso una nuova idea di commissariato on line, il cui obiettivo principale sia quello di diventare un punto specialistico di riferimento per i frequentatori della rete.

14. Il notevole incremento dei fenomeni di criminalità "cyber" riscontrato in questi ultimi anni è dovuto alla maggior diffusione dell'utilizzo dei sistemi informatici e telematici ed alla presenza in essi di vulnerabilità, dovute a difetti di progetto o di implementazione, che adottando opportune tecniche possono essere sfruttate come varchi di sicurezza per penetrare le difese dei sistemi e prenderne il controllo (Corrado Giustozzi). Recentemente però si sono avute diverse prove che le stesse tecniche vengono adottate anche da organizzazioni governative impegnate nella lotta al crimine o nello spionaggio, le quali utilizzano nelle proprie attività dei veri e propri *malware di stato* sulla cui liceità giuridica non tutti sono concordi.

15. Quando la scena del crimine è il Web si assiste ad un ampliamento delle opportunità e dei pericoli e ad una diversa percezione dei rischi (Isabella Corradini). Il crimine in Rete si manifesta in modalità "cyber" ma la sua natura essenziale è ben nota. Furti di identità, frodi, stalking, bullismo, terrorismo, vengono compiuti sfruttando le opportunità di Internet che, al contempo, ne amplifica gli effetti.

16. Negli ultimi anni la criminalità informatica e la sicurezza informatica hanno assunto una crescente importanza, sia per la rilevanza nell'economia e nella sicurezza nazionale delle infrastrutture critiche informatizzate sia per l'interazione delle politiche che affrontano la protezione dei dati (Claudia Ciampi). L'obiettivo principale degli attacchi informatici, qualunque sia la modalità con la quale vengono realizzati, è la compromissione, il furto o l'uso improprio di dati e informazioni gestite da aziende pubbliche e private o scambiate da queste attraverso la rete. La Cyber Security

è stata identificata tra i primi cinque "Più Probabili" rischi per lo sviluppo globale. La crescita dei rischi informatici aumenta la necessità per le aziende, sia nel settore pubblico che in quello privato, di attuare meccanismi interni reali ed efficaci per salvaguardare la protezione dei dati e delle infrastrutture ICT.

Il Direttore della Rivista
Donato A. Limone

Autori di questo numero

Eugenio Albamonte

Magistrato dal 1995 ha svolto funzioni di pubblico ministero a Cosenza ed a Grosseto. Dal 2004 al 2009 ha prestato servizio presso il Consiglio Superiore della Magistratura. Attualmente é Sostituto presso la Procura della Repubblica di Roma e si occupa di criminalità informatica, di contrasto alla pedofilia e alla pedopornografia, di contrasto al cyber terrorismo ed é componente dei relativi gruppi specialistici. É autore di numerosi articoli e contributi ad opere collettanee in materia di diritto penale sostanziale e processuale e in tema di ordinamento giudiziario. Svolge una intensa attività internazionale iniziata quale rappresentante del CSM nell'ambito di organismi europei dedicati alla formazione giudiziaria, proseguita in qualità di short term expert nell'ambito di programmi di supporto finanziati dall'Unione Europea e dalle Nazioni Unite in favore delle autorità giudiziarie albanesi, macedoni e palestinesi e, da ultimo in qualità di rappresentante del Ministero della Giustizia e di capo delegazione interministeriale in occasione di conferenze internazionali in tema di contrasto al cyber Crime. Partecipa frequentemente, in qualità di relatore, a convegni, seminari ed incontri di studio organizzati dalla Scuola Superiore della Magistratura, da Ordini ed associazioni professionali, da organizzazioni private, da ultimo concentrando i propri studi su temi sostanziali e processuali connessi alla criminalità informatica. É stato più volte docente presso le Scuole di Formazione alle Professioni Legali delle Università di Lucera, Siena, e LUISS di Roma, nonché docente presso l'Universitá Fedrico II di Napoli ove ha tenuto un corso in materia di cooperazione giudiziaria internazionale nel settore penale.

E-mail: eugenio.albamonte@giustizia.it

Antonio Apruzzese

Dirigente Superiore della Polizia di Stato; è Direttore del Servizio di Polizia Postale e delle Comunicazioni. Nella prima parte della sua carriera ha operato in reparti investigativi della Polizia di Stato impiegati nel contrasto della criminalità comune e organizzata.Transitato nella Polizia Postale e delle Comunicazioni ha coordinato complesse operazioni di polizia giudiziaria riguardanti organizzazioni di criminali informatici dediti al traffico illecito dei dati, alla violazione dei sistemi di home banking e di monetica nonché ai traffici di contenuti a carattere pedopornografico via web con costanti risvolti di carattere transnazionale. Nello specifico settore della prevenzione è stato particolarmente interessato in problematiche di tutela di reti e di infrastrutture critiche informatizzate nazionali e internazionali. Ha concorso anche alla realizzazione di innovativi sistemi di prevenzione precoce di fenomeni criminali in danno di sistemi bancari informatizzati. Ha fatto parte di gruppi specializzati per la elaborazione delle più adeguate strategie di tutela di sistemi informatizzati complessi di rilievo istituzionale anche in ambito europeo. Specializzato in Criminologia è autore di numerose pubblicazioni scientifiche ed ha svolto pluriennali incarichi di insegnamento presso Università e Scuole di Polizia.

E-mail: dipps.uffdir.comunicazioni@interno.it

Fulvio Berghella

Vice Direttore Generale Vicario di OASI – Outsourcing Applicativo e Servizi Innovativi SpA (Gruppo Istituto Centrale delle banche Popolari Italiane -ICBPI); nonché responsabile della B.U. Antiriciclaggio, Compliance e Sicurezza che svolge attività di consulenza e servizi in materia di antiriciclaggio, compliance, sicurezza dei dati e dei sistemi. Ha ricoperto ruoli di responsabilità di direzione sempre in aziende interbancarie. Autore di molte pubblicazioni, saggi ed articoli sulla sicurezza dei dati e dei sistemi e in materia di prevenzione del rischio di riciclaggio e finanziamento del terrorismo. Ha collaborato con Università e centri di ricerca e Autorità. E' stato membro del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni e del Comitato scientifico della Poltel. Fondatore dei primi servizi per la sicurezza informatica avviati in Italia: il Club sul Computer Crime® per lo studio delle frodi e dei crimini informatici che ha portato all'attenzione pubblica, nel 1989, il nascente fenomeno degli hacker e dei virus informatici; e nel 1991 di SercurityNet®, in primo network e servizio antivirus e prevenzione dai crimini informatici. Ha ottenuto la certificazione CISM (Certfied Information Security Manager) e CEPAS (Ict senior security manager). Nel 2000 ha partecipato, in delegazione italiana, alla conferenza del G8 di Parigi sulla sicurezza del "cyberspazio" E' coautore della procedura GIANOS® per la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio e finanziamento del terrorismo. Insignito nel 2003 del Premio internazionale PAUL HARRIS FELLOW" per il contributo dato allo studio della criminologia informatica e la sicurezza del Paese"

E-mail: f.berghella@oasi-servizi.it

Francesco Buffa

Già dipendente della Banca d'Italia nel settore Vigilanza sull'intermediazione finanziaria, è dal 1993 magistrato, dapprima giudice del Tribunale di Lecce, quindi, dal 2007 alla Corte Suprema di Cassazione, dove presta servizio al Massimario e attualmente alla IV sezione civile. E' inoltre giudice della Commissione tributaria provinciale di Roma. È stato giudice distaccato presso la Corte europea dei diritti umani in Strasburgo (Francia), dal 2011 al 2012, nel quadro del programma annuale di scambio per magistrati europei organizzato dall'*European Judicial Training Network* di Bruxelles, ed ha preso parte anche a *stages* presso la Corte di Giustizia dell'Unione europea in Lussemburgo nonché in uffici giudiziari in Norvegia. È professore a contratto di Diritto del Lavoro alla Scuola di specializzazione per le professioni legali dell'Università di Roma la Sapienza ed ha insegnato per vari anni Diritto dell'Informatica all'Università di Lecce; ha insegnato in lingua inglese e francese in *Corsi di formazione professionale per magistrati europei,* per giuristi della Russia e dirigenti pubblici della Cina, partecipando altresì a vari incontri di studio internazionali in Europa. È direttore della Collana di ebook "*Orientamenti di Strasburgo*", redattore di numerose riviste giuridiche, anche telematiche, e cura la rubrica fissa "*Pillole di CEDU*" sulla rivista *Questione giustizia*. È autore di 45 volumi monografici e di oltre 600 note e saggi, editi sulle principali riviste giuridiche, anche telematiche; si segnalano, tra gli altri, il libro *Internet e criminalità: la finanza telematica offshore*, Giuffré, 2001 (selezionata per il premio internazionale Falcone-Borsellino 2002), nonché il *Quaderno n. 1 del Massimario* della Cassazione, ed il trattato in due tomi *Il lavoro degli extracomunitari*, Cedam, 2009.

E-mail: francescobuffa@tin.it

Claudia Ciampi

ICT Security Manager, Compliance Senior Professional ed Internal Auditor, opera attualmente come libero professionista per il mercato italiano ed è Information Security & Data Protection Manager per la Multimedia Consulting. In più di 15 anni di esperienza professionale nel settore dell'Information Security Management, ha acquisito forti competenze integrate (gestionali, strategiche, legali, tecnologiche e di marketing) con ruoli di responsabilità in strutture aziendali e in progetti complessi. Ha lavorato per Aziende del settore privato (Poste Italiane, Telecom Italia, WID, Poste Mobile, Cosmic Blue Team, RFI, IG O&M, Eurfacility, Postecom, KPMG FSA, Banca Intesabci, Banca Popolare di Verona) per Pubbliche Amministrazioni (Ministero delle Infrastrutture, Agenzia per l'Italia Digitale, Dipartimento delle Pari Opportunità, Dipartimento dell'Amministrazione Penitenziaria) e presso Aziende di Consulenza Direzionale (Ernst & Young, Cap Gemini e Deloitte Group) con ruoli operativi e strategici ottenendo importanti risultati nell'ambito della Security Governance. Certificato Lead Auditor ISO/IEC 27001:2013, Consulente Privacy e Privacy Officer UNI CEI EN ISO/IEC 17024:2004, Lead Auditor ISO 9001:2008 e Lead Auditor BS 7799. Membro di Associazioni di Sicurezza e Privacy (CSA, ANDIG, Federprivacy) e Gruppi di Lavoro è docente su tematiche legate al Diritto dell'Informatica per organizzazioni private e pubbliche e sui temi dell'Information Security Management per Master universitari.

E-mail: claudiaciampi@me.com

Giuseppe Corasaniti

Magistrato ordinario, Sostituto Procuratore Generale presso la Corte Suprema di Cassazione, è autore di numerosissimi studi in tema di diritto dell'informazione e dell'informatica. Docente in Informatica giuridica, presso il Dipartimento di Informatica, Facoltà di Scienze matematiche, fisiche e naturali dell'Università di Roma "La Sapienza". Docente di Diritto penale dell'informatica presso l'Istituto Superiore di Polizia, di Diritto penale della comunicazione e dell'informatica presso la Scuola di Polizia Tributaria della Guardia di Finanza. Docente di Diritto penale e criminologia informatica presso il Master di II livello in Scienze Forensi dell'Università degli Studi di Roma "La Sapienza" I Facoltà di Medicina e Chirurgia. È componente del Comitato Scientifico della Polizia Postale delle Comunicazioni. È stato consulente del Ministro per le politiche comunitarie in materia di comunicazione interattiva e politiche culturali nell'ambito della struttura di missione presso l'Unione Europea e Presidente del Comitato consultivo per il diritto d'autore presso il Ministero per i Beni e le attività culturali. E' referente informatico per il distretto della Corte d'appello di Roma. Delegato dal Governo Italiano (ministero della Giustizia) e dall'Autorità per le garanzie nelle comunicazioni ai lavori del gruppo G8 a Berlino sul tema *Security and confidence in Cyberspace-Berlino 26/28 ottobre 2000*. Delegato dall'Autorità per le garanzie nelle comunicazioni, nella delegazione italiana del gruppo G8 sul tema *Security and confidence in Cyberspace-data retention group Tokyo 22/24 maggio 2001*. Delegato dall'Autorità per le garanzie nelle comunicazioni al workshop "*Information security in a networked word"* Tokyo 12/13 settembre 2001 organizzato dall'OCSE, dal Governo del Giappone e dall'IPA *Information-technology Agency* del Giappone.

E-mail: giuseppe.corasaniti@giustizia.it

Isabella Corradini

Psicologa sociale, specialista in psicopatologia forense e criminologia clinica, è esperta nei temi della sicurezza (Safety, Security e Cybersecurity). In tali ambiti è consulente per primarie aziende italiane e relatrice in eventi nazionali e internazionali. Nel 2003 ha fondato il Centro Ricerche Themis, del quale è Presidente, focalizzato sullo sviluppo di modelli comportamentali per la sicurezza e la prevenzione con approccio interdisciplinare. E' responsabile della divisione Sicurezza e Reputazione per la società di comunicazione Reputation Agency. E' Membro del Gruppo di Lavoro "Cyber World" dell'OSN (Osservatorio Sicurezza Nazionale) presso il CASD (Centro Alti Studi per la Difesa). Dal 2006 è professore a contratto presso la Facoltà di Psicologia dell'Università dell'Aquila dove attualmente insegna psicologia sociale e psicologia applicata all'analisi del comportamento criminale. Per lo stesso Ateneo segue diversi progetti a livello internazionale nell'ambito delle scienze sociali (Progetti Tempus) tenendo conferenze in diversi Paesi (Russia, Kazasthan, Ukraina, Moldavia, Francia, ecc.). È docente in corsi di perfezionamento e master per diverse strutture e Università italiane, tra le quali SIOI (Società Italiana per l'Organizzazione Internazionale), FORMIT (Fondazione per la Ricerca sulla Migrazione e Integrazione delle Tecnologie), UNINT (Università degli Studi Internazionali di Roma), Università Guglielmo Marconi, Campus Bio-Medico, Scuola Superiore dell'Economia e delle Finanze, Scuola Internazionale Etica&Sicurezza. Due sono le principali linee di ricerca nelle quali si esplica l'attività di docenza, pubblicazione e consulenza: area psico-sociale e criminologica. È autrice di numerose pubblicazioni il cui elenco è consultabile sul sito *www.themiscrime.com* e all'indirizzo linkedin *it.linkedin.com/pub/isabella-corradini/51/287/a0b*.
E-mail: isabella.corradini@cc.univaq.it

Isabella de Vivo

Laureata in giurisprudenza presso l'Università LUISS G. Carli di Roma con voti 110/110 e lode con tesi in diritto penale dell'informatica dal titolo "Pedofilia telematica" ritenuta dalla Commissione degna di Speciale Menzione. Sin dall'inizio del suo percorso universitario ha manifestato particolare interesse verso il diritto penale, scegliendo per tale ragione il profilo penalistico. All'interno di tale percorso si è immediatamente distinta per una particolare inclinazione verso il diritto penale dell'informatica ed in particolare verso i reati a sfondo sessuale realizzabili attraverso la rete. Dopo il conseguimento del Diploma di Laurea ha approfondito i temi trattati nella tesi, scrivendo articoli e partecipando attivamente a seminari aventi ad oggetto la pedofilia telematica. I suoi attuali ambiti di ricerca sono: internet e criminalità; prostituzione *online*; pornografia minorile; detenzione di materiale pedopornografico; pornografia virtuale. Attualmente i suoi studi sono rivolti principalmente alla ricognizione della legislazione penale in materia di pedofilia telematica nei diversi paesi appartenenti all'Unione Europea. Da quasi due anni collabora con lo Studio Galdieri, all'interno del quale ha più volte partecipato ad attività di consulenza nei settori sopra menzionati.
E-mail: isaoh@hotmail.it

Giovanni Floris

Giornalista e saggista, è nato a Roma il 27.12.67. Laureato in Scienze politiche alla Luiss, dal 2002 è conduttore e autore di Ballarò, talk show di approfondimento politico del martedì sera di Rai Tre. In precedenza è stato inviato e conduttore del Giornale Radio Rai. Entrato in Rai grazie al primo concorso della Scuola di Giornalismo Radiotelevisivo di Perugia, ha condotto i Gr del mattino, Radioanch'io e Baobab, notizie in corso. Come inviato ha seguito i principali avvenimenti economico, politico e sociali dal '95 al 2001 (nascita dell'euro, varie inchieste in Asia, Europa, Americhe). Nel 2001, dopo aver seguito da New York per radio e tv i fatti dell'11 settembre, è stato nominato corrispondente dagli States. Dal 2002 è alla guida di Ballarò. Ha scritto e pubblicato diversi saggi. Dopo "**Una cosa di centrosinistra**" (Mondadori), ha pubblicato "**Monopoli**" (edizioni Rizzoli, un viaggio nell'economia italiana dei privilegi e delle caste") e "**Fatti chiari**", scritto insieme a Filippo Nanni e a Pergentina Pedaccini (edizioni CDG, un manuale sul linguaggio giornalistico). Poi è stata la volta di "**Risiko**: i veri problemi degli Italiani, le finte guerre della politica". Nel 2007 è uscito "**Mal di Merito**". Nel 2008 è la volta de "**La fabbrica degli ignoranti**", l'inchiesta su scuola e università, che in qualche modo conclude il ciclo che con Rizzoli abbiamo voluto dedicare alla formazione degli italiani ed alla struttura del nostro Paese. Nel 2009 è stata la volta di "**Separati in patria**", un'inchiesta che racconta la nostra penisola, spaccata drammaticamente tra Nord e Sud. E poi in sequenza: "**Zona retrocessione**" (2010) sulla crisi dell'economia italiana che la classe politica continuava a non voler affrontare, "**Decapitati**" (2011) sulla parabola della classe dirigente italiana, che di lì a poco sarebbe stata commissariata da Mario Monti ed i suoi tecnici, e "**Oggi è un altro giorno**" (2013), analisi della politica che verrà. A febbraio è in uscita il suo primo romanzo, per Feltrinelli: "Il confine di Bonetti".

E-mail: contatti@giovannifloris.it

Paolo Galdieri

Avvocato Cassazionista, Docente di Informatica Giuridica presso la Facoltà di Giurisprudenza dell'Università Luiss - Guido Carli. Coordinatore didattico del Master di II Livello in "Diritto dell'Informatica e Teoria e Tecnica della Normazione" presso l'Università degli Studi, La Sapienza di Roma. Già Docente di Diritto Penale dell'Informatica presso la facoltà di Economia dell'Università degli Studi di Chieti – Pescara, "G. D'Annunzio" e presso la Facoltà di Giurisprudenza dell'Università Luiss, Guido Carli di Roma. Già Professore a contratto integrativo presso l'insegnamento di Abilità Informatica della Facoltà di Giurisprudenza dell'Università degli Studi - "Federico II" di Napoli. Già Professore a contratto di Diritto Penale e Diritto Processuale Penale, Facoltà di Giurisprudenza, Università Telematica Unitelma Sapienza. E' stato Docente di Diritto Penale dell'Informatica presso numerosi corsi di perfezionamento e Master presso le Università di Chieti – Pescara, "G. D'Annunzio", Facoltà di Economia, Università LUMSA di Roma, Università di Lecce. È autore di più di cinquanta pubblicazioni in materia di Diritto Penale dell'Informatica, tra le quali la monografia *Teoria e Pratica nell'interpretazione del reato informatico*, Giuffrè, Milano, 1997. Nel 2005 ha redatto per conto dell'Unione Europea un rapporto sulla legislazione e prassi giudiziaria in materia di reati informatici in Italia, rapporto incluso nel'"Handbook of legislative procedures of computer

and network misure in EU countries". Ha partecipato a Quito (Ecuador) nell'ottobre del 2001 al "I Congreso Mundial de Derecho Informatico" con una relazione dal titolo: "Il delitto informatico nella prassi giudiziaria". Unico rappresentante europeo al convegno sulla cyber criminalità tenutosi alla UAE University di Dubai (Emirati Arabi Uniti) il 24 novembre 2010 con una relazione dal titolo *Italian Criminal legislation concerning ICTs.*

E-mail: paolo.galdieri@tiscali.it

Corrado Giustozzi

Impegnato sui temi della sicurezza informatica sin dal 1985, attualmente si occupa in particolare di: crittografia, steganografia e tecniche di *data protection*; sicurezza delle informazioni nelle organizzazioni complesse; crimini ad alta tecnologia e loro contrasto; indagini digitali, *computer forensics* e tecniche di *antiforensics*; *cyberwarfare* e *cyberterrorismo*; rapporti tra tecnologia e diritto (firma digitale, *privacy*, *governance* & *compliance*); aspetti socioculturali di rischio nell'uso delle nuove tecnologie. È membro del Permanent Stakeholders' Group dell'Agenzia Europea per la Sicurezza delle Reti e delle Informazioni (ENISA). Fa parte del "Expert Roster" della International Telecommunications Union (ITU) e collabora con l'Ufficio delle Nazioni Unite per il Controllo della Droga e la Prevenzione del Crimine (UNODC) su progetti internazionali di contrasto alla cybercriminalità ed al cyber terrorismo. Collabora da oltre quindici anni con il Reparto Indagini Tecniche del Raggruppamento Operativo Speciale dell'Arma dei Carabinieri nello svolgimento di attività investigative e di contrasto del *cybercrime* e del cyberterrorismo; fa parte del Comitato Scientifico dell'Unità di Analisi del Crimine Informatico della Polizia delle Telecomunicazioni; è Perito del Tribunale Penale di Roma in materia di criminalità informatica. Come professore a contratto insegna i temi della sicurezza e del contrasto al *cybercrime* presso diverse università italiane. Come consulente ha condotto importanti progetti di *audit* ed *assessment* di sicurezza logica, e progettato infrastrutture di sicurezza e *trust*, presso grandi aziende e pubbliche amministrazioni. Giornalista pubblicista e membro dell'Unione Giornalisti Italiani Scientifici (UGIS), fa parte del comitato scientifico della rivista *on-line* InterLex con la quale collabora sin dal 1995 con articoli e saggi sui rapporti tra sicurezza informatica e diritto. Ha al suo attivo oltre mille articoli e quattro libri.

E-mail: corrado@nightgaunt.it

Rocco Lotierzo

Laureato in Giurisprudenza, ha poi conseguito, all'Università di Roma La Sapienza, il Master in diritto dell'informatica e teoria e tecnica della normazione, oltre al perfezionamento in informatica giuridica e diritto delle nuove tecnologie. È avvocato penalista, perfezionatosi alla Scuola Nazionale dell'Unione delle Camere Penali. Dopo aver maturato una specifica esperienza professionale in materia di criminalità informatica presso lo Studio Galdieri, ha continuato il percorso professionale intrapreso in autonomia, perfezionando le sue competenze in alcuni specifici settori del diritto penale, ed in particolare nell'ambito dei rapporti tra privacy e diritto penale, dei delitti commessi in rete, nonché dei reati societari perpetrati anche attraverso le tecnologie dell'informazione. Ha svolto incarichi universitari

alla Università Telematica Unitelma Sapienza, presso la cattedra di diritto processuale penale, e, alla LUISS G. Carli di Roma, presso la cattedra di diritto penale dell'informatica. Presso la LUISS G. Carli ha anche tenuto cicli di lezioni in tema di tutela penale della riservatezza. E' attualmente docente dell'insegnamento di Antropologia del reato presso l'Università degli Studi dell'Aquila - Dipartimento di Medicina clinica, sanità pubblica, scienze della vita e dell'ambiente. Tiene relazioni nell'ambito di convegni e Master universitari, oltre ad essere autore di diverse pubblicazioni in materia di diritto penale sostanziale.

E-mail: rocco.lotierzo@libero.it

Marco Mattiucci

Ufficiale del Ruolo Tecnico Ingegneri dell'Arma dei Carabinieri, Comandante/Fondatore della Sezione Telematica del Reparto Tecnologie Informatiche (RTI) interno al Raggruppamento Carabinieri Investigazioni Scientifiche (RaCIS). Scopo della Sezione è svolgere attività scientifico-forense nello specifico settore dei crimini ad alta tecnologia con competenza su tutto il territorio nazionale a supporto dell'Arma e della magistratura. In tale ambito l'ufficiale opera in funzione di investigatore, coordinatore di indagini complesse, ricercatore scientifico e docente.Insegna presso i maggiori reparti addestrativi dell'Arma quale referente unico ed esternamente, presso Corsi di laurea, di specializzazione e master nelle maggiori università italiane. È chiamato periodicamente a diffondere la materia del digital forensics presso i corsi del CSM, delle maggiori Procure d'Italia, delle Scuole di SMD e delle Scuole Interforze di Polizia. Specializzato in intelligenza artificiale ed ha pubblicato articoli scientifici di profilo altamente tecnico sui sistemi informatici distribuiti nonchè diversi articoli e libri di natura tecnico/legale inerenti le indagini informatiche forensi. A livello internazionale è referente per l'Arma nell'ENFSI-FIT-WG (Gruppo di lavoro internazionale sull'informatica criminale e forense del ENFSI, network europeo dei cabinetti di polizia scientifica). È membro del comitato scientifico dell'ICAA (International Crime Analysis Association). È membro del comitato scientifico dell'IISFA (International Information System Forensic Association - Italian Chapter). È Auditor / Responsabile Gruppo di Audit di Sistemi di Gestione per la Qualità (Corso EN/ISO/IEC 17025 - Roma, Anno 2009 - Qualificato CEPAS). È Direttore di Laboratorio riconosciuto con trascrizione a matricola dell'Arma dei Carabinieri. (marco.mattiucci@hwarangdo.it)

Luigi Montuori

Laurea in giurisprudenza conseguita presso l'Università "La Sapienza" di Roma (1987) e avvocato; Specializzazione post-universitaria COR.CE come vincitore della borsa di studio dall'Istituto Nazionale per il Commercio con l'Estero e comprendente stage all'estero (1989-1990); abilitazione all'insegnamento per le discipline giuridiche ed economiche nelle scuole ed istituti d'istruzione secondaria - classe XXV tab.A conseguita nel 1990; perfezionamento in Teoria dell'interpretazione ed informatica giuridica presso l'Università La Sapienza di Roma (1991); cultore della materia presso l'Università La Sapienza di Roma nell'Istituto di informatica giuridica e teoria dell'interpretazione (dal 1991 al 1994); e docente all'Università

degli studi "La Sapienza" - Istituto di teoria dell'interpretazione e di informatica giuridica – nel Master in diritto dell'informatica e teoria e tecnica della normazione; docente presso la Scuola Superiore Pubblica Amministrazione dal 2000 al 2008; incarico di ricerca, per l'anno 2002, presso la Scuola Superiore Pubblica Amministrazione, del progetto denominato "La pubblica amministrazione e la tutela della privacy: gestione e riservatezza dell'informazione nell'ambito della P.A."; dirigente al Garante per la protezione dei dati personali nel 2001, a capo del dipartimento comunicazioni e reti telematiche nonché del Servizio di segreteria del collegio. Nel periodo 2010/2012 ha assunto anche le funzioni di vice segretario generale; componente di diverse commissioni in concorsi pubblici; ha collaborato con articoli e studi pubblicati su riviste di carattere giuridico, in particolare sulla contrattualistica della P.A. e in materia di Privacy; componente del Comitato di redazione della rivista "Sicurezza e Giustizia"

E-mail: l.montuori@garanteprivacy.it

Emanuela Napoli

Vice Questore Aggiunto della Polizia di Stato, è Direttore di una Sezione del Servizio Polizia Postale e delle Comunicazioni. Con una pregressa pluriennale esperienza maturata nell'ambito delle Questure ove ha ricoperto incarichi di dirigente dell'Ufficio Prevenzione Generale e Soccorso Pubblico, D.I.G.O.S., Capo di Gabinetto, ha svolto gran parte della sua attività in settori operativi sia nel campo della prevenzione che in quello info-investigativo. E' recentemente approdata nella Specialità con compiti di coordinamento e di raccordo delle attività logistico-gestionali tra il Servizio Centrale ed i Compartimenti di Polizia Postale presenti sul territorio. Attivamente impegnata in attività di educazione alla legalità destinate alle giovani generazioni e finalizzate alla prevenzione sui rischi e pericoli connessi all'utilizzo della rete internet.

E-mail: dipps.uffdir.comunicazioni@interno.it

Alberto Reda

Nei 28 anni di servizio in Guardia di Finanza, dopo il corso Ufficiali presso l'Accademia della Guardia di Finanza, ha svolto incarichi di Comando di reparto isolato e di Ufficiale addetto presso Nuclei PT in sede di capoluogo di Regione in Campania, Lombardia e nella città di Roma. Successivamente, ha prestato servizio per quattro anni presso lo Stato Maggiore del Corpo – III Reparto Operazioni. Ha frequentato il corso presso l'I.S.S.M.I., è stato Comandante Provinciale Guardia di Finanza di Reggio Calabria e, poi, Vice Comandante operativo dello SCICO. Dal luglio 2012 ha assunto il Comando del Nucleo Speciale Frodi Tecnologiche. Dal 2003 al 2008 ha partecipato : - al Gruppo di Lavoro interistituzionale presso l'Osservatorio socio-economico sulla criminalità del Comitato Nazionale dell'Economia e del Lavoro; al Comitato per la Lotta contro le Frodi Comunitarie presso il Ministero delle Politiche Europee; al Comitato tecnico art. 5 D.M. del n. 44/2003 presso il Ministero delle Politiche Agricole, Alimentari e Forestali. Dal 2013: è membro dell'Osservatorio Europeo sui diritti di proprietà intellettuale; collabora con il Nucleo di Sicurezza Cibernetica istituito presso la Presidenza del Consiglio dei Ministri.

E-mail: urp@pec.gdf.it

Marco Schipani
Avvocato. Docente di Diritto Penale dell'Informatica presso il Master di II livello in "Diritto dell'informatica e Teoria e Tecnica della Normazione", presso l'Università degli Studi di Roma, "La Sapienza". Già assistente di Diritto Penale dell'Informatica presso la Facoltà di Giurisprudenza dell'Università "Luiss", Guido Carli di Roma. Già assistente di Diritto Penale e Diritto Processuale Penale presso l'Università Telematica Unitelma Sapienza. Autore di articoli in materia di criminalità informatica e relatore a diversi convegni aventi ad oggetto il Diritto Penale e le Tecnologie dell'Informazione. All'interno dello Studio Legale Galdieri si occupa, tra l'altro, da anni di reati commessi attraverso le nuove tecnologie, nonché della redazione dei modelli organizzativi ex D. Lgs 231/2001, con particolare riferimento ai reati informatici. Attualmente i suoi ambiti di ricerca sono: phishing, furto d'identità, stalking virtuale, criminalità organizzata e tecnologie dell'informazione, diffamazione online, accesso abusivo a sistemi informatici e telematici.
E-mail: marco.schipani@hotmail.it

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 17-18

Media e reati informatici

Giovanni Floris

Abstract: Nella cosiddetta società dell'informazione le tecnologie assumono un ruolo centrale modificando i rapporti sociali ed individuali, con ripercussioni nell'ambito della politica, dell'economia e della vita di tutti i giorni. La stessa attività giornalistica non può prescindere dall'uso di nuovi mezzi anche se ciò non deve e non può modificare il modo di pensare del giornalista quanto al suo *modus operandi*. La società dell'informazione, tuttavia, non si caratterizza tanto e solo per gli aspetti positivi, registrandosi, inevitabilmente, quale rovescio della medaglia in negativo il fenomeno della criminalità informatica, fenomeno complesso che mette tra l'altro in ballo discussioni intorno alle contrapposte esigenze di sicurezza da un lato e libertà della rete da un'altra.

Parole chiave: giornalismo, internet, democrazia, criminalità informatica

Sommario: 1. Il giornalista nella rete. 2. La criminalità informatica quale rovescio della medaglia della società dell'informazione.

1. Il giornalista nella rete

Il giornalista non cambia lavoro con l'avvento dei social network, né con lo sviluppo delle opportunità che offre la rete. Se vuole svolgere bene il suo compito diventa però più rigoroso.
Il giornalista è stato tale con l'arrivo della radio, della tv, farà il suo lavoro anche con internet. Fino a che non verrà inventato il teletrasporto (!) le cose in linea di massima non cambieranno. Cambiano però alcuni metodi di lavoro, cambia la facilità di accesso alle fonti, si complica e diviene più delicato il lavoro di verifica. Oggi si comunica in maniera estremamente veloce e frammentata, il ciclo delle notizie e delle informazioni è attivo 24 ore su 24 e passa dai cellulari, dalle tv *all news*, da internet , ma il giornalista fa sempre (e se è bravo *fa solo)* il giornalista.
In realtà sono convinto che fino a che non verrà inventato – che so – il teletrasporto (!) il nostro lavoro non cambierà. La rete e le sue tante possibili utilizzazioni naturalmente però amplificano e rendono più potente il nostro prodotto.
E quindi bisogna stare più attenti.
Le notizie arrivano subito, e subito bisogna classificarle e selezionarle: è necessario essere sempre pronti, non puoi prenderti troppo tempo per ragionare. Tutti vivono in diretta, non solo chi fa tv. Oggi lo spettatore ha più fonti, segue molto Internet, ma fondamentalmente il metodo resta sempre lo stesso. Le informazioni raccolte vengono filtrate con la propria testa e ci si fa semplicemente un'opinione.

Articolo pervenuto il 2 settembre 2013, approvato il 28 novembre 2013

La velocità della comunicazione e l'aumentare del numero delle fonti disponibili tende però a ridurre in tutti noi la soglia di attenzione. Il bravo giornalista la deve invece sollevare. Nel mondo della rete veloce e sempre aperta ci si rischia di distrarre, di selezionare poco, di credere a molto. la nostra pazienza si esaurisce, non si sta molto ad ascoltare. luoghi e tempi di fruizione sono oggi più frammentati, più disordinati, anche perché l'offerta insegue ormai le esigenze del fruitore. *Facebook*, *Twitter*, il blog, sono strumenti che restano sempre aperti e tramite i quali riceviamo commenti per tutta la settimana.

Non c'è più tempo, si chiedono risultati subito, ed è giusto che sia così. Non si può e non si deve scegliere tra velocità ed esattezza, tra modernità e credibilità. La sfida del giornalista è garantire tutto ciò, ma in fondo lo è sempre stata.

Questa è d'altronde una matrice che riguarda ogni attività, ogni professione. Prendiamo la politica. C'è stata l'epoca delle leadership alla radio, poi quella dei leader tv, oggi a dare il tratto all'era in cui viviamo è per molti aspetti, la rete. Questo ci porta a ragionare attorno alle tecnologie come opportunità o meno di una vera democrazia o piuttosto quale strumento "demagogico".

2. La criminalità informatica quale rovescio della medaglia della società dell'informazione

Di certo la leadership positiva che si forma nella rete è una rete orizzontale non verticale, richiede un tipo di leader che sappia mobilitare non che dia ordini. Una sorta di leadership condivisa, che raggiunga obiettivi ma che non sia il vertice di una piramide. Il leader moderno responsabilizza, ispira, muove ideali e sentimenti, anima interessi collettivi . Anche la nuova leadership deve essere veloce. E' quella che gli addetti ai lavori chiamano la *fast politic*.

Insomma, tutto è *fast* oggi. Lo dobbiamo essere tutti noi, quale che sia la nostra professione, ma dobbiamo mantenere anche alti i nostri standard di rendimento. E per il giornalista la prima qualità da garantire è la credibilità.

Resta poi la consapevolezza, da parte di un operatore del settore dei media, che i nuovi fenomeni di criminalità informatica vanno affrontati anche con leggi apposite, leggi che però non dovranno mai limitare le enormi chance di libertà che internet offre. Come sempre ci vuole equilibrio. Come nell'era di Gutemberg, così nell'era di Steve Jobs.

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 19-43

Reati informatici: normativa vigente, problemi e prospettive

Paolo Galdieri

Abstract: Nel volgere di circa venti anni l'Italia si è dotata di una legislazione penale in materia di tecnologie dell'informazione ampia ed articolata, in grado di contrastare la criminalità informatica nelle sue diverse declinazioni. Ciò posto, rimangono numerose questioni aperte legate all'interpretazione delle nuove disposizioni, delle tecnologie che ad esse si riferiscono, dei contesti all'interno dei quali le norme vanno applicate. Sul piano del diritto positivo le maggiori questioni attengono al fatto che, per la prima volta, all'interno dell'ordinamento giuridico, vengono inseriti termini tecnici che possono prestarsi ad interpretazioni eterogenee. Vi sono poi problemi interpretativi legati al mezzo impiegato per commettere il reato, ad esempio la rete, quali quelli relativi all'accertamento del reato, del suo autore e dell'individuazione del luogo in cui il delitto è stato commesso. Questioni peculiari attengono, infine, alla delicata fase dell'acquisizione della prova informatica, essendo ancora incerti i requisiti che la stessa debba avere per "resistere" nel corso del dibattimento.

Parole chiave: società dell'informazione, tecnologie dell'informazione, Internet, reato informatico, reato telematico, indagini informatiche.

1. Il reato informatico in ambito internazionale ed europeo

In ambito internazionale ed europeo il fenomeno della criminalità informatica è stato affrontato sia sul piano generale che particolare, ovvero tenendo conto della specificità dei diversi reati oggetto di valutazione.

Sul piano generale si registra una prima frase caratterizzata da un ampio dibattito in ordine alla

Articolo pervenuto il 10 ottobre 2013, approvato il 28 novembre 2013

necessità o meno di nuove norme idonee a contrastare il fenomeno della criminalità informatica.
Da una parte, infatti, c'era chi sosteneva che gli illeciti realizzabili attraverso le tecnologie dell'informazione fossero sostanzialmente una evoluzione dei reati tradizionali in chiave tecnologica e che, quindi, potesse essere applicata la normativa previgente.
L'opinione dominante, tuttavia, era quella secondo cui per il principio della tassatività proprio del diritto penale e del divieto di analogia *in malam partem*, molte delle nuove ipotesi delittuose, realizzabili attraverso l'informatica e la telematica, non potevano essere sanzionate attraverso disposizioni di legge che non le prevedevano espressamente.
Acquisita, quindi, la consapevolezza dell'incremento della criminalità informatica, e constatata l'impossibilità di utilizzare semplicemente la normativa previgente, sono state fatte una serie di scelte che hanno portato all'introduzione di importanti novità sul piano del diritto positivo, ponendo, altresì, questioni interpretative non sempre di agevole soluzione.
In ambito europeo ben presto si è compreso come i reati informatici sarebbero diventati sempre di più reati telematici, ovvero, reati realizzabili attraverso la rete e, per tali ragioni, si sono sollecitati interventi normativi in grado di armonizzare le legislazione penali dei diversi Paesi membri in modo da garantire un effettivo contrasto ad un tipo di criminalità che si è presentata da subito come transnazionale.
In tale ottica, si pone la Raccomandazione 89/9[1] attraverso la quale viene stilata una lista, cosiddetta minima, delle ipotesi illecite particolarmente diffuse e che, quindi, dovevano essere contemplate dalle legislazioni penali di tutti gli Stati membri. Gli interventi urgenti, costituenti la cosiddetta lista minima, riguardavano i seguenti atti: frode informatica, falso informatico, danneggiamento dei dati e dei programmi informatici, sabotaggio informatico, accesso non autorizzato, riproduzione non autorizzata di un programma informatico protetto, riproduzione non autorizzata di una topografia informatica. Veniva rimessa alla discrezionalità di ciascun Stato, lista facoltativa, invece, la previsione di norme relative: all'alterazione dei dati o dei programmi informatici, allo spionaggio informatico, all'utilizzazione non autorizzata di un programma informatico protetto.
Parimenti con la raccomandazione R 95/12 si sollecita l'armonizzazione dei codici di procedura penale, al fine di consentire l'effettiva perseguibilità dell'autore del reato. La strada tracciata trova conferma nella Convenzione internazionale sul cybercrimine (Strasburgo, 29 giugno 2001 CDPC(2001)17) ed in altri documenti quale ad esempio la Comunicazione della Commissione europea "Creare una società dell'informazione sicura, migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica"(COM-2000-890)[2] ove si individuano come temi da affrontare in modo univoco ed approfondito: a) le intercettazioni di comunicazioni; b) la conservazione dei dati relativi alle comunicazioni; c) l'accesso e utilizzo anonimi; d) la cooperazione concreta a livello internazionale; e) i poteri in materia di procedura penale e giurisdizione; f) il valore probatorio dei dati informatici.
Innanzi alle spinte in ambito internazionale ed europeo i diversi Paesi si sono posti il problema di come intervenire in questo delicato settore. Secondo un orientamento assai diffuso in Europa i nuovi delitti non introducevano nuovi interessi meritevoli di tutela, bensì producevano soltanto

---

1 V. Frosini, *Contributi ad un diritto dell'informazione*, Liguori, Napoli, 1990, p. 165 ss..

2 Il testo integrale è consultabile in:www.privacy.it/com2000-890.

nuove modalità di aggressione di beni giuridici preesistenti. Questo orientamento portava a sostenere il cosiddetto metodo evolutivo e cioè la necessità di introdurre singole disposizioni specificatamente riferite all'informatica all'interno delle normative penali previgenti. In tale direzione si sono mosse, tra l'altro, la Danimarca, la Germania, il Lussemburgo, la Svizzera, il Portogallo e l'Italia.

Per altro indirizzo dottrinario, sviluppatosi per lo più nei Paesi anglosassoni, le nuove tecnologie determinavano l'insorgere di nuovi interessi suscettibili di protezione e, quindi, era auspicabile un intervento specifico ed autonomo in grado di disciplinare separatamente dalle normative previgenti l'intero fenomeno criminale (metodo della cd. legge organica).

Il metodo delle legge organica è stato adottato negli Usa, dove attraverso il *Counterfeit Access Device and Computer Fraud and Abuse Act* del 1984, modificato successivamente dal *Computer Fraud and Abuse* del 1986, furono formulate ipotesi di reato ben precise ed adatte ad arginare i fenomeni esistenti in quella realtà.

Nella stessa direzione la legge francese n. 88.19 del 5 maggio 1988, che ha introdotto il nuovo capo III del titolo II del libro III del codice penale, intitolato "Alcune infrazioni in materia informatica".

Accanto a queste indicazioni di carattere generale in ambito europeo si è ben presto compreso che il reato informatico pone problematiche particolari a seconda del contesto in cui viene realizzato, per esempio la rete, ed in considerazione delle modalità operative e del fine illecito perseguito.

Si sono succeduti nel tempo, quindi, una serie di interventi volti a contrastare fenomeni particolari quali ad esempio la criminalità in rete, la pedofilia telematica, il *cyberterrorismo*.

Un primo intervento ha come scopo precipuo quello della sicurezza della rete, anche al fine di favorire la circolazione dei beni e servizi all'interno di Internet. Passo fondamentale per realizzare questo disegno si registra il 24 aprile 1996, quando il Consiglio chiede alla Commissione di redigere un compendio dei problemi posti dal rapido sviluppo di Internet e di valutare, in particolare, l'opportunità di una disciplina comunitaria o internazionale. Successivamente, il 24 ottobre 1996, la Commissione trasmette al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle Regioni una Comunicazione relativa alle informazioni di contenuto illegale e nocivo su Internet e un Libro Verde sulla tutela dei minori e della dignità umana nei servizi audiovisivi e dell'informazione. Recepita la Comunicazione, con la Risoluzione del 17 febbraio 1997 il Consiglio e i rappresentanti dei governi, riuniti in sede di Consiglio, hanno chiesto agli Stati membri e alla Commissione di intraprendere una serie di azioni per difendere Internet dai contenuti illegali e nocivi. Nell'ambito di questa strategia si inserisce la Dichiarazione Ministeriale, adottata alla Conferenza ministeriale internazionale sulle "Reti globali di informazione: realizzare il potenziale", tenutasi a Bonn il 6-8 luglio 1997 su iniziativa del governo tedesco, che sottolinea il ruolo che il settore privato può assumere nella tutela degli interessi dei consumatori e nella promozione e nel rispetto degli *standards* etici, grazie ad efficaci sistemi di autoregolamentazione conformi al sistema giuridico e da esso sostenuti.

Altro atto della strategia adottata in ambito europeo è costituito dalla Decisione 276/1999 CE del Parlamento Europeo e del Consiglio del 25 gennaio 1999, con la quale viene adottato il piano pluriennale d'azione comunitario per promuovere l'uso sicuro di Internet attraverso la lotta alle informazioni di contenuto illegale e nocivo diffuse per mezzo delle reti globali.

Diverso intervento è quello finalizzato a limitare al massimo la diffusione di reati nella rete.

In tale direzione si muovono, oltre che la Raccomandazione del Consiglio d'Europa R (89) 9 e la

Raccomandazione R (95)13, delle quali si è detto: il Parere del Comitato consultivo " razzismo e xenofobia del 26 gennaio 1996 "sulla diffusione dell'odio razziale mediante mezzi informatici o telematici"; la Risoluzione del 9 maggio 1996 sulla proposta di decisione del Consiglio che proclama il 1997 " anno europeo contro il razzismo", nonché l'azione comune del 15 luglio 1996 adottata dal Consiglio.
L'esigenza di contrastare la *cybercriminalità* traspare anche da altri documenti come quello, pubblicato nella Gazzetta Ufficiale dell'Unione Europea, intitolato "Prevenzione e controllo della criminalità organizzata" (2000/C124/01), che, nel fare il punto sulle strategie dell'Unione Europea per l'inizio del terzo millennio, dichiara esplicitamente la necessità di avvicinare ed armonizzare le legislazioni nazionali dei Paesi membri su alcuni reati, tra cui quelli legati alla diffusione delle nuove tecnologie.

2. Il reato informatico nella normativa penale italiana

La maggior parte delle norme penali riferite all'uso delle tecnologie della informazione è stata introdotta nel codice penale attraverso la legge 23 dicembre 1993 n. 547.
Dalla lettura della legge risulta evidente come il legislatore italiano abbia optato per il metodo evolutivo ritenendo, a ragione, che le tecnologie incidano sulle modalità di aggressione a beni giuridici o interessi che rimangono comunque invariati.
Ne consegue che a differenza di altri Paesi, ad esempio Stati Uniti e Francia, che hanno rispettivamente dedicato ai delitti informatici leggi *ad hoc* o un titolo apposito all'interno del codice penale, in Italia le nuove norme sono state inserite in diversi parti del codice penale, ciascuna vicino alla disposizione previgente ritenuta simile.
L'opera del legislatore si muove all'interno di tutto il *corpus iuris* penale interessato dal fenomeno informatico, ad eccezione dell'ipotesi del c.d. furto di dati. Quest'ultima non viene, infatti, contemplata da un'autonoma norma incriminatrice, in quanto si è ritenuto che <<la sottrazione di dati, quando non si estenda ai supporti materiali su cui i dati sono impressi (nel qual caso si configura con evidenza il reato di furto), altro non è che una presa di conoscenza di notizie, ossia un fatto intellettivo rientrante, se del caso, nelle previsioni concernenti la violazione dei segreti. Ciò, ovviamente, a parte la punibilità ad altro titolo delle condotte strumentali, quali ad esempio, quelle di violazione di domicilio (art.614 c.p.), ecc >>[3].
Vengono inseriti in primo luogo reati fino ad oggi non previsti, quali: l'accesso abusivo ad un sistema informatico o telematico; la detenzione e diffusione abusiva di codici d'accesso; la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico; il falso informatico; il danneggiamento informatico e la frode informatica.
Si procede poi all'aggiornamento di norme preesistenti al fine di renderle applicabili anche alle

[3] Relazione Introduttiva al Disegno di Legge n.2773. Per cogliere l'intenzione del legislatore, ci riferiremo spesso alla relazione introduttiva del disegno di legge in quanto l'articolato su cui si discute riprende interamente lo stesso, assorbendo, nei limiti in cui con questo non contrastava, la proposta di legge Cicciomessere ed altri: *Introduzione degli articoli 623-ter, 623-quater, 623-quinquies, 623-sexies e 623-septies del codice penale per la repressione dei reati informatici e telematici* (n.1174). Sul furto dei dati cfr. E.Giannantonio, *Manuale di Diritto dell'Informatica*, Cedam, 1994, p.419 ss..

condotte realizzate per mezzo delle tecnologie. In tale ambito si colloca l'esercizio arbitrario delle proprie ragioni con violenza su di un bene informatico, il novellato delitto di attentato ad impianti di pubblica utilità, le intercettazioni informatiche e telematiche, la violazione di corrispondenza informatica.

Le modifiche apportate al codice penale attraverso la legge 547 si sono arricchite di recente di contenuti nuovi grazie alla legge 18 marzo 2008, n. 48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento interno"[4].

Con la Convenzione per la lotta contro la criminalità informatica si era stilato un documento ispirato dalla convinzione che i nuovi fenomeni potevano essere ben contrastati solo attraverso una armonizzazione delle legislazioni, che tenesse conto della dimensione transnazionale dei crimini informatici .

In questa prospettiva si era ribadita l'esigenza di prevedere nelle legislazioni interne norme penali idonee a sanzionare determinate condotte, disposizioni processuali capaci di rendere effettivamente punibili i reati previsti, previsioni normative che contemplassero finalmente una responsabilità delle aziende per reati informatici commessi al loro interno.

Nel recepire tali indicazioni, la legge n. 48 opera su tre piani: quello del diritto sostanziale, processuale e della rilevanza penale di alcune condotte in ambito aziendale. Quanto a tale ultimo profilo, sul quale si tornerà in seguito, si estende alle aziende la responsabilità amministrativa, già prevista per numerosi reati dal Decreto legislativo 231, a praticamente tutti i delitti informatici commessi dai vertici o dai dipendenti, sempre che siano realizzati nell'interesse dell'ente o per l'ipotesi che lo stesso ne abbia tratto un vantaggio.

Importanti novità si registrano anche nell'ambito del diritto sostanziale.

L'art. 615 *quinquies*, originariamente volto a sanzionare *la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*, reprime oggi *la diffusione di apparecchiature, dispositivi o programmi informatici diretti danneggiare o interrompere un sistema informatico*. La norma, così come novellata, punisce , quindi, *chiunque , al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno , si procura, riproduce , importa, diffonde, comunica consegna o , comunque mette a disposizione di altri apparecchiature, dispositivi o programmi informatici aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, delle informazioni, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale , o l'alterazione del suo funzionamento*.

Si prevedono poi più ipotesi di danneggiamento informatico e segnatamente:

il danneggiamento di informazioni, dati e programmi informatici (art.635 *bis*); *il danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità* (art. 635 *ter*); *il danneggiamento di sistemi informatici e telematici* (art. 635 *quater*); *il danneggiamento di sistemi informatici e telematici di pubblica utilità* (art. 635 *quinquies*).

Maggiori spunti innovativi attengono, tuttavia, alla disciplina penale del documento informatico e della firma digitale. In tale direzione si registra l'eliminazione della definizione di documento informatico introdotta dalla legge 547 del 93, per dar spazio a quella più corretta, già contenuta nel regolamento di cui al Decreto del Presidente del Repubblica 10 novembre 1997, n. 513 e

[4] Su tale argomento cfr. L. Luparia (a cura di), *Sistema penale e criminalità informatica*, Giuffrè, Milano, 2009; P.G. De Marchi (a cura di), *I nuovi reati informatici*, G. Giappichelli, Torino, 2009.

ripresa dal Codice dell'amministrazione digitale. Anche ai fini penalistici , quindi , per documento informatico non si intenderà più "il supporto informatico contenente dati o informazioni aventi efficacia probatoria", bensì "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti". Opportuna risulta poi l'introduzione dei reati di *falsa dichiarazione o attestazione al certificatore sull'identità o su qualità personali proprie o di altri* (art.495 *bis*) e di *truffa del certificatore di firma elettronica* (art.640 *quinquies*).

Interessanti modifiche si registrano, infine, in ambito processuale, atteso che sino ad oggi i maggiori problemi applicativi delle norme sulla criminalità informatica dipendevano proprio dalla poca chiarezza in ordine a ciò che gli organi inquirenti potevano fare nella delicata fase dell'accertamento del reato.

Si prevede espressamente la possibilità per l'autorità giudiziaria di disporre, in sede di ispezione, rilievi e altre operazioni tecniche sui sistemi, di perquisire gli stessi anche se protetti da misure di sicurezza, di esaminare presso le banche anche i dati, le informazioni ed i programmi informatici. E' contemplata altresì una disciplina sulle modalità di acquisizione dei dati oggetto di sequestro presso i fornitori di servizi informatici e telematici o di telecomunicazioni, nonché un provvedimento che permetta il congelamento temporaneo ed urgente dei dati personali. Viene prevista, infine, la concentrazione della competenza per i reati informatici presso gli uffici di procura distrettuali al fine di facilitare il coordinamento delle indagini e la formazione di gruppi di lavoro specializzati in materia.

Sul piano del diritto sostanziale va registrata la recente previsione dell'ipotesi di frode informatica commessa con sostituzione di identità digitale[5], mentre in ambito procedurale viene prevista la confisca obbligatoria per i beni utilizzati per la commissione di alcuni reati informatici[6].

Accanto alla legge 547/93 si individuano altre norme riferite espressamente o comunque riferibili ai reati informatici.

La duplicazione abusiva del *software* e la commercializzazione del programma contraffatto è sanzionata penalmente dall'art. 171 *bis* della legge 22 aprile 1941, n. 633 (tale articolo è stato introdotto dal decreto legislativo n. 518 del 29 dicembre 1992, successivamente modificato dalla legge 18 agosto 2000, n. 248) .

La divulgazione e cessione telematica di materiale pedopornografico e la sua detenzione nel sistema informatico sono punite rispettivamente dagli art. 600 *ter e 600 quater c.p.*[7].

L'assistenza a gruppi terroristici apprestata fornendo strumenti di comunicazione e, quindi, anche telematici, assume rilevanza penale in virtù di quanto disposto dall'art. 270 *ter* c.p.[8].

---

[5] Il D.L. 14 agosto 2013 n. 93 "Disposizioni urgenti in materia di sicurezza e per il contrasto per le violenze di genere, nonché in tema di protezione civile e di commissariamento delle provincie", inserisce un terzo comma all'interno dell'art. 640 *ter* al fine di sanzionare la frode informatica commessa con sostituzione di identità digitale.

[6] Legge 15 febbraio 2012, n. 12 "Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica".

[7] Disposizioni introdotte nel codice penale dalla legge 3 agosto 1998 , n. 269 "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù", successivamente modificata dalla l. 38/2006, contenente disposizioni in tema di lotta contro lo sfruttamento sessuale dei bambini e pedopornografia

[8] Inserito nel codice penale dalla legge 15 dicembre 2001, n.438, che ha convertito in legge, con modificazioni, il decreto-legge 18 ottobre 2001, n.374, recante disposizioni urgenti per contrastare il terrorismo internazionale

Norme penali in qualche modo riferibili a condotte correlate all'uso delle tecnologie dell'informazione sono rintracciabili anche nel "Codice in materia di protezione dei dati personali", introdotto attraverso il decreto legislativo 30 giugno 2003, n.196.
Si tratta, invero, di disposizioni non direttamente riferite all'informatica, atteso che la legge disciplina il trattamento dei dati personali, quale che sia il metodo utilizzato (tradizionale o automatizzato), ma comunque sovente applicabili al mondo informatico, considerato che la maggior parte dei trattamenti avviene mediante computer.
Sono attualmente sanzionati penalmente l'illecito trattamento dei dati personali (art. 167), la falsità nelle dichiarazioni e notificazioni al Garante (art. 168), l'omessa adozione di misure di sicurezza (art. 169), l'inosservanza di provvedimenti del Garante (art. 170).

3. La Legislazione penale vigente ed il contesto applicativo

A circa venti anni di distanza dalla prima legge specificatamente riferita ai reati informatici, cui sono seguiti, come detto, interventi in alcuni specifici ambiti, è possibile tracciare un bilancio di ciò che è stato fatto e delle questioni ancora aperte.
Sul piano generale può osservarsi che esiste al momento una legislazione penale dell'informatica tutto sommato esaustiva, essendo state disciplinate più o meno tutte le condotte realizzabili con le tecnologie o almeno quelle immaginabili fino ad oggi.
Si discute attualmente di fenomeni quali il *cyberbullismo*, il *phishing* ed il *cyberstalking*, che, tuttavia, possono essere puniti anche con la normativa esistente e, quindi, in assenza di disposizioni ad essi esplicitamente riferite.
Sul piano del diritto positivo allora, il vero problema è quello dell'interpretazione delle norme, considerato che esse introducono termini tecnici sino a poco tempo fa non presenti nell'ordinamento giuridico e, quindi, sconosciuti ai giuristi.
Da questo punto di vista "lo sforzo" da fare è quello di assimilare le nuove nozioni, ma anche e soprattutto di acquisire una consapevolezza del modo di pensare di coloro che utilizzano le tecnologie dell'informazione. In altre parole serve una sorta di alfabetizzazione giuridico-informatica.
L'avvicinamento dell'ambito giuridico a quello informatico, consentirebbe una applicazione delle norme in grado di centrare gli obiettivi prefissati e, quindi, di contrastare con maggior forza la criminalità informatica.
Questione diversa e più complessa è quella dell'applicazione delle norme nel contesto specifico in cui le stesse sono chiamate ad operare.
È indubbio ad esempio che ogniqualvolta la norma penale, anche se non espressamente riferita alle tecnologie dell'informazione, vada applicata ad un reato commesso attraverso la rete si incontrano questioni particolari quali quelle relative all'individuazione dell'autore e del luogo del commesso reato.
Ne deriva che molte delle questioni giuridiche di non facile soluzione non dipendono soltanto e soprattutto dal contenuto delle norme, quanto dal contesto in cui vengono applicate. Contesto che

è bene sottolineare si caratterizza sempre più per la sua immaterialità e per il fatto che i soggetti non si incontrano fisicamente e gli eventi antigiuridici si possono realizzare in tempo reale ed a distanza.
Occorre quindi che l'interprete tenga conto anche del continuo evolversi delle tecnologie rispetto a quando fu emanata la prima legge in materia di reati informatici.
Quando all'inizio degli anni novanta la maggior parte dei Paesi europei decisero di dotarsi di una legislazione penale in questo settore la cosiddetta società dell'informazione era ancora in divenire. I grandi centri di calcolo erano presenti solo all'interno di importanti e strategiche strutture pubbliche e nelle aziende di grandi dimensioni e la cosiddetta alfabetizzazione informatica, caratterizzata da un utilizzo capillare del personal computer, non si era ancora realizzata in pieno.
Di fronte ad uno scenario di questo tipo, il legislatore ha focalizzato la propria attenzione sulle tecnologie di fronte ad i suoi occhi e, quindi, sostanzialmente sui programmi e sui sistemi informatici e telematici, immaginando tutti i reati realizzabili attraverso o contro tali beni.
Nel volgere di pochi anni, tuttavia, la nostra società si è trasferita dal piano reale a quello virtuale e questo grazie, in un primo momento, all'utilizzo su vasta scala di Internet in tutto il mondo, successivamente, arricchendosi di contenuti nuovi rappresentati dal diffondersi dei *social network*s, che hanno aperto scenari, anche giuridici, fino a qualche anno fa impensabili.
L'utilizzo continuo della rete è stato a sua volta favorito dall'evoluzione della telefonia mobile, attraverso la quale si può veicolare qualsiasi tipo di contenuto in tempo reale.
Recentemente, infine, lo scenario si è arricchito di nuove applicazioni informatiche, quali l'internet degli oggetti[9] (IdO) ed il *cloud computing*[10].
L'arricchimento dei contenuti delle tecnologie ha ovviamente un riflesso su tutte le condotte umane e, quindi, anche su quelle costituenti reato.
Rispetto al 1993, sempre più spesso, si parla di nuove condotte antisociali, molte delle quali hanno preso piede grazie alla diffusione della rete, quali ad esempio il *phishing,* il *cyber bullismo,* il *cyberstalking* ed il *cybericiclaggio*.
Tale nuovo scenario ha altresì fatto aumentare i problemi legati all'individuazione del reato, del suo autore, e, se pensiamo al *cloud computing,* alla localizzazione del luogo del commesso reato.
Innanzi ad un contesto sempre più immateriale, questioni giuridiche di non facile soluzione si pongono in ordine alle modalità di acquisizione, conservazione, e tenuta nel processo della prova digitale o *digital evidence*, tant'è che nel tempo si è sviluppata una disciplina specifica, denominata "*computer forensic*" o "*digital forensic*", il cui compito è proprio quello di analizzare i requisiti che deve avere il bene informatico per esser assunto come prova valida a tutti gli effetti all'interno di un processo.
Il consolidarsi della società dell'informazione, tuttavia, non pone questioni nuove solo rispetto all'applicazione delle norme penali ed all'accertamento del reato, ma anche rispetto al modo di agire e di pensare del soggetto agente.

---

[9] L'Internet degli oggetti, chiamato anche informatica "ubiquitaria" o "intelligenza ambientale", comprende determinate tecnologie (R.f.i.d., TCP/IT, Bluetooth, ecc), che collegate insieme consentono di identificare oggetti, raccogliere dati, trattarli e trasferirli.

[10] Si tratta di una nuova metodologia della struttura IT tramite la banda larga, concretandosi in una automazione dei servizi di gestione.

Da questo punto di vista è agevole osservare come il mutamento del contesto ha finito con il modificare sensibilmente le motivazioni del "delinquente" informatico, considerato che l'*hacker* dell'inizio degli anni novanta era principalmente mosso da un movente politico e libertario, in sostanza contro il monopolio o l'oligopolio delle informazioni, mentre oggi esiste una vera e propria professionalità informatica nell'ambito del crimine, tant'è che esperti informatici vengono assoldati all'interno dei gruppi terroristici e dalle mafie di tutto il mondo. Il reato informatico è sempre più un reato economico, con tutte le conseguenze che si possono immaginare.
Da un pò di anni a questa parte si è compreso anche che le tecnologie dell'informazione non modificano solo il modo di agire delle persone ma anche il modo di pensare. Per quanto concerne l'ambito penale è interessante notare come ormai da anni si parli di dipendenza da internet equiparata a psicopatologie quali la bulimia ed il gioco d'azzardo, e sempre più diffuse sono le cosiddette "droghe tecnologiche".
Una nuova frontiera del diritto da qui a breve potrebbe essere quella che analizza le ripercussioni sulla mente umana della mediazione tecnologica, al fine di verificare se ciò possa avere una ricaduta sull'interpretazione di alcuni istituti, quali l'imputabilità, i motivi a delinquere, ecc..

4. I reati informatici

Quando ancora non esisteva una legislazione penale dell'informatica, le condotte correlate all'uso del computer venivano indicate con locuzioni di tipo criminologico quali "*computer crime*", "*computer related crime*", ed in Germania "*computer kriminalitat*". Successivamente, con l'introduzione delle specifiche disposizioni di legge, si è iniziato a parlare di reati informatici, e, se commessi attraverso i mezzi di comunicazione, di reati telematici.
In questa fase si distingueva tra reati commessi attraverso l'informatica, ad esempio l'accesso abusivo, o rivolti contro un bene informatico, danneggiamento dell'*hardware*, contraffazione del *software*, ecc.
Nel volgere di pochi anni con l'espandersi della rete sempre più spesso si parla di reati di Internet per individuare tutte quelle condotte illecite, non necessariamente contemplate da norme penali informatiche, pensiamo alla diffamazione via Internet, che pongono questioni particolari, quali quelle, come detto, del commesso reato, del suo autore e della relativa giurisdizione e competenza.
Attualmente è sempre più difficile definire con una "etichetta unica" i reati commessi attraverso le tecnologie sia perché, come visto, le stesse tecnologie evolvono a ritmo incessante, per cui spesso termini come informatica o telematica possono considerarsi superati o arricchiti nei loro contenuti, sia perché ha sempre meno senso distinguere fra reati tradizionali e reati informatici, visto che con il consolidarsi della società dell'informazione questi ultimi si presentano ormai quasi con la stessa frequenza dei primi.
L'incremento dei reati commessi attraverso le tecnologie, anche a seguito dell'evolversi delle stesse, ha fatto si che l'attenzione dei giuristi prima, e delle aule di giustizia poi, si concentrasse sempre di più su condotte criminali non trattate dalla legge del 1993.
Fenomeno sempre più al centro dell'attenzione è quello della cosiddetta pedofilia telematica, intendendosi con tale locuzione una serie di condotte illecite realizzate attraverso la rete ed aventi

ad oggetto lo sfruttamento sessuale dei minori.
Con la legge 269 del 1988, successivamente modificata dalla legge 38 del 2006, vengono, tra l'altro, puniti la distribuzione, diffusione e detenzione di materiale pedopornografico, anche virtuale, ovvero frutto di fotomontaggi o manipolazioni informatiche.
Altra pratica delittuosa in continua crescita è quella del cosiddetto *cyberstalking*, spesso agevolato da contesti virtuali, quali i *social networks*, che consentono a l'ex fidanzato o coniuge, o allo spasimante rifiutato, talvolta anche attraverso furti d'identità, di rendere la vita impossibile alla vittima designata. Tali condotte sono attualmente disciplinate dall'art. 612 *bis* c.p. (atti persecutori)[11].
Fenomeno più raro, ma non per questo non meritevole di attenzione, è quello del *cyberterrorismo*, riguardante l'uso delle tecnologie dell'informazione da parte dei gruppi terroristici.
Su di esso si è concentrato l'interesse all'indomani dell'11 settembre 2001, considerando che nelle democrazie occidentali, tutte le informazioni strategiche sono contenute all'interno di sistemi, e temendo quindi attacchi dimostrativi o distruttivi.
Per contrastare tale fenomeno, oltre alle disposizioni previste dalla legge 547/93, e quelle già presenti nel codice penale, ad esempio, nella parte dedicata ai delitti contro la personalità dello Stato, contro l'ordine pubblico e l'incolumità pubblica, di recente il legislatore ha introdotto l'art. 270 *ter*, che punisce anche colui che fornisce strumenti di comunicazione ai partecipanti alle associazioni terroristiche[12].
In questi ultimi anni ci si è soffermati sulle problematiche che il reato informatico pone nel momento in cui viene realizzato all'interno dell'azienda.
Tale attenzione si è sviluppata principalmente a seguito delle modifiche apportate al Decreto legislativo 231 dalla l. n. 48 del 2008, per cui le aziende possono essere chiamate a rispondere per la maggior parte dei reati informatici commessi dai suoi vertici e dipendenti[13].
Si tratta di una grande novità atteso che fino ad oggi, sulla base del Decreto Legislativo 231/01, tale responsabilità era prevista solo per residuali ipotesi di reato informatico, quali quelli di frode informatica commessa a danno dello Stato o di altro Ente pubblico, di assistenza a gruppi terroristici apprestata fornendo strumenti di comunicazione, di distribuzione, cessione e detenzione di materiale pedopornografico.
Le suddette modifiche creano preoccupazione nelle aziende, non soltanto per l'estensione di tale responsabilità a tutti i delitti informatici, ma per la circostanza che la stessa possa essere imputata anche nelle ipotesi in cui non venga rintracciato l'autore materiale del reato. Ne consegue che la mancata individuazione del soggetto attivo del reato, non infrequente in materia di criminalità informatica, possa non far comprendere esattamente all'organo giudicante le motivazioni dello stesso e quindi determinare un'attribuzione di responsabilità anche quando l'autore del reato abbia agito per fini esclusivamente personali e non nell'interesse del suo datore di lavoro.

La preoccupazione non può che aumentare quando si consideri che l'azienda ritenuta responsabile è soggetta, oltre che all'esborso di ingenti somme di danaro, a sanzioni interdittive quali: a)

---

[11] Articolo introdotto dall'art. 7 del D.L. 23 febbraio 2009 n. 11.

[12] Articolo introdotto dalla legge 15 dicembre 2001, n. 438, che ha convertito, con modificazioni, in legge il Decreto-legge 18 ottobre 2001, n. 374, intitolato "Disposizioni urgenti per contrastare il terrorismo internazionale";

[13] Sul reato informatico in azienda cfr. P. Galdieri, C.Giustozzi, M. Strano, *Sicurezza e privacy in azienda*, Apogeo, Milano, 2001.

l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) il divieto di pubblicizzare beni o servizi.
Di fronte a tale nuovo scenario l'azienda è inevitabilmente costretta a studiare delle strategie preventive idonee, da un lato, ad impedire la commissione di reati informatici al suo interno e dall'altro, capaci di escluderne una sua responsabilità nelle ipotesi in cui le misure adottate non siano state in grado di evitare la commissione del reato.
Tali accorgimenti vanno proprio nella direzione del Decreto Legislativo 231 del 2001, che prevede l'esonero di una responsabilità dell'ente allorquando lo stesso dimostri di aver predisposto modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi.
Ovviamente non basta redigere il predetto modello organizzativo, essendo necessario che lo stesso risponda alle seguenti esigenze:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

5. L'interpretazione del reato informatico

Le norme penali che contemplano reati informatici, pur diverse tra loro, presentano alcune caratteristiche comuni.
In primo luogo esse si differenziano nel contenuto da quelle previgenti, in quanto utilizzano termini tecnici sino ad oggi non presenti nelle disposizioni di legge. Si pensi a tal proposito ai continui richiami a definizioni quali "sistema informatico e telematico", "programma informatico", " dato e informazione", "misure di sicurezza".
In secondo luogo si riferiscono a condotte nuove, non immaginabili sino a pochi anni fa. Pensiamo all'accesso abusivo all'interno di un sistema informatico o alla diffusione di *virus* informatici, che si realizzano e pongono problemi sensibilmente diversi da quelli posti sino ad oggi dalle attività delittuose già note.
In terzo luogo trovano applicazione in contesti anch'essi modificati. Un reato commesso in un'azienda non automatizzata pone, infatti, problemi differenti da quelli che determina all'interno di un'impresa la cui attività è totalmente gestita dagli elaboratori.
Infine si riferiscono, talvolta, a comportamenti che non sono soltanto diversi sotto il profilo oggettivo, ma anche sotto il profilo soggettivo. E'indubbio, infatti, che determinate azioni sono

realizzate perché le tecnologie offrono nuove opportunità, per es. quella di mantenere l'anonimato, così come alcune condotte trovano ispirazione proprio da quel confronto-scontro con le tecnologie: è il caso degli *hackers* che entrano nei sistemi altrui con il fine esclusivo di contrastare, a loro dire, una nuova forma di potere definita appunto "potere informatico".
Caratteristiche analoghe a quelle sinora descritte si rinvengono nelle norme "tradizionali" allorquando le stesse sono applicate a condotte informatiche. Pensiamo al delitto di diffamazione commesso attraverso Internet. La norma che trova applicazione è l'art. 595 c.p., che non si riferisce espressamente al mezzo telematico, ciononostante, allorquando essa va applicata ad ipotesi dove è coinvolta la rete, si ripropongono problemi riconducibili direttamente al mezzo impiegato per commettere il reato, ad es. quello dell'individuazione del luogo del commesso reato.
Caratteristiche comuni, e quindi problemi particolari, pongono anche quelle norme del codice di procedura penale che consentono agli organi inquirenti di contrastare i reati commessi attraverso le tecnologie dell' informazione (es. norme che si riferiscono alle intercettazioni informatiche e telematiche o al sequestro probatorio dei computer).
Dall'interpretazione delle norme, delle condotte cui le stesse si riferiscono, del contesto in cui le disposizioni di legge vanno applicate, dipende l'esito stesso del procedimento penale instaurato.
Volendo indagare sui problemi interpretativi posti da ciascuno degli elementi indicati pare opportuno affrontarli seguendo l'iter di un procedimento penale che, come noto, si compone di due fasi fondamentali ovvero quella delle indagini preliminari e quella dell'eventuale conseguente giudizio, intendendo con quest'ultimo riferirci anche all'eventuale giudizio di appello e di Cassazione.
Nella prima fase gli organi inquirenti e quindi il pubblico ministero, coadiuvato dalle forze di polizia, si muovono alla ricerca di quegli elementi che possono risultare utili per sostenere l'accusa all'interno del processo. Nella seconda fase, quella del giudizio, ruolo centrale viene ricoperto dall'organo giudicante (Tribunale, Corte d'Appello, Cassazione), il quale dovrà confrontarsi con le norme, anche alla luce delle tesi prospettate dall'accusa e dalla difesa.
Nel corso delle indagini preliminari i problemi posti dai reati informatici sono principalmente quelli delle modalità di acquisizione delle prove, sul piano fattuale e giuridico. Nella fase del giudizio le questioni poste dai delitti informatici sono riconducibili al contenuto delle norme, delle condotte e dei contesti , ovvero a tutti quegli elementi dei quali il giudice dovrà tener conto ai fini del decidere.

6. Il reato informatico nelle indagini preliminari

In tema di indagini preliminari aventi ad oggetto i reati informatici è possibile svolgere alcune considerazioni di carattere generale.
La prima è che nel volgere di alcuni anni si è giunti ad una più adeguata preparazione, anche sotto il profilo tecnico, da parte degli organi inquirenti e delle forze dell'ordine.
Nelle prime esperienze investigative si è pagato lo "scotto" di un'inadeguata preparazione delle forze dell'ordine e di una normativa in tema di indagini informatiche non ancora ben collaudata.
È questo il periodo in cui si registrano sequestri immotivati di oggetti per nulla attinenti al *thema probandum* ad es. di tappetini e *mouse*: si è arrivati ad apporre i sigilli nella camera da letto dove si

trovava un computer, non sapendo cosa fare in assenza di specifiche disposizioni da parte del Pubblico Ministero!
Attualmente all'interno delle forze dell'ordine sono state create sezioni altamente specializzate, ciascuna con specifiche competenze tecniche
La seconda considerazione è che i diversi problemi che si incontrano nelle indagini aventi ad oggetto crimini informatici, traggono tutti origine dalla natura stessa del delitto oggetto di investigazione, che pone questioni peculiari in ordine al suo concreto accertamento, all'individuazione del suo autore, nonché al modo stesso in cui vanno acquisiti gli elementi probatori.
La terza considerazione è che la natura stessa della rete, idonea a mettere in contatto soggetti che neanche si conoscono tra loro, favorisce la nascita di procedimenti a carico di numerosi coindagati: basti pensare alle continue "maxi retate" in tema di pedofilia telematica.
A prescindere da valutazioni di merito, che presupporrebbero la conoscenza degli atti del singolo procedimento, rileva come in linea generale un procedimento con tanti indagati per delitti che si prescrivono al massimo in sette anni e mezzo è destinato "a morire" ancor prima di emettere "il primo vagito". Rispetto ai reati per i quali è più diffusa la pratica di maxi operazioni, ovvero quelli di cessione e distribuzione di materiale pedopornografico, si registra l'ulteriore rischio di tralasciare aspetti che destano un maggiore allarme sociale, ad esempio la vera e propria produzione delle immagini, per dedicarsi al contrasto di fenomeni che, seppure deprecabili, manifestano un minore disvalore sociale.
Quarta considerazione è che in tema di indagini informatiche sovente si registra un affievolimento delle garanzie dell'indagato.
Benché, come detto, sia nettamente migliorata la competenza tecnica da parte delle forze dell'ordine, ancora troppo spesso si assiste a perquisizioni e sequestri privi di adeguata motivazione.
Prassi sicuramente censurabile, poi, è quella di restituire il materiale ritenuto superfluo ai fini delle indagini con grande ritardo e sovente con ingiustificato danno per l'indagato.
Tuttavia, la maggiore compressione delle garanzie dell'indagato non è dovuta tanto alle indagini in sé, ma alla pubblicizzazione che delle stesse viene fatta dagli organi d'informazione.
Si pensi, a titolo di esempio, alle continue notizie fornite dai media su indagini in corso in materia di pedofilia telematica, la cui risonanza ha spinto, purtroppo, in alcuni casi l'indagato addirittura a togliersi la vita.
Posto che qualunque fatto di cronaca trovi legittimo accesso nei canali della informazione, perché grave sarebbe il contrario, è altresì necessario apprestare adeguata cautela allorquando si forniscono informazioni su procedimenti dall'esito ancora incerto.
Il problema di carattere generale, perché riferibile a qualsiasi tipo di indagine, assume connotati peculiari in tema di criminalità informatica.
È agevole a tal riguardo constatare come i reati commessi attraverso le tecnologie suscitino interesse nell'opinione pubblica, e talvolta addirittura simpatia, così da divenire argomento ben gradito dai fruitori delle informazioni e, quindi, da coloro che dalla diffusione delle informazioni traggono utili economici.

7. I mezzi di ricerca della prova

Momento centrale della fase delle indagini è sicuramente quello della ricerca della prova necessaria a sostenere un eventuale accusa all'interno del processo[14].

I mezzi di ricerca della prova sono disciplinati dal titolo III , libro terzo del codice di procedura penale, che considera tali le ispezioni (artt. 244-246), le perquisizioni (artt. 247-252), i sequestri (artt. 253-265), le intercettazioni (artt. 266-271).

Di queste norme espressamente riferite alla realtà informatica è l'art. 266 *bis* " *Intercettazioni di comunicazioni informatiche e telematiche*", introdotto dall'art. 11 della l. 23 dicembre 1993 n. 547, che consente l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi, oltre che rispetto ai delitti per i quali è consentita l'intercettazione telefonica, anche per i reati commessi mediante le tecnologie informatiche o telematiche.

Tali intercettazioni, sulla base di quanto disposto dal comma 3 *bis* dell'art. 268 c.p.p.- a differenza di quanto avviene per quelle telefoniche, dove l'operazione deve essere di regola compiuta mediante impianti installati nella procura della Repubblica, salvo che tali impianti risultino insufficienti o inidonei ed esistano ragioni di urgenza, nel qual caso il pubblico ministero può disporre con provvedimento motivato il compimento delle operazioni mediante impianti di pubblico servizio o in dotazione alla polizia giudiziaria-, possono essere compiute anche mediante impianti appartenenti a privati su disposizione del Pubblico Ministero.

Norme fondamentali ai fini dell'indagine e segnatamente riferite alla realtà informatica sono poi l'art. 14 della legge 269/98, in materia di delitti legati all'abuso e sfruttamento sessuale dei minori e l'art. 4 della legge 15 dicembre 2001 n. 438 (che ha convertito con modificazioni, in legge il Decreto-legge 18 ottobre 2001, n. 374 " Disposizioni urgenti per contrastare il terrorismo internazionale) in tema di contrasto al terrorismo.

Tralasciando di esaminare la portata di tali norme, preme evidenziare come le maggiori questioni attinenti i mezzi di ricerca della prova riguardavano sino ad oggi le modalità attraverso le quali si perveniva al sequestro dei computer.

Il problema nasceva poiché non esisteva nel nostro ordinamento una norma espressamente riferita al sequestro dei computer e quindi occorreva di volta in volta verificare le conseguenze di una disciplina pensata per beni che hanno caratteristiche sensibilmente diverse da quelle proprie dei sistemi informatici.

Sulla base di quanto disposto dal primo comma dell'art. 253 c.p.p.: " L'autorità giudiziaria dispone con decreto motivato il sequestro del corpo del reato e delle cose pertinenti al reato necessarie per l'accertamento dei fatti". Il secondo comma del medesimo articolo precisa come" : Sono corpo del reato le cose sulle quali o mediante le quali il reato è stato commesso nonché le cose che ne costituiscono il prodotto, il profitto o il prezzo".

Partendo dal tenore letterale della norma si ponevano una serie di interrogativi.

Ci si chiedeva quale fosse il bene oggetto di sequestro, ovvero se andasse sequestrato solo il contenuto del computer, se eventualmente solo quella parte di contenuto ritenuta rilevante, o se

---

[14] In tema di indagini informatiche cfr: M. Chirizzi, *Computer Forensic – Il reperimento della fonte di prova informatica -,* Laurus Robuffo, Roma, 2006; L. Luparia, G. Ziccardi, *Investigazione penale e tecnologia informatica – L'accertamento del reato tra progresso scientifico e garanzie fondamentali -,* Giuffrè, Milano, 2007.

viceversa, fosse da sequestrare anche l'*hardware* ed eventualmente i relativi accessori (*mouse*, *scanner*, stampanti, ecc.)[15].
Molti dei problemi prospettati potrebbero oggi attenuarsi grazie alle novità introdotte dalla l. n 48 del 2008, che prevede espressamente la possibilità per l'Autorità giudiziaria di disporre, in sede di ispezione, rilievi e altre operazioni tecniche sui sistemi, di perquisire gli stessi anche se protetti da misure di sicurezza, di esaminare presso le banche anche i dati, le informazioni ed i programmi informatici. E' contemplata altresì una disciplina sulle modalità di acquisizione dei dati oggetto di sequestro presso i fornitori di servizi informatici e telematici o di telecomunicazioni, nonché un provvedimento che permetta il congelamento temporaneo ed urgente dei dati personali. Viene prevista, infine, la concentrazione della competenza per i reati informatici presso gli uffici di procura distrettuali al fine di facilitare il coordinamento delle indagini e la formazione di gruppi di lavoro specializzati in materia[16].

8. L'individuazione del luogo del commesso reato informatico

Tra le diverse questioni legate alla fase dell'accertamento di un delitto commesso attraverso le tecnologie vi è quello dell'individuazione del luogo del commesso reato quando lo stesso viene realizzato attraverso la rete.
Partendo dalla premessa che in tali casi è possibile realizzare un evento antigiuridico in luogo diverso da quello ove è stata posta in essere la condotta, sorge il problema dei criteri da utilizzare per individuare il luogo del commesso reato[17], poiché da ciò dipende l'identificazione dell'Autorità Giudiziaria competente ad indagare e successivamente a giudicare.
Nel nostro ordinamento punto di partenza è sicuramente l'articolo 3 del codice penale, che sancisce il c.d. principio di territorialità, onde la legge penale italiana si applica a qualsiasi fatto commesso nel nostro Stato. Fondamentale è, poi, l'articolo 6, che, accogliendo il principio dell'ubiquità, considera commesso in Italia un dato reato quando nel suo territorio si è realizzata almeno una parte della condotta o dell'evento. Altrettanto interessanti ai fini della presente indagine sono gli articoli 9 e 10 c.p., rispettivamente riferiti ai delitti comuni commessi all'estero dal cittadino italiano e dallo straniero.
Alla luce delle disposizioni appena indicate è agevole intuire come non sorgano questioni eccessivamente complesse ogni qualvolta la condotta e l'evento si realizzino in Italia o nel caso in cui nel nostro Paese si realizzi una parte dell'una o dell'altro. Sulla base di quanto previsto dall'art.

---

[15] Cfr: Corte di Cassazione, Sezione V penale, n. 649/95; ordinanza del 7 febbraio 2000, Tribunale Penale di Torino, Sez. Riesame; Corte di Cassazione Sez. III penale, 1778/03.

[16] Cfr: G. D'Aiuto, L. Levita, *I reati informatici Disciplina sostanziale e questioni processuali* -, Giuffrè, Milano,2012, p. 159 ss.; L. Luparia, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007, p. 161 ss..

[17] Sul tema cfr. P. Galdieri, *Internet e illecito penale*, in "Giurisprudenza di merito", Fasc. 4-5, 1998, p. 861 ss.; Id., *Le tecnologie dell'informazione nell'ordinamento penale*, in AA.VV., *Prospettive giuridiche delle tecnologie dell'informazione,* ESI, Napoli, 2000, p. 147 ss.; L. Picotti, *Profili penali delle comunicazioni illecite via Internet*, in "Diritto dell'informazione e dell'informatica", 1999.

6 secondo comma, infatti, si applicherà la legge penale italiana tanto nell'ipotesi in cui il soggetto agente, digitando sul proprio *computer* a Napoli, produce effetti negativi sul *server* situato a Torino, quanto nel caso in cui a Roma si realizzi soltanto parte della condotta o dell'evento, mentre l'altra parte costitutiva del reato viene posta in essere in una città straniera.
Qualora, invece, condotta ed evento si realizzino fuori dall'Italia, perché possa essere applicata la legge nostrana occorre che in Italia vi sia un qualche riflesso del reato commesso. L'ipotesi prospettata non è puramente teorica laddove si consideri che ciò che avviene via rete può essere ricevuto, o comunque percepito, anche da soggetti diversi dai destinatari originari. In questi casi, il richiamo all'art. 6 secondo comma deve essere fatto tenendo ben presente la natura eccezionale di questa disposizione. Infatti, essendo di regola applicabile la legge penale italiana solo a fatti commessi nel territorio nazionale, l'ultrattività della nostra legislazione deve mantenersi nei limiti del contenuto letterale dell'art.6 secondo comma ed in ossequio al principio del *favor rei*, onde la normativa italiana sarà applicabile solo qualora in Italia si realizzi effettivamente parte della condotta o dell'evento, così come descritti nella fattispecie penale di riferimento.[18] Posto che queste sono le regole da seguire per individuare l'Autorità avente giurisdizione, pare utile riportare alcune soluzioni proposte in altri Paesi rispetto alle seguenti ipotesi verificabili nella pratica: 1) gli effetti negativi di una medesima condotta si manifestano in più Paesi, con la conseguenza che lo stesso soggetto possa essere chiamato a rispondere del medesimo reato di fronte ad autorità giudiziarie appartenenti a Stati diversi (rischio che si corre poiché in ambito internazionale non vige il principio del *ne bis in idem)*; 2) parte della condotta o dell'evento si realizzi in un Paese dove il fatto non sia previsto dalla legge come reato.
Rispetto alla prima ipotesi si è evidenziata la possibilità di richiamare quanto enunciato dalla Corte di Giustizia della Comunità Europea, con riferimento all'azione di risarcimento dei danni per illeciti << transfrontalieri>>, commessi a mezzo stampa. L'applicazione del medesimo principio in questo settore determinerebbe una competenza concorrente dei singoli ordinamenti per la parte che li riguarda, alla stregua della loro specifica legislazione, con una autolimitazione, tuttavia, nell'esercizio del loro potere punitivo, quantomeno in sede di commisurazione, che rispetti l'esigenza di proporzione rispetto alla complessiva dimensione transnazionale del fatto stesso, e ciò tenendo conto della sua punibilità e delle sanzioni già eventualmente inflitte in altri ordinamenti cui pure rilevi.[19]
Rispetto alle ipotesi in cui gli effetti negativi prodotti in un Paese siano il risultato di una condotta considerata lecita nel luogo in cui si realizza, la Giurisprudenza americana offre utili spunti di riflessione. Attualmente il criterio più utilizzato dalle Corti americane è quello del "minimum contact", ossia del contatto telematico minimo idoneo a radicare la giurisdizione di uno Stato su una condotta realizzata all'estero da un soggetto ivi residente. Tale criterio, utilizzato talvolta in modi differenti, si è venuto nel tempo uniformando al punto da richiedere per la sua sussistenza la verifica dei seguenti requisiti: 1) quantità dei contatti del soggetto agente; 2) natura e qualità

[18] In tale ottica deve leggersi la sentenza del 24 novembre 2000, emessa dal Tribunale di Torre Annunziata, che, chiamato a decidere sulla competenza territoriale in materia di distribuzione di immagini pedopornografiche, ha fissato come luogo del commesso reato quello in cui si è realizzato l'invio delle immagini incriminate, ritenendo la consumazione del delitto in parola realizzata all'atto dell'invio.

[19] Così L.Picotti, *Profili penali delle comunicazioni illecite via Internet*, cit, p.333-334.

dei contatti medesimi; 3) connessione tra la causa dell'azione ed i contatti; 4) interessi dello Stato nell'affermare il foro di competenza; 5) convenienza delle parti.
Altro criterio sperimentale elaborato dalle Corti suddette è quello del "the most significant interest", secondo cui, per affermare la giurisdizione di uno Stato sulla condotta realizzata all'estero, occorre verificare la prevalenza dell'interesse a prevenire un dato reato rispetto all'interesse del Paese da cui si muove il soggetto agente a mantenere *standards* meno severi di valutazione rispetto al medesimo comportamento.
Prescindendo da valutazioni di ordine giuridico sull'operatività di tali princìpi nel nostro Paese, valutazioni che ci porterebbero ad affrontare tematiche eccessivamente complesse, è agevole, comunque, rilevare come tali criteri possano essere considerati iniqui, visto che determinano l'affermazione di una responsabilità penale da parte di un soggetto che ha rispettato la propria legge.
Di fronte alle incertezze evidenziate ed alla necessità di trovare delle soluzioni adeguate, non resta che incamminarsi verso due strade tra loro alternative.
La prima, auspicata da molti, è quella di un codice penale di Internet, accettato da tutti gli Stati ed avente ad oggetto esclusivamente i reati commessi attraverso la rete. Tale soluzione, tuttavia, presta il fianco a numerose obiezioni di carattere giuridico e pratico. Se da un lato, infatti, si evidenzia l'impossibilità, *rebus sic stantibus*, di sottrarre alla sovranità di ciascuno Stato la materia penale, dall'altro, si segnala il rischio che ciò possa portare a situazioni di disparità, nel senso che uno stesso reato, ad. es. il delitto di diffamazione, possa essere soggetto a pene diverse a seconda che sia realizzato attraverso la rete o per vie tradizionali.
Minori problemi comporta l'altra opzione, cioè quella di uniformare le singole legislazioni penali interne, così da garantire che un comportamento ritenuto illegale in un Paese sia considerato come tale in tutti gli altri e viceversa.

9. L'accertamento dell'autore del reato informatico

Sempre la rete pone questioni peculiari in ordine all'individuazione dell'autore del reato. Sia che venga considerata uno strumento, sia che la si consideri un luogo, certo è che nella rete, o tramite essa, si muovono soggetti senza volto, senza voce ovvero, per riprendere un 'espressione felice "uomini senza ombra". Tale dato è al contempo "croce e delizia" della rete stessa, perché è ciò che ne ha favorito la sua nascita ed espansione, perché è ciò che ne può determinare la sua limitazione o addirittura la fine.
L'opportunità di agire senza essere agevolmente identificabili consente all'individuo "di tirar fuori ciò che ha dentro", sul piano umano, sociale, individuale e collettivo, scevro da quei freni inibitori che, tal volta anche inconsciamente, scattano quando si è costretti a comunicare personalmente e fisicamente. La stessa opportunità, vista con uno sguardo in negativo, si traduce in garanzia di totale o di maggiore probabilità di impunità.
Sul piano giuridico, e segnatamente penale, l'opportunità di agire senza essere visti pone il problema dei criteri da utilizzare per individuare l'eventuale autore di un reato. Nei delitti commessi nei contesti tradizionali si può risalire all'autore anche attraverso l'ausilio di informazioni raccolte da soggetti che hanno assistito visivamente all'atto. Nei delitti realizzati attraverso altri mezzi di

comunicazione che non necessitano di una presenza fisica, è il caso delle molestie telefoniche, si può individuare il presunto responsabile mediante riconoscimento vocale reso possibile da un 'intercettazione preventiva. Nel delitto commesso in rete, data l'assenza della presenza fisica e di altri elementi distintivi, quale appunto la voce, la rintracciabilità dell'autore diviene sicuramente più complessa.

Per quanto concerne i delitti telematici vi è quindi da osservare come, rispetto ad essi, anche l'indagine svolta in modo ineccepibile consenta di risalire al *computer* del quale si è servito il soggetto agente, ma mai direttamente a lui.[20] Ciò spiega ad esempio perché quasi sempre soggetti appartenenti a gruppi terroristici inviino i loro messaggi non da casa, ma da luoghi aperti al pubblico che garantiscano la connessione ad Internet, i c.d. *Internet cafè*. E' evidente, quindi, che l'individuazione dell'autore del reato telematico può avvenire in termini di certezza quando accanto all'individuazione del *computer* utilizzato vengano raccolti ulteriori elementi, es. il *computer* era in dotazione esclusiva di una singola persona, qualcuno ha visto il soggetto X utilizzare quel *computer*, quel giorno ed a quella precisa ora, ecc.

L'individuazione dell'autore è resa, poi, ancor più complicata atteso che attraverso le tecnologie è possibile, come detto, agire a distanza, cancellare le tracce del reato commesso, nonché differire nel tempo gli effetti della propria condotta. Quanto a quest'ultimo aspetto, a titolo esemplificativo, pensiamo all'ipotesi di "bomba logica" inserita nel *computer* altrui i cui effetti distruttivi vengono volontariamente differiti ad un momento successivo da quello della sua immissione.

Talvolta l'identificazione dell'autore è resa ancor più difficoltosa perché il soggetto agente utilizza un server "ponte" per commettere un reato, es. dal computer di Roma, va nel *computer* collocato a Toronto e da lì fa partire l'azione delittuosa contro un *computer* che si trova a Parigi. E' evidente che un tale modo di agire rende più difficile o quanto meno più laboriosa l'attività di indagine.

Ciascuno di questi problemi, riconducibili direttamente alle opportunità citate, necessita di soluzioni che passano attraverso scelte di campo in cui si fronteggiano interessi di pari dignità e rilevanza. Ancora una volta sicurezza e libertà, esigenza di *privacy* ed esigenza di prevenzione, si fronteggiano nella dimensione virtuale, imponendo, tuttavia, opzioni con inevitabile ricaduta sul mondo reale.

Il diritto a muoversi liberamente in rete non può tradursi in diritto a negare la raccolta dei propri dati personali sempre e comunque. Il diritto all'anonimato finisce con il trovare il limite posto dal diritto di perseguire colui che, nascondendosi dietro l'anonimato, ha agito in modo delittuoso.

Giusta mediazione dei diversi interessi in campo sembra offrire la scelta ad oggi predominante in ambito europeo di riconoscere il c.d. "anonimato protetto", ovvero di garantire la possibilità di celare la propria identità nel corso della navigazione, dopo, tuttavia, aver fornito i propri dati identificativi al *provider*, così da consentire a quest'ultimo di fornirli all'autorità giudiziaria laddove gli venisse richiesto.

Per poter risalire alla persona che ha commesso una data azione in rete è necessario che i suoi dati identificativi rimangano in possesso del soggetto che ne ha permesso la "navigazione".

Altro grande problema giuridico è quindi quello della durata massima di conservazione di tali dati, non essendo possibile immaginare una conservazione degli stessi all'infinito. Sino a poco tempo

---

[20] Sulle problematiche in materia di indagini informatiche cfr.: T. Caloyannides, *Computer Forensics and privacy*, Norwood, Artech House, Inc, 2001.

fa queste informazioni, e precisamente quelle relative al traffico telefonico, erano mantenute esclusivamente per esigenze di fatturazione. Oggi si tende a prevedere un obbligo di tenuta dei dati per un certo lasso di tempo anche per consentire all'autorità giudiziaria di perseguire i reati. Il vero problema è quindi quello di trovare una soluzione capace di soddisfare sia coloro che sostengono l'impossibilità di conservare tali dati in eterno sia quelli che affermano come, talvolta, anche a distanza di molti anni, gli organi inquirenti possano avere l'esigenza di raccogliere informazioni.

10. Il reato informatico nel giudizio penale

Il rapporto che intercorre tra diritto penale e tecnologie dell'informazione si arricchisce di contenuti allorquando lo si valuta sul piano concreto ovvero facendo riferimento all'interpretazione svolta sulle singole norme dal giudice.

Da questo punto di vista un primo dato che emerge è che la normativa penale riferibile alle tecnologie va a disciplinare un contesto nato e sviluppatosi in assenza di regolamentazione, favorendo così il convincimento, ad esempio, che all'interno della rete qualsiasi condotta sia pienamente legittima. Conseguenza è che molti dei divieti posti nel volgere di pochi anni possano non essere compresi e, talvolta, considerati addirittura ingiusti. In tale ottica si pongono le azioni dimostrative di alcuni *hackers* che agiscono al sol fine, almeno a loro dire, di contrastare un sistema volto a favorire e preservare regimi di monopolio ed oligopolio in materia di produzione delle tecnologie e controllo dell'informazione.

Altro dato è che essa pare sovente rivolta alla tutela di interessi economici, che potrebbero trovare più adeguata protezione attraverso norme di natura civilistica. Tale obiezione viene mossa ad alcune delle disposizioni penali introdotte all'interno della legge sul diritto d'autore per contrastare condotte illecite aventi ad oggetto il programma informatico.

Per l'ambito di nostro interesse rileva come la previsione della sanzione penale per la duplicazione abusiva "per fine di profitto", che consente di punire anche chi duplica per fini personali, pare sproporzionata tanto rispetto alla tipologia di danno arrecato che rispetto al reale disvalore sociale della condotta. Discutibile è la previsione di sconti di pena per colui che prima che la violazione gli sia specificatamente contestata in un atto dell'autorità giudiziaria, la denuncia spontaneamente o, fornendo tutte le informazioni in suo possesso, consente l'individuazione del promotore o organizzatore dell'attività illecita, di altro duplicatore o distributore, ovvero il sequestro di notevoli quantità di supporti, strumenti o materiali serviti o destinati alla commissione dei reati.

E' agevole in tal caso evidenziare la sproporzione nell'utilizzo di uno strumento, "il pentitismo", sicuramente più adatto e ragionevole per contrastare fenomeni ben più pericolosi quali mafia, traffico di sostanze stupefacenti e terrorismo.

Lo spostamento di interesse dalle libertà fondamentali agli interessi economici è testimoniato da altre disposizioni. Sintomatico di tale impostazione è il fatto che il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) non tuteli solo le persone fisiche ma anche le persone giuridiche, gli enti e le associazioni (art.4 comma 1 lett. b) ed i)).

Il minor peso attribuito ai diritti fondamentali della persona è visibile anche in altre disposizioni, quale ad esempio la norma sull'accesso abusivo, volta a proteggere sulla carta il diritto del singolo

di vivere serenamente nel suo domicilio informatico, che, tuttavia, prevede degli aggravamenti di pena allorquando l'intrusione riguardi sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

Altro fattore da considerare è che la legislazione penale della tecnologie dell'informazione si distingue per l'impiego di un linguaggio "tecnico" sinora sconosciuto nell'ambito dell'ordinamento penale. Le nuove disposizioni si riferiscono a "sistemi informatici e telematici", a "misure di sicurezza", a "programmi informatici, senza mai spiegarne il significato.

Discorso a parte va fatto poi rispetto alle norme penali non espressamente riferite a condotte realizzabili attraverso le tecnologie, è il caso di delitti quali la diffamazione, estorsione, truffa, che essendo a forma libera possono essere realizzati con qualsiasi mezzo e quindi anche attraverso l'informatica e la telematica. In ordine a queste ultime, infatti, il tratto distintivo risiede nel fatto che esse vanno adattate alle nuove fenomenologie attraverso processi interpretativi di aggiustamento.

Come tutto ciò possa influire nelle decisioni dei giudici lo dimostra la lettura di alcune sentenze, dalle quali traspaiono diversi "momenti di condizionamento", alcuni direttamente riconducibili al tenore letterale del disposto normativo, altri al contesto in cui la disposizione deve essere calata, altri ancora ad una visione personale della rete da parte dell'interprete .[21]

Allorquando la condotta non è espressamente regolamentata, il giudice può essere influenzato da valutazioni di carattere tecnico. Rispetto al delitto di violazione di corrispondenza, ad esempio, si può giungere a conclusioni differenti a seconda che si consideri la posta elettronica in tutto e per tutto uguale alla posta tradizionale ovvero si evidenzino eventuali differenze.[22]

Stesso discorso per quanto attiene al delitto di diffamazione via Internet, la cui consumazione si riterrà dimostrata con la semplice prova dell'invio del messaggio ove si consideri la rete strumento analogo ad altri media, ritenendosi, viceversa, necessaria ai medesimi fini la prova dell'avvenuta ricezione da parte di terzi nel caso in cui si reputi la rete mezzo diverso, rispetto al quale la lettura di un 'informazione non può essere presunta.[23]

---

[21] "Applicare una legge non è come risolvere un'equazione algebrica o altro problema di matematica, rispetto alla cui soluzione non v'è alternativa tra il risultato esatto, da un lato, e l'errore dall'altro (l'uno e l'altro egualmente incontrovertibili e dimostrabili matematicamente), non implica tanto una capacità di ragionare, quanto soprattutto una ricchezza di sentimento, perché è quest'ultima che ci guida nel costante sforzo di mantenere il diritto sul binario della Giustizia. Come affermava il Kirchman, le decisioni sulle questioni di diritto (cioè il modo di interpretare e coordinare le leggi)scaturiscono più dal cuore che dalla mente", così R.Borruso, *L'interpretazione della legge e l'informatica*, in R.Borruso, R.Maria Di Giorgi, L.Mattioli, M.Ragona, *L'informatica del diritto*, Giuffrè, Milano,2004, p. 350.

[22] Cfr. ordinanza del 10 maggio 2002 del GIP di Milano, con la quale viene archiviato un procedimento aperto a seguito di denuncia-querela sporta da un dipendente nei confronti del responsabile del reparto e del legale rappresentante della società per violazione di corrispondenza. All'interno di tale provvedimento, infatti, si evidenziano le differenze tra posta tradizionale ed elettronica: "Né può ritenersi conferente ogni ulteriore argomentazione che, facendo apoditticamente leva sul carattere di assoluta assimilazione della posta elettronica alla posta tradizionale, cerchi di superare le strutturali diversità dei due strumenti comunicativi (si pensi, in via esemplificativa, al carattere di "istantaneità" della comunicazione informatica - operante come un normale terminale telefonico - pur in presenza di un prelievo necessariamente legato all'accensione del personal e, quindi, sostanzialmente coincidente con la presenza stanziale del lavoratore nell'ufficio ove è presente il *desk-top* del titolare dell'indirizzo) per giungere a conclusioni differenti da quelle ritenute da questo giudice".

[23] Cfr. sentenza 112/02 del Tribunale di Teramo ove si afferma che : " Né può affermarsi, è da aggiungere, che in tale caso sia possibile presumere la conoscenza del messaggio da parte di terzi, come potrebbe sostenersi nel caso della stampa o della diffusione televisiva ……Infatti del tutto diverso in questi casi è il mezzo di diffusione, rispetto

In che modo la " lettura " delle tecnologie dell'informazione possa influire sull'applicazione della norma viene dimostrato da una serie di decisioni in ordine alla rilevanza penale delle scommesse raccolte in Italia per via telematica e trasmesse con lo stesso mezzo a *bookmaker* presente in un Paese dove quella condotta è ritenuta legittima. Orbene, in ordine a tale materia, se alcune decisioni conferiscono alla rete il ruolo di un semplice mezzo di comunicazione, escludendo il delitto sull'assunto che il gestore dell'*internet point* si limita a consentire la stipulazione a distanza di un contratto di scommessa[24], altre ammettono la sussistenza del delitto reputando la trasmissione via rete condotta concorrente a quella posta in essere all'estero.[25]

Ulteriori problemi interpretativi possono, tuttavia, sorgere, quando il giudice è chiamato ad applicare norme espressamente riferite a condotte realizzate attraverso le tecnologie dell'informazione.

Prendendo, ad esempio, il delitto di accesso abusivo, che punisce l'intrusione all'interno di un sistema informatico o telematico protetto da misure di sicurezza, la sua sussistenza potrà essere affermata o negata anche a seconda del significato attribuito al termine "sistema" - non è , infatti, ancora pacifico se in tale concetto possa rientrare l'impianto televisivo satellitare[26] o il centralino telefonico[27]-, o all'espressione "misure di sicurezza".[28]

Altre questioni interpretative possono dipendere dalla genericità con la quale alcune nome fanno riferimento alle tecnologie. Di fronte alla disposizione che punisce la distribuzione per via telematica di materiale pedopornografico, intendendosi per tale la trasmissione ad un numero indeterminato di destinatari, l'invio all'interno di una *chat* potrà essere valutato diversamente a seconda della volontà e competenza del giudice di comprendere il funzionamento del servizio utilizzato e sottoposto alla sua attenzione.[29]

al quale può ritenersi effettivamente ragionevole dare per provato che un giornale sia letto da più persone o una trasmissione televisiva raggiunga più spettatori. Peraltro quanto alla diffamazione a mezzo stampa va detto che una prima diffusione comunque già si realizza al momento della consegna da parte dello stampatore delle prescritte copie in adempimento dell'obbligo previsto dalla l. 2 Febbraio 1989 n 374, che ovviamente non ha riscontro nel caso in esame per le peculiarità del mezzo tecnico. Nella diffamazione a mezzo Internet quanto alla visibilità del messaggio va evidenziato che nessun sito può essere raggiunto per caso. E' necessario conoscerlo o quantomeno procedere ad una precisa interrogazione di un motore di ricerca. Il motore di ricerca è a sua volta un sito, all'interno del quale è possibile consultare degli elenchi, aggiornati periodicamente, che contengono delle brevi recensioni di ogni sito web e consentono di raggiungerlo grazie ad un collegamento ipertestuale."

[24] Cfr. Tribunale di Santa Maria Capua Vetere sentenza 14 luglio 2000; nella stessa direzione Tribunale di Siena sentenza 23 ottobre 2000.

[25] Cfr. Tribunale del Riesame di Palermo, ordinanza 19 giugno 2000.

[26] Cfr.Cass. Sez.VI n.4389/98;in senso contrario le argomentazioni proposte nella richiesta di archiviazione avanzata dalla Procura di Crotone(PM Torriello)in data 18 marzo 2002.

[27] Cfr. Cass. Sez.VI n.3067/99.

[28] Cfr. sentenza Tribunale di Torino 7 febbraio 1998 e Cass.Sez.V n.12732/00 secondo cui per la sussistenza del delitto basta qualunque misura di protezione, anche esterna; vedi anche sentenza del Tribunale di Roma del 4 aprile 200, Sez.VIII Gip Landi,secondo cui necessitano "mezzi efficaci di protezione".

[29] Cfr. Cass. Sez. III n.5397/01 ove, tra l'altro, si afferma che " Non può però ritenersi che, per la sussistenza del delitto di cui al terzo comma dell'art. 600 ter, cod. pen., sia sufficiente, come a volte invece capita di leggere, la mera circostanza che le foto pornografiche di minori siano veicolate attraverso la rete Internet, a parte che non si comprende che cosa si intenda con tale espressione, data la sua vaghezza. Così, il delitto in esame è certamente configurabile qualora il soggetto, ad esempio, inserisca le foto pornografiche minorili in un sito accessibile a tutti ovvero quando le propaghi attraverso *usenet*, inviandole ad un gruppo o lista di successione, da cui chiunque le possa scaricare. Al converso, pare ipotizzabile non il delitto in esame, ma quello più lieve di cui al quarto comma, quando, ad esempio, il soggetto invii la foto ad una persona determinata allegandola ad un messaggio di posta elettronica. E

Differenti valutazioni possono, infine, dipendere dall'entroterra culturale dello stesso organo giudicante. Il giudice è un uomo ed in quanto tale soggetto con una propria visione del mondo ed inevitabilmente con un suo sentire politico.[30] Piaccia o non piaccia la sua storia può influenzare le sue decisioni, e ciò sovente senza che lo stesso se ne accorga.
Emblematica in tal senso quella sentenza con la quale è stato assolto un extracomunitario sorpreso a vendere *compact disc* contraffatti, ritenendosi applicabile al caso di specie l'esimente dello stato di necessità e ciò dopo aver criticato apertamente i regimi di oligopolio esistenti ed aver rilevato le difficoltà di adattamento in una società siffatta.
Alla luce delle valutazioni svolte in ordine al rapporto intercorrente tra giudice, norma e contesto in cui la stessa va applicata, emerge un ulteriore ruolo delle tecnologie in ambito giuridico: le tecnologie quale "misuratore" della tenuta dell'ordinamento giuridico.
In un recente passato proprio le tecnologie dell'informazione hanno messo in crisi il "mito" della completezza dell'ordinamento giuridico, imponendo la previsione di nuove regole adatte a regolamentare nuove realtà.
Oggi, che le norme ci sono, le tecnologie si pongono come osservatorio dal quale guardare l'impatto effettivo della nuova e precedente legislazione, rilevandone le contraddizioni interne e quelle direttamente riconducibili ai differenti punti di vista degli organi giudicanti.

11. Nuove psicopatologie e ripercussioni sull'accertamento della colpevolezza informatica

Sino ad oggi in ambito penale le tecnologie dell'informazione sono state studiate solo in funzione di come le stesse incidono sulle modalità di aggressione dei beni giuridici meritevoli di tutela. In altre parole sono state viste come un nuovo mezzo per commettere reati.
Da un po' di tempo, tuttavia, alcuni studi nell'ambito della psichiatria, psicologia e criminologia, hanno evidenziato come le tecnologie dell'informazione non incidono esclusivamente sul modo di agire, ma anche sul modo di pensare.
In ambito criminologico, si è sottolineato come un soggetto agisca con minori freni inibitori tanto

nemmeno sembra significativo, per la configurabilità del reato in questione, limitarsi a rilevare che la cessione delle foto è avvenuta attraverso un programma o stanza o canale di discussione (in inglese, *chat line*) del tipo IRC, come quello utilizzato nella specie, o similari, dovendosi invece distinguere l'ipotesi in cui si sia trattato di una sola isolata cessione avvenuta nel corso di una discussione privata con una singola determinata persona, di modo che la foto sia stata di fatto ceduta ad una sola persona e solo questa abbia avuto la possibilità di prelevarla, dall'ipotesi in cui invece la foto sia stata ceduta in un canale aperto a tutti gli utenti, di modo che qualsiasi soggetto si trovi nella stanza o nel canale abbia avuto la possibilità di prelevarla, oppure sia stata ceduta comunque ad una pluralità di soggetti sia pure attraverso una serie di diverse conversazioni private".

[30] "Politica: questa è la parola dirompente che bisogna avere il coraggio di usare in riferimento all'interpretazione delle leggi: interpretare le leggi è in un certo senso, fare politica, anche se nel senso più elevato e nobile che a questa espressione può darsi perché- si torna a ripetere- svolgerla comporta più un impegno del cuore, che non della mente, coinvolge più i sentimenti, le passioni, gli ideali che non asettici ragionamenti: esattamente come avviene nella lotta politica", così R.Borruso, *L'interpretazione della legge e l'informatica*, cit., p. 352.

maggiore sarà l'astrazione della vittima[31]. Si è a tal proposito osservato che è più agevole sul piano motivazionale sottrarre un bene all'interno di una grande struttura piuttosto che sottrarlo sapendo che a pagare le colpe di questo gesto sarebbe una persona ben identificata.
Orbene poiché molti dei reati di nostro interesse si realizzano in rete e, quindi, a distanza, con la conseguenza che l'autore del reato non vede la vittima, è legittimo chiedersi se tale elemento possa un domani essere considerato ai fini della valutazione sull'intensità del dolo e sul grado della colpa ed anche per affermare una maggiore o minore pericolosità sociale.
Sempre in questo ambito si evidenzia come l'utilizzo spasmodico di Internet provoca, ad avviso di alcuni autorevoli studiosi, una dipendenza equiparata a psicopatologie comportamentali come il gioco d'azzardo e la bulimia[32].
All'interno della categoria concettuale della dipendenza telematica definita IAD (*Internet Addition Disorder*) è stata individuata una categoria specifica nota come IRP (*Internet Related Psicopatology*), consistente nell'incapacità di resistere al gioco d'azzardo in rete e nella dipendenza da cyberspazio[33].
Altri esperti si sono spinti più avanti a tal punto da affermare che l'utilizzo del computer possa produrre vere e proprie forme di schizzofrenia[34].
Tali studi possono rappresentare un punto di partenza per valutare se, in alcuni casi, l'utilizzo della rete possa determinare nel soggetto agente un vero e proprio vizio di mente rilevante ai fini della valutazione sulla sua capacità di intendere e di volere così come stabilita dagli artt. 85 e ss. del codice penale.
Sempre questi studi potrebbero spingere a valutare l'applicabilità delle norme che regolano la capacità di intendere e di volere provocate dall'abuso di sostanze stupefacenti ed alcooliche.
Come evidenziato, pare già allo stato dimostrabile che l'uso delle tecnologie produca forme di dipendenza. Tale dipendenza determina sicuramente effetti dannosi nell'individuo a tal punto da sollecitare la nascita di associazioni che si occupano specificatamente della disintossicazione da Internet con sistemi simili a quelli utilizzati per disintossicare gli alcolisti.[35]
A ciò si aggiunga che da tempo negli USA, dove per prima si sono studiati gli effetti delle tecnologie, si parla di "LSD elettronica", mentre si ha notizia che in Giappone sono diffuse particolari applicazioni tecnologiche con il nome significativo di "video droga"[36].
I rischi di conseguenze sulla mente umana, derivanti da abuso di tecnologie, sono ancora più tangibili quando si esaminano le opportunità offerte dai programmi di realtà virtuale.
Questi programmi, che consentono di simulare il reale in modo perfetto, sembrano incidere

---

31 cfr. M.Correra, P. Martucci, *I reati commessi con l'uso del computer-Banche dei dati e tutela della persona*-Cedam, Padova, 1986, p.42 ss.. Sull'argomento cfr anche M.Strano, *Computer Crime*, Apogeo, Milano,2000, p.6.

32 Cfr.: Kimberly S.Young, *Presi nella rete- intossicazione e dipendenza da Internet*, Calderini ediagricole,2000; T.Cantelmi, *"La mente in Internet", una guida alla "psicopatologia delle condotte on line".*

33 Anche in Italia il fenomeno è da qualche anno oggetto di studio ed un certo allarme ha suscitato un recente fatto di cronaca secondo cui il collegamento su Internet, protratto senza sosta per circa tre giorni, avrebbe portato al ricovero in ospedale di un soggetto per disturbi quali stato confusionale, allucinazioni e deliri.

34 S.Turkle, *Vita sullo schermo*, Apogeo,1997.

35 Negli USA sono nate associazioni che mediante terapie di gruppo, analoghe a quelle utilizzate dagli Alcolisti Anonimi tentano di "disintossicare" dalla droga elettronica. La più frequentata si chiama "Caught in the web (intrappolato nella rete).

36 C.Sarzana, *I riflessi giuridici delle nuove tecnologie informatiche*, in *Diritto dell'informazione e dell'informatica*, 1994, p.504-505.

profondamente sulla psiche del soggetto a tal punto da far perdere un certo tipo di sensibilità quando lo stesso agisce nel reale. A tal riguardo è stato osservato come in ambito militare minore sensibilità sia stata dimostrata da quei militari che si erano precedentemente esercitati con programmi di questo tipo[37].Quanto ai programmi di realtà virtuale di contenuto erotico già da tempo ci si interroga se questi possano favorire la commissione di reati a sfondo sessuale.
Alla luce di tali sintetiche considerazioni è possibile immaginare che in sede di applicazione delle norme riguardanti l'imputabilità l'interprete possa seguire tre strade differenti. Potrebbe infatti considerare irrilevante l'incidenza delle tecnologie, negando l'operatività delle disposizioni in parola, come anche valutarla determinante per affermare una totale o parziale non imputabilità, potrebbe, infine, addebitare allo stesso reo la colpa di aver utilizzato la tecnologia proprio per determinarsi una forma di incapacità tale da agevolarlo nella condotta delittuosa[38].

12. La legislazione penale dell'informatica: questioni aperte e prospettive di riforma

L'uso delle tecnologie dell'informazione è attualmente disciplinato da una legislazione ampia ed articolata che consente di punire i diversi reati che in concreto possono realizzarsi.
Come detto attraverso la legge 547, e successive modifiche, sono state introdotte numerose ipotesi di reato. Sono state previste, altresì, ulteriori disposizioni di legge che consentono di sanzionare penalmente fenomeni quali il *cyberterrorismo*, la pedofilia telematica, il *cyberstalking*. A tali disposizioni si aggiungono quelle riferite alla contraffazione del *software* ed alla violazione della *privacy*.
Il vero problema allo stato non è tanto, quindi, quello di introdurre nuove norme, ma di giungere ad una interpretazione delle disposizioni vigenti il più omogenea possibile per evitare quel clima di incertezza che più di una volta è stato registrato.
Occorre che sempre meno siano le opinioni divergenti in ordine alla interpretazione dei termini tecnici, del mezzo utilizzato per commettere il reato, del contesto all'interno del quale la norma va applicata.
E' necessario che tutti i soggetti chiamati ad operare a diverso titolo in questa materia acquisiscano accanto alle conoscenze giuridiche, conoscenze tecniche e di contesto che consentano di interpretare la norma nel modo più corretto possibile.
A tale fine sarebbe utile che i diversi tribunali, ed in particolare quelli ove operano i *pool* contro la criminalità informatica, siano dotati finalmente di un sistema all'interno del quale fare confluire le sentenze di merito in modo da avere costantemente "il polso" degli orientamenti in tale delicato settore.
Considerato che le tecnologie evolvono a ritmo incessante ha fatto bene il legislatore a prevedere norme con un contenuto più ampio possibile in modo di evitare la necessità di "aggiustamenti" quotidiani.

---

[37] C.Sarzana, *I riflessi giuridici delle nuove tecnologie informatiche*, cit., p. 505 nota n.8.

[38] In tal caso troverebbe applicazione l'art.87 c.p.

Ciò comporta, ovviamente, una maggiore responsabilità per l'interprete, il quale dovrà di volta in volta adeguare la norma al nuovo contesto tecnologico davanti ai suoi occhi.
Per un effettivo contrasto della criminalità informatica serve, infine, una maggiore uniformità di vedute in tema di indagini informatiche, ed in particolare regole certe sui requisiti della prova digitale.
Da questo punto di vista occorre prestare maggiore attenzione agli sviluppi della *digital forensic*, così da coniugare nella misura corretta le esperienze di carattere tecnico con il contenuto delle nuove disposizioni riguardanti i mezzi di ricerca della prova.

N. 2 - 2013 · pp. 44-54

Furto d'identità, frodi informatiche e phishing

Marco Schipani

Abstract: Il numero dei furti d'identità in rete negli ultimi anni è cresciuto in modo esponenziale. Nel momento in cui è divenuto più difficile attaccare i *server* centrali di grandi aziende o istituzioni, i cybercriminali hanno deciso di spostare la loro "attenzione" sul punto più debole della catena della sicurezza sulla rete: i singoli internauti. Ciò è in larga parte dovuto al fatto che in rete è sempre più semplice riuscire a sostituirsi all'identità digitale di altri per porre in essere condotte delittuose, evitandone le conseguenze penali. In questo contesto opera il *phishing*, che è una tecnica di ingegneria sociale volta a carpire informazioni personali altrui da poter utilizzare sulla rete con svariate modalità.

Contrastare tale fenomeno è apparso, sin da subito, alquanto problematico, dal momento che nel nostro ordinamento giuridico non esiste una norma che punisca il *phishing* tout court. Dottrina e Giurisprudenza sono tuttavia concordi nel ritenere che le singole condotte in cui può essere scomposto un *phishing attack* spesso possono essere fatte rientrare nell'alveo di norme quali quelle che puniscono la sostituzione di persona, il trattamento illecito di dati, l'accesso abusivo ad un sistema informatico o telematico, la frode informatica. Il legislatore è ultimamente intervenuto in materia con l'art. 9 del D.L n. 93 del 14 agosto 2013. Attraverso tale norma si è tentato di combattere il fenomeno del *phishing* con l'introduzione del reato di frode informatica commessa con sostituzione d'identità digitale.

Parole chiave: identità digitale, identity crime, phishing, sostituzione di persona, accesso abusivo ad un sistema informatico o telematico, trattamento illecito di dati, frode informatica commessa con sostituzione d'identità digitale.

1. Il furto d'identità

L'evoluzione delle tecnologie delle informazioni ha finito con il trasformare la rete in un luogo virtuale in cui è sempre più agevole porre in essere molteplici condotte delittuose. La rete, tra

Articolo pervenuto il 2 ottobre 2013, approvato il 28 novembre 2013

l'altro, attualmente non è più solo uno strumento per commettere reati, ma è divenuta essa stessa l'ambiente in cui trovano spazio nuovi comportamenti illeciti.
Il cyberspazio, inteso come luogo immateriale che mette in comunicazione una miriade di *device* di tutto il mondo in un'unica rete che permette agli utenti di interagire tra loro, d'altra parte, viene considerato oggi come il quinto dominio.
Il nuovo contesto tecnologico, la diffusione capillare di Internet e fenomeni quali i *social network* hanno fatto sì, infatti, che l'attenzione dei criminali si rivolgesse verso nuove forme di *cybercrime* che hanno ragione di esistere in quanto sfruttano l'immaterialità del cyberspace.
Tali reati, proprio in ragione del contesto immateriale in cui si inseriscono, pongono particolari problematiche in ordine all'individuazione del *tempus* e del *locus commissi delicti*, tant'è che autorevole dottrina ritiene gli stessi segnalino il passaggio dalla fase dei "*computer crimes*" a quelli "dell'epoca di internet"[1].
Quanto detto vale innanzitutto per quelle nuove forme di crimini informatici che si sostanziano in abusi di profili identitari altrui nel *cyberspace*, ovvero il furto d'identità digitale[2], il *phishing*, l'abuso di identità "virtuale", le frodi identitarie, fenomeni questi che possono essere ricondotti nella categoria generale degli "*identity crime*".
Tale categoria comprende in pratica tutte quelle condotte delittuose che comportano una aggressione all'identità digitale altrui, dovendosi intendere con tale espressione quell'insieme di informazioni presenti online e relative ad una persona, un ente, un *brand*, ecc[3].
La riconduzione di detti fenomeni in un'unica categoria, d'altra parte, appare giustificata anche dal fatto che gli stessi hanno in comune tra di loro il fatto di presentarsi come una iniziale raccolta di dati di un ignaro internauta (da semplici informazioni personali a passwords di accesso a servizi di *home banking*, ecc.), da utilizzare successivamente per sostituirsi ad esso e compiere le più svariate attività illecite sulla rete, così nascondendo nel contempo la propria identità.
Essenzialmente si tratta, pertanto, di comportamenti volti a reperire quei dati necessari per utilizzare l'identità digitali di altri sulla rete, cui consegue normalmente un danno patrimoniale per la vittima di tali condotte.
Se d'altra parte la sostituzione di persona è un fenomeno antico, oggi la tendenza ad assumere l'identità altrui è sicuramente favorita dalle caratteristiche del *cyberspace*, dove si muovono soggetti tra i quali sono assenti contatti materiali e che hanno una scarsa conoscenza delle insidie che si nascondono sul *web*.
Gli "*identity crime*" hanno avuto una espansione vertiginosa negli ultimi anni anche in ragione della sempre maggiore importanza, soprattutto economica, dei dati personali di coloro che navigano sulla rete e dell'inadeguato trattamento degli stessi proprio da parte di chi dovrebbe proteggerli. Occorre considerare, ad esempio, che per le aziende che operano sulla rete è fondamentale conoscere i gusti dei consumatori al fine di rendere il loro marketing più efficiente. Non è un

---

1 Picotti, L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Picotti, L., *Il diritto penale dell'informatica nell'epoca di Internet*, Cedam, Padova, 2004, p. 21;

2 Cipolla, P., *Social network, furto d'identità e reati contro il patrimonio*, in Giur. merito 2012, 12, pag. 2672; G. Resta, *Identità personale e identità digitale*, in Dir. informatica, 2007, 03, pag. 511;

3 Flick, C., *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*, in Riv. inf. e informatica, 2008, 4-5, pag. 526;

caso quindi se oggi esiste un vero e proprio mercato dei dati personali, il cui volume d'affari è in continua crescita[4].
Per comprendere il valore economico dei dati oggetto degli identity crime, basta d'altra parte pensare che il furto di dati subito dal Playstation Network della Sony nell'aprile del 2011 ha comportato per il colosso giapponese una perdita di 171 milioni di dollari per l'anno fiscale 2011 ed un impatto indiretto, in termini di mancato guadagno, stimabile addirittura sopra i 200 milioni[5].
In ogni caso la comparsa di tali fenomeni sulla rete ha avuto sicuramente l'effetto di incidere negativamente sul senso di sicurezza di chi naviga in Internet e ciò non può che avere ripercussioni negative sullo sviluppo economico della rete stessa. Si pensi, al riguardo, agli effetti che tali condotte delittuose possono avere sulla fiducia delle persone verso i servizi di *home banking* e di *e-commerce*.
Se, peraltro, l'obiettivo perseguito dai cybercriminali attraverso tali condotte delittuose é sempre quello di entrare in possesso di informazioni personali altrui, le modalità con le quali queste possono essere sottratte sono svariate. Si va, infatti, dall'utilizzo di tecniche di ingegneria sociale sulla rete o attraverso di essa (*phishing*), all'intervento forzato sui sistemi telematici altrui (*hackering*), alla sottrazione dei dati necessari attraverso documenti smarriti o addirittura rinvenuti nella spazzatura (*trashing*), all'utilizzo di elenchi pubblici, come, ad esempio, quelli telefonici.
Attraverso tali tecniche si potrà duplicare l'identità digitale altrui o anche creare una nuova identità digitale da utilizzare successivamente per porre in essere ulteriori condotte illecite, che, anche se circoscritte alla rete dal punto di vista operativo, saranno sicuramente destinate ad esplicare i lori effetti nel mondo reale.
Il reo, infatti, potrebbe impossessarsi delle credenziali di accesso del malcapitato ai suoi conti correnti e così sottrargli del denaro con semplici operazioni bancarie online, acquisire i dati delle sue carte di credito così da poterle utilizzare successivamente, coinvolgerlo per realizzare operazioni di riciclaggio, farlo incriminare per reati non commessi.
Tra le modalità attraverso le quali i cybercriminali sono ormai soliti entrare in possesso di dati personali altrui per creare o clonare identità digitali da utilizzare in rete, la più pericolosa, per le tecniche con cui viene posta in essere, è il *phishing*.

2. Il phishing

Negli ultimi anni, come detto, abbiamo assistito ad un notevole incremento di frodi on line basate sul furto di informazioni personali. Per realizzare ingegnose *identity related fraud* con i dati personali altrui sottratti sempre più spesso i cybercriminali si servono della tecnica del *phishing*, tecnica questa particolarmente pericolosa perché molto spesso realizzata con la collaborazione della vittima stessa.
Il termine *phishing*, comparso sulla rete per la prima volta intorno al 1996, è stato coniato parafrasando il verbo inglese "*to fish*", che significa pescare. Tramite questa tecnica, infatti, i

[4] Cipolla, op. cit., pag. 516.

[5] Hachman, M., *PlayStation Hack to Cost Sony $171M; Quake Costs Far Higher*, su pcmag.com http://www.pcmag.com/article2/0,2817,2385790,00.asp

cybercriminali cercano appunto di "pescare" i dati personali di utenti della rete per successivamente utilizzarli per le più svariate attività delittuose.
I primi attacchi con questa tecnica, sono stati realizzati nel Nord America, tant'è che già nel 2008 negli Usa il Senato ha deciso di adottare uno specifico "*Anti-phishing Act*". In Italia, invece, il *phishing* è apparso per la prima volta nel 2005 quando numerosissimi internauti ricevettero sulle loro caselle di posta elettronica una email civetta che sembrava provenisse da Poste Italiane.
Con il *phishing* i cybercriminali, per raggiungere i loro loschi obiettivi, si affidano a raffinate tecniche di ingegneria sociale, si "concentrano" sullo studio del comportamento di un dato individuo al fine di carpirne le informazioni personali[6].
Il *phishing* pertanto può essere definito come "una metodologia di comportamento sociale indirizzata a carpire informazioni personali o abitudini e stili di vita"[7]. Attraverso tale tecnica si induce l'utente a fornire dati personali che consentono l'accesso ad informazioni riservate (*identity theft*), ad esempio le credenziali di accesso a servizi di *home banking*, in modo tale da utilizzarli per successivamente realizzare una frode identitaria (*identity fraud*).
In tali direzione va la definizione fornita dalla nostra Suprema Corte, secondo la quale "il *phishing* è quell'attività illecita in base alla quale, attraverso vari stratagemmi (o attraverso fasulli messaggi di posta elettronica, o attraverso veri e propri programmi informatici ed *malware*) un soggetto riesce ad impossessarsi fraudolentemente dei codici elettronici (*user* e *password*) di un utente, codici che, poi, utilizza per frodi informatiche consistenti, di solito, nell'accedere a conti correnti bancari o postali che vengono rapidamente svuotati"[8].
Nel momento, in pratica, in cui diveniva sempre più difficile attaccare con successo i server contenenti i dati di migliaia di utenti, i cybercriminali hanno pensato di rivolgere le loro attenzioni all'anello debole della catena della sicurezza: gli utenti finali. Così facendo, infatti, invece di affrontare server dotati di più livelli di sicurezza, gestiti da soggetti che hanno tutto l'interesse a che gli stessi non vengano violate, si è passati ad attaccare i singoli internauti, che molto spesso hanno scarse conoscenze informatiche.
Benché attualmente il *phishing* possa essere realizzato attraverso varie tecniche, all'inizio i *phishing attacks* erano posti in essere attraverso l'invio casuale di email, con la tecnica dello *spamming*[9], ad un elevato numero di internauti. Tali comunicazioni elettroniche erano camuffate di modo che sembrassero provenire soprattutto da istituti bancari o da società di carte di credito, in modo da indurre l'utente a compiere una particolare operazione attraverso la quale involontariamente lo stesso forniva i propri dati personali.

---

[6] Cajani, F., Costabile, G., Mazzaraco, G., *Phishing e furto d'identità digitale - Indagini informatiche e sicurezza bancaria*, Milano, Giuffrè, 2008, pag. 12.

[7] Flor, R., *Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente*, in Riv. it. dir. proc. pen., 2007, pag. 900.

[8] Vedi Cass. Pen., Sez. II, sentenza n. 9891/2011, nello stesso senso vedi Trib. Monza, sentenza del 7 maggio 2009, in cui si legge "la condotta cosiddetta di "phishing" consiste nel pescare, mediante abusivo inserimento nel sistema informatico di una istituzione finanziaria o mediante false email dirette ai clienti delle banche o delle poste, i dati significativi dei rapporti di conto corrente intrattenuti dagli stessi, dati che vengono successivamente utilizzati in modo fradudolento …"..

[9] Lo *spamming* è l'invio massivo di messaggi indesiderati, molto spesso commerciali, che viene attuato soprattutto attraverso i messaggi di posta elettronica, ma che comunque può essere posto in essere ricorrendo a qualunque sistema di comunicazione

Normalmente per convincere il malcapitato a fornire i propri dati personali, tali messaggi segnalano all'utente presunti malfunzionamenti al proprio servizio di home banking per risolvere i quali lo stesso viene indotto a seguire un link contenuto nella email civetta, che lo spingerà a fornire i propri dati o le proprie informazioni

Ovviamente tanto più saranno minacciosi ed allarmanti i toni della email civetta e maggiori saranno le possibilità che il malcapitato possa cadere nel tranello.

A questa prima tipologia di *phishing*, comunemente detta *phishing* ingannevole o *deceptive phishing*, con il tempo se ne sono aggiunte diverse altre. La sempre maggiore informatizzazione degli strumenti di gestione dei conto correnti e di pagamento sulla rete ha poi finito con il far esplodere il fenomeno.

Attualmente il settore più colpito è quello dei servizi di pagamento, seguito a ruota da quello dei servizi finanziari[10].

3. Tipologie e fasi del phishing

Dalla sua comparsa sulla rete abbiamo assistito ad una evoluzione delle modalità con le quali vengono posti in essere dai cyber criminali gli ormai temutissimi *phishing attacks*.

Nonostante comunque oramai il *phishing* possa oggi essere posto in essere con le più svariate tecniche, all'interno di un *phishing attack* è possibile distinguere varie fasi[11].

Il *phisher*, infatti, dovrà innanzitutto individuare il bersaglio del suo attacco e scegliere la tecnica da adoperare per conseguire l'obiettivo voluto (*Planning*); si preoccuperà poi di predisporre gli strumenti necessari per programmare l'attacco (*Setup*). Solo dopo queste due fasi preparatorie, il *phisher* passerà alla fase dell'attacco vero e proprio, che potrà essere realizzato attraverso l'uso di *email* civetta, *dialer*, *malware*, *trojan*, *social network* (*Attack*).

Una volta riuscito l'attacco si passa alla quarta fase (*Collection*), la più importante: il *phisher*, stabilito il contatto con l'utente attraverso le più svariate tecniche di ingegneria sociale, si impossesserà dei dati del malcapitato.

Ottenute le informazioni di cui ha bisogno, il cybercriminale utilizza i dati ottenuti per le più svariate attività fraudolente (*Fraud*) che, sebbene realizzate sulla rete, sono comunque destinate ad avere effetti nel mondo reale, effetti spesso molto dolorosi per la vittima dell'attacco di *phishing*.

Realizzata la frode, nell'ultima fase (*Post attack*) il *phisher* provvede a cancellare le sue tracce così da rendere ancor più difficile la sua individuazione.

Per quanto riguarda le modalità attraverso le quali possono essere realizzati tali attacchi, ben presto i cybercriminali hanno abbandonato l'invio massivo di email attraverso la tecnica dello spamming, e sono passati ad utilizzare software malevoli (*malware*), *trojan* o *spyware*.Questi si sono dimostrati sin da subito più difficile da combattere, poiché sono in grado di operare sul computer della vittima senza che questa se ne accorga.

---

[10] Vedi il report redatto dalla APWG (Anti-phishin Working Group), pubblicato il 30 luglio 2013, e disponibile all'indirizzohttp://docs.apwg.org/reports/apwg_trends_report_q1_2013.pdf;

[11] Cajani, F., op. cit., pag. 16;

Il *malware* può, peraltro, assumere varie forme, tant'è che possiamo distinguere all'interno di questa tipologia di *phishing*, quello basato su dei *keylogger* (o *screenlogger*), quello che sfrutta i dirottatori di sessione (*session Hijacking*) o i *web trojans*, o, ancora, quello posto in essere con attacchi di riconfigurazione del sistema.
Abbiamo poi il *phishing* basato sui motori di ricerca e quello realizzato con la tecnica del "man in the middle".

4. Il phishing ed il diritto penale vigente

Le svariate modalità con cui possono essere portati a termine i *phishing attacks* hanno posto non pochi problemi al momento di inquadrare tale fenomeno all'interno di specifiche fattispecie penali.
Innanzitutto è opportuno precisare che nel nostro ordinamento giuridico non esiste un reato che prenda in considerazione in maniera specifica il *phishing*, anche se, come già detto, con il D.L. n. 93 del 14 agosto 2013, con l'art. 9 è stato introdotto il reato di frode informatica commessa con sostituzione d'identità digitale.
Un'attenta analisi delle condotte in cui possono essere scomposti i *phishing attacks*, ci permette in ogni caso di comprendere agevolmente che le stesse, singolarmente considerate, possono essere ricondotte a diverse norme incriminatrici.
Oltre che a specifiche fattispecie penali, talvolta il *phishing* potrà essere altresì ricondotto anche ad illeciti civili. Si pensi al riguardo all'art. 122 del Codice della privacy, con il quale si impedisce a chiunque l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente; o all'art. 15 del Codice Privacy, che punisce, invece, con un risarcimento ai sensi dell'art. 2050 del codice civile, chiunque arrechi un danno "per effetto del trattamento di dati personali".
Per quanto attiene, invece, l'inquadramento del *phishing* in specifiche norme penali, come detto, occorrerà "frazionare" il *phishing attacks* in singole condotte, sempre rispettando, ovviamente, i principi fondamentali del diritto penale.
Di fronte alle singole condotte in cui potrà essere un *phishing attack* occorrerà di volta in volta stabilire se le stesse possano essere inquadrate in specifiche norme incriminatrici, quali quelle che puniscono la sostituzione di persona (art. 494 c.p.), l'accesso abusivo in un sistema telematico o informatico (art. 615 *ter* c.p), la frode informatica (art. 640 *ter* c.p.), il trattamento illecito di dati (art. 167 D. Lg. 196/2003).
Un discorso a parte va fatto invece per il reato introdotto con il D :l del 14 agosto 2013.

5. Phishing e sostituzione di persona

Nella fase iniziale di un *phishing attack*, il cybercriminale per "far abboccare" le sue vittime, molto spesso forma ed invia messaggi di posta elettronica apparentemente provenienti da mittenti "reali".
Tale attività, che attiene soprattutto al *deceptive phishing*, è stata considerata dalla giurisprudenza della

Suprema Corte come integrante, in alcuni casi, gli estremi del delitto di sostituzione di persona, punito dall'art. 494 c.p..

La condotta tipica di tale norma si realizza nell'indurre taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno.

Stante la sua formulazione, l'art. 494 c.p. potrebbe trovare applicazione, *in primis*, allorquando il *phisher*, nel preparare le sue false email, utilizzi gli estremi identificativi di un mittente reale, così attribuendosi un falso nome.[12]

La Corte di Cassazione ha ritenuto sussistente tale fattispecie penale, d'alta parte, nel caso di chi provvede a creare un account di posta elettronica, apparentemente intestato ad altri, da utilizzare successivamente per allacciare rapporti con diversi utenti[13].

In tale sentenza leggiamo, infatti, che "oggetto della tutela penale, in relazione al delitto preveduto nell'art. 494 c.p., è l'interesse riguardante la pubblica fede, in quanto questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali. E siccome si tratta di inganni che possono superare la ristretta cerchia d'un determinato destinatario, così il legislatore ha ravvisato in essi una costante insidia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome"[14].

Più recentemente sul punto la Cassazione ha confermato che "integra il reato di sostituzione di persona, di cui all'art. 494 c.p., la condotta di colui che crei ed utilizzi un account di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete internet, nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese"[15].

Quanto detto vale ovviamente per i casi in cui il phisher assuma una identità comunque riferibile ad una persona determinata.

Qualora la persona sostituita rimanga, invece, assolutamente indeterminata, ad esempio nel caso in cui come mittente appaia un organismo, una istituzione, una società, sembrerebbe da escludere l'applicazione della norma di cui all'art. 494 c.p.[16] In questi casi non è possibile parlare di sostituzione della propria all'altrui persona[17].

Al di là degli spunti offerti in tal senso dalla dottrina, non mancano pronunce nella Giurisprudenza di merito, in cui il *phisher*, è stato ritenuto responsabile del delitto di cui all'art. 494 c.p. anche con l'invio di false email, che rappresentavano problemi di sicurezza, e la creazione di false pagine web, in tutto simili a quelle di istituti di credito di cui la vittima era cliente, pur essendo, pertanto, la persona sostituita indeterminata[18].

---

12 Flor, op. cit., pag. 901.

13 Cass. Pen., Sez. V, sentenza n. 46674/2007.

14 Cass. Pen., Sez. V, sentenza n. 46674/2007.

15 Cass. Pen., Sez. III, sentenza n. 12479/2011.

16 Cosseddu, A., *Il cittadino nella "rete" informatica: tutela penale e limiti del sistema* su www.dirittoestoria.it

17 Flor., op. cit,, pag. 903.

18 Vedi Trib. Milano, sentenza del 7 ottobre 2011, Pres. Pellegrino, in cui si legge che "risponde dei delitti di sostituzione di persona (art. 494 c.p.), accesso abusivo ad un sistema informatico o telematico (art. 615

In ogni caso vi è chi sottolinea che l'applicazione della norma in concreto può presentare diverse problematiche anche in ordine alla realizzazione dell'evento consumativo del reato, che consiste nell'induzione in errore di taluno, di cui ci si chiede la compatibilità con l'esecuzione automatizzata di richieste inoltrate ai sistemi informatici[19].

Da scartare, invece, che la condotta del *phisher*, in casi come quello in esame, possa integrare i reati di cui all'art. 617 bis, in materia di falsificazioni del contenuto di comunicazioni informatiche, ed all'art. 491 bis c.p., in materia di falsi aventi ad oggetto documenti informatici[20].

Ad ogni modo il *phisher*, per acquisire i dati personali di ignari utenti della rete, come spiegato in precedenza, potrebbe non ricorrere alla formazione di false email provenienti apparentemente da mittenti reali, ma servirsi di un *malware*.

In questo caso la sua condotta integrerà gli estremi della fattispecie di cui all'art. 615 *quinques* c.p., che punisce la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico[21].

6. Phishing e trattamento illecito di dati

Discussa è, invece, la possibilità di applicare le norme penali in materia di trattamento di dati personali alla condotta del *phisher* che, stabilito il contatto con la vittima del suo attacco, non importa se con false email, *malware* o altro, ne raccolga i dati in vista del loro impiego fraudolento nel cyberspace.

Se, infatti, le operazioni che il *phisher* pone in essere, in particolar modo nella fase detta "*collect*", hanno per oggetto i dati personali del malcapitato, la sua condotta potrebbe integrare gli estremi del reato di trattamento illecito di dati di cui all'art. 167 del Codice della Privacy[22].

In particolare, secondo alcuni autori, nel momento della raccolta dei dati dell'utente, il *phisher* porrebbe in essere un trattamento di dati in violazione con quanto disposto dall'art. 11 lett. a) D. Lgs 196/2003, che impone che i dati vengano trattati in modo lecito e secondo correttezza[23].

Tale soluzione presenterebbe problemi di concreta applicabilità, in particolar modo, con riguardo alla possibilità di individuare uno specifico nocumento in relazione alla condotta in esame, nonché considerato che una applicazione di tale norma a casi come quelli in esame sembrerebbe esclusa dall'art. 5 comma 3 del D. Lgs. 196/2003, che stabilisce che il trattamento di dati personali

ter c.p.) e truffa (art. 640 c.p.) chi, avvalendosi delle tecniche del c.d. *phishing*, mediante artifici e raggiri realizzati attraverso l'invio di false e-mail e la creazione di false pagine *web* in tutto simili a quelle di primari Istituti di Credito, dopo aver indotto in errore l'utente ed essersi fatto rivelare le credenziali di accesso, si introduca nel servizio di home banking della vittima per effettuare operazioni di prelievo o bonifico *on line* non autorizzate".

[19] Flor, op. cit., pag. 903.

[20] Cajani, F., op. cit., pag. 117, 118, vedi anche Corasaniti, G., *La tutela della comunicazione informatica e telematica* in AA. VV., *Profili penali dell'informatica*, 1994, pag. 117 ss..

[21] Pecorella, C., *Diritto penale dell'informatica*, Cedam, pag. 235 e ss..

[22] Bovino, L., *Phishing: aspetti legali*, su www.anti-phishing.it.

[23] Bovino, L., op. cit..

effettuato da persone fisiche per fini esclusivamente personali non è soggetto all'applicazione delle norme del codice della privacy se i dati non sono destinati ad una comunicazione sistematica o alla diffusione[24].

7. Phishing ed accesso abusivo

Indipendentemente dalla tecnica di ingegneria sociale utilizzata, l'obiettivo più ambito da parte dei *phisher* è rappresentato sicuramente dalle credenziali di accesso ai servizi di *home banking* delle vittime dei loro attacchi.

E' evidente, tuttavia, che la condotta del cybercriminale che utilizzi le credenziali di accesso del malcapitato per accedere al suo servizio di *home banking*, protetto da misure di sicurezza e messo a sua disposizione dalla Banca, integri gli estremi del reato di cui all'art. 615 *ter* c.p., l'accesso abusivo a un sistema informatico o telematico.

A tutela del "domicilio informatico", con tale norma il Legislatore ha inteso punire chiunque si introduca abusivamente, o si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo, in un sistema informatico o telematico, che sia protetto da misure di sicurezza.

Ricorrerà, tra l'altro, l'aggravante di cui al comma 2 numero 3 dell'art. 615 *ter* c.p. allorquando il *phishing attack* abbia avuto come effetto quello di bloccare, seppur momentaneamente, l'accessibilità da parte della vittima all'account riservato oggetto dell'attacco.

Solo nell'ipotesi in cui l'accesso abusivo del *phisher* abbia avuto ad oggetto sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico ricorrerà l'ipotesi aggravata di cui al comma terzo.

Non vi sono dubbi, in ogni caso, in ordine all'abusività della condotta del cyber criminale che accende ad una area riservata al controllo della propria vittima, senza averne titolo alcuno e contro la volontà del titolare, eludendo le procedure di sicurezza predisposte per tutelare i dati in essa contenuti.

Nel momento in cui il *phisher* non si limiterà ad accedere all'account riservato del malcapitato, ma manipolerà i dati in esso contenuti, la sua condotta integrerà gli estremi del reato di frode informatica punito dall'art. 640 *ter* c.p., che analizzeremo tra breve.

D'altra parte in un *phishing attack* appare difficile immaginare un accesso abusivo cui non segua anche una alterazione o, comunque, un intervento sul sistema informatico oggetto dell'attacco, se non altro in quella fase (detta "*Post Attack*") in cui il *phisher* interviene per nascondere le tracce dell'accesso abusivo realizzato.

A tal proposito la Corte di Cassazione ha chiaramente affermato che i due reati possono concorrere, avendo gli stessi diversi presupposti giuridici[25]. La condotta di accesso non possiede, comunque, tutti gli elementi puniti dal reato di frode informatica, che richiede, come vedremo, per la sua sussistenza, una manipolazione senza diritto, realizzata con qualsiasi modalità, su dati,

[24] Bellazzi, G., *Aspetti legali del phishing*, Milano, Seminario Clusit, 2006.

[25] Cass. Pen., Sez. II, sentenza n. 9891/2011.

informazioni o programmi[26].
Per quanto attiene le differenze fra le due ipotesi criminose, la Giurisprudenza di Legittimità, ha chiarito che le stesse si ricavano in ogni caso "dalla diversità dei beni giuridici tutelati, dall'elemento soggettivo e dalla previsione della possibilità di commettere il reato di accesso abusivo solo nei riguardi di sistemi protetti,caratteristica che non ricorre nel reato di frode informatica"[27].

8. Phishing e frode informatica

Come detto, nel momento in cui il *phisher* non si limita ad accedere al servizio di home banking del malcapitato, ma manipola i dati in esso contenuti, con la sua condotta integrerà altresì gli estremi dell'art. 640 *ter* c.p..
Tale reato ha la stessa struttura del reato di truffa di cui all'art. 640 c.p., in entrambi l'evento tipico è l'ingiusto profitto con il danno altrui. Ciò che li distingue é il fatto che l'attività fraudolenta poste in essere dall'agente nella frode informatica non investe la persona, come nel caso della truffa, ma il sistema informatico. A differenza di quanto accade nella truffa comune, la condotta offensiva nel reato di cui all'art. 640 *ter* c.p., infatti, non interviene sulla sfera di libera formazione ed autodeterminazione della volontà del soggetto passivo, ma sul corretto e fedele funzionamento di un sistema informatico[28].
Con il reato di truffa la frode informatica ha, invece, in comune il trattamento sanzionatorio e la previsione di una ipotesi aggravata dagli stessi elementi.
La condotta del *phisher* che, avendo carpito i dati di ignari utenti della rete, li utilizzi per accedere ad aree riservate senza averne titolo, per sottrarre o manomettere i dati in esse contenuti, rientra nell'alveo delle condotte punite dall'art. 640 *ter* c.p..
A tal riguardo, d'altra parte, la Corte di Cassazione in una recente pronuncia ha affermato che la condotta del *phisher* integrerebbe gli estremi dell'art. 640 *ter* c.p. in quanto la stessa altro non è se non un intervento senza diritto su informazioni contenute in un sistema informatico[29].
Oltre che nell'ultima fase di un *phishing attack* ci si é interrogati sulla possibilità che il reato di frode informatica ricorra anche nelle fasi iniziali dello stesso, ovvero quando il *phisher* cerca di far "abboccare" al suo amo ignari utenti della rete.
Se, infatti, il reato non sussiste allorché il cybercriminale si limiti ad inviare un messaggio di posta elettronica, contenente un link che conduce ad una pagina *web* non autentica per indurre l'utente a rilevare i propri dati personali[30], un discorso diverso va fatto, invece, per il *phishing* basato su di un *malware*.
In tal caso il ricorso ad un software malevole che va ad autoinstallarsi sul personal computer del

---

[26] Vedi Cass., 2672/2003 riv. 227816; Cass., 1727/2008 riv. 242938.

[27] Cass. Pen., Sez. V, sentenza n. 2672/2004.

[28] Picotti, L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di Internet*, Cedam, 2004, pag. 55

[29] Cass. Pen., Sez. II, sentenza n. 9891/2001.

[30] In quanto in tal caso la condotta del *phisher* non si concretizza in un intervento senza diritto o in una alterazione del funzionamento del sistema informatico oggetto dell'attacco.

malcapitato, potrebbe integrare gli estremi del reato di frode informatica, in quanto comunque, con la sua condotta, il *phisher* provvede ad inserire un elemento logico senza il consenso espresso o tacito dell'utente[31].

9. Frode informatica commessa con sostituzione d'identità digitale e prospettive di riforma

Come più volte accennato, manca nel nostro ordinamento una norma che punisca tout court il *phishing*. Il legislatore ha tentato di colmare, in parte, tale vuoto con l'introduzione, attraverso l'art. 9, co. I, lett. a) del D.L 19 agosto 2013, di una nuova norma incriminatrice rubricata "Frode informatica commessa con sostituzione d'identità digitale". Tale decreto, nonostante al momento della pubblicazione non sia stato ancora convertito in legge, necessita la nostra attenzione in quanto quantomeno indica la via che intende seguire il nostro Legislatore per combattere il fenomeno del *phishing*.

A tal riguardo preme evidentemente segnalare che anziché fare riferimento al reato di cui all'art. 494 c.p., aderendo all'impostazione seguita dalla nostra Suprema Corte, il Parlamento ha pensato di poter arginare i *phishing attacks* intervenendo sul reato di frode informatica.

E' stata, pertanto, introdotta dopo il secondo comma dell'art. 640 *ter* c.p. un'ipotesi aggravata di frode informatica, punita con la reclusione da due a sei anni e della multa da euro 600 a euro 3.000, che ricorre allorquando il fatto è commesso con sostituzione dell'identità digitale in danno di uno o più soggetti.

La scelta del legislatore non pare comunque particolarmente felice: sarebbe stato, infatti, forse più opportuno per reprimere le condotte in cui normalmente si concretizza un *phishing attack*, prevedere una autonoma e distinta norma incriminatrice che, sotto il profilo della condotta, anziché fare riferimento al delitto di "frode informatica", si rifacesse all'art. 494 c.p. in materia di sostituzione di persona.

D'altra parte ciò che caratterizza i *phishing attacks*, e che ci permette di ricondurre all'interno di questa unica categoria una molteplicità di attacchi informatici aventi caratteristiche diverse, è il furto d'identità digitale, ovvero *l'identity theft*.

L'aggressione diretta al profilo identitario virtuale di una persona deve essere oggetto diretto di tutela, indipendentemente dal fatto che il furto d'identità sia sempre strumentale alla commissione di altri reati, che possono essere sia cibernetici, anche "tradizionali"[32]. Si riuscirebbe, d'altra parte, ad ottenere migliori risultati nella lotta agli *identity abuse* se la risposta sanzionatoria penale non arrivasse solo nelle fasi finali di un *phishing attack*.

---

[31] Flor, op. cit., pag. 905.

[32] Flor, op. cit., pag. 918.

N. 3 - 2013 · pp. 55-67

La Pornografia Virtuale

Isabella De Vivo

Abstract: Alla legge n. 269/1998 si deve l'introduzione nel codice penale delle fattispecie di cui agli artt. 600 *ter* e 600 *quater* , norme che consentono di punire la "distribuzione" e la "cessione" di materiale pedopornografico in internet, nonché la condotta di mera "detenzione" .Con la successiva modifica , introdotta con l.38 /2006, il raggio d'incriminazione viene esteso fino a comprendere le condotte aventi ad oggetto immagini c.d. "pseudo-pornografiche". Sono tali ai sensi dell'art. 600 *quater1* , le immagini realizzate attraverso mere elaborazioni grafiche e che pertanto prescindono da un effettivo sfruttamento sessuale di soggetti minori. La disposizione è tuttora oggetto di forti rilievi critici . Controversa è infatti, la natura del bene giuridico sotteso alla tutela penale, da cui le difficoltà di fornire una chiave di lettura che renda il dettato normativo compatibile con il principio costituzionale di necessaria offensività del reato.

Parole Chiave: Internet, pedofilia telematica, materiale pedopornografico, pornografia virtuale.

Sommario: 1.Pedopornografia in rete e normativa penale; 2.l'art.600 quater1: la c.d. pseudo-pornografia; 3. Le ragioni addotte a sostegno dell'incriminazione di cui all'art.600quater1;4. Profili di sospetta illegittimità costituzionale dell'art. 600quater 1; 5. Le ricostruzioni interpretative proposte in dottrina; 6. La pornografia virtuale in rapporto alla libertà informatica e telematica ex art. 21 della Costituzione.

1. Pedo-pornografia in rete e normativa penale

La tutela dei minori in Internet rappresenta una delle più delicate e controverse problematiche legate alla comunicazione telematica e dunque al c.d. *cyberspace*: lo spazio virtuale che superando i confini territoriali non solo nazionali, costituisce una dimensione globale ed aperta per lo svolgersi dei rapporti sociali, ivi compresi quelli di rilievo giuridico, nonché illeciti. Come noto, in Italia non vi era una disciplina penale specificamente destinata a proteggere i minori nel loro sviluppo psico-fisico da indebiti sfruttamenti della loro sessualità. La novella legislativa del 1998 n. 269 ,recante "norme contro lo sfruttamento sessuale della prostituzione, della pornografia, del turismo sessuale in danno dei minori, quali nuove forme di riduzione in schiavitù" fa un grande passo in questo senso: segnalandosi come una delle prime leggi emanate in tale materia in Europa, introduce tra l'altro nel codice penale norme che consentono di punire la "distribuzione e cessione" di materiale pedopornografico in internet, nonché la "detenzione" all'interno del proprio computer.
Tra le disposizioni introdotte, sono strettamente riconducibili alla c. d. pedofilia telematica quelle di cui agli artt. 600 *ter* e 600 *quater* c. p. fattispecie da ultimo perfezionate dalla recente novella :

Articolo pervenuto il 7 ottobre 2013, approvato il 28 novembre 2013

la L. n. 38 del 2006 ,recante "disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo internet",che oltre a modificarne il testo originario viene ad ampliarne lo spettro repressivo attraverso l'introduzione con l' art. 600 *quater1* del concetto di pornografia virtuale , "riscrivendone" ,in parte , l'oggetto materiale del reato.
Non si nega tuttavia, come gli interventi succedutisi in materia siano stati caratterizzati da scarsa chiarezza sistematica, determinando lacune ed incoerenze sia sotto il profilo dei beni giuridici da proteggere, sia sotto quello della tecnica di formulazione delle fattispecie incriminatrici ed in particolare per ciò che riguarda la disposizione da ultimo citata e che di seguito verrà esaminata: la c.d. "pseudo-pornografia"[1].

2. L'art. 600 quater 1 : la c.d. pseudo-pornografia

La fattispecie in esame, estende l'ambito di operatività degli artt. 600 ter e 600 quater c.p., alla c.d. "pornografia virtuale", prevedendo che le norme incriminatrici di cui agli artt. 600 ter e 600 quater c.p., si applichino "anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando minori di anni diciotto o parti di esse, ma la pena è diminuita di un terzo". La norma fornisce poi una definizione di immagini virtuali , stabilendo che sono tali, "le immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire in tutto o in parte come vere situazioni non reali". Per la prima volta si affianca così esplicitamente il *virtuale* al *reale*, l'universo intangibile e sfuggente dello spazio cibernetico,al mondo concreto del crimine. Alla pornografia tradizionale , prodotta attraverso l'impiego sessuale di persone in carne ed ossa, si equipara l'astrattezza di un'immagine realizzata tramite artifici grafici. Tale avvicinamento è parso necessario per una più efficace tutela dei minori, posta in pericolo , nello spazio infinito della *cyber-criminalità,* dall'esistenza della pedofilia telematica. La relazione governativa che ha accompagnato il disegno di legge in Parlamento, ha sottolineato come l'art. 600 quater 1 c.p. sia stato introdotto per adeguare il sistema normativo nazionale, in tema di pornografia minorile, alla più volte menzionata Decisione quadro 2004/68/GAI del Consiglio dell'Unione europea. Quest'ultima ,infatti, definisce pornografia infantile non solo il materiale che ritrae o rappresenta visivamente un bambino reale, implicato o coinvolto in una condotta sessualmente esplicita, ma anche il materiale che ritrae o rappresenta una persona reale che sembra essere un bambino ovvero immagini realistiche di un bambino inesistente. Il disegno di legge introduceva così all'interno del *corpus* codicistico due nuove disposizioni , l'art. 600 quater 1 e l'art. 600 quater 2 , che estendevano il raggio repressivo degli artt. 600 ter e quater c.p. alle ipotesi di materiale pornografico prodotto utilizzando persone che , per le loro caratteristiche fisiche, hanno le sembianze di minori di anni diciotto, e alle ipotesi di realistiche immagini virtuali di minori degli anni diciotto. Durante l'*iter* che ha portato all'approvazione del

[1] In dottrina si veda. Cocco G., p. 878, Fiandaca-Musco, Diritto penale, pt., sp,II, "I delitti contro la persona", II ed., Bologna 2007,i quali rilevano che la riforma del 2006"non appare in linea con i diversi postulati di un diritto penale proprio di uno stato di diritto a cominciare dal principio di materialità e a finire con quello di determinatezza della fattispecie". BIANCHI , sub art. 600 quater, in "trattato di diritto penale, parte speciale, vol. IX, diretto da CADOPPI A., CANESTRARI S, MANNA A., PAPA M., UTET, 2011, P 477 E ss.

disegno di legge, la prima delle due disposizioni , che sanzionava la produzione e la diffusione di materiale pornografico prodotto utilizzando persone che "sembrano " essere minori, (la c.d. pornografia apparente") è stata eliminata. È stato invece definitivamente introdotto l'art. 600 quater 1 che incrimina la produzione e diffusione di materiale pedopornografico virtuale. Anche queste condotte ,infatti, nell'ottica legislativa ," appaiono tali da alimentare il fenomeno della pornografia minorile , inducendo effetti criminogeni nei fruitori del materiale"[2]. L'incriminazione della pornografia virtuale , secondo la relazione governativa, svolge una funzione preventiva e repressiva del fenomeno dello sfruttamento dei minori, sarebbe pertanto compatibile con i principi generali del nostro ordinamento , assumendo i contorni del reato di pericolo astratto o reato-ostacolo : la produzione e la diffusione di materiale pornografico virtuale , infatti, incentiverebbe quei comportamenti devianti , da cui possono originare ulteriori condotte lesive del bene giuridico finale, costituito dall'integrità psico-fisica dei minori[3]. In realtà ,come sottolineato dai primi commentatori della novella legislativa, la nuova disposizione non può che suscitare notevoli perplessità[4]. Le fattispecie delittuose aventi ad oggetto materiale pedopornografico virtuale, infatti, sono prive di offensività, in quanto, essendo il prodotto erotico realizzato senza l'effettiva utilizzazione di una persona minore d'età, mancherebbe non soltanto la lesione al bene giuridico protetto (integrità psicofisica e sano ed adeguato sviluppo del minore) ,ma anche solamente, una sua effettiva esposizione a pericolo . L'idea ,infatti, sottesa alla novella legislativa, e cioè che la produzione , la cessione e la detenzione di materiale pedopornografico virtuale possano accrescere la domanda di prodotti pornografici realizzati tramite l'effettivo impiego di minori, determinando così il pericolo di commissione di più gravi reati , come è stato giustamente rilevato, è discutibile e confutabile[5] .

---

2 Così la relazione governativa al disegno di l. n. 4599

3 Si veda ancora , la relazione governativa al disegno di l. n. 4599.

4 CADOPPI, "L'assenza di cause di non punibilità mette a rischio le buone intenzioni", in Guida al dir.2006 , n. 9, p.63. PISTORELLI, "Colmate le lacune della pregressa disciplina", in Guida al dir. 2006 n.9, p.51. MANNA-RESTA,"I delitti in tema di pedopornografia , alla luce della legge 38/2006. Una tutela virtuale?" in "*Diritto dell'Internet",* n.3/2006 p. 221 e s.s. MUSACCHIO, "La nuova normativa penale in materia di sfruttamento sessuale dei bambini e pedo-pornografia a mezzo internet ", in Riv. Pen. 2006, p.399 ess. Più recentemente , BIANCHI, art.600 quater1, in AA.VV.Commentario alle norme contro la violenza sessuale e contro la pedofilia (a cura di CADOPPI) ,IV ed.Padova, 2006., p. 515 ess.; Id, " La pedo-pornografia virtuale : alla ricerca di un bene giuridico-Fra difficoltà ermeneutiche e istanze politico criminali , in "I delitti di pedopornografia fra tutela della moralità pubblica e dello sviluppo psicofisico del minore, " a cura di BIANCHI ,DELSIGNORE, Padova,2008,139 e ss. COCCO G. ,*Pornografia minorile, in Manuale di diritto penale,pt. sp.,I reati contro le persone, (*a cura di COCCO ,AMBROSETTI),Padova, 2010. Id; *Può costituire reato la detenzione di pornografia minorile?, in Riv.it, dir, Proc.Pen.,2006 , p.863.*

5 Così BIANCHI-DELSIGNORE, "Detenzione di materiale pedopornografico, in "I reati contro la persona", diretto da CADOPPI-CANESRTRERI-PAPA, vol. III.. Torino 2006, p.486, i quali sottolineano come al contrario, la scelta di produrre, acquistare o detenere materiale pedopornografico virtuale possa servire ad appagare , incanalandoli verso condotte inoffensive, gli istinti sessuali che la parafilia genera, così evitando fenomeni di effettivo abuso dei minori.

3. Le ragioni addotte a sostegno dell'incriminazione di cui all'art. 600quater 1 c.p.

Le qualificazioni giuridiche proposte nella relazione governativa ,e le giustificazioni poste a loro fondamento , non sembrano attagliarsi al contenuto delle nuove fattispecie. Le specifiche esigenze a cui risponderebbe la suddetta incriminazione , così come emerso dai lavori preparatori , sono state così individuate dalla dottrina:

1) disincentivare l'offerta di materiale pedopornografico , reprimendone la domanda;
2) prevenire il c.d. *grooming effect*, ovvero il potenziale criminogeno di tali immagini, che si ritiene siano utilizzate dai pedofili per sedurre/adescare i minori;
3) tutelare la dignità dei minori come gruppo, rispetto alla diffusione di materiale che, enfatizzandone la sessualità in contesti particolari, rafforzi la *"deleterious attitude"* già insita nell'uomo. Si tratterebbe cioè di "*attitudinal harm*" , o "danno attitudinale", derivante dal mero possesso di materiale idoneo a degradare e disumanizzare il minore [6]
4) esigenze probatorie: superare cioè le difficoltà legate alla dimostrazione della natura reale od artificiale dell'immagine prodotta mediante le moderne tecniche di elaborazione grafica. Tuttavia le ragioni individuate a sostegno dell'incriminazione, non paiono sufficienti a soddisfare il principio di necessaria offensività del reato. Le esigenze di semplificazione probatoria non possono giustificare l'incriminazione di condotte che, prescindendo totalmente da un rapporto di sfruttamento del minore, rappresentano delle forme -sia pur moralmente riprovevoli-di estrinsecazione della libertà di espressione . Non sembrano fondati gli argomenti del *grooming effect* o del danno attitudinale, perchè non solo empiricamente e scientificamente confutabili, ma altresì inidonei a fondare di per sé un'ipotesi di responsabilità penale . Né La produzione né le condotte di successiva diffusione , cessione o possesso di tale materiale possono reputarsi mezzi di alimentazione e di incremento della domanda e quindi della produzione di un materiale diverso da quello che ne è oggetto(vale a dire di materiale conseguito attraverso l'impiego di minori esistenti , anziché di immagini virtuali). Al contrario si è messo in luce come il possesso di materiale pedopornografico virtuale possa servire ad appagare , incanalandoli verso condotte inoffensive, gli istinti sessuali che la parafilia pedofila genera, così evitando fenomeni di effettivo abuso dei minori[7] .La repressione della pedopornografia virtuale, non potrebbe giustificarsi allora, neppure con l'esigenza (sottesa ad una ricostruzione della fattispecie in chiave di pericolo indiretto) di disincentivare la domanda

---

[6] BIANCHI- DELSIGNORE, "*Detenzione di materiale pedopornografico," in "Reati contro la persona "* diretto da CADOPPI-CANESTRERI -PAPA vol. III Torino 2006 , . p. 515.

[7] Così COCCO G. ; *Può costituire reato la detenzione di pornografia minorile?, in Riv.it, dir, Proc.Pen.,2006* pp.876-877 che non solo rileva l'assenza di basi scientifiche che sostengano l'assunto della incentivazione alla commissione di illeciti quale conseguenza della diffusione di pornografia minorile virtuale o apparente,ma mette in luce i possibili effetti positivi per le vittime in carne ed ossa alla luce della letteratura scientifica .."Cos' anche PICCICHè ., *la pornografia minorile, inquadramento e problematiche,* in "Riv. Pen., n. 7-8, 2009, p.790.
BIANCHI.DELSIGNORE "*Detenzione di materiale pedopornografico" cit.;* BIANCHI, "*Commento all'art. 600 quater1,c.p.* cit. p.629.

di tale materiale. Nell'incriminare condotte del tutto carenti anche di un'astratta pericolosità per lo sviluppo psico-fisico del minore, del quale non presuppongono l'abuso né sembrano idonee ad incentivarlo, le fattispecie relative alla pornografia virtuale, sembrano in effetti introdurre reati senza vittima e senza offesa.

4. Profili di sospetta illegittimità costituzionale dell'art. 600 quater 1.

Non può tacersi, come emerge dalle considerazioni sinora svolte, come la fattispecie di pedopornografia virtuale non appaia perfettamente in linea con i pilastri di "un diritto penale costituzionalmente orientato". La questione principale che si pone riguarda, come detto, il rispetto del principio di offensività, il quale in forza della concezione c.d. realistica del reato è ormai avvalorato nel suo fondamento costituzionale , ex. Art. 25 ,comma II, Cost. come caposaldo del diritto penale a base oggettivistica, da contrapporre a quello a base soggettivistica espressione dell'opposto principio del reato come mera violazione del dovere. In uno Stato laico e liberale questo deve necessariamente sostanziarsi anche nell'offesa ad un bene giuridico , non essendo concepibile un reato senza offesa : *nullum crimen sine iniuria.* Secondo la relazione governativa al disegno di legge , come detto, la condotta assumerebbe *i contorni di reato di pericolo astratto o quelli di reato ostacolo,* tuttavia al momento non esiste un parametro nomologico-deduttivo che permetta di dimostrare con certezza o perlomeno con elevata probabilità, l'esistenza di un rapporto regolare causa-effetto tra pornografia virtuale e messa in pericolo del bene giuridico da tutelare(incremento della domanda di materiale pedopornografico reale- sfruttamento sessuale che ne è a monte).Se le fattispecie penali di pericolo, in continua espansione legale e fattuale , per effetto del progresso tecnologico, costituiscono da sempre una categoria di difficile accertamento in termini causali, il *vulnus* al principio di offensività si pone in maniera particolarmente pregnante nella fattispecie *de quo*. Posta al confine del penalmente rilevante, questa è caratterizzata dalla massima anticipazione della soglia di punibilità: il bene giuridico che si intende proteggere- lo sviluppo armonioso della personalità ancora *in fieri* del minore"reale"-appare troppo distante rispetto alla condotta che si intende punire.
Anche la correlazione tra esperienze sessuali devianti e lo stimolo alla fantasia ,determinato dalla fruizione di opere pedopornografiche virtuali, rimane al momento una congettura. Non sussistendo prove sufficienti per giustificare l'esistenza di un rapporto causale tra il contatto con il materiale illecito e la commissione di reati di abusi sessuale nei confronti di fanciulli, si rischia di legittimare i reati di "mero sospetto[8]" e delegare al giudice un vero e proprio processo alle intenzioni , nell'accertamento

[8] Si veda sul punto, BIANCHI*, art. 600 quater 1I delitti contro lo sviluppo psicofisico dei minori,cit, p.529; S*econdo L'A. prescindendo da ina lettura restrittiva della norma, il nuovo delitto assumerebbe i contorni di "reato di sospetto"," attraverso il quale si punisce il detentore, il diffusore etc, di materiale pedopornografico virtuale in quanto si teme che si sia reso responsabile del reato di cui all'art.600 ter o 600 quater c.p.,ma non si riesce a provare la natura reale dell'immagine, ovvero perché si ha il sospetto che possa commettere futuri reati di pedofilia:"(..) è evidente come l'attenzione si sposti, qui, dal minore vittima del reato ,alla perversione del reo ". Nello stesso senso DELSIGNORE*, art.. 600 quater la detenzione di materiale pedopornografico, I*bidem,P.482,

delle motivazioni presunte, alla fruizione di detto materiale. Se si accetta una siffatta lettura della norma , non potrebbe non condividersi quell'opinione dottrinale che scorgendovi una sanzione verso l'inclinazione soggettiva del soggetto agente verso determinati gusti sessuali, ha ravvisato il sovvertimento del principio di colpevolezza per il fatto , sostituendovi il paradigma per la condotta di vita o per l'inclinazione soggettiva , propria di un diritto penale "del tipo d'autore"[9].
Dato necessario allora, affinchè la nuova fattispecie risulti validamente collocata tra i delitti contro la persona, è che le condotte aventi ad oggetto immagini virtuali possano essere rilette in modo da porre effettivamente in pericolo il bene giuridico da proteggere, pena un'eccessiva relativizzazione del ruolo assiologico dei principi costituzionali. Postulare l'esistenza della capacità offensiva di un'immagine virtuale o *cartoon* è infatti espressione di una prospettiva di tutela *sui generis* ,distinta dalle tradizionali categorie di reato volte ad incriminare un'offesa individuale e concreta, , la quale provoca inesorabilmente un affievolimento delle garanzie sostanziali ,processuali e costituzionali del diritto penale classico in direzione di lesioni eventuali e superindividuali[10]. . . Senza pretendere di risolvere annosi problemi interpretativi, è comunque possibile scandagliare le ragioni della peculiare problematicità del delitto di pedopornografia virtuale, anche alla luce delle recenti pronunce giurisprudenziali, e cercare una mediazione tra esigenze di funzionalità general-preventiva e rispetto dei principi di offensività e colpevolezza, per poter inquadrare costituzionalmente la disciplina vigente.

5. Le ricostruzioni interpretative proposte in dottrina

Molteplici sono stati percorsi ermeneutici proposti in dottrina i quali, pur giungendo ad approdi diversi circa l'identificazione del bene giuridico oggetto di tutela della norma, sono tutti accumunati dallo sforzo di restituire alla fattispecie i caratteri di determinatezza ed idoneità lesiva. Si è individuato ,da parte di alcuni autori,come soggetto passivo del dei delitti di pornografia virtuale i "fanciulli come tali nella loro generalità", e non quelli concretamente utilizzati per la singola produzione pornografica[11]. Questa esegesi parte dal presupposto che "se la pornografia è ora capace di attingere una cerchia indefinita di soggetti -potenzialmente pubblica- con messaggi

---

[9] In questo senso si sono espressi i primi commenti alla fattispecie di cui all'art. 600 quater 1, :c.p.: PISTORELLI, "*Attenzione spostata sulla perversione del reo" in Guida al Dir.,2006* n. 9, p. 51.Parlano di pedofilo trattato come un "nemico",anche CADOPPI A.: "*l'assenza di cause di non punibilità mette al rischio le buone intenzioni" in Guida al dir.* 2006, n. 9, p.43. RESTA F.,*i delitti contro l'integrità psicofisica del minore alla luce delle recenti riforme,IN Dir. e Formaz,2006 n. 2 p.63 ess.*

[10] MANNA ,*profili problematici della nuovo legge in tema di pedofilia,* in *Pedofilia ed internet,:vecchie ossessioni e nuove crociate" in* Indice Penale, 1999 ,p.47 e ss.
La norma solleva dubbi di legittimità costituzionale anche in relazione all'art. 27 commaIII La scelta di incriminare l'immagine di una persona inesistente implica poi pregnanti riflessioni sul piano del rispetto del principio della responsabilità penale personale ex. Art. 27 comma III, Cost. Se è vero che il concetto e le forme del dolo variano al variare del sostrato di tipicità oggettiva , nell'ipotesi in questione , mancando una vittima reale ed essendo l'evento dannoso eventuale e comunque fuori dal fatto , il dolo risulta avere un oggetto diverso da quello dei tradizionali reati, alimentando il rischio di presunzioni di colpevolezza

[11] In questo senso PALAZZO, *Tendenze e prospettive nella titela penale della persona, in La tutela penale della persona,Nuove frontiere , difficili equilibri,* a cura di FIORAVANTI, Milano 2001 p.409 e ss.. MUSACCHIO V.,*Brevi considerazioni sulla nuova normativa penale anti-pedofilia , in Giust.Pen.* ,1998, II.p.666.

sensoriali aventi altissimo contenuto emotivo e condizionante, capace di proporre modelli di rapporti ed indurre comportamenti che offendono profondamente la dignità e qualità di uomo delle vittime, essa può mettere concretamente in pericolo la libertà personale dei fanciulli in ambito sessuale , raffigurandoli quali mero strumento per la soddisfazione altrui [12]. La *ratio puniendi* risiederebbe allora, nell'offesa che la produzione e messa in circolazione del materiale pedopornografico arreca di fatto ai minori in quanto tali: oltre a degradare *virtualmente* l'immagine o rappresentazione degli stessi, essa sarebbe idonea a ledere *realmente* la loro libertà di uomini nella sfera sessuale al punto di violare il riconoscimento ed il rispetto dovuto alla loro persona e individualità. È evidente come anche l'impostazione in parola, non riesca a recuperare l'idoneità lesiva della condotta[13], finendo per avallare l'accertamento giudiziale dell'offesa sulla base di mere regole morali, non avvalorate da alcun parametro logico scientifico in grado di affermare con certezza l'effetto nefasto ,che tali rappresentazioni causerebbero sul delicato sviluppo psico-fisico dei minori. In questa prospettiva infatti, il bene giuridico protetto non sarebbe la personalità del minore, bensì la "dignità umana" come valore superindividuale, che cessa di essere di diretta , "fisica" pertinenza di un singolo soggetto individuale per divenire patrimonio dell'intera umanità[14].
Altro filone dottrinale, sempre nel tentativo di ricondurre la fattispecie entro i confini di legittimità costituzionale, ha ritenuto la norma posta a tutela della funzione istituzionale spettante allo Stato ex art. 31 Cost. di tutela dell'infanzia e della gioventù, quale bene interposto rispetto al bene finale. La norma incriminerebbe pertanto condotte prodromiche ed inoffensive rispetto al bene giuridico finale, quali ad esempio la detenzione di pornografia virtuale, in quanto contrastanti con lo scopo legislativo ,sociale ed istituzionale di estinguere il mercato della pedofilia. Si recupererebbe almeno il bene giuridico identificandolo con lo scopo della norma stessa, vale a dire con quella funzione propria dello Stato Sociale di tutelare l'infanzia in generale[15].
Una strada alternativa rispetto alle prospettate ricostruzioni della fattispecie in chiave di pericolo indiretto, per far fronte al processo di progressiva smaterializzazione del bene giuridico, e quindi di rarefazione ed affievolimento delle garanzie di offensività e legalità,

---

[12] Così PICOTTI: *La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in Internet, (l. 6 febbraio 2006 n. 8) (Parte prima) in Studium iuris, n. 10,* 2007 , p.1069.

[13] *Così CADOPPI, "I delitti contro lo sviluppo psico-fisico dei minori*,"cit. p. 328 ess.secondo cui la descritta impostazione ermeneutica comporterebbe "la smaterializzazione dell'oggetto della tutela" ; in senso critico anche DELSIGNORE, art.600 ter, in op.cit. p. 418 e ss,

[14] Per un esame critico del bene "dignità umana" FIANDACA, "*Considerazioni intorno alla bioetica e diritto penale , tra laicità e postsecolarismo,". In Riv. It. dir. E proc. Pen. ,2007,p. 558e ss.* il quale osseva:"il diffuso consenso tributato alla dignità umana quale bene meritevole di tutela si spiega , verosimilmente, con il fatto che esso rispecchia un valore a forte connotazione etico-emozionale , ma al tempo stesso dal contenuto generico ed indefinito: come tale potenzialmente disponibile-per dir così- a fungere da *deus ex machina* per la giustificazione di ogni incriminazione , rispetto alla quale non si sia in grado di identificare quale oggetto di tutela un bene giuridico più specifico. Sia il contenuto vago , sia la carica emozionale del *topos* della dignità recano dunque un rischio: cioè che esso si presti con eccessiva precipitazione e con soverchio automatismo a fungere da da bene-ricettacolo delle reazioni di panico morale(..)". Per la distinzione tra il concetto di "dignità" bene meta individuale, rispetto a quello di "onorabilità", inteso come dimensione esteriore e dunque specifico aspetto della personalità e dunque riferibile al singolo individuo, si veda DELSIGNORE, art.600 ter, in op.cit. p. 418 e ss. RESTA G.*la disponibilità dei diritti fondamentali e i limiti della Dignità (Note a margine della Carta dei diritti) in Riv. Dir. Civ. 2002 ,II, 825 e ss.*

[15] Sulla tutela penale delle funzioni, quale allontanamento dai presidi garantistici della dannosità sociale, e dalla sua incarnazione classica sintetizzata nel canone nullum crimen sine iniuria MANES: *Il principio di offensività nel diritto penale . Canone di politica criminale, criterio ermeneutico, parametro di ragionevolezza,* "Giappichelli . 2005, p.127

è quell'impostazione che ,costruita sulla falsariga del modello nordamericano, interpreta in maniera restrittiva il concetto di pornografia virtuale così come descritto dalla norma. Secondo tale opzione ermeneutica, che fa leva sull'interpretazione testuale del dato normativo (sulla circostanza cioè che il legislatore richieda che le immagini virtuali non siano semplicemente realistiche, ma siano realizzate "utilizzando" persone minori d'età)[16] non sarebbe sufficiente ai fini dell'integrazione della fattispecie, un'immagine graficamente realistica di un minore inesistente, ma sia al contrario ,in ogni caso, necessaria la rappresentazione di un minore in carne ed ossa: il carattere virtuale deriverebbe dal fatto che l'immagine reale è associata , tramite tecniche di rielaborazione grafica, in tutto od in parte a situazioni non reali, così da rappresentare il minore in scene e pose sessualmente esplicite che egli in realtà non ha tenuto. Ad essere incriminata sarebbe per tanto la sola pornografia c.d. "parzialmente virtuale". Viceversa non sarebbero ricomprese le immagini totalmente virtuali, ossia quelle che non contemplano l'utilizzo, neanche in parte, dell'immagine di un minore .Le raffigurazioni devono essere realizzate attingendo a immagini di minori reali o a parti di esse. Il termine parte, si precisa, andrebbe poi interpretato restrittivamente , limitandolo a quelle sole porzioni dell'immagine che configurano "parti riconoscibili" del minore, ossia che possano condurre ad una sua identificazione[17]. Stando a tale tesi restrittiva l'applicazione della norma dovrebbe essere di conseguenza limitata ai soli fotomontaggi realizzati con l'utilizzo di parti *riconoscibili* della vittima.

Si tratta di un'interpretazione che , come anticipato, sembra ricalcare la scelta operata dall'esperienza comparatistica americana, nel c.d. caso sulla" pedopornografia virtuale". La Corte Suprema degli Stati Uniti , con decisione del 16 aprile 2002[18], ha infatti dichiarato illegittime le disposizioni del *Child Pornography Prevenction Act (CPPA) del 1996:* la c.d. legge antipedofilia americana .Nello specifico, la norma colpita da illegittimità costituzionale per violazione del Primo Emendamento della Costituzione americana ,(*freedom of speech)* , è l'art. 2256(8) che includeva nella fattispecie di pornografia "ogni rappresentazione visiva , inclusa la fotografia, il video, il film, o immagine realizzata a computer dove ..B) tale rappresentazione visiva è, o appare essere di un minore impegnato in un'attività sessualmente esplicita (pornografia apparente)..D) tale rappresentazione visiva è presentata ,pubblicizzata descritta, distribuita in

---

[16] Così almeno stando alla locuzione che compare nel comma 1dell'art, 600 quater 1 (*immagini virtuali realizzate* utilizzando immagini di minori o parti di esse), che se interpretata letteralmente, farebbe ritenere che all'origine del materiale prodotto vi debbano sempre essere immagini (o parti di immagini) "di minori" reali. Così BIANCHI M, Commento all'art. 600 quater 1c.p., cit. p.276; Id, Pornografia virtuale, in " i delitti contro lo sviluppo psicofsico dei minori, cit, p.524; condivide l'impostazione GIZZI L.,cit, p. 416

[17] Così ,BIANCHI M,.cit. p. 524,;Secondo la quale una tale conclusione è conseguenza necessaria dell'accoglimento dell'interpretazione restrittiva del I comma dell'art. 600 quater 1, volta cioè a limitare l'incriminazione alla pornografia parzialmente virtuale. Rileva l'A.come una diversa e più ampia nozione di "parte"comporterebbe invece una sostanziale coincidenza fra "pornografia parzialmente virtuale"e "pornografia totalmente virtuale":." Se a tale concetto si attribuisse il suo significato letterale, ossia "ciascuna delle porzioni o degli elementi in cui è diviso il tutto" si dovrebbe concludere che *parte dell'immagine del minore* , è qualsiasi parte della sua fisicità, sia essa il volto, il corpo, ma anche una mano, un braccio etc, Immagini realizzate utilizzando *parti reali non riconoscibili* non si differenzierebbero in alcun modo dalle immagini *totalmente virtuali* soprattutto in termini di inoffensività giuridica :l'immagine virtuale, realizzata con l'utilizzo della mano di un minore reale, non arrecherebbe alcun pericolo allo sviluppo psico-fisico del minore la cui mano è stata utilizzata.

[18] Si tratta di una delle più importanti pronunce sul tema, tratta dal Caso *Ashcroft v. Free Speech Coalition ,(N. 00- 795. Argued October 30, 2001- Decided April 16, 2002)* commentato da MARRA : "*La pornografia virtuale vista con gli occhiali di J.S.Mill,* in *Studi Urbinati , n.55/2004 pp.647-672. In argomento si veda* BIANCHI M*., cit., p. 537 ess.;* RESTA F.,cit.

modo da suscitare l'impressione che ritragga un minore impiegato in un'attività sessualmente esplicita " c.d. (pornografia virtuale).
n tale decisione la Corte ha ritenuto infondati gli argomenti addotti dall'*Attorney General* a sostegno della legittimità delle disposizioni ed in particolare quelle inerenti la finalità del possesso di immagini pedopornografiche, anche virtuali, identificate da Ashcroft nell'intenzione di soddisfare istinti pedofili. La Corte ha rigettato l'eccezione affermando che proprio perché la norma incrimina una mera intenzione, non può ritenersi legittima alla luce del principio *cogitationis poena nemo patitur*. Il più pregnante argomento della ritenuta idoneità del materiale in esame a condurre abusi su bambini reali " è stato altresì rigettato dalla Corte, in ragione dell'assenza di "*empirical evidence"* a giustificazione dell'assunto, che avrebbe quindi instaurato tra la detenzione di immagini pedopornografiche virtuali ed eventuali abusi su minori una relazione causale che in realtà è meramente " contingente ed indiretta".
La Corte statunitense con tale pronuncia ha, dunque ,ristretto la portata applicativa della fattispecie di pornografia virtuale alle sole ipotesi di "rappresentazioni visive che siano state create, modificate o adattate ,in modo tale da sembrare che un minore *identificabile* sia coinvolto in un'attività sessualmente esplicita" (lett.c della S.2256(8))[19]. Questa sotto-categoria rileva la Corte, in un breve ma fondamentale *obiter dictum,*si distinguerebbe dalle altre forme di "pseudo-pornografia"frutto della fantasia perversa del reo, per l'implicazione d'interessi individuali di minori reali e al pari di quanto avviene nella pedopornografia tradizionale.
Anche tale impostazione correttiva,applicata alla "nostra legge"antipedofilia, non è andata esente da critiche. Da un lato si è rilevato come l'interpretazione risulti troppo restrittiva tendendo a forzare eccessivamente la lettera della norma, laddove l'utilizzo del termine indefinito "parte" ex art. 600 quater 1, comma I, c.p. ,porterebbe ad estendere l'incriminazione ad immagini contenenti qualsiasi aspetto della corporeità della persona fisica,[20].
Dall'altro, pur nel tentativo di recuperarne i caratteri di offensività, anche una simile lettura della norma ,non sarebbe sufficiente a renderla effettivamente lesiva del bene giuridico che si vorrebbe tutelare *i.e.* l'integrità psico-fisica del minore. Verrebbero ricomprese nelle maglie dell'incriminazione penale in ogni caso anche composizioni grafiche ritraenti parti di minori

---

[19] Si tratta del c.d. *morphing*,ossia immagini realizzate attraverso sofisticati sistemi grafico-informatici in modo da apparire vere. Il *morphing* è stato definito come quel processo di nuova produzione di pornografia minorile , per mezzo del quale il fotografo "scannerizza" l'immagine fotografica del volto di un bambino e successivamente l'assembla con la rappresentazione pornografica di un adulto. Quindi attraverso i sofisticati strumenti tecnologici , affina la composizione risultante in modo da omogeneizzare l'immagine e creare un opera pedopornografica convincente.

[20] Così PICOTTI L., "*La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in internet(L. 6 febbraio 2006,n. 38)(parte prima)* cit. pp. 1072-1073,, Scrive l'A., " che si debba trattare di immagini di minori reali non è scritto, e dunque non è voluto dal legislatore italiano(..)" Una tale esegesi basata sulla sola lettera del I comma (immagini virtuali realizzate *utilizzando* minori degli anni diciotto o parti di esse), isolata dalla connessione logica e sintattica con il II comma, (in violazione del criterio ermeneutico di cui all'art. 11 disp.prel. c.c.), si porrebbe in contrasto con la *voluntas legis* di dare piena attuazione alla decisione quadro riducendone la portata innovativa: "anche *l'utilizzazione di immagini di minori* se circoscritta ai soli casi in cui le immagini siano di minori reali, costituirebbe pur sempre *un'utilizzazione di minori*".In questo senso anche CANTAGALLI C. ,"*Il delitto di pornografia minorile (art. 600 ter,terzo , quarto e quinto comma, c.p.)* cit. p. 447., Rispettando i canoni dell'interpretazione teleologica e sistematica, prevalenza deve essere accordata al II capoverso che esplicita il concetto di immagini virtuali:quelle cioè" non associate in tutto o in parte a situazioni reali".La categoria sarebbe dunque ampia e atta a ricomprendere secondo l'A. tanto le situazioni in cui la persona(esistente)"appaia" essere un minore(pedopornografia apparente), sia quelle in cui non vi sia alcun minore nè altra persona reale all'origine dell'immagine.

in atteggiamenti non sessualmente significativi, rimanendo ,di fatto, la norma inoffensiva in relazione allo specifico bene oggetto di tutela. Ad essere offesi sarebbero altri beni, come quello all'immagine o anche all'onorabilità sessuale del minore, che troverebbero però adeguata tutela in norme civili o penali diverse da quelle in commento.[21].

Quest'ultimo rilievo, tuttavia, non appare condivisibile. Diversa infatti deve essere la lettura dell'oggettività giuridica sottesa a questa ricostruzione del disposto normativo, che a ben vedere verrebbe a staccarsi dalla controversa categoria di reati a" vittima diffusa.". Il bene giuridico sotteso alla di tutela penale consisterebbe infatti nello sviluppo armonico della personalità del minore(ivi rappresentato e riconoscibile), inteso nella sua interezza e scomponibile in due distinti interessi: la protezione della personalità in divenire nella sua dimensione interiore (quale integrità psico-fisica), e la protezione della personalità in divenire nella sua dimensione esteriore (relazionale o sociale). In rapporto a quest'aspetto della personalità che si proietta verso l'esterno, si è parlato di "onorabilità sessuale" , individuando con il termine, lo specifico interesse che viene ad essere tutelato della norma in questione [22]:non allora l'onore in quanto tale ,o il diritto all'immagine, ma ciò che essa mira ad evitare è la lesione , arrecata dalla circolazione di materiale pornografico in questione, a quel particolare aspetto "relazionale" della personalità del minore in corso di formazione (tanto la reputazione sessuale presso terzi,quanto ,laddove vi sia la consapevolezza di tale circolazione da parte del minore coinvolto, la percezione che lo stesso ha del proprio valore sociale) ed il conseguente rischio che ciò riverberi i suoi effetti negativi sullo sviluppo complessivo della personalità intesa nella sua interezza[23]. L'impostazione sembra del resto conforme alla *ratio legis*, laddove nel preambolo della precedente legge n. 269/1998 si parla di salvaguardia "dello sviluppo sociale". In altri termini la tutela sarebbe apprestata alla personalità del minore ancora *in fieri,* nell'aspetto esteriore e sociale e dunque, secondo lo schema del pericolo astratto[24], dalle ripercussioni che l'offesa alla reputazione sessuale può sortire sulla sua dimensione psichica interiore.

Una siffatta ricostruzione ermeneutica sembra invero cogliere la nuova prospettiva di tutela sottesa all'intero impianto normativo della legge in esame ,imposta dalla forte incidenza delle tecnologie della comunicazione sui comportamenti quotidiani e sui rapporti sociali. Diversa è, infatti , la capacità offensiva della diffusione e comunicazione in rete - compresa accanto ad internet quella della telefonia mobile e della multimedialità di ogni natura- di simili immagini, filmati ,prodotti, rispetto a beni e diritti fondamentali della persona , il cui concreto pericolo di offesa dipende dall'efficacia delle condotte che si collocano "a valle" della produzione di materiale pornografico

---

[21] Così C.CANTAGALLI ,"*Il delitto di pornografia minorile (art. 600 ter,terzo , quarto e quinto comma, c.p.)in op.* cit. p. 447. Analogamente GIZZI L. Il *delitto di pornografia minorile (art. 600 ter I e II comma c.p. e art. 600 quater.1 c.p.)" in i "reati sessuali ,i reati di sfruttamento dei minori e di riduzione in schiavitù per fini sessuali* ", a cura di F.Coppi , Giappichelli, Torino,2007 pp. 413 e ss.

[22] Così ,DELSIGNORE,"*Pornografia minorile",* cit. pp.406 e ss.. , L'A, che Individua "nell'onorabilità sessuale" lo specifico oggetto di tutela delle fattispecie di cui all'art. 600 ter II,III eIV comma,600 quater e ,in prospettiva de iure condendo 600quater 1

[23] "Se gli altri perdono il rispetto questo incide negativamente sulla formazione della sua personalità;se il minore perde il rispetto per sé stesso , a causa di ciàò che egli teme gli altri pensino di lui, la formazione della sua personalità viene da ciò, almeno potenzialmente intaccata" ,DELSIGNORE,"*Pornografia minorile",* cit. p.410.

[24] Secondo l'impostazione in parola non occorrerebbe pertanto l'accertamento nel caso concreto degli effetti distorsivi sulla personalità, provocati dalla circolazione del materiale in questione , né il concreto pericolo in tal senso. Così DELSIGNORE, CIT. P.422; BIANCHI,cit,

e non soltanto dall'episodio di "sfruttamento del fanciullo in carne ed ossa"che si collochi " a monte" su cui viceversa si imperniava la legislazione, la dottrina e la giurisprudenza anteriori , cercandovi chiaramente anche una legittimazione politico criminale per queste nuove fattispecie. Non condivisibili appaiono allora le critiche mosse da parte di quella dottrina, che ancorata a tale impostazione,reputa l'interpretazione correttiva insufficiente a recuperare la concreta idoneità lesiva delle condotte in esame, sulla base del rilievo che rimarrebbero ricomprese nelle maglie dell'incriminazione penale anche composizioni grafiche ritraenti minori in atteggiamenti non sessualmente significativi[25]. Come detto non è nell'effettivo sfruttamento di fanciulli in carne ed ossa che va mantenuta o cercata l'oggettività giuridica delle fattispecie incriminate, ma è negli effetti a valle che deve essere accertato e misurato concretamente il pericolo per gli interessi da tutelare: la produzione e circolazione di materiale pedopornografico non solo degrada virtualmente l'immagine o rappresentazione dei fanciulli , ma lede realmente la loro libertà di uomini nella sfera sessuale perché viola il riconoscimento e rispetto dovuto alla loro personalità [26]. Se da un lato allora si impone una diversa chiave di lettura dell'oggettività giuridica di condotte, che manifestando la loro carica offensiva " a valle", prescindono dall'episodio di concreto sfruttamento,dall'altro resta il problema di descriverne con sufficiente determinatezza il nuovo profilo lesivo ai fini del dovuto rispetto del principio di necessaria offensività . Troppo vago ed indeterminato è dunque apparso , il ricorso a concetti astratti e sovraindividuali quali "la dignità" dei minori intesi nella loro generalità: esso garantirebbe probabilmente una più ampia tutela dei fanciulli ,ma in quanto difficilmente afferrabile ed identificabile[27], verrebbe a porre problemi non dissimili dall'altrettanto discussa categoria di moralità[28], (quasi a sembrarne un riaggiornamento in chiave evolutiva) in termini di idoneità ad assurgere a bene meritevole di tutela penale[29]. L' impostazione in commento sembra allora aver trovato adeguato punto di mediazione tra l'esigenza di una diversa e nuova valutazione del fenomeno della produzione e messa in circolazione di materiale pedopornografico, ed il rispetto dei principi cardine del sistema penale ,quali determinatezza e offensività della fattispecie, individuando il bene giuridico da tutelare in uno specifico tratto della personalità in divenire del minore [30]. Non si negano tuttavia i limiti di una siffatta lettura, che -oltre a fondarsi ,come

---

[25] Così C.CANTAGALLI ,"*Il delitto di pornografia minorile (art. 600 ter,terzo , quarto e quinto comma, c.p.)* cit. p. 447. Analogamente GIZZI L. Il *delitto di pornografia minorile (art. 600 ter I e II comma c.p. e art. 600 quater.1 c.p.* ",cit. pp. 413 e ss.

[26] Così PICOTTI L. *La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in internet(l.6 febbraio 2006 n. 38)(parte prima) cit. p.1069*

[27] Sul tema in particolare MANES V.: *Il principio di offensività Nel diritto penale . Canone di politica criminale, criterio ermeneutico, parametro di ragionevolezza, "*Giappichelli . 2005 - 79-83

[28] CADOPPI VENEZIANI, Elementi di diritto penale, parte speciale, Padova 2007, 215.

[29] Così BIANCHI M, art. 600 quater 1, cit. p528, Per un approfondimento sul concetto si dignità e per un'analisi critica del suo utilizzoquale bene giuridico meritevole di tutela penale, DELSIGNORE S., art. 600 ter, cit. pp.415 e ss. nonchè Id.*Mercificazione della persona e delitti di pornografia minorile, cit. p. 44.* Rileva l'A. come la nozione di dignità intesa in prospettiva oggettivistica e sovraindividuale, quale prerogativa dell'umanità nel suo complesso, o di una categoria di soggetti(i minori in questo caso),mostra un rapporto non sempre chiaro con il concetto di autonomia e autodeterminazione. Prescindendo dal singolo individuo, ma potendo essa stessa essere imposta dall'esterno, rischia di prestarsi ad operazioni neomoralizzatrici, che potrebbero finire per compromettere le prerogative individuali anziché rafforzarle.

[30] Bene giuridico di matrice costituzionale, secondo ill dato letterale dell'art. 2 Cost. e precisamente la parte della disposizione in cui il Costituente ha riconosciuto e garantito i diritti inviolabili dell'uomo sia come singolo ,sia nelle

sopra evidenziato, su di un' interpretazione particolarmente restrittiva tesa a forzare la lettera della norma- nel tentativo di salvare la norma da una probabile pronuncia d'incostituzionalità, rischia di tradire il vero spirito del legislatore , ossia quello di distruggere definitivamente il mercato della pedopornografia nella sua globalità , comprese le immagini totalmente virtuali[31]. Allo stato pertanto , stando ad un'interpretazione letterale del dettato normativo, nonché alla *voluntas legis* espressa negli stessi lavori preparatori, la norma non potrebbe che collocarsi nell'ambito dei reati "ostacolo", in quanto si presume che il materiale virtuale possa istigare alla commissione di ulteriori reati di pedopornografia o di pedofilia o di violenza sessuale in danno dei minori[32].
Malgrado quindi la condivisibile enunciazione di intenti del legislatore della riforma, nel tentativo rispondere nel modo più efficiente possibile alle nuove esigenze repressive, frutto del progresso tecnologico, resta compito dell'interprete al momento ,cercare di recuperare le fattispecie introdotte dal rischio di un 'eccessivo arretramento della soglia di punibilità e quindi della funzione critica e selettiva del concetto di bene giuridico. Spetterà poi alla prassi , affermare interpretazioni che ne recuperino la compatibilità con il principio di offensività, attraverso l'accertamento in sede processuale della concreta pericolosità dei fatti oggetto della disciplina penale delineata dalla nuova legge anche quando si tratti di scambio di immagini meramente virtuali.

6. La pornografia virtuale in rapporto alla libertà informatica e telematica ex. Art. 21 della Costituzione

Come emerge dalle osservazioni finora svolte, l'attuale formulazione della fattispecie di pedo-pornografia virtuale, se interpretata in base ad un criterio semantico sembra peccare di ipertrofia penalistica, equiparando con presunzione *iuris et de iure* la pornografia reale, a quella puramente virtuale, frutto di mera immaginazione (rappresentazione virtuale di un bambino inesistente), consistente in disegni, immagini, fotomontaggi, risultati di evolute tecniche di elaborazione informatica. Ora, se nell'ottica di un adeguato bilanciamento di interessi e valori fra cui la tutela dello sviluppo psico-fisico del minore ex. Artt.2 e 31 della Costituzione e la libertà di parola, indubbia prevalenza è da accordare alla prima esigenza, diversa valutazione va per quei casi in cui il bene giuridico che si vorrebbe tutelare tramite la sanzione penale e per cui legittimamente si pongono limiti alla libertà di espressione, sembra porsi sullo sfondo e per una sorta di eterogenesi dei fini divenire marginale. La fattispecie se reinterpretata come direttamente lesiva della moralità

formazioni sociali ove " si svolge "la sua personalità. La personalità dell'uomo è cioè considerata come un dato in continua e progressiva evoluzione.é dunque un'interpretazione letterale, che evoca l'idea della tutela del diritto di libertà sessuale non solo come posizione acquisita bensì, più latamente, come libertà *in fieri,*in costante evoluzione soprattutto se riferita al minore

[31] DI GIOVINE, sub.art. 600 quater, in Codice penale, rassegna di giurisprudenza e dottrina, LATTANZI G. ,LUPO E.,(diretto da) V ed.Milano, 2000.;DELSIGNORE, . *mercificazione della persona e delitti di pornografia minorile, cit. 41 e ss.*

[32] NATALINI, "Stretta .contro la pedopornografia in rete. Così Roma si allinea ai dettami della UE, " in Dir. e Giust. N.9/2006,p.114; BENVENUTO, sub. Art. 600 quarter 1 c.p., "Reati contro la persona" a cura di MANNA A., Torino, 2006.. p. 538; PISTORELLI, sub art. 600 quater1 c.p.,p.4171 in Codice penale commentato,(a cura di MARINUCCI-DOLCINI) II ed. IPSOA,Milano, 2006.

pubblica[33], sarebbe pursempre conforme ai limiti logici che la stessa Costituzione pone alla libertà d'espressione: l'ordine pubblico ed il buon costume. Se però il bene giuridico oggetto di tutela è meta-individuale e diversi sono i termini in rapporto dicotomico i.e. libertà di manifestazione del pensiero e la pubblica moralità, è evidente come diversa sarà anche l'attenzione che il legislatore dovrà porre nell'esercizio legittimo della propria discrezionalità in materia penale[34]. Se da un lato la vicinanza tra norme penali e norme culturali è volta a garantire l'efficacia e l'effettività del sistema penale nel suo complesso, dall'altro vi è l'esigenza che il principio di laicità, anche contatto con le esigenze pratiche di tutela dei nuovi fenomeni criminosi non subisca deroghe o lesioni .Principio che deve guidare il legislatore negli interventi in settori particolarmente delicati come quelli che vedono coinvolti le tecnologie dell'informazione e la loro influenza nella crescita , socio-psicologica del minore. Si pensi ai nuovi "non – luoghi della "cyber-pedofilia dove a rischio non è solo l'integrità psicofisica del minore , ma anche la sua normale capacità di rapportarsi con il sesso, le relazioni interpersonali , la dimensione affettiva dei rapporti umani. La fluidità di genere, cioè l'assunzione di una pluralità di differenti identità sessualmente diversificate(non solo maschile/femminile ma anche indeterminata) è evento ricorrente all'nterno dei *queerness(*spazi comunicazionali lett. Bizzarri o eccentrici) e in alcuni MUD (*Multi –users Dimensions Dungeos),* di solito effettuati da *alter-ego* alla ricerca di incontri sessualmente stimolanti, in una dimensione non reale. Il rischio che ne deriva vede l'adolescente-non più il bambino-come bersaglio di esperienze sessuali virtuali destinate poi ad essere rilasciate da altri utenti per un *continuum* di sollecitazioni che, certamente, non contribuiscono ad una serena crescita del minore. Sono questi "non luoghi", dove la pornografia perde il connotato di "evidenza" di abuso compiuto, per assumere quello di strumento di avvicinamento, di convincimento per indurre il giovane interlocutore a ritenere "normali" certe raffigurazioni ed in cui vorrebbe farsi spazio l'intervento del legislatore[35], che hanno dato nuova linfa al secolare dibattito sul confine tra diritto e morale, di fronte a quell'"attentato culturale" che internet rappresenta.

---

[33] Così criticamente COCCO G., CIT. P. 878, secondo cui collegamento con il bene della personalità sessuale *in fieri* del minore è talmente indiretto –se non addirittura inesistente , da indurre a ritenere che l'unico interesse ipotizzabile possa essere la moralità pubblica ; nello stesso senso, MANNA: "*Reati contro la persona,* vol II, Giappichelli , 2007,cit. pp.219-240.;MANNA-RESTA, cit. P.224; MONTELEONE M.: *"Lo sfruttamento sessuale dei bambini e la pedopornografia nella legge 6 febbraio 2006 n.38*, in Giurisp. Di Merito, n.9, 2007,p.2208.PICOTTI L.,cit- p. 329 secondo cui nonostante la diversa enunciazione d'intenti da parte del legislatore, a seguito della riforma del 2006 ed in particolare con l'aggiunta dell art.600 quater1,è proprio tale oggettività giuridica che sembra riaffiorare.

[34] Sul tema si veda la già citata sentenza del 16 aprile 2002, della Corte Suprema degli Stati Uniti ,caso *Ashcroft vs Free speach Coalition,*che ha dichiarato l'illegittimità costituzionale per violazione del I Emendamento(*freedom of speach)* dell art. 2256(8) del *"Child pornography Prevenction Act (CPPA)* relativamente all'incriminazione del possesso di pedopornografia totalmente virtuale :trattasi della più importante pronuncia in argomento, dopo il caso *Miller vs. California,413 US* 15, 93, S.Ct.,2607, (1973) in cui la Corte statunitense distinse tra *hard –core pornography*, e *soft-pornography*, che limitandosi a simulare l'atto sessuale poteva ritenersi riconducibile alla sfera di tutela del I emendamento.

[35] Il riferimento è in particolare al d.d.l. 2326 , approvato dalla camera dei Deputati il 19-1-2010 ed attualmente all'esame del Senato, recante "Misure di sensibilizzazione e prevenzione, nonché repressione dei delitti contro la persona e nell'ambito della famiglia, per l'orientamento sessuale l'identità di genere ed ogni altra causa di discriminazione", il cui art. 12 inserisce una fattispecie dai contorni poco definiti di *grooming:* si tratta della tecnica mediante cui l'adulto, potenziale abusante, "cura" (*grooms)* ,la potenziale vittima, inducendo gradualmente il ragazzo a superare le resistenze ,attraverso tecniche di manipolazione psicologica. La condotta incriminata consiste dunque , nel compimento di atti volti a carpire la fiducia del minore di età inferiore a 16 anni, attraverso artifici, lusinghe o minacce posti in essere anche mediante internet, o altri mezzi di comunicazione.

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 68-84

Reati nell'e-commerce e tutela dell'utente

Francesco Buffa

Abstract: Nell'ambito dell'e-commerce, particolare rilevanza assumono, anche per la loro diffusione, varie forme di truffa. A protezione degli utenti sono applicabili alcune norme civilistiche, ma queste sono in diversi casi insufficienti, non disponendo il singolo consumatore di strumenti effettivi di ricerca dell'autore della frode e di tutela nei suoi confronti, mentre l'applicazione delle norme penali assicura risultati più proficui nella scoperta e repressione delle frodi. Le norme penali rilevanti sono diverse, a seconda delle modalità di perpetrazione del reato e dell'oggetto della condotta.

In the context of the e-commerce, different types of fraud may occur, and they are relevant also for their spread, being the area of the victims wide. To protect consumers some rules of civil law apply, but these are in many cases insufficient, as the individual users have not adequate tools to reach an effective protection against the author of the fraud and to discover his identity, while the application of criminal rules is more useful to discover and punish frauds. The relevant criminal rules are many, being their application depending on the way of commission of the offense and the object of the conduct.

Parole chiave: truffa, frode, indirizzo IP, consumatore

1. Truffe on line.

Tra le varie fattispecie criminose che possono venire in considerazione nell'ambito dell'e-commerce, particolare rilevanza assumono, anche per la loro diffusione, le varie forme di truffa. Il fenomeno delle truffe in rete è fortemente diffuso e la pericolosità e diffusività delle fattispecie criminose che si vanno ad analizzare emerge sol che si consideri (con M.Strano, *Computer crime*, Apogeo, 2000, 161-162) che per alcuni soggetti, completamente estranei al mondo del crimine, la navigazione in rete può rappresentare l'opportunità di venire a conoscenza di tecniche illegali in precedenza reperibili solo in ambienti subculturali criminali, e che, inoltre, la relativa facilità di perpetrare frodi in rete, operando dal comodo ambiente domestico ed in modo "virtuale" piuttosto che fisicamente con i rischi della realtà, determina una alterazione della percezione del crimine.

Articolo pervenuto il 18 ottobre 2013, approvato il 30 dicembre 2013

Negli USA, l'*Internet fraud watch della National Consumer League* (www.ifcc.org) ha segnalato in apposito rapporto le principali forme di truffe telematiche, di seguito riportate in ordine di rilevanza (v. M.Strano, *Computer crime*, Apogeo, 2000, 153-154, e da T.Malagò e M.Mignone, *Le frodi con carte di credito*, Franco Angeli, 2001, pag. 2 ss.):

- finte vendite all'asta sul *web*, con merci offerte e mai inviate ai clienti o con prezzi gonfiati;
- vendite di merci generiche su catalogo *on line*, con merci mai inviate o diverse rispetto a quanto pubblicizzate;
- offerta di servizi gratis su *Internet*, che si rivelano poi a pagamento;
- vendita di *software* su catalogo *on line*, con merci mai inviate o diverse rispetto a quanto pubblicizzato;
- schemi di investimento a piramide e *multilevel business*;
- offerte di lavoro a casa con acquisto anticipato di materiale necessario all'esecuzione del lavoro stesso;
- opportunità di affari e *franchising*;
- prestiti di denaro (mai concessi) con richiesta di pagamento anticipato di commissione;
- false promesse di rimuovere informazioni negative per l'ottenimento di crediti (ad es. rimozione da *black lists*);
- false promesse di concessione di carte di credito (con richiesta di commissione) a soggetti con precedenti negativi.

Numerose frodi sono state registrate nel settore delle offerte di investimento proposte in rete (sul tema, T. Malagò, A Scartezzini, G.Meluzzi, *I nuovi rischi criminali nella cyberfinanza*, Franco Angeli, 2000, p. 59).

Le frodi finanziarie si servono sia di nuovi mezzi che di vecchi schemi, utilizzati in *Internet*.

Quanto ai primi, si richiamano i siti *web*, le *on line messages areas*, le *e-mail*, le *on line investment news letters*.

I siti *web* innanzitutto: come si è rilevato, un sito *web*, la cui realizzazione è assai facile e a bassissimo costo, conferisce al promotore del raggiro una visibilità planetaria, consentendogli di reclutare le proprie vittime su scala internazionale.

Si è pure detto che la volatilità dello strumento permette, una volta realizzata la frode, di far sparire il proprio sito dalla rete così velocemente come è apparso ed in più senza lasciare tracce.

Si è pure osservato che la predisposizione del sito va affiancata ad altri strumenti, quali *link* in pagine strategiche che rimandano al sito ovvero o evidenze in *newsletters* compiacenti che esaltano le offerte economiche del sito.

In tale ambito, anche le aree informative possono essere strumento di frode sia direttamente, quale veicolo di informazioni distorte e compiacenti, sia quali strumenti di raccolta di indirizzi di posta elettronica dei partecipanti alle aree, da contattare poi privatamente per proposte commerciali fraudolente.

Vengono poi spesso utilizzate in *Internet* schemi fraudolenti per così dire "classici", nel senso di esser stati già sperimentati fuori dai circuiti telematici della rete.

Rientrano in tale ambito il *pump and dump*, gli schemi piramidali alla Ponzi, gli schemi di arricchimento facile *risk free* ovvero *get rich quick*.

Il *pump and dump* consiste nel diffondere informazione di comodo su una data impresa (occasioni di sviluppo, dati contabili, notizie varie, ecc.) al fine di incidere sull'apprezzamento del pubblico

verso la stessa: non si tratta di meri strumenti pubblicitari, ma di divulgazione di notizie non vere o "gonfiate" da parte di soggetti apparentemente neutrali, al fine di attirare l'attenzione di investitori o acquirenti in buona fede, che vengono così indotti ad acquistare beni o servizi offerti in rete da quella data società.
Gli schemi piramidali alla Ponzi (dal nome di un famoso operatore attivo nel settore) sono strumenti di marketing consistenti nel convincere la gente ad acquisire la facoltà di vendere ad altri il diritto di commercializzare un determinato bene o servizio; in tale schema, il profitto deriva non tanto dal vendita del prodotto quanto dal reclutamento di nuovi investitori, i quali andranno a loro volta alla ricerca di altre persone da inserire nella struttura distributiva. In tale sistema di vendita, è richiesto ai vari elementi della catena un investimento iniziale, che gli stessi riescono poi a recuperare con il reperimento dei nuovi distributori; peraltro, il recupero finanziario è spesso possibile solo per chi ha dato inizio allo schema, laddove man mano che la catena avanza l'investimento in favore dei precedenti elementi della catena è sicuro, mentre il recupero verso gli elementi successivi della catena lo è sempre meno.
Altre volte, si offre la possibilità di inserirsi, con un piccolo versamento, in un investimento che promette di ripagare la vittima in poco tempo, e si invita la persona a diffondere ulteriormente l'offerta; per i primi tempi si assicura alle vittime un ritorno delle somme, ed anche un guadagno e successivamente lo stesso (le cui difese sono ridotte dai guadagni iniziali) viene indotto ad effettuare sempre nuovi versamenti che risulteranno essere -a frode consumata- a "fondo perduto".
Una variante degli schemi piramidali è data dalle c.d. catene di S.Antonio (M.Strano, *Computer crime*, Apogeo, 2000, 155), nelle quali ad esempio si offre al destinatario l'illusoria possibilità di diventare ricco in breve tempo operando nel modo che segue: viene inviato una lista di nomi con l'invito al destinatario ad inviare poche somme al nome che si trova in cima alla lista; la vittima viene invitata a spedire la somma e successivamente a cancellare il nome della persona cui ha inviato le somme e a scrivere il proprio nome in calce alla lista; la vittima, in tal modo, finisce con il credere che dopo un certo numero di passaggi -che opportunamente potrà sollecitare inviando a catena l'*e-mail* ai suoi conoscenti- egli raggiungerà la cima della lista e riceverà così il denaro (in quantità notevolmente superiore a quella a suo tempo inviato) da tutti coloro che sono dopo di lui nella lista: naturalmente, le possibilità che un incauto navigatore possa ottenere i guadagni promessi da una catena del genere è infatti praticamente nulla.
Infine, gli schemi di arricchimento facile comprendono offerte finanziarie di elevatissimo rendimento e tuttavia di enorme rischio speculativo: esse peraltro si svolgono al di fuori dei circuiti finanziari e bancari tradizionali e solitamente in rete, senza sottostare dunque ai controlli -di regolarità delle operazioni e di stabilità patrimoniale dell'intermediario finanziario- delle autorità di vigilanza nazionali, e presentano così ulteriori profili di sicuro rischio.

Tra le frodi occorse nell'ambito del commercio elettronico, vanno ricordate quelle in cui il fornitore fraudolentemente offre beni apparentemente privi di vizi e con le qualità pubblicizzate e poi consegna invece al proprio cliente articoli difettosi o priva delle qualità promesse.
Con specifico riferimento al pericolo di frodi relativo al consumatore nell'ambito degli acquisti *on line* di beni e servizi, alcune regole cautelari consentono un livello minimo di sicurezza.
Occorre così assicurarsi di trattare con esercenti *Internet* affidabili, controllando con la Camera di commercio e con le associazioni di consumatori se ci sono state denunce o proteste effettuate da altri utenti. Per verificare l'attendibilità di un negozio *on line* si possono controllare sul sito stesso

una serie di informazioni, come ad esempio note sulla politica di *privacy* seguita, informazioni precise sull'offerta, sulle garanzie e sul diritto di recesso, indirizzo e numero di telefono del negoziante, modalità di protezione dei dati. Utile è sempre un riferimento alla *reputazione informatica* del venditore (configurabile in modo neutro in sistemi chiusi, come ad es. in *ebay*, ove il feedback indicato dai precedenti acquirenti informa i nuoti acquirenti della serietà e correttezza del venditore). Il consumatore deve essere cauto nel proteggere i propri dati personali e, a tal fine, non deve fornire mai né la *password* con cui si ha accesso al proprio *Internet provider* né quella del proprio conto corrente *on line*. È bene poi stampare o salvare su supporto durevole tutti i dati della transazione *on line*.

2. Truffa contrattuale.

Potrà trovare applicazione in materia l'art.640 cod.pen., che punisce, tra i delitti contro il patrimonio mediante frode, il reato di truffa, punendo colui che, con artifici e raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno.
Nell'ambito della truffa rileva quale figura speciale la truffa contrattuale, nella quale la frode determina la volontà rispetto alla stipula di un contratto ovvero alla determinazione del contenuto di un contratto: in altri termini, l'inganno determina un errore sulla motivazione del volere e provoca una inesatta conoscenza della situazione di fatto sulla cui base la volontà si determina alla conclusione del contratto, diversamente non concluso, o concluso a condizioni diverse.
Possiamo evidenziare nella struttura della truffa contrattuale due distinti processi causali: uno fra il comportamento dell'agente e l'errore altrui; l'altro fra l'errore e l'atto di disposizione patrimoniale del soggetto truffato.
Sotto il primo profilo, occorre individuare artifizi ed inganni (previsti dalla norma in via alternativa) di natura antigiuridica tali da incidere in modo significativo sul processo di formazione della volontà. L'artifizio è collegabile alla c.d. messa in scena e, cioè, ad una trasformazione della realtà, diretta a far ritenere "esistente l'inesistente" oppure a nascondere l'esistenza stessa; nel raggiro invece vi sarebbe un'aggressione dell'altrui psiche, tramite un'attività ingegnosa e menzognera, finalizzata ad indurre in errore. In entrambi i casi, l'artifizio o il raggiro devono essere tali da incidere sulla volontà negoziale del soggetto passivo, secondo una valutazione effettuata alla stregua delle valutazioni sociali medie e delle specifiche condizioni del soggetto passivo. Una volta in atto la "messa in scena", le modalità rapide di interazione tra i contraenti offerte dai mezzi telematici fanno il resto, consentendo una rapida ed istantanea conclusione del contratto, senza adeguata ponderazione da parte del contraente debole.
La condotta fraudolenta è necessariamente diretta a creare nella psiche del destinatario una falsa rappresentazione della realtà, ma la legge non predetermina le modalità della stessa, che è pertanto libera. Rileva così la consapevole alterazione del vero quale condotta positiva che, come logica conseguenza, induce una falsa rappresentazione della realtà nel destinatario della condotta stessa. Rileva altresì il mendacio, quando sia comportamento positivo rivolto ad incidere sulla volontà negoziale della controparte, e ciò a prescindere dall'esistenza di un obbligo di dire la verità nel caso. Per converso, non costituiscono artifizi gli elogi o le valutazioni particolarmente positive della propria merce da parte del venditore verso il compratore.

Più controversa la possibilità di ravvisare l'artifizio o il raggiro in fatti negativi o omissivi: al riguardo, parte della dottrina e la giurisprudenza prevalente (cfr. per tutte Cass. Sez II, 2/03/1996, Capra) ritengono l'art. 640 cod.pen. applicabile anche alle condotte omissive, partendo dalla considerazione che nella realtà dei rapporti giuridici non solo vi può essere un dolo omissivo, ma anche una condotta omissiva posta in violazione di regole comuni di correttezza nella condotta, sulla base delle quali il soggetto passivo si aspetta informazioni rilevanti che invece non riceve. Più di recente, Cass. s*ez.* 2, s*entenza n.* 41717 *del* 30/10/2009 ha affermato che gli artifizi o i raggiri richiesti per la sussistenza del reato del reato di truffa contrattuale possono consistere anche nel silenzio maliziosamente serbato su alcune circostanze da parte di chi abbia il dovere di farle conoscere, indipendentemente dal fatto che dette circostanze siano conoscibili dalla controparte con ordinaria diligenza. (Fattispecie di tentata truffa in cui il venditore di un immobile aveva taciuto il fatto che il mutuo per l'acquisto dello stesso era stato stipulato da soggetto coinvolto in reato di corruzione con il rischio di possibile confisca per equivalente dell'immobile stesso).
Così, un onere di informazione deriva spesso dal generale obbligo di correttezza. Esso tuttavia è specificato con riferimento alla prestazione di servizi della società di informazione dall'art. 5 della direttiva 2000/31/CE.
Al di fuori di questo ambito, l'art. 1175 e 1375 cod.civ. obbligano le parti del rapporto obbligatorio o contrattuale ad una lealtà e correttezza di comportamento, definendo un modello di comportamento rilevante anche per gli effetti penali (ad es. per la valutazione della divergenza del comportamento tenuto dal soggetto agente rispetto alla normalità del comportamento contrattuale e dunque alla attribuzione di rilevanza alla reticenza della parte).
Secondo un orientamento diffuso, il diritto vieta solo la creazione intenzionale e dolosa di motivi nella determinazione altrui e non vieta invece ai soggetti di trarre profitto da favorevoli contingenze quali possono derivare anche da una deviata formazione di tali motivi, sicché non rientrerebbero nella truffa contrattuale i fatti commessi approfittando del mero errore in cui si trova la vittima.
Certo, altro è lasciare taluno nell'ignoranza, altro è indurre in errore taluno, o mantenere l'errore in violazione dell'obbligo di rettifica o precisazione o informativa, ovvero consolidare con il proprio comportamento mendace l'errore altrui, o ancora sfruttare contrattualmente l'erroneo convincimento in cui la controparte si trovi. In tutte queste ipotesi da ultimo indicate non sembra seriamente contestabile l'efficienza causale della condotta del soggetto agente nella formazione dell'errore di chi sarà la controparte contrattuale.

L'errore rileva ove porti il soggetto passivo, tramite artifizi e raggiri, a concludere un contratto che diversamente non avrebbe mai compiuto: per Cass. *Sez.* 2, sentenza 32859 *del* 21/08/2012, ricorrono gli estremi della truffa contrattuale tutte le volte che uno dei contraenti ponga in essere artifizi o raggiri diretti a tacere o a dissimulare fatti o circostanze tali che, ove conosciuti, avrebbero indotto l'altro contraente ad astenersi dal concludere il contratto.
Ma il reato sussiste anche se il truffato conclude il contratto a condizioni diverse da quelle che avrebbe altrimenti accettato (Cass. sez. II, 15/01/1999, Solinas): infatti, la distinzione civilistica tra *dolus causam dans* e *dolus incidens* non è rilevante in sede penale. Infatti, per il diritto civile, infatti, solo quando il dolo è stato decisivo per la determinazione della volontà negoziale, cioè quando senza quell'inganno il *deceptus* non avrebbe prestato il consenso al contratto, il dolo è causa di annullamento, mentre invece quando è servito unicamente a stabilire patti più gravosi, è soltanto causa dell'obbligo di risarcimento per la parte in mala fede; la nozione penalistica invece

è autonoma, potendo integrare gli estremi della truffa contrattuale anche il dolo incidente, e non solo quello determinante, richiedendo la norma che la condotta fraudolenta abbia determinato una situazione comunque pregiudizievole per l'altra parte.
L'errore per essere rilevante ai fini penali non deve necessariamente, secondo l'indirizzo che appare preferibile, cadere su elementi essenziali del negozio, potendo rilevare anche l'errore su elementi accessori (magari ai quali le parti davano particolare rilevanza: cfr. Cass. 2/02/1998, n. 985).
Secondo l'indirizzo prevalente in dottrina, le categorie giuridiche civilistiche e penalistiche divergono nella tutela degli interessi coinvolti dalla truffa contrattuale: infatti, mentre ai fini civilistici il vizio della volontà rileva in sé a prescindere dagli effetti sul piano patrimoniale e consente l'attivazione delle tutele di legge, in ambito penale la violazione del dovere di buona fede è in sé insufficiente ad integrare gli estremi del rato di truffa, essendo questo un reato contro il patrimonio. Così, si è detto, la mera stipulazione di un contratto in quanto tale, se esaurisce e perfeziona l'azione del *reus*, non importa in sé alcuna effettiva diminuzione patrimoniale, ma pone in essere solo il pericolo che l'ingannato compia una prestazione che sminuisca il suo patrimonio senza un corrispettivo equivalente.
Lo sfasamento temporale tra il conseguimento del profitto e la produzione del danno e la diversa rilevanza data della mera stipula quale danno si riflettono nella valutazione della fattispecie sotto il profilo del momento consumativo del reato: secondo l'orientamento prevalente, il reato si consuma non nel momento in cui la vittima assume l'obbligazione, ma quando l'agente consegue il profitto, e cioè la concreta disponibilità del bene, con l'effettivo corrispondente danno altrui (C.Parodi - A.Calice, *Responsabilità penali ed Internet*, Il sole 24 ore, 2001, p. 194; in giurisprudenza, v. Cass. sez. un., 21 giugno 2000, Franzo e altri), avendosi in precedenza solo un tentativo punibile.
Quanto ai soggetti del rapporto costituendo, non vi sono grosse particolarità: va peraltro ricordato che secondo la giurisprudenza, la truffa contrattuale ex art. 640 cod.pen. può operare anche nel caso in cui una delle parti contrattuali sia una macchinetta automatica, sicché il carattere informatico dell'oggetto materiale della condotta non rileva affatto ad escludere la truffa.
Né, ove si tratti di sistemi informatici o telematici, può prospettarsi la possibilità di applicazione della norma sulla frode informatica, posto che di questa non ricorrono sempre i presupposti di legge (e può aversi errore nella determinazione contrattuale senza alcuna interferenza illecita su dati informazioni o programmi o sul funzionamento del sistema informatico o telematico).
Ulteriore problema è stato individuato, sempre nell'ambito della formazione del contratto, nella c.d. truffa *in re illecita*, che sussisterebbe ogniqualvolta lo stesso soggetto passivo, in realtà, o provi a truffare la controparte ovvero sia spinto da motivazioni *contra legem*. In tali casi, allora, ci si è chiesti se siano punibili entrambi i soggetti o solo chi ha truffato di più.
In particolare, infatti, è stato sottolineato da parte della dottrina come lo stesso ingiusto profitto con conseguente danno altrui, andrebbe controbilanciato con il danno subito a causa della condotta fraudolenta della controparte, sicché sarebbe punito solo chi avrebbe causato in concreto il danno.
Tale orientamento, tuttavia, non convince altra parte della dottrina che pone l'accento sul concetto stesso di ingiusto profitto, considerando per tale quello conseguente agli artifizi e ai raggiri posti in essere tali da indurre in errore la controparte; la condotta, cioè, sarebbe ingiusta indipendentemente dal quantum del danno causato. In questo senso, allora, in caso di truffa c.d. reciproca sarebbero punibili entrambi i soggetti.
Si è invece sottolineata l'impossibilità di configurare una sorta di elisione dei due doli, rilevandosi

anzi che il dolo della persona offesa non neutralizzi la pericolosità del reo, ma la ponga in maggiore evidenza in quanto il truffatore deve superare la più acuta astuzia dell'uomo in mala fede.

3. Insolvenza fraudolenta.

Gli artifizi possono consistere anche nella messa in scena di un'attività commerciale apparentemente seria ed affidabile, che induca il compratore a fidarsi del contraente e ad effettuare pagamenti *on line* per beni e servizi ancora da ricevere, e poi di fatto mai inviati dal venditore.
In tali casi, può trovare applicazione la norma relativa alla truffa, e ciò anche ove vi sia stata nel venditore l'intenzione di non adempiere l'obbligazione sin dal momento in cui veniva contratta. Se peraltro fosse stato presente uno stato di insolvenza del venditore sin dal momento dell'assunzione dell'obbligazione, la norma applicabile sarà quella dell'insolvenza fraudolenza telematica, reato di chi, dissimulando il proprio stato di insolvenza contrae un'obbligazione col proposito di non adempierla, qualora l'obbligazione non sia adempiuta (art. 641 cod.pen.).
Nel caso di contatti telematici, infatti, la dissimulazione dello stato di insolvenza può ben ravvisarsi secondo la dottrina (C.Parodi, A.Calice, *Responsabilità penali ed Internet*, Il sole 24 ore, 2001, p. 197) e la giurisprudenza (Cass. 26.11.92, rv. 193160), nel silenzio circa la propria condizione, e ciò almeno nel caso in cui tale stato non sia manifestato alla controparte ed il silenzio su di esso sia legato al preordinato proposito di non adempiere.

4. Frode in commercio elettronico.

L'art. 515 cod.pen. punisce chi, nell'esercizio di un'attività commerciale, ovvero in uno spaccio aperto al pubblico, consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita.
La sanzione prevista è, qualora il fatto non costituisca un più grave delitto, quella della reclusione fino a due anni o della multa fino a quattro milioni di lire; se si tratta di oggetti preziosi, la pena è della reclusione fino a tre anni o della multa non inferiore a lire duecentomila.
La fattispecie è senza dubbio applicabile anche all'attività esercitata in rete nell'ambito del commercio elettronico, e ciò sia nel commercio elettronico diretto che in quello indiretto: infatti, le modalità telematiche di consegna del bene ceduto non rilevano ai fini della configurazione della fattispecie, per la realizzazione della quale occorre solo la diversità obiettiva del bene consegnato nel senso sopra indicato.

Il presupposto della fattispecie è la stipulazione di un contratto: non rilevano le modalità di perfezionamento dell'accordo, né la forma dello stesso, operando la norma anche nel caso di conclusione automatica del contratto o di accordo telematico, e quali che siano le forme dell'incontro della volontà delle parti (proposta ed accettazione, offerte incrociate, *point and click*, aste telematiche, negozi su apparecchi automatici, ecc.).
Non occorre che il contratto sia valido o lecito, secondo un orientamento; secondo altro indirizzo, invece (che risale a F.Antolisei, *Manuale di diritto penale*, parte speciale, Giuffré, Milano), la frode

in commercio presuppone un contratto, che non deve essere né inesistente né illecito; ne deriva, secondo tale indirizzo, l'inapplicabilità della norma a chi commetta frode nelle pattuizioni relative a merci di contrabbando,a sostanze stupefacenti, a contrattazioni che si svolgono nel mercato nero.

Il contratto cui fa riferimento la norma non è solo quello di compravendita, potendo operare anche nel contratto estimatorio, nella permuta, nel contratto di somministrazione, ed in qualunque altro contratto che importi l'obbligo di consegna di una cosa mobile ad un acquirente, ossia ad un soggetto che acquista un potere di disposizione sulla cosa corrispondente ad un diritto di proprietà o reale.

Il reato nel commercio elettronico indiretto si consuma, secondo un orientamento, con la spedizione della merce o con l'affidamento al vettore, mentre nel commercio elettronico diretto con l'invio del *file*, ed a prescindere dal momento di ricezione della merce: nel detto precedente momento, infatti, si avrebbe il c.d. svincolo, ossia la fuoriuscita del bene dalla sfera di controllo dell'alienante; secondo altro orientamento, invece, la frode postula un contenuto relazionale della condotta, sicché occorrerebbe pur sempre, ai fini della consumazione del reato, che la merce sia giunta all'indirizzo del destinatario o comunque entrata concretamente nell'ambito della sua sfera di controllo.

La consegna del bene diverso importa l'applicazione della norma a prescindere dal fatto che l'agente abbia usato particolari accorgimenti per ingannare l'acquirente. Peraltro, ove siano stati posti tali accorgimenti, si pone il problema del rapporto della fattispecie in esame con la tuffa, ed in particolare con la truffa contrattuale. Al riguardo, deve rilevarsi che la norma sulla frode in commercio trova applicazione quando l'inganno non ha avuto alcuna influenza sulla conclusione del contratto, ma si è verificato esclusivamente nella fase successiva dell'esecuzione e, in particolare, nell'atto della consegna, ovvero nel caso in cui l'inganno è stato sì la causa determinante del contratto, ma non ricorrono gli estremi della truffa perché la consegna sleale di altro bene non ha arrecato alcun pregiudizio patrimoniale all'acquirente: ove invece la consegna del bene diverso sia conseguenza della truffa contrattuale e dell'inganno compiuto già nella fase della conclusione del contratto, e si sia verificato un danno patrimoniale (nel senso precisato in proposito in tema di truffa contrattuale), si avrà solo la truffa, essendovi concorso apparente di norme (evidenziato dalla clausola di riserva contenuta nel'art. 515, che prevede l'applicazione della pena salvo che il fatto non costituisca più grave delitto).

E' bene precisare da ultimo che la cessione di determinati beni nell'ambito del commercio elettronico può far applicare altre norme del codice penale, dettate proprio in relazione al bene: per le sostanze alimentari contraffatte o adulterate l'art. 440, per i medicinali guasti l'art. 443, per le sostanze alimentari nocive l'art. 444, per le monete falsificate l'art. 455 e 457, per i valori di bollo falsificati l'art. 459.

5. Frode informatica.

Sul piano penalistico, viene in considerazione quale ulteriore norma di riferimento in materia, l'art. 643 cod. pen., che sanziona la frode informatica. La norma prevede due fattispecie: la prima è costituita dal fatto di chi, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico, procura a sé o ad altri un ingiusto profitto con altrui danno; la seconda, dal fatto di chi, intervenendo senza diritto con qualsiasi modalità su dati informazioni programmi di un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno.

Come precisato da Cass. Sez. 2, Sentenza n. 44720 del 20/11/2009, il reato di frode informatica si differenzia dal reato di truffa perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema. (Nella fattispecie l'imputato, dopo essersi appropriato della "password" rilasciata a un terzo, responsabile di zona di una compagnia assicurativa, manipolava i dati del sistema predisponendo false attestazioni di risarcimento dei danni).

Nella frode informatica, l'alterazione o l'intervento manipolativo penalmente rilevanti possono essere effettuati in qualsiasi modo; l'intervento peraltro può riguardare i dati (es. immissione, alterazione, cancellazione abusive), le informazioni (modificando il significato delle connessioni dei dati, con o senza incidenza sugli stessi), i programmi (anche senza incidenza sui dati e sulle informazioni).

L'alterazione e l'intervento manipolativo non sono le condotte direttamente punite dalla norma in esame, ma modalità dell'azione attraverso la quale il soggetto procura a sé o ad altri un ingiusto profitto con altrui danno: la frode informatica, infatti, è un reato contro il patrimonio.

Ove le modalità dell'azione siano poste in essere ma l'evento non si verifichi, potranno eventualmente ricorrere gli estremi della tentata frode informatica, in presenza di atti idonei diretti in modo non equivoco a commettere il delitto (art. 56 cod. pen.).

Quanto alla consumazione del reato, per Cass. Sez. 3, Sentenza n. 23798 del 15/06/2012, ai fini della determinazione della competenza territoriale, nel reato di frode informatica il momento consumativo va individuato nel luogo di esecuzione della attività manipolatoria del sistema di elaborazione dei dati, che può coincidere con il conseguimento del profitto anche non economico. (Fattispecie nella quale il luogo di commissione del reato è stato individuato nella sede della società gestita dagli imputati, presso la quale si trovavano i server contenenti i dati oggetto di abusivo trattamento). In tema, Cass. Sez. 2, Sentenza n. 6958 del 23/02/2011 ha precisato che il reato di frode informatica aggravata, commesso in danno di un ente pubblico, si consuma nel momento in cui il soggetto agente (nella specie: il pubblico dipendente infedele) interviene, senza averne titolo, sui dati del sistema informatico, alterandone, quindi, il funzionamento.

La Cassazione si è occupata per la prima volta diffusamente della fattispecie in un caso (Cass. 4 ottobre 1999, in *Foro it.*, 2000, I, 134 con nota di Fanelli e in *Cass. Pen.*. 2000, 2990, con note di Aterno, *Sull'accesso abusivo a sistema informatico o telematico*, e di Cuomo, *La tutela penale del domicilio informatico, definisce il sistema informatico o telematico*), ritenendo che integra il delitto di frode informatica, aggravata dall'essere compiuta da operatore di sistema, il fatto di chi, mediante la digitazione su apparecchi telefonici collegati a linee interne di una filiale Telecom di una particolare sequenza di

cifre, effettui una serie di chiamate internazionali, procurando danno alla Telecom, tenuta a versare agli enti gestori della telefonia nei paesi di destinazione l'importo corrispondente al suddetto traffico telefonico, e profitto per sé, ricevendo parte delle dette somme dagli enti gestori esteri.
Successivamente, la Cassazione ha fatto applicazione della norma in varie altre fattispecie. Per Cass. Sez. 2, Sentenza n. 17748 del 6/05/2011, integra il delitto di frode informatica, e non quello di indebita utilizzazione di carte di credito, la condotta di colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi, tra cui quella di prelievo di contanti attraverso i servizi di cassa continua Secondo Cass. n. 9891 del 11/03/2011, integra il reato di frode informatica, e non già soltanto quello di accesso abusivo ad un sistema informatico o telematico, la condotta di introduzione nel sistema informatico delle Poste italiane S.p.A. mediante l'abusiva utilizzazione dei codici di accesso personale di un correntista e di trasferimento fraudolento, in proprio favore, di somme di denaro depositate sul conto corrente del predetto. Cass. Sez. 2, Sentenza n. 13475 del 22/03/2013 ha ritenuto in tema che integra il reato di frode informatica, nelle forme dell'intervento senza diritto su dati e informazioni contenuti in un sistema informatico, oltre che quello di accesso abusivo ad un sistema informatico, la condotta del dipendente dell'Agenzia delle Entrate che, utilizzando la "password" in dotazione, manomette la posizione di un contribuente, effettuando sgravi non dovuti e non giustificati dalle evidenze in possesso dell'ufficio.
Quanto al sistema informatico e telematico, la cui nozione non è dato desumere espressamente dall'ordinamento giuridico, esso è qualificato dalla giurisprudenza richiamata (poi confermata dalle successive pronunce) come una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche, di tecnologie cioè caratterizzate dalla registrazione o memorizzazione per mezzo di impulsi elettronici su supporti adeguati di "dati e di informazioni", effettuata attraverso simboli (bit) numerici in combinazioni diverse.
La soluzione potrebbe non apparire così automatica, trattandosi di sistema elettronico informatizzato e non informatico tout court, ma la soluzione diversa lascerebbe ampi vuoti di tutela.
La Cassazione, in precedenza, si era pronunciata in materia di accesso abusivo a sistema informatico o telematico, facendone applicazione in un caso di uso di *pic-cards*, schede informatiche che consentono di vedere programmi televisivi criptati attraverso la decodifica di segnali trasmessi via satellite (Cass. 2 luglio 1998, n. 4389, in Cass. Pen., 2000, 535, con nota di Aterno, Aspetti problematici dell'art. 615-qua*ter* cod.pen.), e dunque già recependo una nozione ampia di sistema informatico e telematico, comprensivo di sistemi televisivi in presenza di apparecchi (c.d. *decoder*) di decodifica dei messaggi televisivi satellitari criptati.
In dottrina, per la nozione di sistema informatico, si vedano: R. Borruso, *La tutela del documento e dei dati*, in AA.VV., *Profili penali dell'informatica*, Giuffré, Milano, 1994, 4 ss.; R. Borruso, *Informatica e diritto*, relazione al convegno *Avvocati e nuove tecnologie della comunicazione*, organizzato in Roma, 23-24 giugno 2000, da Avvocatinrete, 4. G. Buonomo, *Metodologia e disciplina delle indagini informatiche*, in AA.VV., *Profili penali dell'informatica*, Giuffré, Milano, 1994, 148; Cuomo, *La tutela penale del domicilio informatico*, in *Cass. Pen*. 2000, 2999.
La norma prevede alcune circostanze aggravanti: così se il fatto è realizzato ai danni dello Stato

o di altro ente pubblico, o con pretesto di far esonerare qualcuno dal servizio militare, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.
Particolare l'aggravante dell'operatore di sistema.
Si tratta di un'aggravante nuova rispetto a quelle classiche del sistema penale, previste oltre che per il reato di accesso abusivo anche per la frode informatica e per altri reati informatici (artt. 617 *quater*, co. 4, n. 2, e 635 *bis* cod. pen.). La pronuncia della Cassazione sopra richiamata ravvisa gli estremi dell'operatore di sistema nel dipendente Telecom che, pur non specificamente addetto a sistemi informatici né al centralino telefonico della stessa Telecom, mediante la digitazione su apparecchi telefonici collegati a linee interne di una filiale Telecom di una particolare sequenza di cifre, abbia effettuato una serie di chiamate internazionali, procurando danno alla Telecom, tenuta a versare agli enti gestori della telefonia nei paesi di destinazione l'importo corrispondente al suddetto traffico telefonico, e profitto per sé, ricevendo parte delle dette somme dagli enti gestori esteri. Anche in tale ambito può segnalarsi, in assenza di un preciso dettato normativo, una posizione interpretativa quanto meno estensiva della qualità rispetto alla nozione recepita in dottrina (mentre in giurisprudenza non constano altre pronunce specifiche sul punto). Col termine di operatore di sistema (*system operator* o *sysop*), infatti, si comprende tradizionalmente sia l'operatore in senso stretto (cioè colui che è addetto alle operazioni di input, output, *bootstrap*, controllo, trasmissione telematica dei dati, stampa, ecc., del computer) sia il programmatore, il sistemista, l'analista (R. Borruso, *La tutela del documento e dei dati*, cit., 33), fino ad includere qualunque soggetto legittimato ad operare sul sistema (G. D'Aietti, *La tutela dei programmi e dei sistemi informatici*, in AA.VV., *Profili penali dell'informatica*, Giuffré, Milano, 1994, 74): si tratta di nozione che si fonda non su qualifiche astratte ma su un concreto specifico ed attuale (G.Pica, *Diritto penale delle tecnologie informatiche*, UTET, 1999, 77) collegamento funzionale di un soggetto con il sistema informatico (G.Pica, *Reati informatici e telematici*, *Digesto, disc. pen.*, Torino, 531), idoneo come tale ad evolversi continuamente in relazione alle nuove attività del mondo informatico e telematico (comprendendo così ad esempio oggi le figure del *system administrator* o del *webmaster*). Si è peraltro osservato (G.Giordanengo-M.Strata, *Osservazioni su alcune fattispecie di reato nel commercio elettronico*, 2000, 664) che, siccome si tratta di fattispecie aggravata di ipotesi base che già reca un momento abusivo, il più gravoso trattamento sanzionatorio non possa scattare neppure per la mera vicinanza al sistema, ossia per la mera qualità di soggetto che opera sul sistema, dovendo richiedersi altresì il possesso di conoscenze ulteriori e specifiche in relazione all'accesso. L'aggravante opera solo ove vi sia abuso della qualità specifica di operatore di sistema, non essendo sufficiente che vi sia abuso della qualità di dipendente dell'azienda -come sembra essere accaduto nel caso oggetto della su richiamata pronuncia della Cassazione- né sotto altro profilo che vi sia un operatore che non abusi delle conoscenze particolari possedute per ragioni di servizio: occorre dunque un uso distorto di poteri inerenti la qualità medesima, essendo volta la norma a colpire lo sfruttamento del vantaggio che deriva al soggetto agente dalla sua specifica conoscenza della struttura e organizzazione del sistema su cui agisce e dai poteri di intervenire sul sistema informatico, e dunque del "rapporto privilegiato" con il sistema idoneo a favorire l'accesso e l'interferenza nel sistema informatico (G.Pica, *Diritto penale delle tecnologie informatiche*, Utet, 1999, 76).
Circa il rapporto dell'aggravante in discorso con quella ex art. 61 n. 11 cod. pen. (abuso di relazioni d'ufficio o di prestazione d'opera), si è ritenuto poi che l'applicazione dell'aggravante dell'operatore assorba la seconda, impedendone l'applicazione congiunta, e che l'aggravante ex art. 61 n. 11 cod.

pen. possa trovare applicazione (solo) ove non si applichi la prima.
Quanto al concorso di reati, problematica appare la configurabilità del concorso tra la frode informatica e l'accesso abusivo. Così, il mero accesso con fine di lucro dovrebbe integrare gli estremi dell'accesso abusivo e non quello di tentata frode informatica, salvo che ricorrano specifici interventi manipolativi del sistema diversi da quelli relativi all'accesso, mentre ove non riesca l'accesso abusivo nel sistema la finalità di frode sarà irrilevante penalmente, restando ancora sul piano delle intenzioni del reo, sicché si realizza solo il tentativo di accesso abusivo e non il tentativo di frode informatica. Si è poi ritenuto che, ove all'accesso abusivo a scopo di lucro si accompagni il conseguimento dello stesso con altrui danno a mezzo di manipolazioni, la necessaria prodromicità logica e fisica dell'azione di accesso abusivo rispetto alla frode non è tale -attesa l'articolazione della frode esclusivamente sulla manipolazione- da escludere la possibilità di concorso fra le norme, sia formale (per quanto più raro) che materiale, essendo diversi nei due casi l'azione, l'oggetto della condotta -essendo violata una protezione del sistema solo nell'accesso abusivo-, il bene giuridico tutelato. Con ottica contrapposta, si è osservato da altri (Fanelli, nota a Cass. citata, in *Foro it*., 2000, I, 134) che, ove invece all'accesso abusivo a scopo di lucro si sia accompagnato -a seguito di manipolazioni del sistema o dei dati informazioni o programmi in esso contenuti- il conseguimento di un vantaggio patrimoniale senza alcuna violazione della riservatezza individuale, la punizione del fatto a titolo di frode informatica dovrebbe coprire ogni disvalore penale della fattispecie, con conseguente assorbimento del reato di accesso abusivo -che verrebbe a ridursi a mero *ante factum* non punibile della frode-, come può argomentarsi sulla base dalla circostanza che l'accesso abusivo realizza un "intervento senza diritto su dati, informazioni o programmi" (che è già uno degli elementi costitutivi del reato di frode informatica), e del fatto che secondo *l'id quod plerunque accidit* l'accesso abusivo è lo strumento più comunemente utilizzato per commettere frodi informatiche; analogamente, Aterno, *Sull'accesso abusivo a sistema informatico o telematico*, cit., 2997, osserva che il concorso di reati possa aversi solo ove all'oggettività giuridica comprendente la condotta di introduzione-furto di servizi o la violazione del domicilio informatico si accompagni la violazione del diritto alla riservatezza informatica e telematica.
In giurisprudenza, in tema di concorso di reati di frode informatica ed accesso abusivo, per Cass. Sez. 5, Sentenza n. 1727 del 16/01/2009 i delitti possono concorrere diversi essendo i beni giuridici tutelati e le condotte sanzionate, in quanto la norma dell'accesso abusivo tutela il domicilio informatico sotto il profilo dello "ius excludendi alios", anche in relazione alle modalità che regolano l'accesso dei soggetti eventualmente abilitati, mentre la frode informatica contempla l'alterazione dei dati immagazzinati nel sistema al fine della percezione di ingiusto profitto. (In applicazione di questo principio la S.C. ha ritenuto immune da censure la decisione con cui il giudice di appello ha ritenuto il concorso tra i due reati nei confronti dell'imputato che, in qualità di dipendente dell'Agenzia delle entrate, agendo in concorso con altri dipendenti nonché con commercialisti e consulenti tributari, si era abusivamente introdotto nel sistema informatico dell'amministrazione, inserendovi provvedimenti di sgravio fiscale illegittimi perché mai adottati,in relazione a tributi già iscritti a ruolo per la riscossione coattiva, così alterando i dati contenuti nel sistema in modo tale da fare apparire insussistente il credito tributario dell'Erario nei confronti di numerosi contribuenti).
Anche secondo Cass. Sez. 5, Sentenza n. 2672 del 27/01/2004, il delitto di accesso abusivo a un sistema informatico previsto dall'art. 615-ter cod. pen. può concorrere con quello di frode

informatica di cui all'art. 640-ter cod. pen., in quanto si tratta di reati diversi: la frode informatica postula necessariamente la manipolazione del sistema, elemento costitutivo non necessario per la consumazione del reato di accesso abusivo che, invece, può essere commesso solo con riferimento a sistemi protetti, requisito non richiesto per la frode informatica.
Quanto ai rapporti tra la frode informatica ed altri reati, si sono ritenute applicabili congiuntamente le fattispecie di frode informatica e di falso informatico (in giurisprudenza, con riferimento al falso in atto pubblico ed alla truffa relativamente ad un archivio informatico dell'Inps, trib. Como 25 settembre 1995), quelle di frode informatica e di falsificazione di comunicazioni informatiche o telematiche ex art. 617 sexies cod. pen. (ritenendosi la manipolazione della comunicazione altrui in corso come alterazione del funzionamento del sistema telematico di cui al reato di frode informatica: G.Pica, *Diritto penale delle tecnologie informatiche*, Utet, 1999, 162), nonché la frode informatica e l'uso indebito di carte di pagamento di cui all'art. 12 della legge n. 197/91 (ove all'utilizzazione indebita della carta di pagamento si accompagnino manipolazioni volte a carpire particolari utilità dal sistema informatico). Si è invece esclusa la possibilità di concorso tra frode informatica e truffa, essendo distinte le fattispecie, atteso che la frode prescinde dall'errore di persona fisica e da atti di disposizione patrimoniale operati dal soggetto passivo ed è destinata ad operare ove vi sia l'obiettiva manipolazione dei dati con l'elemento patrimoniale (G.Pica, *Diritto penale delle tecnologie informatiche*, cit., 162; Fanelli, nota a Trib. Lecce 12 marzo 1999, cit., 609).

6. Sostituzione di persona e problemi investigativi connessi.

Più complesso, in tutte le descritte fattispecie, può profilarsi il problema della ricerca dell'autore del reato.
La giurisprudenza ha avuto modo di intervenire sull'illiceità penale anche dell'uso di strumenti informatici per occultare l'autore della comunicazione: si è così ritenuto che integra il reato di sostituzione di persona (art. 494 cod. pen.), la condotta di colui che crei ed utilizzi un "*account*" di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete 'internet' nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese, subdolamente incluso in una corrispondenza idonea a lederne l'immagine e la dignità (nella specie a seguito dell'iniziativa dell'imputato, la persona offesa si ritrovò a ricevere telefonate da uomini che le chiedevano incontri a scopo sessuale). (Cass. pen., Sez. 5, Sentenza n. 46674 del 14/12/2007)
Per altro verso, come si è già visto, gli artifizi posti in essere dal truffatore possono consistere anche nella messa in scena di un'attività commerciale apparentemente seria ed affidabile, che induca il compratore a fidarsi del contraente e ad effettuare pagamenti *on line* per beni e servizi ancora da ricevere, e poi di fatto mai inviati dal venditore.
Va ricordato peraltro in proposito che la disciplina civilistica assicura, trattandosi di contratti a distanza, conclusi fuori dei locali commerciali e con un consumatore, il diritto di recesso della parte. Tale tutela può rivelarsi peraltro insufficiente, come accade tutte le volte in cui il privato non abbia alcuno strumento per individuare la vera identità della controparte e dunque di attivare le tutele previste dalla legge (es. rimborso del prezzo a seguito della restituzione per recesso; es. risarcimento danni da evizione, vizi della cosa venduta o altro).

Può accadere pure in *Internet* che, approfittando delle condizioni di "anonimato" che -in misura più o meno ampia e diretta- garantisce la rete, siti poco affidabili che svolgono attività commerciale o finanziaria in rete "spariscano" dal *web*, dopo aver ingenerato fiducia commerciale negli utenti operando per un certo periodo con regolarità e dopo aver incassato somme ingenti con tale espediente.
In generale, però, va evidenziato che l'identità del vero autore di una comunicazione informatica è spesso celata nell'anonimato grazie proprio agli stessi strumenti tecnici adoperati per creare o per trasmettere il file.
Sul punto, occorre premettere che all'atto del collegamento alla rete da parte del *client* il provider gli assegna un indirizzo IP, Internet Protocol: si tratta di una serie di quattro numeri separati da un punto), che identifica in modo univoco un calcolatore collegato ad Internet.
L'indirizzo IP può essere sempre il medesimo (c.d. statico, come d esempio con la connessione *adsl*, o in relazione ai siti web) ovvero può variare volta per volta (c.d. dinamico, essendo assegnato lo stesso numero a vari *clients* in tempi diversi i ragione delle rispettive connessioni).
L'indicazione dell'indirizzo IP è peraltro essenziale con riferimento all'apparato mittente ed a quello destinatario, atteso che è necessario che i computer si vedano reciprocamente per trasmettersi pacchetti di dati.
I dati della connessione sono conservati nei c.d. *files di log*.
Con riferimento ai *files di log* si è già detto che questi consentono di stabilire che un determinato utente in un particolare giorno ed ora si è collegato alla rete tramite un *provider* che gli ha assegnato un indirizzo IP, ossia un numero identificativo in modo univoco (spesso in modo temporaneo, ossia univoco ma con riferimento ad un dato momento temporale), ed ha compiuto una data attività in rete (accesso a dati siti, ricezione o trasmissione di email o messaggi, *upload* o download di *files*, partecipazioni a *newsgroup, ecc.)*.
E' possibile richiedere al *provider* - con le medesime forme utilizzate per lìacquisizione dei tabulati, ossia, in base alla più recenti indicazioni, con decreto motivato del pubblico ministero- i files di log di una data connessione. Tali indagini peraltro hanno vari limiti.
Poiché i *providers* di solito collaborano, non avendo particolare interesse a coprire attività illecite in rete, il principale limite risiede nella esattezza e completezza dei dati a disposizione del provider, essendo possibile spesso costituire rapporti con *provider* senza una idonea, completa e veritiera identificazione, essendo varie le modalità ed i tempi di conservazione dei *file* di *log* (che sono meri *files* di testo, modificabili ed alterabili, e che, occupando memoria, dopo un certo periodo di conservazione sono distrutti), ed infine occorrendo (specie nel caso di indirizzi IP dinamici) che i dati siano raccolti con riferimenti temporanei oggettivi o ricostruibili in modo esatto.
Non va dimenticata poi l'esistenza di norme che hanno inciso sui tempi di conservazione dei dati, specie a tutela della privacy, escludendola o limitandola nel tempo (v. l'art.132 del decreto legislativo 30 giugno 2003, n. 196, e per altro verso, si segnalano le norme che in deroga prevedono dei tempi di conservazione di dati per finalità di investigazione relativa ai reati ritenuti dal legislatore più gravi: v. il d.l. 144/2005,convertito in L. 31 luglio 2005, n 155, nonché le successive normative del 2008, che reiterano tali ultime deroghe).
Infine, l'utilizzo di *providers* esteri può rendere difficile e onerosa sotto il profilo procedurale la richiesta di tali dati, stante la necessità di ricorrere, in tali casi, a richiesta per rogatoria *ex* art.727 ss cod. proc. pen..

Infine, dal *file* di *log* risulta l'indicazione non di un "utente" registrato da un *provider,* ma più frequentemente la semplice indicazione di una utenza telefonica, della quale occorrerà individuare l'effettivo utilizzatore; in questo senso l'indagine potrà quindi essere completata da richieste ordinarie di tabulati telefonici o da intercettazioni telefoniche sulla linea.
Gli informatici hanno ben evidenziato le difficoltà di acquisizione dei *files di log* ed i pericoli di loro alterazione o addirittura distruzione. Il computer forenser esperto sa bene che ad oggi non esiste un modo per acquisire un *file di log* con l'assoluta certezza che non sia stato modificato in qualche modo. Tutti i *files di log*, siano essi binari o di testo (come la maggior parte), possono essere alterati. Se non li ha alterati l'*attacker*, può averlo fatto l'amministratore di sistema, o addirittura il sistema stesso in fase di rotazione o sovrascrittura dei file (Gherardini M., *Computer forensic*, Apogeo, 2009). Va peraltro ricordato che nella maggior parte delle reti esistenti vige la più completa anarchia riguardo alla gestione dei *files di log*; inoltre, molti eventi non vengono neppure trattati, ma gli stessi file sono sovrascritti regolarmente.
Anche quanto all'analisi dei *logs*, l'analisi di un *log* svolta da un *computer forenser* sarà totalmente differente da quella svolta da un *sysadmin*, atteso che mentre quest'ultimo vuole conoscere le anomalie possibilmente in tempo reale, così da poter intervenire tempestivamente, un *computer forenser* effettua l'analisi a posteriori e senza le emergenze su rappresentate, ha necessità di prodotti che possano esaminare ampie quantità di testo ed effettuare, se possibile, una correlazione di eventi.
Altro problema rilevante dei *files di log* è quello del loro formato, atteso che spesso i sistemi usano formati differenti, che poi il *forenser* deve normalizzare a fini di analisi.
È fondamentale, poi, come già anticipato il fattore temporale, perché occorre confrontare il tempo dei sistemi sui quali sono stati registrati i *log* con l'ora esatta: solo in questo modo, infatti, si potranno individuare con esattezza i tempi di assegnazione degli IP dinamici e correlare in maniera corretta gli eventi, così da ricostruire l'esatta sequenza temporale degli avvenimenti.

Poco proficuo può essere talora in concreto il tentativo di ricostruire l'identità del reo ricercando a ritroso l'autore di una *email* utilizzata per organizzare il piano criminoso.
Infatti, con riferimento alla persona fisica che si collega in rete, la registrazione presso il provider può essere avvenuta in forma telematica, senza verifica della genuinità dei dati; inoltre, con riferimento invece al computer utilizzato, si può mascherare l'IP con appositi programmi *software*; ancora, si può ricorrere all'interposizione nel traffico telematico di altri *servers* (c.d. *proxy*), di modo che al destinatario dell'email risulti l'indirizzo IP del *proxy*; o infine, ci si può rivolgere ad appositi siti, c.d. *remailer* (i *remailer,* che talora peraltro offrono la possibilità di concatenare più *remailers* tra loro, nella versione più evoluta consento di inviare messaggi attraverso blocchi di risposta crittografati che vengono composti a destinazione) che assicurano tale servizio interpositorio che realizza l'anonimato, prestando un loro IP casuale e senza registrarne i dati; infine, si può operare da *internet café* che assicurano la connessione (i quali hanno, ma non ovunque, l'obbligo di identificare l'utente, ma non controllano direttamente la sua attività in rete quanto ai contenuti).
Sempre più spesso, poi, accade che si riscontrano casi in cui la comunicazione telematica risulta originata da un computer identificato, ma che questo sia stato in realtà una macchina bucata, uno *zombie*, come si dice nello *slang* degli *hackers*, ossia un computer infettato surrettiziamente con programmi *trojan* (ossia programmi che svolgono funzioni informatiche occulte) che abbiano fatto acquistare all' *hacker* il controllo della *root*, sicché in realtà le funzioni svolte dal computer

in discorso sono eseguite, spesso nella piena ignoranza del titolare della macchina, per conto di soggetti terzi.
Va poi aggiunto che i server interposti possono essere anche all'estero, anche in paesi *off shore*, sicché, l'identificazione del percorso dei dati incontrerà ulteriori complicazioni connesse con la scarsa o nulla collaborazione delle autorità dei paesi in questione (mi si consenta sul punto di rinviare a F.Buffa, *Internet e criminalità, Finanza telematica offshore*, Giuffré, Milano, 2001, che analiticamente esamina questi problemi).
Inutile dire, poi, che i passaggi possono moltiplicarsi all'infinito, rendendo più difficile la ricostruzione (a ritroso) del flusso informatico.
Non va dimenticato poi che, per aumentare la sicurezza del traffico anonimo e la non rintracciabilità dell'informazione, i sistemi possono utilizzare connessioni cifrate o avvalersi di tecniche steganografiche (e qui va evidenziata la particolarità della comunicazione informatica, che consente di inserire file di testo all'interno di file di diverso tipo, ad esempio fotografici, e viceversa, senza che i file inseriti siano visibili).
Se si passa poi alla comunicazione *peer to peer*, propria dei sistemi di *file sharing*, le cose si complicano, in quanto ogni computer collegato alla rete può diventare un nodo del sistema e condividere in tempo reale le informazioni con altri sistemi informatici. La struttura della comunicazione, di solito studiata in relazione al *downloading* di *files* musicali o cinematografici, riguarda invece più in generale anche l'invio di messaggi, e dunque la creazione di comunicazioni telematiche.
Il *peer to peer* (P2P)si distingue dai sistemi di file sharing *client-server*, i quali sono basati su un sistema centralizzato, laddove nel modello *peer to peer* il *server* o ha una mera funzione di motore di ricerca (come in Napster) ovvero non esiste affatto e la comunicazione avviene solo tra *clients*.
Nella comunicazione *peer to peer,* ogni *client* possiede una lista locale di altri *client*, nell'ambito dei quali viene effettuata la ricerca di dati *files*; se questi *client* in lista possiedono il *file*, lo inviano al richiedente, altrimenti girano la richiesta ad altri *clients*, sicché il numero di nodi attraversati dalla richiesta determina la profondità di ricerca che può variare a seconda del sistema. Una volta che sono state raccolte le informazioni circa tutti i *clients* collegati che contengono l'informazione cercata si può iniziare a scaricare il file cercato: la cosa interessante, è che il file non viene scaricato da una sola sorgente, ma parti diverse del file vengono scaricate, in modo automatico, da sorgenti diverse. Ne deriva che in tali sistemi risulta intrinsecamente complesso, se non impossibile, risalire alla sorgente di un *file*: parti di un *file* sono in possesso di utenti diversi, e non è poi così improbabile che nessuno abbia il file completo (e ciò benché sia possibile scaricare egualmente un file funzionante) (si pensi all'uso, anch'esso penalmente rilevante, di tali modalità di comunicazione, nel trasferimento di *files* la cui trasmissione, come nei *files* protetti da *copyright*, o il cui contenuto, come ad esempio nei *files* pedopornografici, è proibito dalla legge).
Non solo, ma nel *file sharing* le operazioni possono anche essere interrotte e riprese successivamente; in tal modo, si sfrutta anche la possibilità di utilizzare *clients* diversi per completare un'operazione di *download*.
Infine, va ricordato il fenomeno delle *darknet*, che, a differenza di reti di condivisione di dati P2P, sono anonime e criptate. Così, ad esempio, la rete TOR fornisce servizi di connessioni anonime in uscita e di fornitura di '*hidden services*' (servizi nascosti). Qui l'individuazione dell'autore di una comunicazione telematica può essere anche tecnicamente impossibile. Va detto però, a conclusione di questa disamina, che si tratta già di comunicazioni cui accedono utenti evoluti, sicché, nella gran

parte delle operazioni commerciali *on line*, le normali regole di cautela sopra ricordate potranno essere sufficienti ad assicurare una tutela preventiva adeguata agli utenti, restando invece comunque difficile l'intervento successivo investigativo e repressivo.

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 85-101

Cybercrime e diritto d'autore: un rapporto controverso tra punti fermi internazionali ed europei e mutevoli interpretazioni italiane

Giuseppe Corasaniti

Abstract: L'attuazione della Convenzione di Budapest sul Cybercrime attraverso la legge 48 del 2008 ha lasciato aperta una incertezza interpretativa di fondo in relazione ai limiti della intervenuta integrale ratifica delle disposizioni riguardanti i reati contro la proprietà intellettuale commessi via web. L'attuazione della Convenzione comporta ,infatti, non solo la doverosa cooperazione internazionale per il contrasto alla criminalità nel settore ,ma ,soprattutto l'accettazione dei principi di fondo che la Convenzione fissa ,limitandosi agli tali atti commessi deliberatamente, su scala commerciale e attraverso l'utilizzo di un sistema informatico.Ne consegue perciò un impatto interpretativo di ordine generale sulle disposizioni penali della legge n. 633 del 1941 più volte modificate ed integrate che deve tener conto anche delle più recenti posizioni europee della Corte di giustizia.

Parole chiave: convenzione sul cyber crime, pirateria online, software peer to peer, file sharing.

1. I reati contro la proprietà intellettuale nella Convenzione sul Cybercrime: una ricerca internazionale di buon senso e di equilibrio.

Il titolo IV della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica firmata il 23 novembre 2001 ,all'art. 10 prevede la possibilità di applicazione della Convenzione (e conseguentemente della possibilità di acquisizione di prove in ambiente digitale mediante un articolato sistema di cooperazione internazionale) per *i "reati contro la proprietà intellettuale e i diritti connessi "* .

Articolo pervenuto il 7 ottobre 2013, approvato il 28 novembre 2013

Nello schema della Convenzione ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale la *violazione della proprietà intellettuale*, come definita in base alla legge di quella Parte, tenendo fede agli obblighi che ha assunto in base al "Paris Act" del 24 luglio 1971 che ha modificato la Convenzione di Berna sulla protezione delle opere letterarie e artistiche, l'Accordo sugli aspetti commerciali dei diritti sulla proprietà intellettuale e il Trattato OMPI sulla proprietà intellettuale, con l'eccezione di tutti i diritti morali conferiti da queste convenzioni, se tali atti sono commessi *deliberatamente, su scala commerciale e attraverso l'utilizzo di un sistema informatico.*

Inoltre ogni parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale la violazione di diritti connessi come definiti dalla legge di quello Stato Parte, tenendo fede agli obblighi che ha assunto in base alla Convenzione Internazionale per la protezione degli artisti, interpreti ed esecutori, produttori di fonogrammi e organismi di radiodiffusione (Convenzione di Roma),all'Accordo sugli aspetti commerciali dei diritti sulla proprietà intellettuale e il Trattato OMPI sull'interpretazione e l'esecuzione e i fonogrammi, con l'eccezione di tutti i diritti morali conferiti da queste convenzioni, se tali atti sono commessi deliberatamente, su scala commerciale e attraverso l'utilizzo di un sistema informatico.Una Parte può ,tuttavia, riservarsi il diritto di non imporre la responsabilità penale in determinate circostanze, a condizione che altri rimedi efficaci siano disponibili e che tale riserva non deroghi agli obblighi internazionalmente assunti da questa Parte in applicazione degli strumenti internazionali prima menzionati.

La Legge 18 marzo 2008, n. 48 contenente "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*" [1] non contiene a riguardo alcuna esplicita disposizione attuativa , in tal modo autorizzando due possibili e distinte linee interpretative : secondo la prima vi è stata implicita ratifica del testo (e soprattutto degli strumenti operativi) della Convenzione mediante il richiamo generale al testo della Convenzione contenuto all'art. 2 della legge di attuazione ,specie tenendo conto della esplicita menzione normativa alla "intera" esecuzione dell'accordo. In base alla seconda linea interpretativa ,tuttavia ,l'attuazione non sarebbe stata effettiva non esistendo alcun preciso articolo di riferimento e, soprattutto, esistendo una non sovrapponibilità tra normativa penale vigente e il testo della Convenzione stessa (in particolare gli art. 171 bis e ter della legge 22 aprile 1941 n. 633 e segnatamente agli artt. 171 lett. a bis (introdotto con il decreto legge 31 gennaio 2005, n. 7) ,171 bis (introdotto con l'art. 10, D.Lgs. 29 dicembre 1992, n. 518 e concernente la tutela del *software*) ,171 ter e octies (riguardanti rispettivamente i contenuti multimediali e la decodificazione di trasmissioni televisive ad accesso condizionato introdotti con la legge 18 agosto 2000 n. 248 c.d. *"antipirateria"*).

Poiché la prima linea interpretativa sembra avere una certa coerenza si deve allora osservare come la norma della Convenzione recepita finisca oggettivamente per determinare una significativa incisione sulla valutazione dell'elemento soggettivo di tali ipotesi di reato qualora commesse attraverso l'uso di un sistema informatico poiché intende rimarcare come la violazione al diritto d'autore debba essere non solo intenzionale ma consapevolmente deliberata ,e cioè con coscienza

1 Cfr. AA.VV. *Cybercrime ,responsabilità degli enti,prova digitale* ,a cura di CORASANITI G. e CORRIAS LUCENTE A. ,Milano 2009 pag. 22.

e volontà di ledere l'altrui posizione giuridica.
Un criterio- internazionalmente convenuto- finisce così per influire ,di fatto, sulla stessa rilevanza penale di condotte nelle quali non vi è (puntuale) consapevolezza circa l'altrui proprietà intellettuale e ,molto più spesso, laddove la violazione dei diritti d'autore non sia immediatamente percepibile sul piano della volontà di produrre effetti dannosi mediante fruizione indebita di contenuti elaborati da altri.
La necessità di individuare ,ai fini della cooperazione internazionale, esclusivamente le condotte "su scala commerciale" pone ,inoltre un ulteriore ,e non secondario ,profilo problematico ,se cioè *la "scala commerciale"*[2] sia riconducibile ,almeno immediatamente, alle finalità di lucro o di profitto che la norma italiana (rispettivamente agli art. 171 ter e bis) individua. Si tratta ,indubbiamente, di una nozione molto più estesa che sembra conferire alla condotta incriminata una potenziale ,e rilevante, connotazione ,che è quella consistente nella (stabile) organizzazione (riproduttiva o distributiva) informatica di contenuti onde fruire di una controprestazione o di un corrispettivo di carattere economico , direttamente o indirettamente ,riferibile al contenuto stesso immesso in rete al fine specifico della sua commercializzazione in termini produttivi o di servizio.
Una conferma indiretta della funzionale limitazione ad ambiti commerciali della disciplina del diritto d'autore viene proprio dalla inclusione nell'ambito dei reati presupposto della responsabilità degli enti ai sensi del Decreto legislativo 8 giugno 2001, n. 231 *Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*, dei reati in materia di diritto d'autore[3] ,si tratta di una inclusione che sembra confermare il carattere prevalentemente ,se non essenzialmente, commerciale delle violazioni considerate ,inquadrandosi il presupposto applicativo della responsabilità dell'ente proprio nell'ambito di una organizzazione sistematica e stabile di risorse e mezzi collaterale alle attività costituenti reato [4].

---

[2] E l'espressione peraltro è tipicamente statunitense riferibile ad ogni attività di persone o proprietà a qualsiasi prezzo , tassa, tasso, carica o altra corrispettività direttamente o indirettamente in relazione a qualsiasi attività commerciale o di impresa *destinata a scopo di lucro* (USC 18).

[3] L'intervento si è realizzato con l'art. 15 della legge "sviluppo" Legge 23 luglio 2009, n. 99 "Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia" Art. 25-novies *(Delitti in materia di violazione del diritto d'autore*). In relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a-bis), e terzo comma, 171-bis,171-ter, 171-septies e 171-octies della legge 22 aprile 1941, n. 633,si applica all'ente la sanzione pecuniaria fino a cinquecento quote. . Nel caso di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore ad un anno. Resta fermo quanto previsto dall'articolo 174-quinquies della citata legge n. 633 del 1941. Peraltro la stessa norma include nell'alveo dei reati presupposto anche quelli di contraffazione industriale ex art. 474 cp. e 517 cp . Mentre appare evidente la connessione in materia di software (uso sistematico di copia non licenziata nell'ambito del proprio sistema informatico così realizzando appunto un vantaggio per l'ente) il rapporto di vantaggio per l'ente che implica la responsabilità amministrativa da reato non avrebbe senso alcuno se non in relazione ad attività (commerciali) a carattere integrativo o ausiliario dell'attività (produttiva distributiva o commerciale) costituente reato . Sicché tra i modelli organizzativi ,essenziali ai fini di non incorrere in responsabilità l'ente dovrebbe prevedere adeguate forme di controllo onde riscontrare la legittima provenienza dei contenuti diffusi ,il che costituirà certamente un nuovo profilo problematico quasi esclusivamente nei settori della comunicazione interattiva e della distribuzione on line.

[4] Si tratta perciò di valutare in particolare le connotazioni della struttura organizzativa in concreto in quanto ambiente potenzialmente idoneo a configurare la responsabilità ex art. 5 della legge 231 e cioè nelle ipotesi di reati commessi nel suo interesse o a suo vantaggio da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché' da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso o da persone comunque sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali . In ogni caso la responsabilità sarebbe esclusa se tali soggetti hanno agito

Peraltro la intervenuta estensione ai delitti in materia di proprietà intellettuale della responsabilità degli enti costituisce ,di fatto, una nuova saldatura tra tali reati e l'ambiente "classico" dei reati informatici poiché tale responsabilità era "in nuce" prevista proprio nell'ambito della Convenzione di Budapest del 2001 (art. 12) ,e non espressamente menzionata nella legge di attuazione del 2008. La questione centrale ,allora, viene a definirsi progressivamente in relazione alle molteplici attività imprenditoriali nell'ambito del mercato digitale (globale) e non appare di poco conto ,ove si consideri che è proprio la problematica dell'aspetto soggettivo dei reati contro la proprietà intellettuale a permeare tutte le condotte poste in essere via *web* ,condotte molto più frequenti rispetto alla tipologia "classica" dei reati informatici (accesso illecito, danneggiamento informatico ,frodi ,falsificazioni digitali) e talora prive di un vero e proprio "allarme sociale" ,considerandosi anzi la condivisione tra comunità o l'immissione di contenuti privati per un uso comune ad altri utenti indeterminati una delle caratteristiche essenziali del *web 2.0*.

2. L'ambiguo e tormentato percorso normativo italiano.

Il percorso normativo di adeguamento della legge n. 633 del 1941 sul diritto d'autore è apparso a dir poco contraddittorio e tormentato poiché con un primo Decreto-legge 22 marzo 2004, n. 72, convertito in legge 21 maggio 2004, n. 128 (recante interventi per contrastare la diffusione telematica abusiva di materiale audiovisivo) erano stati previsti strumenti di carattere informativo su ogni contenuto protetto immesso on line . Perciò al fine di promuovere la diffusione al pubblico e la fruizione per via telematica delle opere dell'ingegno e di reprimere le violazioni del diritto d'autore, l'immissione in un sistema di reti telematiche di un'opera dell'ingegno, o parte di essa, avrebbe dovuto esser ' *corredata da un idoneo avviso circa l'avvenuto assolvimento degli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi*" . La comunicazione, di adeguata visibilità, contiene altresì l'indicazione delle sanzioni previste, per le specifiche violazioni, dalla legge 22 aprile 1941, n. 633, e successive modificazioni (artt. 171 e seguenti più volte modificati negli ultimi decenni) . Le relative modalità tecniche e i soggetti obbligati sarebbero state poi definite con decreto del Presidente del Consiglio dei Ministri, di concerto con il Ministro delle comunicazioni, sulla base di accordi tra la Società italiana degli autori ed editori (SIAE) e le associazioni delle categorie interessate. Fino all'adozione di tale decreto, l'avviso avrebbe dovuto avere comunque caratteristiche tali da consentirne l'immediata visualizzazione. Si trattava ,cioè ,di un vero e proprio "bollino" digitale improbabilmente destinato a connotare (solo) le opere italiane e protette in Italia entro un sistema di comunicazione universale. Non solo ,ma il medesimo decreto legge ,completamente contraddicendo le normative comunitarie in materia affidava al Dipartimento della pubblica sicurezza del Ministero dell'interno il compito di raccogliere le segnalazioni di interesse in materia di prevenzione e repressione delle violazioni di cui alla lettera a-bis) del comma 2 dell'art. 171-ter della legge 22 aprile 1941, n. 633, assicurando il raccordo con le Amministrazioni interessate. A seguito di provvedimento dell'autorità giudiziaria, i prestatori di servizi della società dell'informazione, di cui al decreto legislativo 9 aprile 2003, n. 70, avrebbero dovuto comunicare

nell'interesse esclusivo proprio o di terzi.

quindi alla polizia le informazioni in proprio *possesso utili all'individuazione dei gestori dei siti e degli autori delle condotte segnalate.*

A seguito di provvedimento dell'autorità giudiziaria, per le violazioni commesse per via telematica essi avrebbero anche posto in essere tutte le misure dirette ad impedire l'accesso ai contenuti dei siti o a rimuovere i contenuti medesimi. Si trattava di disposizioni confuse e volte a confondere il piano della repressione amministrativa con le garanzie di carattere civile e penale ,e soprattutto destinate alla concreta inattuazione (tra l'altro neppure formalmente abrogate con la successiva legge 31 marzo 2005, n. 43 che ha convertito il successivo decreto-legge 31 gennaio 2005, n. 7. All'art. 3 sexies si è scelta così una altra strada ,mantenendo sostanzialmente il medesimo trattamento penale per le condotte incriminate e forse addirittura peggiorandolo dato che ,almeno, nella prima versione la condotta era prevista la sanzione degli atti di immissione on line di opere protette "per trarne profitto" (e quindi con chiaro riferimento alla esigenza di conseguire un utile economico dalla immissione del contenuto stesso in rete) mentre con la riforma ne scaturiscono due diverse ipotesi di reato ,una più lieve (art. 171 lettera a bis) consistente nella multa (da 51 a 2065 euro) per chi "*mette a disposizione del pubblico immettendola in un sistema di reti telematiche mediante connessione di qualsiasi genere*" una opera protetta o parte di essa ,ed una più consistente all'art. 171 ter ,dove la medesima condotta qualora sia connotata da fine "*di lucro*" (e non più di profitto) viene sanzionata con la pena della reclusione da uno a quattro anni e con la multa da 2500 euro fino a 15.500 euro. Poche sono le disposizioni di apertura [5], se non una vera e propria oblazione (riferita insolitamente ad un delitto) prevista dall'art. 171 così riformato (e quindi nella sola ipotesi più lieve) e comportante il pagamento della metà del minimo della pena pecuniaria (cioè il versamento di 1000 euro) per ottenere l'estinzione del reato prima dell'apertura del dibattimento o della emissione del decreto penale di condanna.

Pochi sono i dati disponibili circa tale strumento, evidentemente più esplicitamente deflattivo anche se inutilmente punitivo, e tutto lascia intendere che per tali ipotesi di reato si sia lasciato aperto il varco alla prevedibilissima prescrizione delle ipotesi di reato (punite con sola pena pecuniaria) salvo ricorrere estesamente alla ben più grave sanzione amministrativa prevista all'art. 174 bis con il poco razionale risultato di produrre ingiunzioni milionarie (e quindi destinate a non esser mai eseguite specie nei confronti di soggetti aventi risorse economiche ordinarie) poiché l'ammontare della sanzione viene stabilita nel pagamento di euro 100 (e con il massimo di 1000 euro) *per ogni*

---

[5] E tra queste va segnalato il maldestro inserimento di una disposizione di (limitatissimo) "far use" digitale con l'inserimento di una comma 1 bis entro l'art. 70 della legge n. 633 riguardante la libertà di citazione L'intervento di innesto è avvenuto con l'art. 2 della legge 9 gennaio 2008 n.2 che ha previsto : *." È consentita la libera pubblicazione attraverso la rete internet, a titolo gratuito, di immagini e musiche a bassa risoluzione o degradate, per uso didattico o scientifico e solo nel caso in cui tale utilizzo non sia a scopo di lucro. Con decreto del Ministro per i beni e le attività culturali, sentiti il Ministro della pubblica istruzione e il Ministro dell'università e della ricerca, previo parere delle Commissioni parlamentari competenti, sono definiti i limiti all'uso didattico o scientifico di cui al presente comma"* . Un intervento improvvido e doppiamente incostituzionale ,da un lato poiché di fatto sottopone a autorizzazione amministrativa ,in contrasto con l'art. 21 Cost. quanto è già garantito dalla libertà di critica ,di insegnamento e ricerca scientifica ,e poi perché fraintende completamente la realtà della rete imponendo ,una qualità digitale "degradata" (termine risibile e peraltro tecnicamente inesistente ed aberrante) proprio a contesti (quello scolastico e universitario) dove la qualità incide essenzialmente su diritti fondamentali universalmente riconosciuti. La disposizione si è così avviata alla sostanziale e facile inattuazione a documentare in concreto l'incultura digitale "bipartizan" del nostro legislatore Per una attenta ricotsruzione sullo stato della giurisprudenza staunitense sul "fair use" v. invece BRICENO M.L. *Arte appropriativa elaborazioni creative e parodia*.in Riv. Diritto industriale 2011 pag. 357.

violazione ,e soprattutto per ogni esemplare abusivamente duplicato o riprodotto.
Scarsa,se non del tutto inesistente, è stata l'attenzione alle sanzioni amministrative in ambiente digitale ed alla ragionevolezza del combinato disposto delle disposizioni ,che sembrano produrre un effetto "volano" di inasprimenti per condotte talora di inesistente allarme sociale ,ma il mero riferimento alla disciplina delle sanzioni amministrative previste dal codice della strada basterebbe per porre ,non infondatamente, la questione della relativa costituzionalità non solo in rapporto all'art. 3 della Costituzione italiana, ma alle stesse direttive comunitarie che impongono sanzioni "*proporzionate*" e cioè tali da obbedire ad un minimo criterio di equilibrio tra gravità del comportamento lesivo accertato e quantificazione pecuniaria della sanzione erogata .
Al di là dello squilibrio, anche questo evidente, esistente in termine di graduazione delle fattispecie penali[6] tanto più considerando figure di reato di ben più ampio allarme sociale (basti il riferimento alla circolazione stradale o alle frodi assicurative o ,appunto ,informatiche) non risulta poi affatto perseguita la strada, alternativa della autoregolamentazione. Così sempre nella legge del 2005 *(3-sexies*) viene abbozzato un meccanismo di autoregolamentazione poi ,di fatto mai realizzato[7].

3.Contrasto alla "pirateria" on line e tutela dei diritti umani.

Si pone ,quindi, insieme il problema della *graduazione* del sistema sanzionatorio mediante una attenta comprensione di condotte "effettivamente" dannose in relazione al bene giuridico tutelato (nella specie il diritto dell'autore ma soprattutto il diritto al suo editore /distributore esclusivo) ,come pure il problema della compatibilità di tale rigido regime sanzionatorio con la libertà di diffusione delle idee (e dei contenuti ideali) che è propria dell'art. 21 della Costituzione e che

---

[6] Su cui mi si permetta di rinviare a CORASANITI G. *Sanzioni penali e diritto di autore* , Il Diritto d'autore 2006 pag. 1.

[7] Al fine di utilizzare la rete quale strumento per la diffusione della cultura e per la creazione di valore nel rispetto del diritto d'autore, il Presidente del Consiglio dei ministri o il Ministro delegato per l'innovazione e le tecnologie, di concerto con i Ministri per i beni e le attivita' culturali e delle comunicazioni, promuove, nel rispetto delle normative internazionalmente riconosciute, forme di collaborazione tra i rappresentanti delle categorie operanti nel settore, anche con riferimento alle modalita' tecniche per l'informazione degli utenti circa il regime di fruibilità delle opere stesse. Nell'ambito delle forme di collaborazione di cui al presente comma, il Presidente del Consiglio dei ministri o il Ministro delegato per l'innovazione e le tecnologie, di concerto con i Ministri per i beni e le attività culturali e delle comunicazioni, promuove anche la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verifica la conformita' alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto. I codici sono trasmessi alla Presidenza del Consiglio dei ministri unitamente ad ogni informazione utile alla loro applicazione. I codici sono resi accessibili per via telematica sui siti della Presidenza del Consiglio dei ministri, del Ministro per l'innovazione e le tecnologie, dei Ministeri delle comunicazioni e per i beni e le attività culturali, nonché su quelli dei soggetti sottoscrittori. Peraltro ,al di là del maldestro tentativo di intervento normativa i codici di condotta formano il cuore della direttiva sul commercio elettronico quale strumento a carattere preventivo in grado di attenuare le situazioni potenzialmente conflittuali ,cfr. FIENGO G. *I codici di condotta per il commercio elettronico* Diritto & Formazione 2002 pag. 1207.

rientra nel quadro dell'art. 27 comma 1 della dichiarazione universale dei diritti umani ONU che assicura (prima significativamente del diritto alla proprietà intellettuale contenuto al 2 comma) ad ogni individuo il diritto di prendere parte liberamente alla vita culturale della comunità, di godere delle arti e di partecipare al progresso scientifico ed ai suoi benefici.
La materia riveste i contorni di una vera e propria guerra di posizioni (che non è azzardato definire "santa" per come si disvelano in concreto oltranzismi e fanatismi) che vede schierati da una parte i sostenitori pregiudiziali della proprietà intellettuale (ed in particolare i produttori di contenuti) e dall'altra il (variegato) mondo del *web*, ma in particolare gli organizzatori di servizi ,attenti a contemperare le esigenze di libertà individuale e collettiva con le pretese di tutela prioritaria delia proprietà intellettuale in ambiente digitale. Da una parte si prospetta il continuo rischio di inaridimento ,se non altro delle fonti di finanziamento e di investimento per le imprese multimediali, e dall'altra si ribadisce l'esigenza di non imporre eccessivi vincoli alle imprese impegnate in ambiente digitale ,specie nel settore dei servizi ,compromettendo anche eccessivamente le libertà dei singoli utenti .
Spesso peraltro non viene considerata la sostanziale e profonda diversità delle forme di fruizione individuale in termini di qualità e di accesso ai contenuti, e sempre più spesso (il che in verità induce a qualche amara riflessione sul reale livello di comprensione culturale delle tematiche della interattività poste dal web in ambito giuridico ed economico) si fraintende e si sovrappone ciò che è tecnicamente differente (siti *web*, pagine *web*, spazi individuali di *social network*, mail, sistemi di condivisione *peer to peer* tra singoli utenti,*streaming* audio e video) nell'ambito di una vaga -e assolutamente generica- definizione di "pirateria" digitale connotata in termini altrettanto vaghi di "illegalità", dimenticandosi che della pirateria il legislatore italiano ha dato una definizione ben formale e puntuale, ed in genere pressoché ignorata dai commentatori e dai numerosi riformatori che si rinviene espressamente nell'art. 144 del Codice della proprietà industriale (Decreto legislativo 10 febbraio 2005 n. 30) per cui *sono atti di pirateria le contraffazioni e le usurpazioni di altrui diritti di proprietà industriale, realizzate dolosamente in modo sistematico.*

4. Le (scarne) posizioni della giurisprudenza italiana e il rilancio degli interventi amministrativi di controllo .

La giurisprudenza ,peraltro, è sembrata attenta alle esigenze di protezione dei contenuti via *web* e (almeno finora) meno concentrata sulla *reale offensività* delle condotte ,come pure sulla sostanziale sovrabbondanza del regime sanzionatorio (che prevede sanzioni inibitorie di carattere civile ,le predette sanzioni di ordine penale e persino sanzioni amministrative che operano autonomamente e potenzialmente di importo ingentissimo) in rapporto al bene giuridico tutelato (la proprietà intellettuale degli individui) .
Una prima ,e molto significativa, posizione della Corte di cassazione [8] in sede penale (Sez. 3, Sentenza n. 49437 del 29/09/2009) ha sottolineato la possibilità di concorso nel reato di

8 Cfr. a riguardo MERLA F. *Diffusione abusiva di opere internet e sequestro preventivo del sito web il caso the pirate bay*, Diritto dell'informazione e dell'informatica 2010 pag. 437.

diffusione mediante la rete Internet di un'opera dell'ingegno protetta dal diritto d'autore (art. 171 ter, comma secondo, lett. a-bis) da parte del titolare di sito web che, portando a conoscenza degli utenti le "chiavi di accesso" e le informazioni in ordine alla reperibilità, in tutto o in parte, dell'opera, consenta agli stessi lo scambio dei *files* relativi mediante il sistema di comunicazione "*peer to peer*". In tale ambito è stato giudicato anche legittimo il provvedimento cautelare con cui il giudice penale, in relazione a condotta di diffusione abusiva in rete di opere dell'ingegno, contestualmente al sequestro preventivo del sito il cui gestore concorra nell'attività penalmente illecita, imponga ai fornitori di servizi internet operanti sul territorio dello Stato italiano di inibire l'accesso al sito al limitato fine di precludere l'attività di diffusione di dette opere. La Corte ha ,a tal fine, richiamato gli artt. 14 -17 del D.Lgs. n. 70 del 2003 attuativo della Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico") secondo cui l'autorità giudiziaria può esigere, anche in via d'urgenza, che il prestatore di un servizio della società dell'informazione impedisca o ponga fine alle violazioni commesse ovvero impedisca l'accesso al contenuto illecito.

Per altro verso ,sempre la Corte di Cassazione (Sez. 3, Sentenza n. 33945 del 04/07/2006)[9] aveva ritenuto già configurabile il concorso nel reato di abusiva diffusione, mediante internet, di immagini protette da diritto di esclusiva anche in capo al soggetto che, pur non avendole immesse in rete, abbia inoltrato sul web, in epoca antecedente alla loro immissione ad opera di altri, informazioni sui collegamenti e sui programmi necessari alla loro visione, in tal modo agevolando la connessione e la loro indebita diffusione. Nel caso specifico erano stati sottoposti a sequestro preventivo di due portali "web", attraverso i quali erano state illecitamente trasmesse in diretta via internet partite del campionato di calcio italiano, mediante connessione ad emittenti cinesi che, acquistato il diritto di diffonderle localmente dal titolare dell'esclusiva, avevano ritenuto di immettere in rete la trasmissione degli eventi sportivi[10].

Più attenta, invece, agli aspetti soggettivi del reato appare invece una importantissima e poco menzionata pronuncia della Corte di Cassazione (3 sezione sentenza gennaio 2007, n. 149) che sottolinea come non appare dubbio che le differenti espressioni adoperate dal legislatore nella diversa formulazione degli articoli 171bis (in tema di *software*) e ter (in tema di contenuti multimediali) abbiano esplicato la funzione di modificare la soglia di punibilità del medesimo fatto, ampliandola allorché è stata utilizzata l'espressione "a scopo di profitto" e restringendola allorché il fatto è stato previsto come reato solo se commesso a "fini di lucro", Con tale ultima espressione, infatti, *deve intendersi un fine di guadagno economicamente apprezzabile o di incremento patrimoniale da parte dell'autore del fatto, che non può identificarsi con un qualsiasi vantaggio di altro genere, né l'incremento patrimoniale può identificarsi con il mero risparmio di spesa derivante dall'uso di copie non autorizzate di programmi o altre opere dell'ingegno, al di fuori dello svolgimento di un'attività economica da parte dell'autore del fatto,* anche se di diversa natura, che connoti l'abuso.

Più complesso appare invece il panorama degli interventi dei giudici civili ,che si sono mossi in via d'urgenza talora con inibitorie rivolte ai *provider*s (fornitori di accesso) onde ottenere i dati

---

[9] SCOPINARO L. *Rilevanza penale della divulgazione via web di programmi tv.in* Diritto penale e processo ,2007 pag. 651.

[10] Sulla tematica cfr. SAMMARCO P. ,*Le partite di calcio in TV e la loro ritrasmissione non autorizzata via Web*.,Diritto dell'informazione e dell'informatica 2010 pag. 908 a comm. Trib. di Roma 11-2-2010.

identificativi dei loro utenti impegnati in attività presentate come illecite (scambio di dati per uso personale, *file sharing* di opere in formato digitale) ma sempre più spesso riferite alla figura soggetto economico responsabile del motore di ricerca[11] (figura sempre più marcatamente definita dopo la Direttiva sul commercio elettronico)[12] . Quasi sempre l'intervento è stato motivato anche qui con riferimento alle disposizioni del decreto legislativo Decreto legislativo 9 aprile 2003, n. 70 *(Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno)* [13] ma a dir poco vaga è stata l'analisi tecnica delle soluzioni tecnologiche coinvolte ,sulla sostenibilità dei costi imposti all'operatore e ,soprattutto sui rapporti tra iniziative di tutela civile (sostenute dal fondamentale principio dell'onere della prova) in via d'urgenza ,e altrettanto forti esigenze di tutela dei dati personali di utenti terzi[14].

Più in generale il tema della responsabilità dei *providers* in ordine alla trasmissione di contenuti protetti dal diritto d'autore si è posto sul piano della tutela civilistica [15] non senza rimarcare le possibili incongruenze di una tutela estesa e incondizionata ,volta a sanzionare indiscriminatamente ogni forma di condivisione senza scopo di lucro ,tipica, peraltro dei nuovi "*social networks*" [16] .

Le nuove forme di condivisione ,sia mediante l'accesso diretto ai contenuti delle opere protette mediante spazi segnalati o condivisi ,sia attraverso la creazione di propri circuiti di "*files sharing*" (ad accesso riservato ad utenti limitati) [17] .

Da un lato si sottolinea il danno (preminente) che tali forme massive di condivisione comportano per i produttori di contenuti ,fino potenzialmente a annientarne le potenzialità distributive ,dall'altro si sottolinea invece come tali forme di condivisione non si manifestino poi non solo con un grado di effettiva nocività per i contenuti ,non ponendosi su un piano di concorrenza effettiva nel mercato ,ma quali utilizzazioni prive di rilevanza economica e ,soprattutto, limitate a circuiti chiusi di utenti che non inciderebbe ,se non in minima parte, sulle potenzialità di accesso

---

[11] GIOVANELLA F. *YouTube attracca (per ora) in un porto sicuro. In tema di responsabilità del Service Provider.*,IN Danno e responsabilità 2012 pag. 243.

[12] Ed il tema è posto acutamente anche in relazione al rapporto di consumo digitale in relazione alla Direttiva . 2011/83/UE sui diritti dei consumatori.,cfr. DE FRANCESCHI A. *Il commercio elettronico nell'Unione europea e la nuova direttiva sui diritti dei consumatori,* in Raseegna di diritto civile 2012 pag. 419.

[13] Cfr. DELFINI F. *Il D. Lgs 70/2003 di attuazione della direttiva 2000/31/CE sul commercio elettronico, I contratti 2003 pag. 612.,SICA S. Recepita la direttiva sul commercio elettronico Il Corriere giuridico 2003 pag. 1247, SODINI E. La normativa comunitaria sul commercio elettronico: la direttiva 2000/31/CE Il nuovo diritto 2003 pag. 7* , BERNARDI G.*Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno* ,in Le nuove leggi civili commentate 2003 pag. 1267.

[14] Cfr. a riguardo FALLETTI E. , *Tutela della privacy e dei dati personali ,* Osservatorio sul rispetto dei diritti fondamentali in Europa (www.europeanrights.eu) ,2008 doc. 12.

[15] GUIDOBALDI L. *YouTube e la diffusione di opere protette dal diritto d'autore. ancora sulla responsabilità dei providers, tra hoster attivi, conoscenza dell'illecito e obbligo di sorveglianza.,* Diritto dell'informazione e dell'informatica 2010 pag. 275.

[16] Sul piano problematico cfr.infatti le preoccupazioni di ERCOLANI S. *Una sommessa riflessione sul diritto d'autore all'epoca della convergenza, Diritto d'autore 2008 pag. 1 GIOVE L. COMELI A. Responsabilità del provider per mancata rimozione di link a materiale illecito.Il diritto industriale 2012 pag. . 84 (a commento Trib. Roma 22 febbraio 2011).*

[17] La tematica investe direttamente i contenuti di carattere audiovisivo : BARZAROTTI Eva ,*File sharing: condivisione di informazioni e violazione del diritto d'autore?* Tecnologia e sistema socio-giuridico a confronto, Cyberspazio e diritto 2007 pag. 111, PASCUZZI G. *Opere musicali si Internet: il formato MP3, Foro It. 2001 pag. 101 (sul caso Napster)* . Ma non mancano anche profili riferibili alle opere dell'ingegno immesse sul web . Cfr. infine ,sulle implicazioni più recenti PIRRUCCIO P. *Diritto d'autore e responsabilità del provider*,Giurisprudenza di merito 2012 pag. 2591.

al circuito distributivo originale[18], e soprattutto sulla consistenza stessa degli importi derivanti dalle vendite di contenuti originali (circuito ,peraltro ,prima limitato e oggi sempre più esteso allo *streaming*)[19].

Si pone, infine ,sempre più spesso il sempre più serio problema della tutela dei dati personali in relazione alle esigenze ,talvolta prospettate, di identificare gli utenti responsabili di condivisioni massive di contenuti protetti [20]. Ed il tema appare di particolare attualità integrando , non solo sul piano civilistico, una potenziale ipotesi di abuso del diritto ,ma soprattutto dal punto di vista penale il reato di trattamento illecito di dati personali di cui all'art. 167 del Decreto legislativo 30 giugno 2003, n. 196 recante il "*Codice in materia di protezione dei dati personali*".

I produttori dei contenuti insistono ,in genere, sulla esigenza –che pretendono di ricondurre a linee generali di orientamento ricollegabili alle vigenti direttive europee - di concepire come illecito qualunque forma di condivisione di opera protetta ,mentre i soggetti esercenti i servizi *on line* muovono dalla uniforme esigenza di "neutralità" della rete (che è innanzitutto una nozione tecnica volta alla assicurazione di compatibilità tecnologica dei sistemi) per definire autonome politiche rispetto ai contenuti, che appaiono legate più a dirette esigenze di sfruttamento commerciale indiretto che non alla consapevole adozione di strumenti di tutela dei consumatori coinvolti . Sicché vi è una perenne situazione conflittuale –talora con toni di accesa esasperazione - mentre in realtà solo la rilevanza economica delle problematiche in campo costituisce il vero fattore determinante per regolazioni commerciali univoche e per di più variabili (a seconda dei contesti strutturali che caratterizzano il mercato ed i suoi protagonisti).

Manca ,tuttavia ancora una condivisa e reale sensibilità "giuridica" diffusa sui temi della *privacy* e della tutela degli utenti /consumatori nelle loro opzioni quotidiane[21]. Le limitazioni alla fruizione

---

[18] *http://www.fondazione-einaudi.it/Documenti/Progetto_RicercaFileSharing_NoTimingBudget.pdf* In merito la ricerca della Fondazione Luigi Einaudi ha confermato la specificità del sistema di *files sharing* quale occasione di sviluppo economico per il settore al fine di assicurare una più penetrante distribuzione di contenuti in mercati tradizionalmente inesplorati dai protagonisti . Si tratta comunque di un tema realmente "incandescente" in quanto da un lato i produttori di contenuti insistono sulla completa illiceità di tale pratica ,mentre i responsabili dei servizi sottolineano come tale piattaforma presenti margini di originalità innovativa e di tutela delle scelte di consumo individuale che non si pongono in effettivo contrasto con il mercato "originale" ,caratterizzato da una segmentazione rigida e da soglie temporali di accesso ai prodotti altrettanto rigidamente predeterminate.

[19] E peraltro non mancano esperienze "killer" quali "*Spotify"* per i contenuti musicali che realizzano un vero e proprio streming gratuito delle opere immesse finanziato integralmente dalla pubblicità. Un isstema del genere trova proprio nella pubblicità il suo limite, coinvolgendo i distributori negli utili e solo in minima parte gli autori delle opere protette, tuttavia è possibile immaginare l'estensione futura di tale metodologia anche alle opere video con il coinvolgimento degli autori attraverso licenze collettive improntate a fasce massive di fruizioni.

[20] *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1495246*, sul c.d. caso Peppermint Logistep Alla fine, nei primi mesi del 2008, dopo la decisione del Tribunale di Roma, il Garante della privacy stabilì con tale provvedimento che Peppermint e la Logistep (incaricata delle ricerhe sul web) avevano abusato del software sviluppato da quest'ultima (in pratica un client P2P modificato per tracciare i dati identificativi quali l'indirizzo IP, il nome utente, l'hash del file condiviso, il valore registrato dal client nel sistema operativo) per avviare così una vera e propria *attività di monitoraggio*, vietata dalle direttive europee sulle comunicazioni elettroniche. Secondo il Garante, oltre ad aver trattato illecitamente i dati, le società coinvolte avevano tenuto anche un *comportamento non trasparente nei confronti degli utenti* , violando quel diritto alla riservatezza nelle comunicazioni elettroniche già ribadito dal giudice. Per tali motivazioni,fu poi stabilita anche la cancellazione dei dati relativi agli indirizzi IP raccolti dagli archivi delle società. Ad analoghe conclusioni tra l'altro era pervenuto prima il Garante svizzero ,avendo ivi sede la società Logistep. Si è trattato del primo ,significativo, episodio di tracciamento degli utenti posto in essere a livello europeo.

[21] Sulle differenti implicazioni di ordine penale v. FAVINO L. *Gli abusi della rete e sul video non consentiti per violazione dei*

individuale della rete costituiscono ,infatti, un elemento tutt'altro che secondario in tale tematica ,poiché è solo partendo dagli interessi degli utenti che è possibile definire qualsiasi intervento normativo di regolazione, al contrario interventi ambigui di coazione o di sanzione finiscono per infrangersi contro tecniche sempre più innovative di condivisione che peraltro connotano in positivo la condivisione stessa , trasformandola in preciso fattore di successo per il contenuto così diffuso, precostituendone una fortuna commerciale dilatata entro un ambiente di promozione globale e, soprattutto, ancora più aderente alle aspettative dei consumatori più di qualsiasi altra indagine di *marketing* finora sperimentata.

Sicché ogni tentativo miope di regolazione si risolve in una assurda proclamazione di principio ,in un vacuo quanto inutile articolato di presupposti che immaginano la rete un oggetto immobile ,destinato a raccogliere passivamente le prescrizioni ,spesso rigide, di chi confessa a volte ingenuamente di non conoscerla a fondo o di non saper neppure utilizzarla.

Una posizione a parte meritano i tentativi di regolamentazione amministrativa in relazione alle competenze della Autorità per le garanzie delle comunicazioni [22] ,su di essi preme l'ambiguo rapporto posto in essere tra ruolo di garanzia (amministrativa) e imposizioni dispositive[23] a operatori ed utenti quanto mai vaghe ,che finirebbero per sovrapporsi ai procedimenti (ed agli accertamenti) di carattere giudiziario .

Lo schema di regolamento che l'Autorità per le comunicazioni ha approvato il 25 luglio 2013 [24] intende tuttavia (almeno nelle sue motivazioni) contemperare la tutela del diritto d'autore con alcuni diritti fondamentali, quali la libertà di manifestazione del pensiero e di informazione, il diritto di accesso ad internet, il diritto alla *privacy*. In quest'ottica, sostiene l'Autorità ,vi traspare un vero e proprio impegno a *concentrarsi soprattutto sulle violazioni esercitate con finalità di lucro* ,assegnando però carattere "assolutamente prioritario" alla lotta contro la pirateria "massiva", escludendo però dal proprio perimetro d'intervento gli utenti finali (*downloaders*) e il *peer-to-peer*. La procedura prevista dal nuovo regolamento ,pur svolgendosi in tempi brevi ,intende assicurare il rispetto del contraddittorio in modo da consentire a tutti i soggetti interessati di far valere le proprie ragioni. In linea con la connotazione del diritto d'autore come diritto soggettivo disponibile, è previsto che il procedimento dinanzi all'Autorità possa essere avviato *solo su istanza del soggetto legittimato*, non d'ufficio, e dopo aver rivolto, senza esito positivo, una richiesta di rimozione al gestore della pagina internet. Tali misure si richiamano direttamente al decreto legislativo n.70/2003 –prevedendo *rimozione selettiva o disabilitazione dell'accesso ai contenuti illeciti* – e si presentano come improntate a gradualità e proporzionalità, tenendo conto della gravità della violazione e della localizzazione del

diritti della persona: dalla pirateria informatica alla contraffazione telematica.,Rivista penale 2009 pag. 643.

[22] ALVANINI S. ,CASSINELLI A. *I (possibili) nuovi poteri di AGCom in materia di diritto d'autore nel settore dei media,* Il diritto industriale 2011 pag. 543 , COLANGELO G. *Comunicazioni elettroniche, contenuti digitali e diritto d'autore: commento al Regolamento AGCOM.*,in Mercato concorrenza e regole 2011 pag. 575.

[23] Cfr. CAMARDI C. *Inibitorie amministrative di attività, Annali del diritto d'autore 2012 pag. 268*.

[24] Delibera Agcom n. . 452/13/CONS *Consultazione pubblica sullo schema di regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del Decreto legislativo 9 aprile 2003 n. 70* . Come è noto tale provvedimento non ha mancato di suscitare ,fondatamente , polemiche e perplessità ,sottolineandosi ,infatti come i provvedimenti di sequestro e di inibizione potrebbero rivolgersi anche al di fuori dello spazio giuridico italiano con conseguenti evidenti problematiche di costituzionalità in relazione al principio di riserva di legge posto dall'art. 21 Cost. V. in merito la giustamente preoccupata posizione di F.SARZANA e di altri autori: *http://www.fulviosarzana.it/blog/libro-bianco-su-copyright-e-diritti-fondamentali-in-internet/*.

server.
Si tratta, tuttavia, di comprendere in che modo, e con quali strumenti di accertamento, una autorità indipendente (italiana) possa muoversi su un terreno quanto mai controverso e rischioso ,non potendosi certamente compensare quello che è un fondamentale ed evidente difetto del tessuto normativo primario con una più generica regolamentazione amministrativa che rischia di aprire ancor di più spazi di confusione ,contraddizione e di impostazione meramente conflittuale ,tanto più che sembrano ancora mancare in Italia precisi strumenti di mediazione e di composizione extragiudiziale nel sistema ,volti a comporre i contrasti tra operatori economici e utenti ,singoli o associati aventi ad oggetto tale tematica.
Del resto normazioni amministrative siffatte non hanno comportato una seria e significativa incisione sul fenomeno se si pensa all'esperienza francese[25] con l'entrata in vigore della HADOPI con Legge 669 /2009 ,nella quale sono emersi specifici profili di costituzionalità in relazione al rapporto tra attività amministrativa discrezionale ed ambito di intervento nel settore della comunicazione[26].
Appare, infine, giustificabile persino sullo sfondo il dubbio che la preoccupazione per la proprietà intellettuale costituisca forse il principale freno ,oggi, all'innovazione e, soprattutto, alla introduzione generalizzata della banda larga di connessione ad internet, poiché l'Italia è attualmente agli ultimi posti in Europa ,come dimostrano i risultati dell'ultimo studio condotto dalla Commissione Europea per la Competitività Digitale . Appena il 31% degli utenti in Italia dispone di una connessione a Internet broadband, mentre la media europea si attesta al 49%. E se un terzo dei cittadini dell'Unione Europea non si è mai collegato alla Rete, in Italia la cifra arriva fino al 50% della popolazione. Appare leggermente migliore la situazione delle imprese italiane, l'81% delle quali dispone di una connessione a banda larga.[27]
Il problema della innovazione della connettività si presenta ,comunque, sia pure con proporzioni differenti rilevante anche in Europa se è vero che dal 2004 al 2008 i cittadini che utilizzano con regolarità Internet sono passati dal 33% al 56% della popolazione UE, solo il 7% dei consumatori si è rivolto alla rete per effettuare acquisti on line in un altro paese membro e, rispetto agli USA e

---

[25] BISI S. *Internet e libertà di manifestazione del pensiero. Le recenti tendenze europee e il caso francese.,Ciberspazio e diritto 2010 pag. 395.*

[26] LUCCHI N. *La legge Création et Internet (Legge HADOPI: Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet): le censure del Conseil constitutionnel.*,Quaderni costituzionali 2010 pag. 375.. In merito cfr. anche ALVANINI S, *La disconnessione da Internet come sanzione per il download illegale,* Il diritto industriale 2010 pag. 183 . HADOPI (acronimo di *Haute Autorité pour la diffusion des oeuvres et la protection des droits sur l'Internet*) è una vera e propria autorità indipendente specifica che si occupa dell'applicazione *della Loi Création et Internet* n. 311 introdotta nel 2009 ed in vigore dal 2010, dedicata al diritto d'autore su Internet, una normativa che prevede una vera e propria "disconnessione forzata" per coloro che violano il copyright, secondo una risposta graduale. La legge infatti prevede tre passaggi: un utente scoperto a scaricare file protetti da copyright sarà prima avvisato via e-mail, in caso di persistenza della violazione riceverà allora una raccomandata, e poi, come ultimo avviso, sarà invitato a comparire davanti ad un giudice, che deciderà un'eventuale multa o la disconnessione forzata. Il destinatario degli avvisi non è ,comunque, l'autore della violazione, bensì il titolare del contratto di abbonamento ad internet. Più di recente si sono sviluppate polemiche anche sugli alti costi di questo sistema ,giudicato del tutto inutile,anche in relazione agli altissimi costi pubblici di gestione, per frenare i comportamenti abusivi.

[27] L'indagine svolta per verificare i frutti della politica di promozione delle tecnologie di comunicazione è stata predisposta dalla Commissione Barroso. *http://ec.europa.eu/italia/attualita/primo_piano/informazione/sondaggio_europei_internet_it.htm*

al Giappone, l'UE appare in forte ritardo in merito agli investimenti per la ricerca e lo sviluppo di tecnologie dell'informazione e della comunicazione e di mercati innovativi quali la *pubblicità on line.*

5. Alla ricerca dell'equilibrio: la posizione della Corte di giustizia europea.

Un importante spunto per la disciplina internazionale ,specificamente con riguardo alla legittimità sul piano comunitario della adozione di politiche di "*filtering*" sulle comunicazioni onde precludere l'accesso via web a contenuti illeciti perché in violazione della proprietà intellettuale è dato dalla sentenza della Corte di giustizia UE 24 novembre 2011 nel procedimento C-70/10 (*Scarlet-SABAM,Societè belge des auteurs, compositeurs et éditeurs)* . Si trattava di verificare la conformità alle direttive europee della richiesta avanzata dalla società di gestione dei diritti al provider di installazione di un tempo, un sistema di filtraggio di tutte le comunicazioni elettroniche, transitanti per i suoi servizi, in particolare mediante l'impiego di software *"peer to peer"*[28],al fine di individuare, nella sua rete, la circolazione di *file* contenenti contenuti protetti e quindi di bloccare il trasferimento di questi, al momento della richiesta o in occasione dell'invio.
La Corte europea afferma come ai sensi degli artt. 8, n. 3, della direttiva 2001/29 e 11, terza frase, della direttiva 2004/48, i titolari di diritti di proprietà intellettuale possono chiedere un provvedimento inibitorio nei confronti degli intermediari i cui servizi siano utilizzati da terzi per violare i loro diritti e ricorda coma proprio dalla stessa giurisprudenza della Corte risulta poi che la competenza attribuita, a norma di tali disposizioni, agli organi giurisdizionali nazionali deve consentire a questi ultimi di ingiungere agli intermediari di adottare provvedimenti che contribuiscano in modo effettivo, non solo a porre fine alle violazioni già inferte ai diritti di proprietà intellettuale mediante i loro servizi della società dell'informazione, ma anche a prevenire nuove violazioni (viene richiamata la sentenza 12 luglio 2011, causa C-324/09, *L'Oréal*).
Quanto alle condizioni che devono essere soddisfatte e alla procedura da seguire, esse devono essere stabilite dal diritto nazionale al pari della loro applicazione da parte degli organi giurisdizionali nazionali, nei limiti ,tuttavia derivanti dalle direttive comunitarie. Perciò riveste una assoluta centralità in ogni forma di regolamentazione e di intervento il disposto dell 'art. 15, n. 1, della direttiva 2000/31,in tema di commercio elettronico che vieta alle autorità nazionali di adottare misure che impongano ad un provider di procedere *ad una sorveglianza generalizzata sulle informazioni che esso trasmette sulla propria rete*[29].

---

[28] Sul rapporto tra condivisione dei files e tutela del copyright si era già pronunciata,negativamente, la Corte Suprema degli Stati Uniti nel caso MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) affermando il principio per cui la distribuzione di un dispositivo con l'obiettivo di promuovere il suo uso onde violare il copyright, finalità peraltro risultante dalle indicazioni fornite agli utenti per favorire la violazione, comporta anche la responsabilità diretta dell'organizzatore per gli atti risultanti di violazione da parte di terzi.

[29] Cfr. in proposito PETRUSO R. *La responsabilità civile degli e-providers nella prospettiva comparatistica*. Europa e diritto privato 2011 pag. 1107 . RICCIO G.M. *La responsabilità degli Internet Providers nel d.lgs. n. 70/2003* Danno e responsabiltà 2003 pag. 1157. Responsabilità civile e previdenza, BUGIOLACCHI L. *Verso un sistema della responsabilità civile dell'Interet Provider? Considerazioni su un recente "anteproyecto" spagnolo di recepimento della direttiva 2000/31/CE sul commercio elettronico,*

Un siffatto divieto comprende in particolare le misure nazionali che obbligherebbero un prestatore intermedio a realizzare una vigilanza attiva su tutti i dati di ciascuno dei suoi clienti per prevenire qualsiasi futura violazione di diritti di proprietà intellettuale. Peraltro, un obbligo siffatto di vigilanza generale sarebbe anche incompatibile con l'art. 3 della direttiva 2004/48, che enuncia che le misure contemplate da detta direttiva devono essere *eque e proporzionate* e *non eccessivamente costose.* Un sistema di filtraggio generalizzato ,osserva la Corte, presupporrebbe in particolare che il provider identifichi, in primo luogo, nell'insieme delle comunicazioni elettroniche di tutti i suoi clienti, i file che appartengono al traffico «peer-to-peer» ,che identifichi, in secondo luogo, nell'ambito di tale traffico, i file che contengono opere sulle quali i titolari dei diritti di proprietà intellettuale affermino di vantare diritti e infine che esso determini quali tra questi file sono scambiati in modo illecito e quindi che proceda al blocco degli scambi di file che esso stesso qualifica come illeciti.
Una sorveglianza preventiva sui contenuti protetti si risolverebbe così in una vera e propria *osservazione attiva sulla totalità delle comunicazioni elettroniche* realizzate sulla rete dell'operatore coinvolto e, pertanto, includerebbe tutte le informazioni da trasmettere e ciascun cliente che si avvale di tale rete.
Perciò una ingiunzione rivolta al fornitore di accesso alla rete di predisporre il sistema di filtraggio controverso lo obbligherebbe a procedere ad una sorveglianza attiva su tutti i dati di ciascuno dei suoi clienti per prevenire qualsiasi futura violazione di diritti di proprietà intellettuale . Tale ingiunzione imporrebbe perciò al destinatario - di fatto – proprio la sorveglianza generalizzata, *che è espressamente vietata dall'art. 15, n. 1, della direttiva 2000/31.*
Quanto al rapporto tra la conformità della ingiunzione al diritto dell'Unione, la Corte osserva come occorra tenere conto delle condizioni che discendono dalla tutela dei diritti fondamentali applicabili, (la tutela dei diritti d'autore, che appartengono alla sfera del diritto di proprietà intellettuale e che possono essere lesi dalla natura e dal contenuto di talune comunicazioni elettroniche realizzate per il tramite della rete) laq Corte osserva che sebbene la tutela del diritto di proprietà intellettuale sia espressamente sancita dall'art. 17, n. 2, della Carta dei diritti fondamentali dell'Unione europea *non può desumersi né da tale disposizione né dalla giurisprudenza della Corte che tale diritto sia intangibile e che la sua tutela debba essere garantita in modo assoluto.* Inoltre ,e qui viene richiamata la sentenza 29 gennaio 2008, causa C-275/06, *Promusicae* la tutela del diritto fondamentale di proprietà, di cui fanno parte i diritti di proprietà intellettuale, deve sempre *essere bilanciata con quella di altri diritti fondamentali.*
Sottolinea quindi la Corte che è compito delle autorità (amministrative) come dei giudici nazionali, nel contesto delle misure adottate per proteggere i titolari di diritti d'autore, garantire un *giusto equilibrio tra la tutela di tali diritti e quella dei diritti fondamentali delle persone su cui incidono dette misure*.
Sicchè tanto le autorità amministrative che i giudici nazionali devono in particolare garantire un *giusto equilibrio tra la tutela del diritto di proprietà intellettuale,* di cui godono i titolari di diritti d'autore, e quella della libertà d'impresa,che deve essere garantita ai fornitori di accesso ad Internet in relazione all'art. 16 della Carta europea .
Su tali basi si perviene alla conclusione che l'ingiunzione di predisporre il sistema di filtraggio controverso implica una sorveglianza, nell'interesse di tali titolari, *su tutte* le comunicazioni elettroniche realizzate sulla rete del fornitore coinvolto. Tale sorveglianza è inoltre illimitata nel

Resp. Civile e previdenza 2002 pag. 292.

tempo, riguarda *qualsiasi futura violazione* e postula che si debbano tutelare non solo opere esistenti, bensì anche opere future, che non sono state ancora create nel momento in cui viene predisposto detto sistema.

Ciò causerebbe una grave violazione della libertà di impresa poiché obbligherebbe i providers a predisporre un sistema informatico complesso, costoso, permanente e unicamente a loro carico, il che risulterebbe peraltro contrario alle condizioni stabilite dall'art. 3, n. 1, della direttiva 2004/48,in tema di comunicazioni elettroniche il quale richiede che le misure adottate per assicurare il rispetto dei diritti di proprietà intellettuale *non siano inutilmente complesse o costose*. Infatti l'ingiunzione (amministrativa o anche giurisdizionale ,si badi) di predisporre il sistema di filtraggio non rispetterebbe l'esigenza di garantire *un giusto equilibrio tra, da un lato, la tutela del diritto di proprietà intellettuale, di cui godono i titolari dei diritti d'autore, e, dall'altro, quella della libertà d'impresa, riferibile agli operatori economici in ambiente digitale* .

Non solo ,osserva espressamente la Corte come persino gli effetti della ingiunzione non si limiterebbero al fornitore coinvolto, poiché il sistema di ,in quanto il sistema di filtraggio appare in sé idoneo a ledere anche i diritti fondamentali dei clienti (tutti) del fornitore , *ossia i loro diritti alla tutela dei dati personali e alla libertà di ricevere o di comunicare informazioni, diritti*, questi ultimi, direttamente tutelati dagli artt. 8 e 11 della Carta europea. Secondo la Corte appare infatti pacifico che l'ingiunzione di predisporre il sistema di filtraggio implicherebbe un'analisi sistematica di tutti i contenuti, nonché la raccolta e *l'identificazione degli indirizzi IP degli utenti all'origine dell'invio dei contenuti illeciti sulla rete, indirizzi che costituiscono dati personali protetti, in quanto consentono di identificare in modo preciso suddetti utenti.* E quindi una tale ingiunzione rischierebbe di ledere la libertà di informazione, poiché tale sistema *potrebbe non essere in grado di distinguere adeguatamente tra un contenuto lecito ed un contenuto illecito, sicché il suo impiego potrebbe produrre il risultato di bloccare comunicazioni aventi un contenuto lecito*. Infatti, è indiscusso che la questione della liceità di una trasmissione dipende anche dall'applicazione di eccezioni di legge al diritto di autore che poi variano da uno Stato membro all'altro. Inoltre, in certi Stati membri talune opere possono rientrare nel pubblico dominio o possono essere state messe in linea gratuitamente da parte dei relativi autori. Di conseguenza con l'ingiunzione che imponga un sistema di filtraggio controverso, il giudice nazionale in questione non rispetterebbe l'obbligo di garantire *un giusto equilibri*o tra, da un lato, il diritto di proprietà intellettuale e, dall'altro, la libertà di impresa, il diritto alla tutela dei dati personali e (*last but not least*) la libertà di ricevere o di comunicare informazioni.

Si tratta di una posizione chiara che appare ribadita con la successiva sentenza 16 febbraio 2012 C-360/10 nella causa *Belgische Vereniging van Auteurs, Componisten en Uitgevers* CVBA (SABAM) contro *Netlog* che è specificamente riferita ai servizi di *hosting* [30].

È quindi in sede europea[31] che la tematica si appresta ad essere meglio definita ,sia sul piano

---

[30] Cfr. BELLIA M.,BELLOMO G.A.M. , MAZZONCINI M. ,*La responsabilità civile dell'Internet Service Provider per violazioni del diritto d'autore*., Il diritto industriale 2012 pag. 341.,ma soprattutto PETRUSO R. *Fatto illecito degli intermediari tecnici della rete e diritto d'autore: un'indagine di diritto comparato*.,in Europa e diritto privato 2012 pag. 1175.

[31] Tra l'altro con una recente sentenza del 19/02/2013 anche la Corte europea dei diritti umani ha avuto modo di affrontare il tema del diritto d'autore in ambiente digitale (Caso: Fredrik NEIJ and Peter SUNDE KOLMISOPPI contro SVEZIA.n. 40397/12) ,si trattava della valutazione dell'ammontare di un risarcimento (5 milioni di euro) giudicato contrastante con l'art. 10 CEDU (sulla Libertà di espressione) a seguito della condanna penale e al risarcimento del danno per la gestione di un sito web che permetteva agli utenti di scambiare materiali in violazione

interpretativo ,definendo doverose priorità in ordine a differenti situazioni giuridiche soggettive e conseguenti meccanismi di garanzia proporzionati ed effettivi ,ma soprattutto non eccedenti allo scopo di tutela dei soggetti interessati e non comportanti il rischio di un monitoraggio invasivo sulle opzioni di consumo degli utenti ,da estendersi fino al controllo individuale sull'uso dell'opera dell'ingegno o sulla relativa diffusione in ambiente "sociale" digitale che è propria di una libera opzione degli utenti ,e che non si svolge spesso in ambito commerciale ,ma finisce al contrario dei tanti timori proprio per costituire una promozione planetaria dei contenuti ,entro un mercato caratterizzato ovunque invece da anomali picchi di concentrazione editoriale e dal sistematico controllo delle attività distributive relative ai contenuti stessi ,che risponde ad interessi economici ormai ben diversificate e certamente estranee al quadro dei diritti della personalità.

Le tematiche emerse a livello internazionale ed europeo non possono essere disconosciute né ridimensionate ,e comportano esse stesse una riconsiderazione complessiva della regolamentazione del diritto d'autore svoltasi finora entro ambiti regolatori riservati e caratterizzati da una sostanziale chiusura rispetto alle prospettive proprie del mondo della comunicazione interattiva nonché degli stessi consumatori ,che ,al contrario, proprio nella regolamentazione europea oggi trovano spazi di garanzia e di tutela non solo di tipo interlocutorio ,ma di vera e propria centralità.

È del resto la stessa corte di giustizia a riferirsi alla Carta costituzionale dell'Unione europea quale riferimento essenziale nell'ambito della composizione dei conflitti giurisdizionali e perciò a offrire agli interpreti un preciso e ben definito quadro di riferimento nel segno della libertà e della garanzia dei diritti fondamentali nell'ambiente digitale globale.

---

del diritto d'autore (pirate Bay) . Nel 2009 la Corte distrettuale di Stoccolma aveva condannato i responsabili ad un anno di reclusione e al risarcimento dei danni cagionati e quantificati approssimativamente in 3,3 milioni di euro. Nel novembre 2010 la Corte d'appello aveva ridotto la pena detentiva ed aumentato quella pecuniaria ed Infine, la Suprema Corte aveva rigettato il ricorso nel 2012.

I ricorrenti affermavano infatti di non poter essere ritenuti responsabili per l'uso da parte di altre persone del sistema di condivisione da loro organizzato il cui scopo iniziale era unicamente quello di facilitare lo scambio di dati su Internet. A loro avviso, solo quegli utenti che avevano scambiato informazioni illecite relative a materiale protetto dal copyright avevano commesso un reato. Dunque, invocando l'articolo 10,della Convenzione europea sui diritti umani avevano lamentato che la loro condanna per concorso nei reati in violazione del Copyright Act svedese avesse di fatto violato il loro diritto alla libertà di espressione. La Corte ha invece ritenuto che l'articolo 10 tutela il diritto di ciascuno a ricevere e diffondere le informazioni su Internet. Sebbene i ricorrenti avessero abbiano agito a scopo di profitto, il loro coinvolgimento nella realizzazione di un sito web finalizzato a facilitare lo scambio di materiale tutelato dal copyright era protetto dal diritto di ricevere e comunicare informazioni. In tal modo, la loro condanna ha interferito con il loro diritto alla libertà di espressione. Tuttavia, dato che il materiale condiviso per il quale erano stati condannati risultava tutelato dal Copyright Act, la Corte ha ritenuto che l'ingerenza delle autorità svedesi sia stata imposta dalla legge. È stato altresì considerato che la condanna penale e il conseguente risarcimento aveva perseguito il fine legittimo di tutelare il diritto d'autore. Infine, la Corte svedese aveva effettuato un motivato bilanciamento tra i due interessi concorrenti, entrambi tutelati dalla Convenzione: il diritto dei ricorrenti di agevolare lo scambio di informazioni su Internet e quello dei titolari del diritto d'autore ad essere protetti contro la violazione del copyright. La Corte ha ritenuto che le autorità svedesi avevano un ampio margine di apprezzamento nel decidere su tali materie, specialmente perché alle informazioni in questione non era stato riconosciuto lo stesso livello di protezione che è invece conferito all'espressione e alla discussione politica, nonché in considerazione del fatto che il dovere delle autorità stesse di garantire il rispetto del diritto d'autore tutelato sia dal *Copyright Act* sia dalla Convenzione ha costituito un importante motivo per la limitazione della libertà di espressione dei ricorrenti. Inoltre, visto che i ricorrenti non avevano rimosso dal sito il materiale protetto dal diritto d'autore sebbene fosse stato loro richiesto, la pena detentiva e la condanna di risarcimento dei danni non potevano in alcun caso esser essere considerate sproporzionate. Dunque, la Corte ha concluso che l'ingerenza statale nel godimento con il diritto alla libertà di espressione dei ricorrenti era stata necessaria ,secondo lo schema proprio dell'art. 10, in una società democratica per la protezione dei diritti altrui e che il ricorso doveva essere rigettato perché manifestamente infondato.

Ma il capitolo finale ,che dovrà essere scritto nel prossimo decennio è quello che riguarda la ridefinizione stessa della proprietà intellettuale entro il nuovo ambiente globale delle comunicazioni interattive, adeguando tutte le convenzioni in materia e forse ,in definitiva, arrivando a superare il tradizionale (e statico) significato di "proprietà" (esclusiva) per definire un più moderno concetto di *concorrenza nella produzione di contenuti cognitivi* ,salvaguardando la diffusione (inclusiva) libera di idee e fruizioni e sanzionando in modo universale (ed effettivo) solo gli sfruttamenti oggettivamente imitativi ed abusivamente espropriativi aventi chiaro carattere commerciale ,cioè basati sulla realizzazione di utili economici direttamente e specificamente legati alla fruizione dei contenuti immessi.

Ed è lecito sperare che in questa prospettiva vi sia anche spazio per i giuristi attenti alla evoluzione dell'informatica globale e non solo per gli analisti di mercato o i lobbisti ,più o meno evidenti, che pretenderebbero di fissare le regole giuridiche ,persino quelle di ordine penale, a seconda delle convenienze economiche del momento dei loro committenti.

È in gioco ,in definitiva, il senso stesso della libertà digitale ,la nostra ,ma soprattutto quella delle generazioni future.

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 102-118

Profili di responsabilità penale per l'internet service provider: tra esigenze garantistiche e valori in conflitto

Rocco Lotierzo

Abstract: Alla luce del ruolo, sempre più pervasivo, assunto da Internet nelle società moderne, è indispensabile stabilire come operino le norme penali rispetto a tale Fenomeno. E, stabilire se, e in quali termini, gli Internet Service Providers - che consentono il funzionamento della Rete delle reti per come la conosciamo - possano incorrere in responsabilità penali, è una delle questioni di maggior momento. Essa coinvolge non solo l'osservanza di precetti garantistici, che trovano base fondativa nella Costituzione; bensì anche la salvaguardia della complessiva gamma di valori che nella Rete possono trovare una risorsa o una minaccia

Parole chiave: Internet service providers – responsabilità penale – concorso di persone nel reato – concorso commissivo – dolo eventuale – concorso omissivo – posizione di garanzia

1. Lo scenario

La fortunatissima parabola, con l'estesa e variegata gamma di usi che ne sono possibili, pone in evidenza quale sia il grado di penetrazione che Internet ha avuto nelle vite di tutti e di ciascuno.
Ovvio è, pertanto, che, poiché esso costituisce al contempo luogo e strumento per l'agire umano, possa risultare ambiente e mezzo anche per la realizzazione di reati.
Per quanto ciò sia vero, non va, tuttavia, taciuto che le peculiarità di Internet, in generale, finiscano con l'implementare i fenomeni criminali.
E infatti, se si concentra l'attenzione, per un momento, sulle attività illecite realizzabili dagli utenti della c.d. Rete delle reti, ci si avvede di come la percezione di un contesto non fisico – seppure non totalmente sprovvisto di infrastrutture materiali – allenti considerevolmente le resistenze alla commissione del reato[1].

[1] V. per puntuali riflessioni in argomento, sotto il profilo criminologico, CORRADINI – PETRUCCI, *I nuovi scenari dello stalking. Da Internet ai luoghi di lavoro*, Edizioni Themis, 2012, p. 53 – 54.

Articolo pervenuto il 2 ottobre 2013, approvato il 28 novembre 2013

Più in dettaglio, influenzano questo esito[2]:

1. l'assenza di contatto fisico con la vittima;
2. la percezione di anonimato riferita alla identità dell'agente;
3. la più debole percezione del disvalore delle condotte realizzate in conseguenza anche della loro perdita di fisicità.

A ciò si aggiunga che il potenziale diffusivo del mezzo di comunicazione utilizzato è incommensurabile, sicché taluni comportamenti criminosi possono raggiungere con minor spesa di tempo ed energia la propria finalità[3].

Rimane, quindi, la chiara impressione che Internet possa non solo facilitare – come, del resto, avviene rispetto a qualsiasi altra attività umana – la realizzazione di reati, ma finanche attrarre nella sfera di quanti ne commettono individui, sui quali, in un differente contesto, sicuramente avrebbe prevalso la controspinta generalpreventiva del precetto penale.

Tale estensione della platea dei soggetti che incorrono nel reato, unita alla schermatura fornita dall'anonimato ed alla possibilità per l'utente di operare anche da luoghi remoti, rende difficile ed onerosa[4], benché non sempre impossibile, la individuazione e punizione dei colpevoli.

È proprio da questo dato di esperienza che deriva la tendenza o la tentazione di sovraccaricare di responsabilità le istituzioni che nell'ambiente Internet, fornendo professionalmente i più disparati servizi, ne consentono il funzionamento con le modalità che conosciamo (cc. dd. Internet Providers).

In altri termini, in un contesto ove il reato – invero, spesso nelle sue forme di manifestazione meno allarmanti[5] – si può rendere fenomeno di massa, è giocoforza tentare di polarizzare l'intervento penale attorno a soggetti (i providers) che, diversamente dai miliardi di utenti (clients) poco visibili ed individuabili, possono essere agevolmente assoggettati a obblighi e sanzioni[6]. Senza dimenticare che, proprio per la centralità delle istituzioni in discussione, sembrerebbe possibile allocare in capo ad esse oneri di prevenzione e impedimento del reato, i quali, tuttavia, pongono seri problemi di fondamento giuridico e fattibilità pratica.

2. Le tipologie di providers e la disciplina del D. lvo 10 settembre 2003 n. 70

La introduzione al tema difetta finora di sufficiente chiarezza, non essendosi fornite, almeno in termini comprensibili, se non proprio tecnicamente corretti, alcune definizioni essenziali.

---

[2] Cfr. INGRASSIA, *Il ruolo dell'Isp nel ciberspazio: cittadino, controllore o tutore dell'ordine*, reperibile all'indirizzo web *http://www.penalecontemporaneo.it/upload/1351711435Il%20ruolo%20del%20ISP%20nel%20cyberspazio%20DPC.pdf,* p. 4.

[3] Si rifletta, ad es., alla creazione di contatti per la nascita e il mantenimento in vita di un'associazione con finalità di terrorismo (art. 270 bis c.p.).

[4] Le indagini informatiche, invero, consentono di accertare giorno ed ora del fatto e, con l'acquisizione dei files di log, di risalire all'utenza telefonica collegata alla connessione internet utilizzata per la commissione del reato.

[5] Molto spesso si tratta di violazioni del diritto d'autore o reati contro l'onore.

[6] In tema v. PICOTTI, *Fondamento e limiti della responsabilità epnale dei service providers,* in *Dir. pen. e proc.*, 1999, pp. 379 ss..

Anzitutto, quella di Internet, che "è una rete mondiale di reti di computer ad accesso pubblico (interconnesse, *ndr*) che offre all'utente una vasta serie di contenuti potenzialmente informativi e servizi[7]". Tra questi ultimi, quello di posta elettronica e il World Wide Web, che permette all'utente di fruire di moltissimi contenuti e altri servizi (ad es., navigazione sulle pagine web).
Una infrastruttura così congegnata prevede per il suo funzionamento l'essenziale contributo di istituzioni quali i providers, classificabili come organizzazioni che offrono agli utenti, dietro la stipulazione di un contratto di fornitura, servizi inerenti all'Internet[8].
Figura *sui generis*, poiché non effettua attività di tipo tecnico, è quella del c.d. content provider ossia del soggetto o ente che predispone i contenuti immessi in Rete.
Possono, invece, propriamente definirsi providers di servizi Internet (cc.dd. Internet Service Providers o, in breve, ISP) quelli che forniscono l'accesso alla Rete o trasmettono, su una rete di comunicazione, informazioni fornite da un destinatario del servizio (attività di mere conduit).
Altro tipo di attività caratterizza gli ISP che effettuano la memorizzazione automatica, intermedia e temporanea di informazioni (attività di caching).
Infine, ancora differente è il compito degli ISP che forniscono gli spazi web allocati sui propri computer servers, su cui i destinatari del servizio memorizzano le informazioni – le pagine web - rendendole accessibili attraverso Internet (attività di hosting).
Dalle caratteristiche tecnico – operative di tali strutture deriva, all'evidenza, un diverso grado di vicinanza e verificabilità, da parte del provider, rispetto alle attività realizzate dagli utenti che si avvalgono del servizio. Dunque, diverse sono anche le condizioni poste per l'eventuale coinvolgimento, a titolo di concorso, del provider stesso nel delitto commesso da un proprio utente.
La classificazione degli ISP per attività svolta è integralmente ripresa dagli artt. 14, 15 e 16 D. Lvo 10 settembre 2003, n. 70 di attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno.
La disciplina tracciata dalle disposizioni appena citate prevede una responsabilizzazione progressiva del provider in considerazione del tipo di attività da esso svolta.
Precisamente, è previsto che il provider che pone in essere un'attività di mero trasporto dei dati o fornisce l'accesso alla Rete "non è responsabile delle informazioni trasmesse a condizione che:

a. non dia origine alla trasmissione;
b. non selezioni il destinatario della trasmissione;
c. non selezioni né modifichi le informazioni trasmesse" (art. 14 co. I D. Lvo n. 70/2003).

Relativamente al provider che effettua un'attività di caching è, invece, stabilito che "il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che:

---

7 V. *http://it.wikipedia.org/wiki/Internet*.

8 Definizione fornita da PIRRUCCIO, *Diritto d'autore e responsabilità del provider*, in *Giur. Merito*, 2012, 12, p. 2594.

a. non modifichi le informazioni;
b. si conformi alle condizioni di accesso alle informazioni;
c. si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore;
d. non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni;
e. agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione" (art. 15 co. I D. Lvo n. 70/2003).

Infine, per il soggetto che effettua attività di hosting, è previsto che esso "non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:

a. non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione;
b. non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso" (art. 16 co. I D. Lvo n. 70/2003).

Norma, in un certo senso, di chiusura è quella dell'art. 17 co. I D. Lvo n. 70/2003, per la quale il provider "non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, nè ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite".

Come preannunciato, i meccanismi di esenzione della responsabilità sono ancorati al grado di conoscenza (o conoscibilità) dei contenuti immessi da terzi fruitori del servizio erogato. Contestualmente vi è, però, la proclamazione del principio per cui non sussiste alcun generale e indefinito obbligo del provider di garantire la liceità del traffico internet che scorre attraverso le proprie infrastrutture.

Il riverbero penalistico di tale assetto è di agevole comprensione: pur essendo, infatti, il Decreto Legislativo in discussione diretto, con alcune specifiche eccezioni applicative[9], a regolamentare il complesso dei servizi della società del'informazione e, pur non ospitando alcuna norma penale, detta negli articoli sopra menzionati regole, che, all'evidenza, costituiscono la guida anche per il fondamento di eventuali responsabilità penali; quanto meno, perché mostrano i modelli comportamentali ai quali riferirsi per il riscontro della sussistenza dell'elemento soggettivo richiesto dalla fattispecie tipica contestata.

[9] V. art. 1 co. II e III D. Lvo n. 70/2003, per cui sfuggono all'ambito di applicazione della normativa in parola, ad es., le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni o le attività dei notai o di altre professioni.

3. I valori in gioco

È facilmente riscontrabile come la tutela penale dei beni giuridici in ambiente Internet debba giocoforza misurarsi con la necessità di tutelare concorrenti beni della vita, costituzionalmente comparabili, che sono da fruire nel medesimo contesto.
La conflittualità in parola emerge con particolare forza laddove si tratti di assoggettare a responsabilità penali colui che fornisce le infrastrutture della Rete per fatti realizzati da chi le utilizza. Ed invero, non può sfuggire, nella determinazione del regime di responsabilità penale del provider, che esso opera in un contesto in cui si confrontano e rischiano di scontrarsi in ogni momento la necessità di tutela dei minori, della sicurezza pubblica, della privacy di terzi o dell'utente, della sua libertà di espressione e comunicazione, della reputazione sua o di soggetti terzi, per finire con la salvaguardia del diritto alla protezione delle opere dell'ingegno. Sullo sfondo, rimane, ancora, la libertà di impresa del provider stesso, incomprimibile se non per le esigenze descritte nell'art. 41 co. II Cost..
In tale scenario, potrebbe accadere che la sopravvalutazione di uno dei valori in gioco conduca a un non giustificato sacrificio di un altro, che, nelle circostanze date, va privilegiato.
Così, esemplificativamente, qualora si intendesse, per finalità di sicurezza pubblica, gravare il provider di obblighi di prevenzione, ad es., prevedendo sistemi di filtraggio dei messaggi di posta dei singoli utenti[10], ciò potrebbe comportare la violazione, da parte dello stesso imprenditore, delle norme penali a tutela della inviolabilità dei segreti[11], con il risultato di pregiudicare il diritto del privato a mantenere segreta la corrispondenza.
In altre parole, si profila all'orizzonte una forte esigenza di bilanciamento tra i valori in potenziale conflitto, tenuto conto che, per lo più, si tratta di beni riconosciuti fondamentali non solo dalla Carta Costituzionale, ma anche dalla Carta Fondamentale dei diritti dell'Unione Europea.
Proprio dall'art. 52 co. I della c.d. Carta di Nizza è enunciato che le limitazioni di diritti fondamentali debbono essere previste dalla legge e rispettare il contenuto essenziale di altri diritti riconosciuti dalla Carta, aggiungendo, decisivamente, che "nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".
Pertanto, finanche la previsione, nella Legislazione di un singolo Paese, di obblighi a carico del provider che non rispettino tale ultimo assunto meriterebbe la patente di illegittimità comunitaria[12].

---

[10] Il riferimento è a sistemi di filtraggio preventivo per categorie estese di soggetti, essendo, invece, obbligo del provider quello di fornire, "senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite" (art. 17 co. II let. b) D. Lvo n. 70/2003).

[11] Cfr. PICA, *Il diritto penale delle tecnologie informatiche*, Utet, 1999, p. 238 ss..

[12] Corte Giustizia UE, III sez., 24 novembre 2011, Scarlet Extended c. SABAM nel procedimento C -70/10, parr. 44-45, reperibile all'indirizzo web *http://www.leggioggi.it/allegati/sentenza-corte-ue-terza-sezione-24-novembre-2011/*.

4. Le declinazioni della c.d. responsabilità penale del provider per i contenuti illeciti di Internet

La delimitazione dei confini entro i quali è invocabile un intervento punitivo rispetto a un ISP per i contenuti illeciti da esso veicolati, non può certamente comportare l'annullamento del "rischio" penale riguardante tali soggetti.

Cionondimeno, prima di procedere nel discorso, pare doveroso soffermarsi a precisare che è soltanto per rendere agevole la esposizione che si è iniziato e si continuerà a parlare di responsabilità penale del provider.

La precisazione, lontana dall'essere pedantesca, mira a sottolineare che, proprio la costituzionalizzazione del principio di personalità della responsabilità penale, al di là di eventuali ricadute sulla responsabilità amministrativa da reato dell'ente, impone in ultimo al giudice di focalizzare l'attenzione sulle persone fisiche, interne alla organizzazione del provider, che hanno commesso il reato o vi hanno partecipato.

Invero, si tratta di un punto non adeguatamente considerato[13], soprattutto alla luce del fatto che gli ISP sono strutturati quasi sempre come enti collettivi e talvolta si tratta di imprese multinazionali, inserite in gruppi[14]. Non pare perciò da sottovalutare la criticità insita sia nella operazione di individuazione dei presunti responsabili sia – forse, soprattutto – nel riscontro dell'elemento doloso richiesto per l'applicazione della fattispecie incriminatrice di parte speciale.

Posto sul tappeto un ulteriore aspetto problematico dell'analisi, che si tenta di compiere rispetto all'attuale regime di responsabilità penale del provider, è il momento di osservare in quali termini essa possa concretamente declinarsi.

Sinteticamente, possono darsi fattispecie in cui il provider è l'autore della condotta tipica del reato in forma monosoggettiva; ed altre in cui il provider è chiamato a rispondere secondo le regole del concorso, omissivo o commissivo, di persone nel reato.

In termini condivisibilmente negativi[15] è invece risolto l'interrogativo se possa applicarsi al

---

[13] Cfr. SIEBER, *Responsabilità per la circolazione di dati nelle reti internazionali di computer, parte seconda*, in *Riv. Trim. dir. pen. eco.*, 1997, p. 1193 in nota 1.

[14] Emblematica è la vicenda cui si riferiscono le sentenze sul caso Google/Vividown, laddove si è posta la esigenza di individuare i presunti responsabili dei reati contestati all'interno di una galassia societaria con la capogruppo avente sede negli Stati Uniti e altre società stabilite nel territorio italiano. V. Trib. Milano 12 aprile 2010, Drummond e altri in *Corr. Merito*, 2010 pp. 960 e ss.., con nota di BEDUSCHI, *Caso Google: libertà di espressione in internet e tutela penale dell'onore e della riservatezza;* nonché, per l'appello, che ha riformato in senso assolutorio la residua condanna per trattamento illecito dei dati personali, Corte App. Milano 21 dicembre 2012, Drummond e altri, reperibile all'indirizzo web h*ttp://www.penalecontemporaneo.it/upload/1362065204Sentenza%20appello%20google.pdf*.

[15] V. Cass. sez. V^, 16 luglio 2010, Ruta, reperibile all'indirizzo web *http://www.penalecontemporaneo.it/upload/Cass.%20resp.%20direttore%20periodico%20telematico.pdf*; conf. Cass. sez. V, 29 novembre 2011, n. 44126 M.D. in Dir. inf. 2012, 1, pp. 82 ss., con nota di CORRIAS LUCENTE, *Al direttore di un periodico on line non si applica il reato previsto dall'art. 57 del codice penale*. Dissonante, invece quanto affermato, nella Giurispudenza di merito, da Tribunale di Aosta, 26 maggio 2006, n. 553, Mancini, reperibile all'indirizzo web *http://www.ilsole24ore.com/art/SoleOnLine4/Speciali/2006/documenti_lunedi/06novembre2006/TRI_AOSTA_26_05_2006_N_553.pdf?cmd=art*; nonché, con argomentazioni certamente più pregevoli, Trib. Firenze, 13 febbraio 2009, n. 982, A.C., reperibile all'indirizzo web *http://www.penale.it/page.asp?IDPag=832*, per cui l'apparente difetto di tipicità verrebbe corretto in forza della Legge n. 62/2001, che nella nozione di prodotto editoriale ricomprende anche il prodotto realizzato su supporto informatico, destinato alla pubblicazione. In dottrina, v. , per analoghe considerazioni, l'opinione di IANNI, *La responsabilità in sede penale*

provider il severo regime dettato rispetto al direttore, al vice direttore responsabile, all'editore ovvero allo stampatore dagli artt. 57 e 57 bis c.p., i quali tipizzano la fattispecie colposa di omesso controllo finalizzato ad impedire reati commessi col mezzo della stampa periodica e non periodica.
Ad ostacolare l'applicazione delle norme penali in discussione al provider v'è, anzitutto, la decisiva circostanza per cui il regime dettato dal D. Lvo n.70/2003 impedisce di coinvolgere in responsabilità penali un ISP per contenuti immessi dagli utenti, ove non sia precisamente a conoscenza del contenuto illecito transitato dalle proprie infrastrutture: nel caso, opposto, di conoscenza, il riferimento normativo diverrebbe, invece, l'art. 110 c.p. sicchè non occorrerebbe invocare le norme penali sopra citate.
Peraltro, al provider difettano i poteri impeditivi rintracciabili, ad es., nel direttore del periodico a stampa: anzitutto, perché la mole di materiale inseribile dagli utenti non è suscettibile di essere preventivamente controllata dal provider[16]; in secondo luogo, poiché l'eventuale diniego alla pubblicazione non implicherebbe impedimento del reato, potendo il contenuto illecito essere contemporaneamente veicolato attraverso, esemplificativamente, un altro sito web.
In ultimo, ma non da ultimo, il più lampante deficit di tipicità si rinviene nella impossibilità di identificare Internet - anche quando veicolo di contenuti ad essa assimilabili – con la stampa. Ciò perché manca il requisito della riproduzione tipografica necessaria, in quanto la stampa del messaggio è, piuttosto, solo eventuale e devoluta al destinatario del messaggio stesso. Infine, poiché diverse sono le sue modalità tecniche di trasmissione: nel caso dello stampato, la consegna materiale; in quello di Internet, la sua diffusione per via telematica[17].
A quanto appena detto, merita aggiungere solo un'ultima annotazione: la gran parte dei precedenti giurisprudenziali, i quali hanno consentito lo stratificarsi di un orientamento che nega l'applicabilità al provider degli artt. 57 e 57 bis c.p. riguardano addirittura testate telematiche strutturate in modo analogo a quelle cartacee. Dunque, l'avere escluso che finanche quanti in effetti svolgono un'attività di *content* provider restino all'interno del perimetro applicativo di quelle norme, a maggior motivo sembra poter fare escludere l'esigibilità di controlli preventivi generalizzati da parte di providers di servizi Internet.

5. Il provider quale autore del reato

L'ipotesi che, tra tutte, suscita minori incertezze applicative è senza subbio quella in cui il provider si renda autore della condotta tipica di reato.
Per comprendere, si pensi al caso del soggetto che allestisce un sito che pubblicizza con foto e contatti l'attività di prostitute (art. 3 L. n. 57/1958)[18] oppure ad un altro che promuova

dell'internet service provider alla luce dei più recenti decisa giurisprudenziali, reperibile all'indirizzo web *http://www.neldiritto.it/appdottrina.asp?id=6135#.Ujc8aH-qUwc*, .

16 V. Cass. sez. V, 29 novembre 2011, n. 44126 M.D, cit..

17 V. Cass. sez. V^, 16 luglio 2010, Ruta cit..

18 V. Cass. sez. III^, 5 novembre 2010, V. M., in *Cass. pen*., 2011, pp. 2751 ss., la quale precisa che per la configurazione del reato di favoreggiamento della prostituzione oltre alla mera pubblicazione di inserzioni pubblicitarie delle prostitute, occorrono "ulteriori attività finalizzate ad agevolarne il meretricio, quali l'indicazione del recapito telefonico e la

un'associazione terroristica, fornendo le informazioni per aderire e per contribuire economicamente alla vita della stessa (art. 270 bis c.p.). Col limite già sopra ricordato per cui la responsabilità penale incombe soltanto sui singoli che operano per conto della organizzazione, potranno applicarsi le corrispondenti fattispecie incriminatrici che si assumono violate.

Evidente è, ad ogni modo, che le ipotesi di autoria nel reato difficilmente[19] – e certamente non quelle appena rappresentate - possono attagliarsi a ISP fornitori di accesso alla Rete o che effettuano attività di caching, necessitando un'approssimazione alla attività di gestione del contenuto, che caratterizza i *content* provider o, al più, quelli che effettuano attività di c.d. *hosting* attivo, intendendosi per tale "l'ISP che non si limiti a memorizzare sui propri server informazioni e dati, ma compia attività ulteriori quali l'indicizzazione, il filtraggio, la selezione o l'organizzazione dei contenuti"[20].

Proprio tale ambito, nel quale non si segnalano apparentemente problemi, deve porgersi, però, molta attenzione ad una recente posizione assunta nella Giurisprudenza di merito[21], secondo cui la amministratrice di un sito web sarebbe addirittura responsabile, autonomamente e, in assenza di contestazione del concorso di persone o della fattispecie di cui all'art. 57 c.p., per i contenuti diffamatori veicolati, provenienti da qualsiasi terzo. Ed infatti, dovrebbe riconoscersi che, nel caso di predisposizione di filtri, il contenuto sia stato scientemente approvato; nel caso di mancata predisposizione di filtri si sia messa in preventivo la eventualità di veicolare anche contenuti non leciti.

L'impostazione indicata, la quale pare rifuggire, peraltro, dal ricorso al modello di responsabilità per mancato impedimento del reato, individua una granitica responsabilità oggettiva in capo a soggetti solo perché assumono un determinato ruolo ed indipendentemente dal riscontro delle effettive capacità di intervento e, tanto meno, del dolo di fattispecie. A risaltare è, dunque, la effettiva obliterazione del principio di colpevolezza, fino alla negazione di prova a discolpa e alla configurazione di una responsabilità per fatto altrui, ciò che è inammissibile finanche in settori in cui il rapporto di vicinanza – e quindi la capacità di un intervento impeditivo – con (gli autori de) il reato è significativamente maggiore.

Del resto, un siffatto modo di intendere la responsabilità penale per reati commessi in Internet comporta, da un lato, la concentrazione di un potere di limitazione della libertà di manifestazione del pensiero in capo a soggetti (spesso provider di contenuti) culturalmente inidonei e, comunque, privi di qualsiasi legittimazione a tal fine[22]; dall'altro, nemmeno può sfuggire il forte disincentivo alla costituzione di canali, tanto alternativi quanto più "istituzionali", di informazione.

---

pubblicazione di foto di nudo e di atteggiamenti provocanti".

19 Il discorso conserva ovviamente validità ove si rimanga nell'ambito di quelli che PICOTTI, *La nozione di "criminaltià informatica" e la sua rilevanza per le competenze penali Europee*, in *Riv. Trim. dir. pen. eco*., 2011, p. 847, definisce reati cibernetici in quanto si tratta di fattispecie che nel tipo contemplano l'elemento di connessione con Internet ovvero di altri reati che quel collegamento si trovino ad avere nel caso concreto.

20 INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., p. 20.

21 GIP Trib. Varese, 22 febbraio 2013, n. 116/2013, reperibile all'indirizzo web *http://www.penalecontemporaneo.it/upload/1370547968595%20sito%20internet.pdf*.

22 Cfr. SPAGNOLETTI, *La responsabilità del provider per i contenuti illeciti di internet*, in *Giur. merito*, 2004, 9, p. 1935, che considera tali limitazioni giustificate soltanto ove a realizzarle siano organi pubblici. Quindi, dotati di legittimazione democratica.

Al di là dei rilievi in punto di osservanza dei principi costituzionali e di allocazione di poteri di censura, la prospettazione appena criticata desta attenzione in quanto la base concettuale che la muove pare essere quella della percezione di una fin troppo estesa capacità del provider di controllo dei contenuti, tenuto conto che nulla escluderebbe di tenere comunque il provider responsabile ove sussistesse il dolo di concorso nel delitto cui partecipa l'utente.
Posta negli oltremodo estesi termini di cui sopra, la prospettazione è, invece, inammissibile se, come nello specifico, commisurata a un provider di contenuti; e tanto più, se dovesse costituire fonte ispiratrice di analoghe ricostruzioni concernenti la responsabilità di Internet service providers.

6. La responsabilità del provider a titolo di concorso con l'utente

A) Aspetti generali
La tematica che merita di esser maggiormente esplorata è, tuttavia, quella concernente la responsabilità dell'ISP in concorso con l'utente.
Si tratta di aspetto saliente se sol si rifletta che, per la giurisprudenza maggioritaria[23] e buona parte della dottrina[24], la causalità di una condotta di concorso, differente dall'azione od omissione tipica, sussiste non solo quando la condotta è condizione necessaria dell'evento, bensì pure quando essa abbia agevolato o facilitato il reato per come si è *hic et nunc* realizzato.
Poggiando su tale fondamento la tipizzazione della condotta concorsuale, non sfugge che il fatto di apprestare le strutture (nel senso di consentire, ad es., l'accesso alla Rete ovvero di mettere a disposizione i propri computer servers) per la realizzazione del reato dell'utente, di per sé faccia ritenere integrato rispetto all'ISP l'elemento oggettivo di una condotta concorsuale rilevante[25].
Il discrimine da cui dipende l'applicazione all'ISP della fattispecie concorsuale è, così, squisitamente attinente all'elemento soggettivo, nel senso che, laddove sia ricavabile dagli elementi caratterizzanti della condotta la effettiva conoscenza dell'attività illecita altrui, potrà dirsi integrato il dolo richiesto dalle singole fattispecie incriminatrici[26]. Ciò fermo restando che il dolo di concorso richiede in aggiunta la volontà di concorrere con altri nel reato.
La guida da cui estrarre i parametri della volontà dolosa del provider è costituita, come anticipato, dagli artt. 14 ss. del D. Lvo n. 70/2003, che, in sostanza, pur diversamente declinando l'esenzione dalla responsabilità in ragione delle peculiarità del provider, àncorano detta esenzione alla

---

[23] V. Cass. sez. V^, 13 aprile 2004 n. 21802, in *CED Cass.* n. 229200; Cass. sez. IV^, 22 maggio 2007, n. 24895, *ivi*, n. 236853.

[24] Cfr. MARINUCCI – DOLCINI, *Manuale di diritto penale parte generale*, IV ed., 2012 pp. 423 ss.; FIANDACA - MUSCO, *Diritto penale. Parte generale*, IV ed., Zanichelli, 2001 p. 463.

[25] Invero, PICOTTI, *Fondamento e limiti*, cit. pp. 379 ss., considera necessario un *quid pluris* che renda tecnicamente possibile la conoscenza del contenuto illecito. In Giurisprudenza, pare nel medesimo senso, Cass. sez III^, 29 settembre 2009, n. 49437, P.M. in proc. Sunde Kuolmisoppi, in *Cass. pen.*, 2011, 3, p. 1102.

[26] Interessanti considerazioni sulle forme che assume il dolo nel campo di interesse provengono da D'AMBROSIO, *Responsabilità degli Internet Provider e Corte di Giustizia dell'Unione Europea: quali spunti per il sistema penale italiano?*, in *Internet Provider e Giustizia penale*, Giuffrè, 2012, p. 72 s..

conoscenza del contenuto illecito che transita in Internet per mezzo del contributo del provider stesso.
Il principio, con le cautele che andranno espresse, è compatibile coi principi in tema di colpevolezza e pare estensibile alla generalità dei cc.dd. reati cibernetici[27], commessi anche mediante il contributo dell'ISP. Pertanto, pur dovendo riconoscere che tra le eccezioni applicative indicate dall'art. 1 co. II D. Lvo n. 70/2003 compaiono, ad es., le violazioni in materia di privacy[28], il regime, appunto in quanto coerente coi principi generali, sembra adattarsi alla generalità delle ipotesi delittuose potenzialmente coinvolgenti il provider.
Ora. A fronte di un simile tracciato normativo, peraltro – non va dimenticato – condiviso a livello comunitario per effetto della emanazione della direttiva 2000/31/CE di cui il Decreto Legislativo costituisce attuazione, potrà risultare anche non indispensabile la differenziazione[29] degli ISP in ragione della passività ovvero attività che li caratterizza.

B) Il concorso commissivo

La "retorica" sul provider quale poliziotto della Rete[30], non deve far trascurare il fatto che gli ISP possono eventualmente concorrere nel reato dell'utente perché forniscono un servizio, ponendo in essere, dunque, una condotta attiva, che va ad inserirsi nel processo deterministico del reato.
Ed in effetti resta quasi complesso formulare ipotesi di concorso omissivo, se si pensa a come la rilevanza di eventuali condotte omissive verrebbe superata dalla sopravvenuta incidenza causale e dal maggior disvalore insito nell'avere fornito lo strumento (il servizio di internet) indispensabile per la commissione del reato per come si è prodotto.
Messa nella corretta prospettiva l'analisi, occorre appuntare l'attenzione sui requisiti indispensabili perché la condotta del provider possa dirsi penalmente rilevante come condotta di concorso.
Prima di tutto, si deve tornare su quanto detto *supra* in ordine alla sufficienza sotto il profilo oggettivo della mera prestazione di servizio.
Quanto sostenuto ha validità ovviamente ove la condotta dell'ISP costituisca un antecedente causale dell'evento di reato. All'evidenza, ciò non accade, però, qualora ci si imbatta in fattispecie in cui il contributo del provider è servito, semmai, ad estendere gli effetti lesivi della condotta dell'utente, giammai a procurarli.

---

27 V. nota 21.

28 Attenta osservazione di INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., p. 19.

29 Invalsa, tuttavia, nella Giurisprudenza comunitaria, come dimostrato da Corte di Giustizia UE, Grande Sezione, 23 marzo 2010, Google inc. c. Louis Vitton Martellier e SA altri, cause riunite C – 236/2008, 237/2008, 238/2008, parr. 114 – 115, reperibile all'indirizzo web *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62008J0236:IT:HTML*

30 Ma v. la delibera AGCOM, 25 luglio 2013, n. 452/13/CONS, di approvazione dello schema di regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003 n. 70, reperibile all'indirizzo web *http://www.agcom.it/default.aspx?DocID=11564*, che pare attribuire agli access provider compiti fin troppo pervasivi di ispezione del web, finalizzati alla tutela del diritto d'autore in ambito Internet. Si tratta, nondimeno, all'evidenza, di "aperture" in evidente contrasto con l'art. 17 D. Lvo n. 70/2003 nel punto in cui vieta la imposizione di generali obblighi di sorveglianza al provider e, quindi, con la direttiva 2000/31/CE, come affermato da Corte Giustizia UE, sez. III^, 24 novembre 2011, Scarlet Extended c. SABAM, cit..

Si fa riferimento a tutte quelle situazioni in cui il reato si deve ritenere già consumato nel momento in cui interviene la prestazione del servizio internet. Ad es., all'ipotesi in cui un sito web contenga il link ad altri siti che, in violazione della L. 633/1941, trasmettono, senza diritti, "opere protette"[31]: in tale fattispecie il contributo causale dell'ISP è mancante e, piuttosto, costituisce in post-fatto non punibile, successivo alla commissione del reato di cui all'art. 171 comma I lett. a) bis L. 633/1941 da parte di coloro che hanno inserito on line l'opera per primi[32].

Radicalmente diverso, invece, il caso in cui la fattispecie incriminatrice preveda quale condotta tipica la pubblicizzazione (ad es. art. 600ter co. III c.p.), potendosi qui ben immaginare un inserimento della condotta dell'ISP in un momento precedente la consumazione del reato.

In definitiva, la rilevanza causale della condotta del provider è una variabile strettamente dipendente dalla struttura della fattispecie incriminatrice e precisamente dalla collocazione dell'evento tipico prima o dopo la condotta di prestazione del servizio da parte dell'ISP.

Dopo aver svolto queste osservazioni, v'è da ribadire che, secondo le regole che governano l'accertamento della causalità della condotta di concorso, non occorre che il servizio reso dall'ISP si connoti – al fine di acquisire rilievo penale - per un *quid pluris,* peraltro non ben definito.

L'impostazione che pare suggerire tale supplementare riscontro, tra l'altro, risulta essere – non la più, bensì - la meno garantista, riversando sul provider, che si trovi in talune condizioni, una responsabilità di posizione, al limite sovvertibile con l'assolvimento dell'onere di provare la non colpevolezza.

La situazione considerata è quella che concerne il provider che esercita attività di hosting c.d. attivo, nel senso che non si limita a fungere da corriere di dati, ma effettua ulteriori attività di organizzazione e indicizzazione dei medesimi, talvolta con possibilità di sfruttamento economico mediante il meccanismo della pubblicità[33].

In effetti, la posizione del c.d. host attivo dovrebbe agevolare la prova del dolo di concorso, risultando più agevole dimostrare che un soggetto con le sue peculiarità operative sia in grado di mettersi al corrente dei contenuti che da esso vengono memorizzati.

La notazione, rasente l'ovvio, non deve però consentire il totale abbandono della verifica dell'elemento soggettivo, che non può essere in *re ipsa,* comunque, e, soprattutto, rispetto a soggetti, i quali gestiscono moli di dati sterminate, sicché si rende estremamente complesso – se non impossibile – il monitoraggio o addirittura filtraggio di tutto il materiale immesso dagli utenti[34].

Lasciano perciò in disaccordo posizioni assunte dalla Giurisprudenza italiana e comunitaria riguardo alla configurabilità di responsabilità per l'hosting provider attivo in concorso con l'utente[35].

---

[31] V. Cass. pen. sez. III^, 4 luglio 2006, n. 33945, in *Dir. inf.*, 2006, p. 741, che, all'opposto, nel caso Sky-Calcio libero, ha ritenuto avesse rilevanza causale la pubblicazione di un link ad un sito, che abusivamente trasmetteva partite di calcio del campionato italiano, in quanto la condotta aveva comportato la diffusione, almeno in maniera più larga, delle opere protette.

[32] INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, pp. 21 ss..

[33] Tipico meccanismo del genere è quello denominato Adwords, utilizzato dal motore di ricerca di Google, che abbina pubblicità di prodotti (con link verso il corrispettivo sito) alla digitazione, da parte dell'utente dello stesso motore, di determinate parole chiave.

[34] Così, ad es., Corte App. Milano, 21 dicembre 2012, Drummond, cit.

[35] Corte di Giustizia UE, Grande Sezione, 23 marzo 2010, Google inc.c. Louis Vitton Martellier e SA altri, cit., pur se

È il caso della decisione concernente, invero in fase ancora cautelare, il sito *www.thepiratebay.org,* cui si contestava la violazione dell'art. 171 ter co. II let a-bis) L. n. 633/1941 per avere consentito attraverso un protocollo *peer to peer* a mezzo di file torrent la condivisione e lo scaricamento di opere protette dal diritto d'autore.
La Suprema Corte, pur escludendo immediatamente che il semplice allestimento di un protocollo informatico potesse integrare una condotta di concorso punibile, ha però considerato che, occupandosi il sito *piratebay* dell'attività di indicizzazione e di tracciamento - essenziale perché gli utenti possano operare il trasferimento dell'opera (che in tal caso va da una pluralità di utenti autori dell'uploading verso una potenziale pluralità di utenti ricettori del downloading) [36]-, rimane l'imputabilità a titolo di concorso nel reato di cui all'art. 171 ter, comma 2, lett. a-bis), L. n. 633/1941.
Non dissimile la *ratio* sottesa a sentenza, stavolta, della Corte di Giustizia UE[37], laddove si è affermato che, per beneficiare della esenzione da responsabilità, l'host deve rimanere neutro rispetto alle informazioni trasmesse o memorizzate, ciò che invece non accade quando esso conservi un interesse diretto alla circolazione di una informazione.
In entrambi i casi, è chiaro che l'host non si limiti al ruolo di mero ospite che mette a disposizione tecnologia con cui l'utente è assolutamente libero di operare. Eppure, il principio di personalità della responsabilità penale non può essere obliterato così come la verifica in ordine alla sussistenza del dolo[38], atteso che la intuizione del ruolo non passivo dell'ISP ancora non implica assenza di neutralità dello stesso. E che, inoltre, la medesima intuizione non può condurre a sovrapporre totalmente all'apparato tecnologico adoperato dal provider le figure professionali (risorse umane) da esso impiegate, giacchè a costoro si tratta di applicare in ultimo la norma penale e per costoro deve essere allora accertata la effettiva conoscenza dei contenuti illeciti veicolati.
D'altronde, la più attenta Giurisprudenza si avvede della complessità tecnica del monitoraggio a tutto campo dei contenuti, pur senza giungere nemmeno a puntualizzazioni concernenti i destinatari ultimi del precetto penale[39].
Da quanto appena detto, sembra, dunque, confermata la impressione per cui l'elemento capace di selezionare le condotte di concorso debba essere il dolo.
L'atteggiarsi del coefficiente soggettivo in concreto non può non fondarsi – come già ripetuto – sulla esigenza di effettiva conoscenza dei contenuti, richiesta al provider dal D. Lvo n. 70/2003[40], che disciplina casi anche più complessi del semplice accordo criminoso.
Ciò ha condivisibilmente condotto taluno[41] ad affermare che il dolo di concorso del provider ha da essere necessariamente diretto e, quindi, caratterizzato da omogeneità tra il rappresentato e il

attinente aspetti civilistici; Cass. sez III^, 29 settembre 2009, n. 49437, cit..

36 Cass. sez III^, 29 settembre 2009, n. 49437, cit..

37 Corte di Giustizia UE, Grande Sezione, 23 marzo 2010, Google inc. c. Louis Vitton Martellier e SA altri, cit.

38 Non disconosce l'esistenza del problema PEZZELLA, *Google Italia. Diffamazione e riservatezza: il difficile compito del provider (e del giudice)*, in *Giur. merito*, 2010, 9, p. 2260, pur se non critico verso Cass. sez III^, 29 settembre 2009, n. 49437, cit..

39 Corte App. Milano, 21 dicembre 2012, Drummond, cit..

40 Cfr. artt. 12, 13, 14 dir. 2000/31/CE.

41 INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, p. 18.

voluto. Non pare possano esservi spazi per costruzioni imperniate su colpa o dolo eventuale[42] per diversi motivi.

In primo luogo, vi è la testuale necessità di effettiva conoscenza, che in maniera estremamente chiara esclude la rilevanza della mera accettazione del rischio di illiceità del contenuto inserito dall'utente. È per questo che le decisioni sopra menzionate appaiono discostarsi dal dato normativo: perché radicano una conoscenza effettiva[43] (*id est* dolo diretto, quando non addirittura intenzionale) a fronte di soggetti per i quali, al più, potrebbe parlarsi di accettazione del rischio di partecipare alla commissione di un reato.

Il secondo motivo rivela perché, anche per le materie indicate nelle eccezioni di cui all'art. 1 co. II D. Lvo n. 70/2003, non possa concedersi spazio al dolo eventuale.

Questo, in fattispecie di concorso di persone, va declinato come rappresentazione ed accettazione di un rischio concreto di concorrere nel reato con terzi, precisando che un rischio si dice accettato "a seguito di una deliberazione con la quale l'agente subordina consapevolmente un determinato bene ad un altro"[44].

Con una simile struttura concettuale, il dolo eventuale entra in crisi quando vi è il tentativo di abbinarlo alla posizione di un ISP rispetto alla immissione di contenuti da parte degli utenti.

Anzitutto, la componente rappresentativa (rappresentazione di un rischio - reato) deve necessariamente tenere conto del fatto che deve proiettarsi su eventuali condotte (reati) di terzi, che si avvalgono di servizi in sé assolutamente leciti. Pertanto, rammentando sempre che, fin quando si tratta di dolo eventuale, non si parla di accordi criminosi o simili, la componente probabilistica della rappresentazione viene disancorata da dati razionali, trasformandosi piuttosto in prevedibilità di un evento, concetto familiare alla colpa e più che al dolo.

Inoltre, la componente volitiva, *sub specie* di accettazione consapevole del rischio, implica l'accertamento che vi sia stata, da parte del'ISP, una subordinazione dei beni sacrificati con la commissione del reato ad altri da esso perseguiti. Tutto ciò comporta necessariamente la preventiva individuazione del bene preferito, che nello specifico potrebbe individuarsi ipoteticamente nel profitto economico d'impresa.

Tuttavia, in un simile contesto, la contemporanea esigenza di continuare a dare esecuzione al rapporto contrattuale che prevede la erogazione del servizio, rispetto a un soggetto che – lo si ricordi – non ha piena contezza dei contenuti immessi dall'utente, pone in una situazione di stallo probatorio. Ed infatti, non riuscirebbe a chiarirsi se vi sia stata accettazione del rischio - reato, subordinandolo ad altro bene (profitto), o, piuttosto, la erogazione del servizio sia stata effettuata in continuità ed in virtù della forza cogente di accordi interprivati.

Anche la c.d. prima formula di Frank[45] - per cui il dolo eventuale sussiste se viene riscontrato che

---

[42] Ancor meno in caso di fattispecie richiedenti il dolo specifico, v. Corte App. Milano, 21 dicembre 2012, Drummond, cit..

[43] Da precisare che la sentenza citata in nota n. 37, pur formulando affermazioni di indubbia rilevanza per la presente trattazione, accede a un contenzioso civilistico.

[44] Cass. sez. I^, 1 febbraio 2011, I. V., n. 10411, reperibile all'indirizzo web *http://www.penalecontemporaneo.it/upload/Cass.%20Pen.,%20Sez.%20I,%2001.2.11%20%28dep.%2015.3.11%29,%20n.%2010411,%20%20Pres.%20Di%20Tomassi,%20Rel.%20Cassano.pdf*. Cfr., in dottrina, sul medesimo crinale, PROSDOCIMI, D*olus eventualis. Il dolo eventuale nella struttura delle fattispecie penali,* 1993, Giuffrè, pp. 31 ss..

[45] Richiamata da PROSDOCIMI, *Dolus eventualis* cit., p. 9 s., nota n. 10.

l'agente, avendo la certezza dell'evento offensivo, ugualmente avrebbe agito – non può svolgere la propria funzione dirimente, in quanto la prestazione del sevizio – eventuale contributo criminoso dell'ISP- ci sarebbe normalmente stata anche in assenza di qualsiasi prognosi di rischi - reato.
Esclusa la rilevanza del dolo eventuale, a maggior ragione non può attribuirsene a un c.d. concorso colposo del provider nel reato doloso[46] dell'utente, nonostante la Giurisprudenza gli riconosca, per ora solo in altri settori, cittadinanza[47]. Al di là delle osservazioni sopra riportate in punto di necessaria effettiva conoscenza dei contenuti[48], non risulta praticabile accedere alla valorizzazione di atteggiamenti colposi riguardo ad eventi che il Legislatore punisce solo se cagionati con dolo, tanto più perché la colpa non può farsi consistere nell'avere fornito, attraverso atti leciti, occasione di delinquere a soggetti pienamente capaci di autodeterminazione[49].
Come si vede, in definitiva, la responsabilizzazione del provider esige un ancoraggio forte a un dolo "pieno", onde evitare che la applicazione non controllata della norma penale finisca col pregiudicare oltre misura il coacervo di Libertà che sono sul tappeto: dalla libertà personale degli operatori del provider, a quella di impresa di quest'ultimo, alla libertà di espressione e comunicazione degli utenti, strettamente legata al corretto funzionamento di Internet.

C) Il concorso omissivo

Pur dopo avere sostenuto che, in quanto si tratta di soggetto che obiettivamente fornisce un servizio, assai difficilmente l'ISP può concorrere mediante omissione nel reato commissivo dell'utente, è nondimeno indispensabile mettere in ordine i termini della questione.
Orbene, la struttura del reato commissivo mediante omissione è radicata sulla preesistenza di una posizione di garanzia ossia di un obbligo giuridico intestato a un garante, il quale è tenuto ad agire, al momento dell'originarsi del pericolo (situazione tipica), per evitare determinati eventi lesivi per soggetti terzi.
Laddove l'obbligo giuridico di cui sopra effettivamente sussista, il garante potrà rispondere penalmente dell'evento cagionato dalla propria omissione in forza della regola di equivalenza causale (art. 40 co. II c.p.).
Fermi tutti i qui condivisi rilievi in punto di adattabilità di siffatta regola a fattispecie diverse dai reati causali puri[50], tra i quali difficilmente possono comparire reati cibernetici, la configurazione della responsabilità del provider in forma di concorso omissivo con il terzo utente, richiederebbe, in primo luogo, un obbligo di impedire il reato di quest'ultimo (posizione di controllo).

---

[46] Invero, tra i cc.dd. reati cibernetici non sembrano ipotizzabili reati colposi.

[47] V. ad es. Cass., sez. IV^, 12 novembre 2008, n. 4107, C. e altro in *CED Cass. n. 242830*.

[48] Ma v. Corte Giustizia Ue, Grande sezione, 12 luglio 2011, L'Oreal SA e a.c/e Bay International AG e al., causa C – 324/2009, par. 120, reperibile all'indirizzo web *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62009CJ0324:IT:HTML*, che, trattando riflessi civilistici della responsabilità dell'ISP, lascia consistenti spiragli alla "conoscibilità" delle informazioni, reputando sufficiente, "affinché il prestatore di un servizio della società dell'informazione non possa fruire dell'esonero dalla responsabilità previsto all'art. 14 della direttiva 2000/31, che egli sia stato al corrente di fatti o di circostanze in base ai quali un operatore economico diligente avrebbe dovuto constatare l'illiceità di cui trattasi e agire in conformità del n. 1, lett. b), di detto art. 14 (dir. 2000/31/CE)".

[49] FIANDACA - MUSCO, *Diritto penale. Parte generale*, cit. pp. 469 s..

[50] FIANDACA, *Il reato commissivo mediante omissione*, Giuffrè, 1979, pp. 35 ss. che sottolinea la improponibilità della equivalenza causale rispetto a reati a fattispecie che prevedono connotati specifici dell'azione.

Il funzionamento del modello pur sempre esigerebbe, per non registrare un deficit di tipicità, che il reato in concorso sia un reato di evento (art. 40 co II c.p. "Non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo")[51]. Superato lo scoglio, il punto nodale resterebbe quello della individuazione di uno specifico obbligo che nel Diritto trovi comunque la sua fonte[52].

Il paradigma[53] delle posizioni di controllo sull'agire di terzi prevede l'incapacità di questi a governare il proprio comportamento, nonchè l'assoggettamento al potere di vigilanza del garante, il quale deve avere, dunque, un potere di signoria effettivo, tale da consentirgli l'impedimento dell'evento (reato).

Nell'ambito di interesse, occorrerebbe dunque, ricercare una fonte giuridica dell'obbligo; inoltre, verificare se non si tratti di obbligo generico, il cui adempimento si rende inesigibile.

Partendo da tale ultimo aspetto, non sembra possa ravvisarsi in capo al provider una posizione di controllo effettivo dell'operato altrui[54], anzitutto, perché si tratta di terzi (utenti), rispetto ai quali non v'è motivo per temere che non siano rispettosi delle leggi. E, poi, perché vi è una fattuale impossibilità di impedirne il reato: in primo luogo, non vi è la possibilità materiale di impedire un reato già compiuto, atteso che la situazione tipica (qui: il reato) coincide con la consumazione del reato, togliendo spazio d'azione all'ISP e, peraltro, escludendo anche la rilevanza causale della omissione; in secondo luogo, con un contributo impeditivo l'ISP può sottrarre le proprie strutture, ma nulla può fare rispetto a quelle di altri ISP di cui si sia contemporaneamente avvalso l'utente per realizzare il reato (si rifletta a messaggio diffamatorio veicolato attraverso numerosi siti web).

D'altronde, la automazione dei processi e l'immensa mole di dati rendono, con difficoltà crescente in base alle caratteristiche dell'ISP, ancor prima tecnicamente inesigibile un pervasivo monitoraggio delle informazioni, al di là del rischio di possibili violazioni di altri valori in conflitto con quello aggredito dal reato da evitare[55].

Sulla sostenibilità ed efficienza dell'introduzione di un siffatto obbligo residuano, allora, pochi dubbi. Rimane soltanto da segnalare il dato non indifferente costituito dalla dichiarazione di assenza di obblighi generali di sorveglianza per il provider, testualmente contenuta nell'art. 17 co. I D. Lvo n. 70/2003, la quale sembra sancire la inammissibilità di un modello di responsabilità concorsuale di tipo omissivo del provider, fondato su un obbligo generale di impedimento del reato dell'utente.

D'altra parte, la Giurisprudenza comunitaria[56], già ha rilevato la illegittimità comunitaria - per

---

51 IBIDEM, p. 181.

52 Sul problema della tipizzazione delle posizioni garanzia v. GIUNTA, *La posizione di garanzia nel contesto della fattispecie omissiva impropria*, in *Dir. pen. proc.*, 1999, p. 620 ss..

53 FIANDACA, *Il reato commissivo*, cit. p. 193

54 Del tipo di quella che vi è, ad es., per il tutore sull'operato dell'incapace di intendere e volere sotto la sua tutela.

55 Osservazioni di SPAGNOLETTI, *La responsabilità del provider*, cit. p. 1938.

56 Corte Giustizia UE, sez. III^, 24 novembre 2011, Scarlet Extended c. SABAM, cit, par. 39 – 41.
Degne di nota anche le argomentazioni proposte nella stessa causa nelle Conclusioni dell'Avvocato Generale Cruz Villalon, reperibili all'indirizzo web *http://csdle.lex.unict.it/Archive/LW/EU%20social%20law/EU%20case-law/Opinions/20130219-111050_Conc_C_426_11itpdf.pdf*, secondo il quale il fondamento normativo di una limitazione delle libertà fondamentali, garantite dalla Carta di Nizza anche agli utenti internet, deve possedere i requisiti di accessibilità , chiarezza e prevedibilità.

contrasto con l'art. 15 co. I Dir. 2000/31/CE - della previsione di obblighi di sorveglianza generale attiva, da parte dell'ISP, sui dati dei clienti, attraverso sistemi di filtraggio. Di più: la stessa Giurisprudenza ha mostrato d'esser sensibile rispetto alla esigenza di ottenere, al momento di porre singoli obblighi all'ISP, un giusto equilibrio tra interessi dello stesso prestatore, libertà degli utenti e ulteriori interessi per la cui tutela serve la introduzione dell'obbligo.
Marginalmente vanno spese alcune considerazioni rispetto ad obblighi "satellitari" che incombono sul provider. Esclusa la efficienza impeditiva di obblighi di segnalazione all'autorità amministrativa o giudiziaria (v. art. 17 co. II D. Lvo n. 70/2003) rispetto a reati già consumati, va verificato se possa discutersi di posizione di garanzia in riferimento all'obbligo introdotto dall'art. 14 quater L.n. 269/1998.
Si discorre, in particolare, del comma I, secondo il quale "14-quater. Utilizzo di strumenti tecnici per impedire l'accesso ai siti che diffondono materiale pedopornografico.
1. I fornitori di connettività alla rete INTERNET, al fine di impedire l'accesso ai siti segnalati dal Centro, sono obbligati ad utilizzare gli strumenti di filtraggio e le relative soluzioni tecnologiche conformi ai requisiti individuati con decreto del Ministro delle comunicazioni, di concerto con il Ministro per l'innovazione e le tecnologie e sentite le associazioni maggiormente rappresentative dei fornitori di connettività della rete INTERNET. Con il medesimo decreto viene altresì indicato il termine entro il quale i fornitori di connettività alla rete INTERNET devono dotarsi degli strumenti di filtraggio".
Può condividersi che la genesi dell'obbligo intervenga, per lo più, nel momento in cui il reato si è già realizzato[57]. Tuttavia residua la fattispecie di pubblicizzazione di materiale pedopornografico (art. 600 ter co. III c.p.p) che, invece, si realizza con l'essenziale contributo del provider. Ora, giacché nell'ipotesi descritta dall'art. 14 quater L. n. 269/1998 l'allerta circa il contenuto illecito di taluni siti proviene da un soggetto pubblico qualificato, potrà ritenersi che la condotta inottemperante sia assistita da dolo – che si faticherebbe a non definire - diretto, sicché non pare l'ISP possa essere esentato dall'esser responsabile in concorso del reato di pubblicizzazione di materiale pedopornografico.
Anche in tale evenienza, tuttavia, parrebbe scorretto configurare l'apporto reso dal provider come omissione, dovendo prevalere le considerazioni per cui, in primo luogo, vi è una condotta attiva oggettivamente riscontrabile e di disvalore assorbente, piuttosto che un suo surrogato normativo (omissione); in secondo luogo, il reato viene causalmente prodotto non dall'omesso filtraggio, bensì dalla prestazione di servizi internet senza dei quali esso non avrebbe potuto esser consumato.

7. Brevi considerazioni conclusive

Alla conclusione di questa certamente non esaustiva disamina dell'attuale regime della c.d. responsabilità penale del provider, vanno espresse poche e brevi considerazioni.
La prima concerne la stessa utilità di ulteriori approfondimenti della materia qui discussa: smentendo

[57] V. INGRASSIA *Il ruolo dell'ISP nel ciberspazio*, p. 33.

il Tribunale del celebre caso Google/Vividown[58], non può certamente dirsi che attorno ad essa si faccia "molto rumore per nulla". Anzi.

La relazione di adattamento tra le esigenze del diritto penale e le peculiarità di funzionamento di Internet e degli Internet service providers, più in dettaglio, incontra difficoltà; è fatta di stop e ripartenze, come suggerisce non solo la Giurisprudenza italiana ma finanche quella di ambito europeo.

Il terreno sul quale attualmente si gioca l'alternativa tra un diritto penale tendenzialmente autoritario anche in Internet ed uno invece minimo e moderno è, dunque, senza dubbio quello dei contenuti del dolo di concorso: la questione è indissolubilmente legata alla comprensione della funzione, dell'attività e dei poteri di un provider e dalla modalità con cui verrà risolta dipende non soltanto il rispetto di fondamentali precetti garantistici – su tutti: il principio di personalità della responsabilità penale -, bensì anche la salvaguardia di un ancor più ampio spettro di libertà fondamentali dell'individuo, che nella Rete trovano ormai il loro luogo privilegiato di espressione.

[58] Trib. Milano 12 aprile 2010, Drummond e altri cit..

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 119-127

Antiriciclaggio tecnologico e sicurezza dei dati trattati

Fulvio Berghella[1]

Abstact: La prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio di proventi illeciti e di finanziamento del terrorismo è un serio e forte impegno di tutti gli Stati componenti l'Unione europea. Gli obblighi prescritti dalle normative sono molti e complessi, essi richiedono il trattamento di una grande mole di dati e informazioni da effettuare con l'ausilio di sofisticate e dedicate procedure informatiche che devono coniugare i principi delle normative con le esigenze di analisi, sicurezza e segretezza. La soluzione italiana è all'avanguardia.

Parole chiave: antiriciclaggio, finanziamento del terrorismo, segnalazione di operazioni sospette, profilatura del rischio, Archivio Unico Informatico, adeguata verifica, GIANOS (Generatore Indici di ANomalia per Operazioni Sospette), UIF, Unione europea, Garante per la protezione dei dati personali.

1. Perché contrastare il riciclaggio

Prevenire e contrastare il riciclaggio dei proventi di attività illecite è una necessaria priorità della società civile, poiché la grande liquidità di cui dispone la criminalità organizzata genera un'economia illecita patologica che convive con l'economia sana e consente investimenti, scalate societarie, prestiti ad imprese, generazioni di posti di lavoro e conseguente consenso sociale. Il riciclaggio tiene in vita le attività criminali e le sviluppa, altera la distribuzione della ricchezza e costituisce una minaccia alla libertà dei mercati e all'assetto democratico degli Stati.

Per questi motivi i governi di molti Paesi hanno preteso la collaborazione attiva degli intermediari nel cercare le "tracce del denaro sporco", elementi che, nella società moderna, sono quasi sempre informatiche. Così, a decorrere dal 1991, per effetto di tre successive direttive dell'Unione europea e delle relative leggi che le hanno recepite[2], nonché dei regolamenti attuativi emanati

[1] Vice Direttore Generale Vicario di OASI SpA (Outsourcing Applicativo e Servizi Innovativi), Gruppo ICBPI (Istituto Centrale Banche Popolari Italiane).

[2] Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione e successive modificazioni e integrazioni.

Articolo pervenuto il 2 ottobre 2013, approvato il 28 novembre 2013

dalle istituzioni competenti, una serie di soggetti, tra cui banche, poste italiane altri intermediari e determinati professionisti, devono fornire spontaneamente informazioni (segnalazioni) ad organismi appositamente preposti (Unità di Informazione Finanziaria) sulle operazioni ritenute sospette, individuate sulla base dei canoni di esperienza e delle regole prescritte dalle normative primarie e secondarie.
Le prescrizioni sono basate sul principio di proporzionalità, secondo il quale i destinatari degli obblighi di controllo devono organizzare idonei presidi organizzativi e informatici proporzionati alla complessità, dimensioni, caratteristiche delle attività svolte, istituire apposite funzioni e formalizzarne i compiti e le responsabilità[3].

2. I pilastri della prevenzione e la collaborazione attiva

I fondamentali per la prevenzione antiriciclaggio sono: l'identificazione e l'adeguata verifica dei soggetti che compiono le operazioni; la registrazione, l'analisi e la conservazione delle operazioni svolte e dei documenti acquisiti (tracciabilità); la segnalazioni di operazioni sospette.
L'adeguata verifica, processo più ampio della semplice verifica dell'identità, deve garantire la piena conoscenza del cliente *[c.d. customer due diligence]*; quando si instaurano rapporti e quando si effettuano operazioni. Comporta il monitoraggio continuo del rapporto.
La tracciabilità delle transazioni finanziarie (registrazione e conservazione), deve consentire la ricerca e utilizzabilità dei dati in caso di indagini, le analisi dell'UIF e di altre Autorità, ed è fondamentale la registrazione tempestiva e codificata dell'operatività posta in essere. Al riguardo è costituito e tenuto un Archivio Unico Informatico da tenere a disposizione delle autorità e dal quale sono estratti mensilmente flussi di dati aggregati che, inviati all'UIF permettono di trarre molte utili indicazioni sull'andamento dell'economia patologica.
L'individuazione delle operazioni sospette (segnalazioni), da inoltrare all'UIF (Banca d'Italia) deve avvenire quando gli addetti alla valutazione sanno, sospettano o hanno motivi ragionevoli per sospettare, che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo.
Per avere un'idea della complessità dell'impianto si consideri che nel nostro Paese, mensilmente, sono poste in essere circa 30 milioni di operazioni di importo pari o superiore a € 15.000,00 e che le segnalazioni di operazioni sospette ricevute dall'UIF sono attestate sulle 60/70 mila l'anno. Inoltre, i dati e le informazioni da acquisire per espletare i controlli antiriciclaggio (che comprendono anche quelli di finanziamento del terrorismo) sono molti e riguardano non solo i tradizionali dati identificativi del cliente, ma anche il controllo di informazioni particolari quali, ad esempio: le evidenze (pregiudizievoli), i rapporti sequestrati o congelati le deleghe rilasciate, gli accessi a cassette di sicurezza, le società dove il cliente è titolare effettivo, l'utilizzo di banconote

[3] Banca d'Italia. Provvedimento recante disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo, ai sensi dell'art. 7 comma 2 del Decreto Legislativo 21 novembre 2007, n. 231. Roma, 10 marzo 2011.

taglio elevato, il reddito e il fatturato annuo, il patrimonio complessivo, la composizione del reddito o del patrimonio, il capitale sociale delle imprese, il risultato economico e le caratteristiche dell'azienda, i collegamenti e le relazioni, la forma giuridica, la cittadinanza, l'uso di valuta estera, le dichiarazione transfrontaliere, la natura e lo scopo del rapporto, le relazioni commerciali o d'affari con Paesi a rischio, il comportamento del cliente o dell'esecutore, le persone politicamente esposte, gli appartenenti a liste di terroristi, ecc. Tutte queste informazioni, unitamente ad altre, devono concorrere a definire il profilo di rischio di riciclaggio e di finanziamento del terrorismo attribuibile a ogni cliente, sulla base delle informazioni acquisite e delle analisi effettuate. In esito alla profilatura, ciascun cliente è incluso in una delle classi di rischio predefinite dai destinatari. A ciascuna classe di rischio è associato un coerente livello di profondità ed estensione degli adempimenti agli obblighi previsti dalla normativa di contrasto del riciclaggio e del finanziamento del terrorismo (adeguata verifica e valutazione delle operazioni sospette)[4].

3. GIANOS, il sistema informatico antiriciclaggio

Per coniugare tutte le molte e complesse esigenze, le banche italiane, le assicurazioni, le poste italiane e molti altri intermediari si sono dotati di una procedura informatica denominata GIANOS®, il primo applicativo antiriciclaggio realizzato in Italia[5]. La prima versione è stata ideata e progettata nel 1993 ed è operativa dal 1994. L'applicativo, nel tempo, è diventato uno standard nazionale. Realizzato in diverse specifiche versioni specializzate per i diversi intermediari, è oggi usato dalle banche italiane, dalla maggioranza dei gruppi assicurativi, da molte società di leasing, factoring, credito al consumo, società di monetica, mediocrediti, banche sammarinesi e da un'autorità estera[6]. Il programma GIANOS ha assunto, nel tempo, una multipla valenza, diventando contemporaneamente, sempre nell'ambito dell'utilizzo quale strumento di ausilio alla valutazione, un'articolata applicazione che consente di elaborare indici di anomalia per operazioni sospette, generare profili di rischio di riciclaggio, organizzare le informazioni per la conoscenza del cliente, controllare gli iter valutativi interni; ciò con una organizzazione logica in relazione all'approccio basato sul rischio e in coerenza alle prescrizioni normative. L'ultima edizione, è composta da un coordinato e interconnesso insieme di elementi applicativi (Moduli) rivolti alla generazione

---

[4] Banca d'Italia. Provvedimento recante disposizioni attuative in materia di adeguata verifica della clientela, ai sensi dell'art. 7, comma 2, del Decreto Legislativo 21 novembre 2007, n. 231. Roma, 3 aprile 2013

[5] L'idea di realizzare la procedura venne preventivamente sottoposta ad un gruppo di studio, principalmente composto da legali delle Associazioni bancarie e delle banche. Alle riunioni furono invitati anche osservatori della vigilanza. Il programma informatico realizzato fu denominato GIANOS, acronimo di **G**eneratore (o Gestione) **I**ndici di **AN**omalia per **O**perazioni **S**ospette e il marchio registrato. Dopo aver constatato l'esito positivo della fase di sperimentazione e collaudo sulle principali banche italiane e aver riscontrato anche l'uniformità di comportamento tra gli aderenti al progetto, venne sancito, con un comunicato dell'Associazione Bancaria Italiana, il termine delle sperimentazioni e l'inizio dell'utilizzo ufficiale dell'uso contemporaneo di GIANOS nelle banche che avevano volontariamente aderito al progetto e che lo avevano già installato. L'avvio fu preceduto da una vasta azione di sensibilizzazione, informazione, formazione e addestramento cui parteciparono, nei momenti più alti e significativi, anche importanti autorità della materia.

[6] Progettato, sviluppato e distribuito da OASI - Otsourcing Applicativo e Servizi Innovativi S.p.A., Azienda del Gruppo Istituto Centrale delle Banche Popolari Italiane.

e gestione di: operazioni inattese, derivate da elaborazioni degli indici di anomalia per operazioni sospette; profili di rischio di riciclaggio e di finanziamento del terrorismo; informazioni per la valutazione dei clienti, basata sul principio della conoscenza del cliente; operatività sotto-soglia, usura e frodi fiscali; monitoraggio continuo e segnalazioni di allarmi; generazione di statistiche anonime; controlli interni; invio segnalazioni operazioni sospette.

3.1 Modulo operazioni inattese per operazioni sospette

Svolge funzioni di ausilio all'obbligo di segnalazione evidenziando operazioni inattese. In coerenza con le Istruzioni di vigilanza è finalizzato a selezionare, attraverso regole basate su parametri quantitativi (importo, frequenza, ecc.) e qualitativi le operazioni inattese (anomale), alle quali dedicare maggiori approfondimenti per valutarne la loro sospettabilità di connessione con operazioni di riciclaggio e di finanziamento del terrorismo, nonché se correlate ad usura o frodi fiscali. Gli indicatori di anomalia trattati derivano sia dalle dalle Istruzioni operative per l'individuazione di operazioni sospette emanate della Banca d'Italia, sia dalle Comunicazioni UIF con schemi rappresentativi di comportamenti anomali, ed anche dalle significative esperienze e conoscenze degli esperti di settore. Sono trattati solo gli indicatori traducibili in indici numerici.

3.2 Modulo per la generazione dei profili di rischio

Per determinare il profilo di rischio di riciclaggio elabora le informazioni derivate da tre variabili fondamentali: le operazioni a maggior rischio, con una profondità storica predeterminata; la storia dell'operatività; i dati anagrafici e di relazione con la banca. Il programma per la generazione dei profili di rischio consente di: osservare il profilo di rischio di riciclaggio riferito ad un periodo specifico, controllarne l'evoluzione nel tempo; inserire una verifica normale o rafforzata; consultare l'elenco delle verifiche immesse; produrre la lista dei profili e per ognuno di essi accedere a funzioni di modifica o visualizzazione; verificare i parametri utilizzati per la profilatura; personalizzare i parametri di rischio di ciascun soggetto, modificando: gli intervalli dei punteggi assegnati ad ogni fascia; i punteggi associati al valore specificato di ogni dato; i punteggi associati alle condizioni definite. Il modulo è dotato di funzioni per le verifiche, dedicato alla gestione dei dati che caratterizzano la profilatura. Un'apposita applicazione consente di gestire la profilatura nei gruppi permettendo a ciascuna società di assumere, per uno stesso cliente, il profilo di rischio più elevato tra quelli assegnati da tutte le società del gruppo; oppure nel caso una società assegni un profilo di rischio più basso di quello assegnato dalle altre società del gruppo, di conservare per iscritto le ragioni di tale scelta.

3.3 Modulo per la conoscenza del cliente "know your customer"

Oltre a gestire tutte le componenti dei moduli per i comportamenti inattesi e la profilatura del rischio, consente la gestione della valutazione del cliente tramite una serie di funzioni dedicate

alla conoscenza del cliente *(Know your customer)*. Le funzioni si avvalgono sia delle risultanze degli applicativi dedicati alle operazioni sospette ed alla generazione dei profili di rischio, sia di ulteriori informazioni elaborate da altre liste esterne al programma. L'insieme delle informazioni è organizzata in modo da generare elenchi di consultazioni, tabelle di valutazione, ricerche storiche, schede per ciascun cliente, gestione di un questionario elettronico per la raccolta dei dati non disponibili, gestione dei dati afferenti ad altre liste (terrorismo, persone politicamente esposte, ecc.). È prevista, inoltre, l'interazione con un ulteriore modulo che esamina informazioni estratte da altri applicativi. Il modulo interagisce con tutte le altre sezioni dedicate alla generazione di anomalie e di profili di rischio, e permette la generazione di particolari messaggi di allarme. Consente il governo di ulteriori regole personalizzabili, anche basate sulle causali di registrazione dell'AUI. In applicazioni più avanzate è gestita la raccolta e della firma del cliente con strumenti grafometrici e l'archiviazione con sistemi di codici a barre.

3.4 Modulo per la valutazione dell'operatività sotto-soglia (schemi di usura) e frodi fiscali.

Acquisisce, attraverso flussi di alimentazione appositamente predisposti, diverse tipologie di informazioni organizzate in appositi archivi, anche al fine di determinare punteggi di rischio specifici per il fenomeno dell'usura, ad integrazione della profilatura del rischio di riciclaggio. Le informazioni registrate sono elaborate mediante regole che generano "evidenze" o "inattesi" di operazioni riconducili agli schemi di usura seguendo il modello predisposto dall'UIF. La gestione del modulo è parametrizzabile è consente diverse modalità d'uso che possono essere adottate in relazione alle specificità organizzative. Ulteriori parametri di estrazione sono dedicati alla selezione dell'operatività connessa alle frodi fiscali internazionali, nelle fatturazioni e all'IVA intracomunitaria in relazione agli schemi rappresentativi emanati dall'Unità di Informazione Finanziaria.

3.5 Modulo per il monitoraggio costante

Genera *alert* ed estrae anomalie seguendo regole e condizioni impostate ed introdotte dal singolo intermediario con appositi interventi di parametrizzazione. La connessione tra la frequenza temporale scelta e l'operatività da monitorare permette di finalizzare, con l'opportuna tempestività, l'evidenza di particolari comportamenti inattesi.

3.6 Modulo per la generazione di statistiche

Genera dati statistici quantitativi anonimi, finalizzati al monitoraggio periodico dell'efficacia e della validità degli algoritmi utilizzati. Il censimento periodico delle anomalie generate ha il solo

scopo di censire il numero di tutti i comportamenti inattesi, per valutare l'efficacia delle regole, esaminarne le necessità di aggiornamento, osservare le anomalie più ricorrenti e consentire alle singole banche un confronto andamentale e di posizionamento tra i propri dati e quelli medi generali.

3.7 Modulo per i controlli interni

È rivolto al controllo dei processi, delle procedure interne e delle attività svolte in materia dalle singole unità operative e dagli incaricati dell'esame di singole pratiche elettroniche generate da GIANOS. Integra i precedenti finalizzati ai controlli sulla clientela. Esso assume particolare rilievo e utilità anche in relazione ad alcune prescrizioni della normativa circa specifiche azioni, responsabilità ed obblighi di vigilanza per i soggetti che, a diverso titolo, interpretano i ruoli di Responsabile o Delegato Antiriciclaggio, Responsabile dell'Internal Audit, Responsabile della Compliance; o fanno parte del Collegio Sindacale, del Consiglio di Sorveglianza, del Comitato di Controllo di Gestione, dell'Organismo di vigilanza ai sensi del d.lgs. 8.6.2001 n. 231. Il modulo è progettato a supporto delle predette esigenze e si pone ad integrazione e completamento delle funzioni dedicate ai controlli sulla clientela. Il modulo esegue controlli sui dati, sulle pratiche informatiche e sulle elaborazioni generate da GIANOS-3D. Verifica i processi operativi per la gestione delle anomalie e delle fasi propedeutiche al processo di istruttoria della segnalazione, le modalità con cui sono gestiti i profili di rischio di riciclaggio e di finanziamento del terrorismo, le distribuzioni delle informazioni in relazione all'ubicazione, il trattamento del rischio paese e di determinati adempimenti quali la prevenzione al finanziamento delle armi di sterminio di massa; verifica la distribuzione territoriale dei clienti in relazione alle liste Mef, Gafi, Ocse, no White, Pep o che effettuano operazioni da e per determinati Paesi soggetti a restrizioni; la distribuzione dei clienti occasionali e non correlate alla residenza; l'estrazione di elenchi per settori e rami economici di appartenenza, importi; l'operatività con zone ad alto rischio di criminalità, le analisi in relazione al numero di conti e l'età, l'evidenza delle filiali che valutano fuori tempo le pratiche assegnate e quelle prive di valutazioni o con giudizi superficiali, nonché quelle in attesa, la concentrazione delle anomalie per filiali e zone, i cambiamenti del punteggio di rischio, le analisi su operatività riconducibile a schemi di usura e tanti altri.

3.8 Modulo per l'invio delle segnalazioni di operazioni sospette

Supporta la predisposizione e gestione dell'invio automatico delle segnalazioni di operazioni sospette all'Unità di Informazione Finanziaria. Il modulo *Facility Upload SOS*, nel compilare e gestire la segnalazione utilizza il maggior numero possibile di informazioni estraibili da tutto il sistema informativo e da GIANOS, sino alla generazione del file contenente il tracciato elettronico in formato XBRL per l'*upload* al sito della Banca d'Italia. Dopo l'invio della segnalazione, che viene

conservata in un dedicato archivio, una funzione aggiorna automaticamente, in GIANOS, lo stato della pratica.

4. Sicurezza e segretezza

La segnalazione di operazioni sospette ha lo scopo di portare a conoscenza della UIF le operazioni per le quali si sa, si sospetta o si hanno ragionevoli motivi per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo. Queste informazioni non sono acquisibili da chiunque, ma solo da soggetti esplicitamente autorizzati secondo le previsioni legislative. La sicurezza tutela l'intero ciclo di vita della segnalazione, del segnalato e del segnalante. Infatti, i soggetti obbligati alla segnalazione adottano, nei modi previsti all'art.45 del d.lgs 231/2007 (Tutela della riservatezza) adeguate misure per assicurare la massima riservatezza dell'identità delle persone che effettuano la segnalazione. Gli atti e i documenti in cui sono indicate le generalità di tali persone sono custoditi sotto la diretta responsabilità del titolare dell'attività o del legale rappresentante o del loro delegato.

Le informazioni da inviare all'UIF sono organizzate seguendo disposizioni standardizzate che ne consentono una più rapida trattabilità. Il modello segnaletico è basato su una piattaforma per la raccolta delle informazioni inviate telematicamente all'Unità di Informazione Finanziaria[7]. Per accedere al portale è necessario che la persona nel ruolo di referente od operatore del segnalante sia già registrata ed acquisito le credenziali di accesso. La comunicazione su rete Internet si avvale del protocollo https[8] ed utilizza certificati digitali emessi dalla "Certification Authority" della B.d'I. Per consentire un agevole accesso l'utente può installare sul proprio browser il certificato "root" della predetta autorità. In ragione del carattere di riservatezza delle informazioni trattate, l'accesso alla piattaforma è consentito solo ad utenti specificamente autorizzati. Il processo di autorizzazione prevede appositi passi esplicitamente indicati in un dedicato provvedimento della Banca d'Italia[9]. La tutela infine, è estesa anche allo scambio di informazioni e collaborazione tra Autorità e Forze di polizia. Tutte le informazioni in possesso della UIF, delle Autorità di vigilanza di settore, delle amministrazioni interessate, degli ordini professionali e degli altri organi deputati, sono coperte dal segreto d'ufficio anche nei confronti della pubblica amministrazione. Sono fatti salvi i casi di comunicazione espressamente previsti dalla legislazione[10].

Per quanto riguarda le funzioni di GIANOS l'architettura informatica è progettata in modo da poter essere utilizzate in relazione agli assetti organizzativi di ciascuna azienda in più modalità: nel loro insieme da un solo operatore, oppure separatamente da operatori diversi. L'applicazione può essere usata indifferentemente sia dalle aziende automatizzate in proprio, sia da quelle che hanno esternalizzato la gestione dei servizi informatici. L'accesso alla procedura avviene nel rispetto di adeguate misure di sicurezza specifiche, oltre all'integrazione con i sistemi di autorizzazione

7 (denominato INFOSTAT-UIF)

8 (connessione sicura)

9 Emanato il 4 maggio 2011.

10 (Art.9 d.lgs. 231/2007).

e di autenticazione adottati dai sistemi informativi dell'azienda in cui è installato. Appositi log consentono di ottenere le informazioni previste dalla disciplina sul tracciamento dei dati prescritta dal Garante per la protezione dei dati personali. L'utilizzo dei dati GIANOS, visto nell'ottica della sicurezza informatica, avviene seguendo contemporaneamente molti principi della riservatezza che in alcuni aspetti, tra i quali le informazioni sulle segnalazioni di operazioni sospette, avviene con regole di segretezza.

In ogni caso è necessario che i trattamenti antiriciclaggio siano sottoposti a preventiva analisi dei rischi di distruzione o perdita, anche accidentale, dei dati stessi (sicurezza fisica, logica e organizzativa), di accesso non autorizzato (da parte di persone prive di incarico scritto di trattare i dati) o di trattamento non consentito (se trattati in violazione di leggi e regolamenti) o non conforme alle finalità della raccolta (se usati per fini diversi da quelli previsti nella raccolta, indicati nell'informativa resa al cliente e indicati nel contratto tra le parti), al fine di stabilire quali siano le più idonee e preventive misure di sicurezza da porre in essere. In relazione alle prescrizioni di cui all'articolo 3, comma 2, della legge antiriciclaggio (d.lgs. 231/2007), ogni eventuale autonoma iniziativa, assunta sul piano applicativo dai soggetti destinatari degli obblighi, dovrebbe comunque svolgersi nel quadro delle prescrizioni e delle garanzie previste dalle disposizioni del Codice e della disciplina in materia di protezione dei dati personali. Ciò, in particolare, per quanto riguarda il previsto utilizzo di dati o di informazioni eventualmente già acquisiti che potrebbero essere ulteriormente utilizzati solo se raccolti per finalità compatibili con quelle del decreto antiriciclaggio (art. 11, comma 1, lett. b), del Codice per la protezione dei dati personali). Assume perciò rilievo il fatto che i dati siano esatti, aggiornati e non eccedenti rispetto a quelli strettamente necessari per le finalità antiriciclaggio, poiché quelli eccedenti non possono essere utilizzati. Pertanto, anche il trattamento dei dati necessari agli obblighi di adeguata verifica della clientela e quelli trattati per l'obbligo di registrazione deve avvenire in termini precisi e conformi alle normative, al fine di poter trattare solo dati pertinenti e non eccedenti rispetto alle finalità perseguite e con modalità proporzionate[11], sia per quanto riguarda l'identificazione del cliente o del "titolare effettivo", sia in relazione alla valutazione del "rischio" di riciclaggio e di finanziamento del terrorismo, nonché per quelli inerenti le registrazioni nell'Archivio Unico Informatico.

Queste previsioni sono alla base delle regole per i trattamenti e contenute già nell'art. 3 del Codice per la protezione dei dati personali (Principio di necessità) secondo il quale i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi. Il Garante, nella Deliberazione n. 53 del 25 ottobre 2007, nel precisare che l'identificazione della clientela rappresenta un obbligo posto in capo agli istituti di credito da diverse norme e, in particolare, da quelle in materia di riciclaggio, e che per tale trattamento, fatta salva l'osservanza dell'obbligo di informativa (fornita anche una tantum al cliente), non è necessario richiedere il consenso dal momento che i dati sono trattati in base a un obbligo di legge o, comunque, per eseguire obblighi derivanti dal contratto o per adempiere a specifiche richieste dell'interessato[12], ha però ribadito che il principio di pertinenza e non eccedenza dei dati deve essere osservato anche in relazione al trattamento di informazioni finalizzate a identificare i clienti

[11] (art. 11 del Codice per la protezione dei dati personali)

[12] (art. 24, comma 1, lett. a) e b), del Codice)

in occasione dell'instaurazione del rapporto contrattuale o in sede di esecuzione di operazioni bancarie. Nella stessa deliberazione, il Garante, precisa che i dati personali, sempre che siano pertinenti e non eccedenti, possono essere trattati solo per perseguire finalità legittime quali, ad esempio, quella di dare esecuzione al rapporto contrattuale o soddisfare obblighi derivanti dalla legge (principio di liceità, pertinenza, trasparenza), quindi il trattamento deve essere svolto: solo da parte di incaricati (nonché, se designati, dei responsabili) del trattamento e limitatamente alle istruzioni loro impartite; nel rispetto dei princìpi di necessità e di qualità dei dati, con riferimento all'esattezza e all'aggiornamento[13].

Le attività antiriciclaggio nell'insieme richiedono l'esame di grande quantità di dati personali e di informazioni sottoposte a singole o combinate operazioni di trattamento, quali: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione. Nella pratica tutte le operazioni previste all'articolo 4, comma 1 del d.lgs. 30 giugno 2003 n.196 (Codice per la protezione dei dati personali)[14].

[13] (artt. 3 e 11)

[14] I principali provvedimenti del Garante per la protezione dei dati personali che hanno impatto sulle attività antiriciclaggio sono:

- Il Provvedimento a carattere generale, del 10 settembre 2009, in G.U. n. 267 del 16 novembre 2009: "Misure relative alle comunicazioni fra intermediari finanziari appartenenti al medesimo gruppo in materia di antiriciclaggio", con il quale il Garante ha ritenuto che ricorrano gli estremi per dare attuazione al c.d. bilanciamento degli interessi disciplinato dall'art. 24, comma 1, lett. g), del Codice e, conseguentemente, che possano formare oggetto di comunicazione (e di conseguente trattamento nell'ambito delle esclusive finalità di contrasto al riciclaggio) i dati personali concernenti le segnalazioni previste dalla disciplina in materia di riciclaggio tra gli intermediari finanziari appartenenti al medesimo gruppo, senza che a tal fine sia quindi necessario acquisire il consenso degli interessati.
- Il Parere del Garante del 25 luglio 2007, in occasione della dovuta preventiva consultazione dell'autorità garante da parte del Mef, sui contenuti della bozza del d.lgs.231/2007: "Nuova disciplina antiriciclaggio";
- La Deliberazione del Garante n. 53 del 25 ottobre 2007: "Linee guida in materia di trattamento di dati personali della clientela in ambito bancario";
- Il Parere del Garante del 12 maggio 2005 circa gli " Obblighi Antiriciclaggio";
- La Newsletter del Garante n.188/2003 circa gli obblighi di acquisizione, conservazione, segnalazione, dei dati personali che sono trattati per finalità di antiriciclaggio.
- Le Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie - 12 maggio 2011, Pubblicato sulla Gazzetta Ufficiale n. 127 del 3 giugno 2011.
- Il provvedimento del Garante del 31 gennaio 2013 "Trattamento di dati biometrici.

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 128-145

Reati informatici e protezione dei dati personali

Luigi Montuori[1]

Abtract: Il presente contributo esamina la questione dei reati informatici, considerati dal peculiare angolo visuale della protezione dei dati personali, anche alla luce di recenti novelle legislative e interventi del Garante, evidenziando le norme e le tutele del Codice (d.lgs. n. 196/2003) di cui si possono giovare le vittime di reati informatici, nonché i rapporti tra l'apparato sanzionatorio amministrativo e quello penale all'interno del Codice privacy. Inoltre, si sofferma sui particolari profili della *data retention*, del trattamento illecito di dati (in particolare mediante lo *spamming*) e del nuovo istituto della "violazione di dati personali". L'Autore propone alcune riflessioni sul possibile impatto sull'attuale sistema giuridico e, più in concreto, sulle imprese, dell'estensione ai delitti del Codice del campo applicativo della responsabilità penale degli enti, come disposta dal recente decreto legge del 14 agosto 2013, ma non confermata in sede di conversione. Infine, si evidenziano i recenti sviluppi relativi alla necessità di assicurare il rigoroso rispetto dei principi di protezione dei dati personali e trasparenza nell'utilizzo dei nuovi strumenti quali le *app*.

Parole chiave: interessato – persona fisica – persona giuridica - dato personale – diritti fondamentali – informativa – consenso - bilanciamento - trattamento illecito – spamming - violazione di dati personali - responsabilità penale degli enti – provvedimento inibitorio e prescrittivo - sanzione amministrativa – sanzione penale - risarcimento del danno

[1] Il presente contributo rappresenta opinioni espresse dall'autore a titolo meramente personale, senza vincolare in alcun modo la pubblica amministrazione di appartenenza.

Articolo pervenuto il 2 ottobre 2013, approvato il 28 novembre 2013

1. Introduzione

La crescente diffusione di strumenti informatici, compresi quelli relativi alla tecnologia dell'informazione, ha comportato, oltre agli innumerevoli risvolti positivi, anche quello della crescita qualitativa e quantitativa dei reati informatici. L'utilizzo dell'informatica sia *hardware* che *software* per commettere crimini informatici ha fatto emergere la necessità di approntare misure di carattere preventivo e repressivo del fenomeno.

Il legislatore europeo a partire dal 1989[2] ha avviato un percorso di sistemazione delle varie tipologie di reati informatici, prevedendo nuove forme di intervento finalizzate a coprire le nuove tipologie di illecito che il progredire della tecnologia rendeva possibile realizzare.

Come si vedrà meglio *infra*, anche l'ordinamento italiano è intervenuto direttamente e indirettamente sulla materia. Basti pensare alle specifiche norme presenti nel Codice penale[3], alle previsioni contenute nel Codice in materia di protezione dei dati personali (di seguito Codice), relative all'obbligo di adottare misure di sicurezza "idonee e preventive" in relazione ai trattamenti svolti, dalla cui mancata o non idonea predisposizione possono derivare responsabilità anche di ordine penale e civile (artt. 15 e 169 del Codice), alla nuova normativa sulla "violazione di dati personali", i cd. *data breach*, introdotta dal decreto legislativo 28 maggio 2012, n. 69[4], in attuazione della normativa comunitaria[5], destinata a venire in rilievo, ad esempio, qualora il *data breach* venga causato dall'attacco di un *hacker* che effettui un accesso abusivo al sistema informatico di un'impresa[6], al recente decreto legge 14 agosto 2013, che innova la disciplina di fattispecie delicate e in continua evoluzione come la frode informatica e a istituti rilevanti quali quello della responsabilità "penale" degli enti che viene estesa anche ai delitti in materia di protezione di dati personali previsti dal Codice.

Non va tra l'altro dimenticata la rilevanza, anche per il nostro ordinamento giuridico, della Convenzione sulla Criminalità Informatica adottata a Budapest il 23 Novembre 2001, che rappresenta il primo strumento multilaterale creato per affrontare giuridicamente i problemi posti dall'espansione delle attività criminali compiute attraverso i computer networks.

---

[2] V. *Recommendation* No. R. (89)9 sulla criminalità informatica del 13 Settembre 1989 emanata dal Comitato Direttore per i Problemi Criminali (CDPC) del Consiglio d'Europa, che peraltro ha provveduto a definire una "lista minima", in cui sono state inserite le condotte criminose che gli stati europei dovevano perseguire per via penale: frode informatica, falso informatico, accesso non autorizzato a sistemi informatici, sabotaggio informatico, danneggiamento di dati e di programmi informatici, intercettazione di dati non autorizzata, riproduzione non autorizzata di programmi protetti, recepite dal legislatore italiano, con la legge n. 547 del 23 Dicembre 1993. Non si può poi trascurare l'adozione della Convenzione sulla Criminalità Informatica (*Convention on Cybercrime*, stipulata a Budapest, il 23 Novembre 2001, quale primo strumento multilaterale creato per affrontare giuridicamente i problemi posti dall'espansione delle attività criminali compiute attraverso i computer networks. Così al riguardo v. Spongano, *La nuova fattispecie giuridica del reato informatico: la legislazione Europea nella regolazione del Computer Crime,* in *www.filodiritto.com,* ins. Il 6 dicembre 2008.

[3] con la legge n. 547 del 23 dicembre 1993 l'Italia inserì all'interno del codice penale la frode informatica, il falso informatico, l'accesso non autorizzato a sistemi informatici, il sabotaggio informatico, il danneggiamento di dati e di programmi informatici, l'intercettazione di dati non autorizzata, la riproduzione non autorizzata di programmi protetti.

[4] pubblicato sulla *Gazzetta Ufficiale* 31 maggio 2012 n. 126.

[5] e in particolare delle direttive 2009/136/CE e 2009/140/CE in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche.

[6] Violazione che, come evidenziato dal considerando 61 della direttiva 2009/136/CE, qualora non venga trattata in modo adeguato e tempestivo, può provocare un grave danno economico e sociale.

2. I reati informatici e la protezione dei dati personali

Considerando comunque tale materia dall'angolo visuale della protezione dei dati personali, è opportuno evidenziare che questa diviene spesso utile all'attività di contrasto ai reati informatici**.** Basti pensare, solo per esemplificare, alle misure di sicurezza e agli altri adempimenti previsti in particolare dall'Allegato B al Codice i quali risultano spesso utili, e talora indispensabili, per prevenire reati, quali ad esempio quelli previsti all'art. 615 ter (l'accesso abusivo a sistema informatico o telematico), all'art. 635 bis (danneggiamento di informazioni, dati e programmi informatici), o all'art. 640 ter (la frode informatica).

In altri contesti, occorre invece operare un bilanciamento tra i vari diritti peraltro di rango costituzionale[7]. Ad esempio, i diritti di cronaca e di critica, cartacea ed *on line*, devono essere bilanciati con il diritto alla riservatezza, alla segretezza della corrispondenza e, più in generale, con il diritto alla protezione dei dati personali, che peraltro va ben al di là dell'originario "*right to be alone"* estrinsecandosi, perlomeno nell'ambito degli Stati membri dell'UE, in un vero e proprio potere di controllo, con il corrispondente sistema di diritti, dell'interessato sulla sfera di tutti i suoi dati personali, sulle modalità e finalità del loro trattamento, oltre che sull'eventuale circolazione dei medesimi, qualora siano oggetto di comunicazione o cessione.

Ciò, nella necessaria consapevolezza che lo sviluppo tecnologico e scientifico è da considerarsi sempre positivamente, ma che, al contempo, deve rispettare criteri e di regole riferiti alle loro modalità d'uso ed applicazione che evitino un loro utilizzo improprio ed effetti dannosi verso diritti e garanzie sanciti dal nostro ordinamento giuridico nazionale.

Tenendo però ben a mente, al contempo, che ciascun diritto fondamentale, incluso quello alla protezione dei dati personali, va salvaguardato nella sua essenza (nel suo "nucleo irriducibile"), ma, proprio perché sottoposto a necessario confronto con altri diritti fondamentali, non può essere difeso in via assoluta, dovendo accettare di subire il ragionevole pregiudizio imposto dall'esigenza di armonia dell'ordinamento giuridico[8]. In questo senso, occorre sempre tenere ben presente come il diritto è essenzialmente una scienza pratica che deve integrare con equilibrio il punto di vista teorico con quello effettuale.

Un interessante spunto di riflessione in materia è dato da uno studio del Parlamento Europeo su cybercrime, data protection e cloud (dicembre 2012) il quale, nell'analizzare in modo approfondito il tema di criminalità informatica e protezione dati, all'interno del dibattito legato alla revisione della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla "tutela delle persone fisiche con riguardo al trattamento dei dati personali", formula alcune raccomandazioni ed espone alcune valutazioni. Tra tali raccomandazioni, appare utile citare in questa sede l'analisi svolta in tema di giurisdizione e diritto applicabile e quella relativa ai criteri che disciplinano i trasferimenti di dati personali. Di estremo interesse risulta l'affermazione che la violazione di dati personali deve essere considerata quale possibile forma di *cybercrime*.

---

[7] Fatte salve le specifiche norme che la nostra Costituzione dedica a specifici diritti, i diritti fondamentali, intesi più in generale, quale categoria, come noto, possono tutti ricondursi nell'alveo dell'art. 2 Cost.

[8] Sulla necessità di bilanciamento fra diritti fondamentali nonché di garanzia del loro nucleo irriducibile, cfr., ex pluribus: Corte Cost. n. 86/1974;n.267/1998; n. 252/2001.

3. Il Codice tra sanzioni amministrative e sanzioni penali

Innanzitutto è bene ricordare quali sono le fattispecie penali presenti nel Codice:

- trattamento illecito dei dati (art. 167);
- falsità nelle dichiarazioni e notificazioni al Garante (art. 168);
- mancata adozione delle misure minime di sicurezza (art. 169);
- inosservanza di provvedimenti del Garante (art. 170);
- altre fattispecie (art. 171).

Il sistema sanzionatorio previsto dal Codice, a seguito delle modifiche apportate con il d.l. n. 207/2008 (convertito con la legge 41/2009), è caratterizzato da una situazione del tutto particolare dove le sanzioni penali si sovrappongono a quelle amministrative rimanendo del tutto indipendenti tra loro.

Mentre in altri settori dell'ordinamento le sanzioni penali sono utilizzate come una graduazione *in peius* per le violazioni più gravi, nel Codice per un medesima violazione vi possono essere contemporaneamente sanzioni sia amministrative sia penali.

Infatti la formulazione delle disposizioni sanzionatorie (artt. 162, comma 2-bis; 169; 170) specifica innanzitutto che la sanzione amministrativa è applicata anche nei casi in cui ricorre la violazione penale. Inoltre emerge la volontà del legislatore di affidare al Garante il compito di applicare la sanzione amministrativa (evitando in tal modo l'applicazione della sanzione amministrativa in sede penale ai sensi dell'art. 24 della legge 24 novembre 1981, n. 689). Ultimo elemento che caratterizza il sistema sanzionatorio previsto dal Codice è dato dal possibilità di applicare la sanzione amministrativa indipendentemente dal verificarsi delle condizioni necessarie per applicare quella penale.

Dalle Relazioni annuali dell'Autorità emergono alcuni aspetti degni di nota. Innanzitutto che a seguito delle istruttorie svolte o a seguito delle stesse ispezioni effettuate *in loco* dall'Autorità possono essere riscontrate violazioni di natura penale a seguito delle quali vengono inviate all'autorità giudiziaria informative di segnalazioni per violazioni penali. Le violazioni penali più frequentemente individuate riguardano l'omessa adozione delle misure minime di sicurezza (art. 169 del Codice), il trattamento illecito dei dati (art. 167), il mancato adempimento a una provvedimento inibitorio del Garante (art. 170) e la falsità nelle dichiarazioni (art. 168).

4. Il trattamento dei dati personali e la *data retention*

Proprio partendo dalla sopra citata Convenzione di Budapest, atto ratificato anche dal nostro Paese con la legge 18 marzo 2008, n. 48**,** va evidenziato che quest'atto interviene sul diritto penale sostanziale e processuale (mediante l'implementazione di alcune disposizioni del codice di procedura penale già esistenti con l'espresso riferimento all'ambito informatico e l'introduzione di disposizioni *ex novo*), interferendo sulla rilevanza penale di alcune condotte in ambito societario ma investendo anche aspetti inerenti la protezione dei dati personali, con particolare riguardo al trattamento dei dati di traffico telematico.

Consapevole di questo aspetto il Gruppo dei Garanti europei[9], con il parere n. 4/2001, è intervenuto sottolineando che, nel prevedere determinate misure, dovessero essere rispettati i principi di necessità, adeguatezza e proporzionalità. Ciò è stato in parte previsto nella Convenzione che impone agli Stati firmatari di assicurare obbligatoriamente il rispetto del "principio di proporzionalità'" (art. 15 della Convenzione). La Convenzione infatti non prevede la conservazione sistematica, da parte di fornitori di servizi di comunicazione elettronica, di dati relativi al traffico ma solo la conservazione temporanea di precisati dati informatici e tra questi i dati di traffico, qualora in possesso dei fornitori di servizi (c.d. "congelamento"), anche per finalità di collaborazione internazionale, quando ciò si riveli necessario per le competenti autorità e vi sia il timore che i tali dati possano essere cancellati o modificati (artt. 16 e 17 della Convenzione).

Nell'interpretare la Convenzione non bisogna dimenticare che questa è del 2001[10], periodo in cui non era prevista nella maggior parte dei Paesi la conservazione dei dati di traffico né era in lavorazione una specifica direttiva sul tema.

La previsione del cd. "congelamento" dei dati, che è intervenuta ancora una volta sul martoriato articolo 132 del Codice, oggetto nel tempo di numerose e non sempre coordinate modifiche, contempla una specifica ipotesi di temporanea conservazione dei dati relativi al traffico telematico a fini di svolgimento di investigazioni preventive o di accertamento e repressione di reati.

Questa modifica in vero trovava ragion d'essere in quel contesto e proprio nei Paesi ove non era prevista la conservazione dei dati di traffico con carattere sistematico o comunque questa era limitata per periodi di tempo molto circoscritti. In Italia, invece, si è assistito nel corso degli anni a uno stratificarsi di norme che, a seconda degli umori politici del periodo, tendevano a estendere o ad accorciare i termini obbligatori di conservazione degli stessi da parte dei fornitori.

Il Garante per la protezione dei dati personali (di seguito Garante) ha cercato di mettere chiarezza con il provvedimento generale del 17 gennaio 2008 ricordando la portata delle norme vigenti e prescritto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico, l'adozione di specifici accorgimenti e misure a garanzia dei dati di traffico conservati sia per finalità di accertamento e repressione di reati, sia per finalità ordinarie[11].

Successivamente con la ulteriore modifica all'art. 132 del Codice operata dall'art. 2 del decreto legislativo 30 maggio 2008, n. 109[12], è stato finalmente previsto un periodo di conservazione di 24 mesi per i dati di traffico telefonico, di 12 mesi per i dati di traffico telematico e di 30 giorni per i dati relativi alle chiamate senza risposta, senza distinzioni in base al tipo di reato[13].

---

[9] Il Gruppo è previsto dall'art. 29 della direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione. Il presidente è eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una volta.

[10] ratificata dal nostro Paese solo nel 2008.

[11] in G.U. 5 febbraio 2008 n. 30, nonché in www.garanteprivacy.it, doc. web n. 1482111;

[12] di recepimento della direttiva 2006/24/Ce del Parlamento europeo e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/Ce.

[13] Le conseguenti modifiche al citato provvedimento del 17 gennaio 2008 sono state apportate dal Garante con il provvedimento 24 luglio 2008 "Recepimento normativo in tema di dati di traffico telefonico e telematico" in G.U. n. 189 del 13 agosto 2008.

In tale contesto va ricordata l'attività posta in essere dal Garante a seguito di un ricorso con il quale un abbonato aveva lamentato l'indebita acquisizione di copia dei tabulati telefonici che lo riguardavano pervenuti allo stesso con lettera anonima. Al di là degli aspetti penali per i quali è intervenuta l'Autorità giudiziaria ordinaria, il Garante, verificata la fondatezza di quanto asserito ha prescritto con proprio provvedimento al fornitore l'adozione di nuove misure di sicurezza a protezione dei dati degli abbonati e degli utenti (provv. 1° giugno 2006 [doc. web n. 1296533).
A seguito di attività ispettive mirate, l'Autorità ha verificato che i sistemi informativi della società non erano in grado di registrare il dettaglio delle operazioni svolte dagli incaricati, esponendo perciò abbonati e utenti a seri rischi di utilizzazione illecita dei dati di traffico. In altre parole, è stata accertata la violazione dell'obbligo di adottare, in aggiunta alle ordinarie misure minime di sicurezza di cui all'allegato B al Codice, idonee misure utili a identificare tutti gli incaricati che accedono ai dati.
L'Autorità con un secondo provvedimento, sempre del 1° giugno 2006 [doc. web n. 1298716], ha poi prescritto alla stessa società di adottare, con riferimento all'intera utenza, misure tecniche a protezione dei dati contenuti nei tabulati in modo da rendere sicuro, trasparente e controllato l'accesso alle banche dati.
Si evincono chiaramente quali sono i poteri e le possibili modalità di intervento riconosciuti dal Codice all'Autorità. Infatti, al Garante spettano non solo i provvedimenti inibitori, la dichiarazione di illiceità dei trattamenti dei dati personali o l'attività sanzionatoria di carattere amministrativo, ma, in un'ottica costruttiva di effettiva attuazione della normativa in materia di protezione dei dati personali, anche l'attività di individuazione e di prescrizione delle misure di sicurezza tese a minimizzare i "rischi di distruzione o perdita, anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta". In tale contesto viene in rilievo il provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008[14] (così modificato in base al provvedimento del 25 giugno 2009).
Questo provvedimento ha sostanzialmente integrato il disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B del Codice e**,** nelle intenzioni dichiarate dalla stessa Autorità**,** mira a promuovere la consapevolezza della delicatezza del ruolo degli amministratori di sistema nella "Società dell'informazione" e dei rischi a esse associati in rapporto a sistemi di elaborazione e banche di dati, evidenziandone la rilevanza rispetto ai trattamenti di dati personali.
Da ultimo si cita anche il provvedimento dell'Autorità su "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" del 13 ottobre 2008 pubblicato in G.U. n. 287 del 9 dicembre 2008. Il provvedimento riguarda tutti quei soggetti che utilizzano strumenti informatici (persone giuridiche, pubbliche amministrazioni, altri enti e persone fisiche), prescrivendo la necessità di adottare idonei accorgimenti e misure volti a prevenire accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere dismesse.

[14] In G.U. n. 300 del 24 dicembre 2008.

5. Norme rilevanti del Codice sulla protezione dei dati personali

In materia di reati informatici, si può sottolineare che varie norme del Codice sulla protezione dei dati personali assumono rilevanza, sotto più profili, come ad esempio con riguardo ai soggetti "interessati" ai fini dell'applicazione e alle tutele azionabili presso il Garante oppure ai trattamenti illeciti di dati personali[15], o comunque riferibili agli artt. 168 e 169 del Codice, relativi a falsità nelle dichiarazioni e notificazioni al Garante e alla mancata adozione delle misure minime di sicurezza.
Negli ultimi anni, l'ambito soggettivo delle disposizioni del Codice e quello dei diritti azionabili dagli interessati ha subito rilevanti modifiche.
In particolare, va considerato che l'art. 40, secondo comma, del d.l. n. 201 del 6 dicembre 2011 (c.d. decreto "salva Italia")[16], ha modificato alcune disposizioni contenute nella parte prima del Codice recante le "Disposizioni generali", quali ad esempio l'art. 4 relativo, tra l'altro, alle nozioni di "interessato" e di "dato personale", in particolare eliminando ogni riferimento alle persone giuridiche o assimilate, ossia enti e associazioni e mantenendo il riferimento alle sole persone fisiche.
Successivamente, anche il d. lgs. 28 maggio 2012, n. 69[17] ha parzialmente modificato alcune disposizioni del capo 1 ("*Servizi di comunicazione elettronica*") del titolo X ("*Comunicazioni elettroniche*") Capo 1, del Codice, di diretta derivazione comunitaria[18] introducendo la qualifica di "contraente"- la quale riguarda certamente anche le persone giuridiche- in luogo di quella di "abbonato".
Gli articoli del Codice interessati dalle modifiche si riferiscono alle definizioni (art. 4), all'oggetto e all'ambito di applicazione (art. 5), alle modalità di esercizio dei diritti dell'interessato (art. 9) e ai trasferimenti dei dati verso paesi terzi (art. 43), norme che ora, a differenza del testo precedente, fanno riferimento alle sole persone fisiche.
A seguito delle suddette modifiche normative e delle conseguenti incertezze interpretative, il Garante per la protezione dei dati personali ha ritenuto opportuno intervenire con il provvedimento generale del 20 settembre 2012 (*doc. web.* n. 2094932), sull'applicabilità del Codice alle persone giuridiche, enti e associazioni[19], con il quale ha evidenziato che le norme contenute

---

[15] Art. 167 riguarda la violazione delle disposizioni su vari articoli e tra questi sul consenso (art. 23); violazione dei principi sul traffico di chiamate (art.123), sulle comunicazioni indesiderate (art.130); violazione dei principi sul trattamento dei dati sensibili (art.20) e giudiziari (art.21); violazione delle norme sulla divulgazione dei dati sanitari (art. 22, VIII co.) e sulla comunicazione e diffusione di dati sensibili e giudiziari ad altre persone o enti (art. 22, XI co.); violazione delle norme sulla comunicazione e diffusione vietate dal Garante o dall'autorità giudiziaria, o riguardanti dati di cui è stata ordinata la cancellazione, o conservati per un tempo necessario già trascorso, o attuate per finalità diverse da quelle dichiarate in notificazione; violazione delle norme sul trasferimento dei dati all'estero (art.45).

[16] convertito con legge del 22 dicembre 2011 n. 214.

[17] a seguito del recepimento della direttiva 2009/136/CE (in G.U. 31 maggio 2011, n. 126).

[18] poiché emanate in attuazione della direttiva 2002/58/CE.

[19] la direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla "tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" aveva lasciato un margine agli Stati membri rimettendo la facoltà di prevedere l'estensione della portata applicativa delle norme in anche alle persone giuridiche ovvero di limitarla esclusivamente ai trattamenti di dati delle sole persone fisiche. Come ha ricordato il Garante nel citato provvedimento del 22 settembre, il legislatore italiano sia nel 1996 sia nel

nel titolo X ("Comunicazioni elettroniche") del Codice, sono di diretta derivazione comunitaria[20] e che pertanto prevale l'obbligo di interpretazione conforme alla normativa comunitaria con la conseguente applicazione anche alle persone giuridiche delle sole disposizioni relative alle Comunicazioni elettroniche.

Come evidenziato dall'Autorità**,** nel titolo X del Codice non viene in rilievo la definizione di "interessato" bensì quella di "abbonato", ora "contraente", e pertanto sulla base d**e**i principi comunitari, tali norme si applicano ai contraenti sia persone fisiche sia persone giuridiche[21].

Il Garante, nel provvedimento citato, ha richiamato a sostegno anche l'art. 130 del Codice, rubricato "Comunicazioni indesiderate", che è stato oggetto di recenti modifiche apportate con il d.lgs. n. 69/2012. Tale articolo, che riguarda le comunicazioni promozionali effettuate con sistemi automatizzati di chiamata oppure per il tramite di strumenti di posta elettronica, telefax, sms o mms, grazie alla modifica, richiama ora la definizione di "contraente", superando la formulazione precedente che indicava l' "interessato" con l'evidente irragionevole conseguenza che tali previsioni risultavano applicabili soltanto ai trattamenti di dati personali delle persone fisiche.

Nonostante l'intervento del Garante che ha chiarito un punto essenziale del Codice, quello relativo ai soggetti cui viene garantita la tutela nella protezione dei dati personali nel settore delle comunicazioni elettroniche, le modifiche legislative intervenute hanno lasciato un'evidente lacuna**.** Infatti, l'art. 141 del Codice, che individua le forme di tutela dinanzi al Garante, non parla di contraenti consentendo quindi ai soli "interessati", persone fisiche, di poterli utilizzare generando una evidente contraddizione, evidenziata in diverse occasioni dall'Autorità, che vede nel titolo X del Codice una tutela piena in capo alle persone giuridiche, ivi compresa l'applicabilità delle sanzioni, sia amministrative sia penali[22], sfornita però dalla possibilità per le stesse di utilizzare dinanzi all'Autorità gli strumenti indicati dal medesimo decreto legislativo quali segnalazioni, reclami ed ricorsi[23].

Tale aspetto comporta vari problemi applicativi. Basti pensare ad esempio alla ricezione di spam via posta elettronica ove alcune volte può risultare difficile distinguere se il destinatario, segnalante, sia una persona fisica o giuridica. Si pensi al caso dei dipendenti che lavorano in una determinata società che ha fornito loro indirizzi di posta elettronica aziendale contenenti le loro generalità (ad esempio, nome.cognome@società.com), oltre al nome dell'impresa.

Qui occorre verificare se chi asserisce di aver subito un trattamento illecito di dati mediante spam

2003, diversamente dalla maggior parte degli altri Stati membri, aveva previsto tutele anche in favore delle persone giuridiche nella specifica qualifica di interessati;

[20] direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche integrato e modificato dal d. lgs. 28 maggio 2012, n. 69; con ulteriore, specifico riguardo al suo capo 1, che interessa i "Servizi di comunicazione elettronica".

[21] Il considerando 12 della direttiva 2002/58/CE, prevede che "gli abbonati ad un servizio di comunicazione elettronica accessibile al pubblico possono essere persone fisiche o persone giuridiche". In tal senso anche l'art. 1, comma 1, lett. a) del d. lgs. 1 agosto 2003, n. 259 (c.d. Codice delle comunicazioni elettroniche) riconosce la qualifica di contraente sia alla persona fisica sia a quella giuridica quando è parte di un contratto con il fornitore di servizi di comunicazione elettronica accessibili al pubblico, per la fornitura di tali servizi";

[22] Basti pensare, ad esempio, alle disposizioni di cui agli artt. 162, commi 2-bis e 2-quater, 162-bis e 167 del Codice.

[23] "Induce, allora, motivate perplessità il fatto che, a fronte di questa circostanza, sia comunque precluso alla persona giuridica oggetto di illeciti di rivolgersi all'Autorità invocandone la tutela amministrativa ai sensi del richiamato art. 141" citato provvedimento del 20 settembre 2012 (doc. web n. 2094932).

può utilizzare gli strumenti tipizzati dal Codice all'art. 141.
In proposito il recente testo delle "Linee guida in materia di attività promozionale e contrasto allo spam", adottate il 4 luglio 2013 e pubblicate sul sito istituzionale *www.garanteprivacy.it* [doc. web n. 2542348], in base al quale -in linea con quanto già precisato dal Gruppo Art. 29[24] tali indirizzi vanno considerati indirizzi "personali" di posta elettronica e i loro rispettivi assegnatari come "interessati", con la conseguente piena applicabilità del Codice e del relativo impianto di diritti e tutele.
Appare utile ricordare un'altra incongruenza, evidenziata anche questa dall'Autorità, data dal fatto che ad ordinamento vigente, l'art. 15 del Codice ("danni cagionati per effetto del trattamento") trova applicazione esclusivamente ai danni verificatisi "per effetto del trattamento di dati personali", quindi alle informazioni relative alle sole persone fisiche, restando così esclusi i "contraenti" persone giuridiche, che quindi non possono usufruire della previsione dell'inversione dell'onere della prova di cui all'art. 2050 c. c.
In concreto, pertanto, persone giuridiche, enti e associazioni, anche qualora siano vittime di reati informatici, anche nel caso in cui ricorrano i presupposti e i requisiti previsti dell'art. 167 del Codice per il reato di illecito trattamento dei dati (di cui diremo *infra* più nel dettaglio) - differentemente dalle persone fisiche- dal 6 dicembre 2011 non possono più presentare segnalazioni, reclami o ricorsi al Garante, né possono esercitare i diritti di cui agli art. 7 ss. del Codice, perché non rientrano nel concetto di "interessati".
Tuttavia, i detti soggetti, qualora ritengano di aver subito un reato informatico, si possono avvalere degli ordinari strumenti di tutela forniti dall'ordinamento, quindi, possono esperire presso l'autorità giudiziaria ordinaria rimedi civilistici quali, ad esempio, l'azione inibitoria e/o l'azione di risarcimento del danno, oppure, qualora ricorrano gli elementi dell'art. 167 del Codice o di altri reati informatici, sporgere denuncia e quindi sollecitare l'attivazione di un procedimento penale con le relative sanzioni.
Inoltre, persone giuridiche, enti e associazioni possono beneficiare dell'eventuale esercizio dei poteri di iniziativa *ex officio* -quanto a provvedimenti inibitori, prescrittivi e/o sanzionatori- da parte del Garante, qualora emergano i presupposti di un trattamento di dati personali non conforme al Codice, e in particolare ai principi di finalità, necessità e non eccedenza del trattamento dati di cui agli artt. 3 e 11 del Codice, o agli obblighi di idonea informativa sul trattamento dei dati personali ex art. 13 e di previa acquisizione di un consenso libero, specifico e documentato di cui all'art. 23 del medesimo, la cui violazione è prevista espressamente dall'art. 167 del Codice sulla protezione dei dati personali quale uno dei possibili presupposti necessari a integrare il reato.

6. Le tutele del Codice azionabili dalle persone fisiche vittime di reati informatici

Chiarito l'ambito soggettivo del Codice, possiamo soffermarci sulle tutele azionabili dalle persone fisiche, che abbiano subito o che comunque lamentano un trattamento dei propri dati personali non

[24] pareri n. 4/1997 e n. 5/2004.

conforme alla disciplina sulla protezione dei dati personali ovvero a causa di un reato informatico, in qualità di "interessati" ai sensi dell'art. 4 del Codice.
Ebbene, la persona fisica che ritiene di aver subito un trattamento illecito dei propri dati personali anche per mezzo di strumenti informatici può rivolgersi al Garante con gli strumenti previsti dall'art. 141 del Codice tramite una segnalazione, lo strumento più informale o mediante un reclamo, ossia esponendo in modo circostanziato la violazione della disciplina rilevante in materia di trattamento di dati personali che si asserisce o ancora mediante ricorso, se l'interessato intende far valere gli specifici diritti di cui all'articolo 7 del Codice secondo determinate modalità.
Il Garante, esercitando la propria discrezionalità amministrativa, nel ravvisare una possibile violazione del Codice, avvia un istruttoria preliminare, al termine della quale può archiviare la segnalazione o il reclamo[25] oppure adottare specifici provvedimenti anche di carattere inibitorio e/o prescrittivo, indicando in tal caso ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi degli articoli 143 e 154 del Codice.
L'Autorità come detto può comminare sanzioni amministrative ma non può riconoscere alcun risarcimento del danno agli interessati, neanche qualora ritenga che questi ultimi siano stati effettivamente vittime di un reato informatico, dato che questa competenza è riservata al giudice ordinario. In tal senso lo stesso art. 15 del Codice nel richiamare i danni cagionati per effetto del trattamento estende la risarcibilità del danno anche al danno non patrimoniale e offre all'interessato - danneggiato lo strumento, ai sensi dell'articolo 2050 del codice civile, dell'inversione dell'onere della prova, posto pertanto a carico del titolare del trattamento che deve provare di aver adottato tutte le misure idonee a evitare il danno.
Si deve osservare inoltre che il Garante, qualora ravvisi i presupposti di un reato e l'interessato non abbia già sporto querela, provvede a comunicare la notizia del possibile reato alla competente Procura della Repubblica[26].

7. Il reato di trattamento illecito di dati

Nell'ampio panorama dei reati informatici si distingue una fattispecie penale, che è espressamente disciplinata dal codice sulla protezione dei dati personali anziché dal codice penale, ove normalmente tali reati trovano la loro fonte normativa, e nella quale le sfere dell'informatica e della privacy possono pericolosamente intrecciarsi in più diverse occasioni di violazione degli obblighi del Codice: quella del trattamento illecito di dati ex art. 167.
In particolare, in base a tale norma, salvo che il fatto costituisca più grave reato, "chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di

[25] Art. 11 Regolamento n. 1/2007 Regolamento concernente le procedure interne all'Autorità aventi rilevanza esterna, finalizzate allo svolgimento dei compiti demandati al Garante per la protezione dei dati personali - 14 dicembre 2007 (G.U. n. 7 del 9 gennaio 2008)

[26] Art. 159, comma 6: "Quando emergono indizi di reato si osserva la disposizione di cui all'articolo 220 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271"

dati personali in violazione di quanto disposto dagli artt. 18, 19, 23, 123, 126 e 130 del Codice, ovvero in applicazione dell'art. 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi"[27]. Inoltre, sempre salvo che il fatto costituisca più grave reato, "chiunque, al fine di trame per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli artt. 17, 20 e 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni"[28].

Tale fattispecie costituisce un reato che, talora, a seconda delle concrete modalità di realizzazione (in particolare quando coinvolge sistemi di comunicazione elettronica**)**, assume carattere informatico, e può investire molteplici profili sanzionatori, atti ad assicurare un'adeguata tutela al diritto alla protezione dei dati personali.

È questo, ad esempio, il caso dello *spam* effettuato nei confronti di indirizzi di posta elettronica rastrellati in rete in maniera automatica via internet (su gruppi *Usenet*, newsgroups, forum, ecc.) mediante speciali programmi (*spambot*, ecc.) o da altre fonti accessibili al pubblico (albi, ordini professionali), o più semplicemente, facendo invii massivi a caso ad indirizzi mail basati sull'uso di nomi comuni, senza avere però alcun consenso degli interessati al trattamento dati o comunque senza averne lo specifico consenso per l'attività promozionale ai sensi dell'art. 23 del Codice.

Va sottolineato inoltre che sul fenomeno dello *spam* spesso si innesta con quello fraudolento, e quindi ancor più insidioso, rispetto all'esigenza di protezione dei dati dell'interessato nonché di tutela del consumatore, del c.d. *phishing* "ossia l'invio di e-mail contraffatte, con la grafica ed i loghi ufficiali di enti privati (in particolare banche e poste) ed istituzioni, che invitano il destinatario a fornire dati personali, motivando tale richiesta con ragioni di natura tecnica od economica, al fine di perseguire scopi illegali, quali, ad esempio, l'accesso alla password del conto corrente o della carta di credito e poter effettuare operazioni dispositive all'insaputa dell'interessato e pregiudizievoli della sua sfera giuridico-economica"[29].

Ciò precisato, a ben chiarire gli elementi costitutivi dell'art. 167 del Codice ha provveduto la Suprema Corte di Cassazione con la sentenza 24 marzo 2011, n. 18908[30], la quale ha sottolineato che è necessario che in capo all'autore del trattamento in violazione del Codice sia configurabile il dolo specifico in quanto egli deve aver voluto agire "al fine di trarne per sé o per altri profitto o di recare ad altri un danno".

Inoltre, secondo la Cassazione, il trattamento di dati personali senza il consenso dell'interessato non configura alcun reato se non ne deriva un nocumento per la persona offesa, poiché quest'ultimo costituisce "condizione intrinseca di punibilità" e non una mera circostanza aggravante, quindi tale illecito penale non è reato di pericolo presunto ma di pericolo concreto, in una concezione, dunque, più rispettosa del principio di "offensività" del diritto penale, per cui l'ordinamento può (*rectius*: deve) intervenire con la sanzione penale solo quando il bene giuridico risulta leso o

---

[27] V. comma 1 art. 167 Codice.

[28] V. comma 2, art. 167 cit.

[29] Cfr. Linee Guida del 4 luglio sopra citate, par. 2.3.

[30] Rispetto alla pronuncia in questione, cfr. utile commento di Di Tullio D'Elisisiis, *Il reato di trattamento illecito di dati personali*, in *www.filodiritto.com.*

perlomeno posto in una situazione di effettivo pericolo.
Peraltro, la Suprema Corte ritiene che il nocumento possa essere inteso come perdita patrimoniale (danno emergente), sia come mancato guadagno (lucro cessante) derivante dalla circolazione non autorizzata di dati personali" , e può non essere "esclusivamente riferibile a quello derivato alla persona fisica o giuridica cui si riferiscono i dati, ma anche a quello causato a soggetti terzi quale conseguenza dell'illecito trattamento", a patto che il danno in questione si concretizzi in un "vulnus" significativo alla persona offesa.
Con particolare riguardo allo *spam*, la Suprema Corte statuisce chiaramente che un siffatto trattamento assume rilevanza penale quando integri gli elementi costitutivi della fattispecie di trattamento illecito di dati prevista dall'art. 167, comma 1 del Codice[31].
In particolare, nella vicenda esaminata dalla citata sentenza n. 23798/2012, l'amministratore delegato e il responsabile del trattamento dei dati di una società**,** che aveva inviato massivamente newsletter promozionali indesiderate**,** sono stati condannati per il reato di cui all'art. 167, perché, in concorso tra loro, con più azioni ed in tempi diversi, al fine di trame un profitto (rappresentato dagli introiti commerciali e pubblicitari derivanti dall'uso, su internet, dei dati informatici i gestiti) avevano effettuato tali invii in violazione degli artt. 23, 129 e 130 del Codice. In sostanza, la società incriminata aveva stipulato un contratto di concessione di spazi pubblicitari con un'altra società, che aveva creato un sito al quale era abbinato un servizio di newsletter dirette alla lista di indirizzi di posta elettronica contenuti in un database composto da quasi cinquecentomila iscrizioni. A seguito della risoluzione unilaterale del contratto, la società in questione, senza consenso e senza informare gli iscritti della cessazione della lista, aveva continuato a recapitare agli stessi altre newsletter non richieste, pubblicizzando altresì i suoi servizi.
Numerosi provvedimenti del Garante per la protezione dei dati personali, già nelle more dell'adozione del Codice del 2003, intervenendo in materia di *spamming*, hanno chiarito che gli indirizzi di posta elettronica costituiscono dati personali e che l'eventuale ampia disponibilità e conoscibilità di fatto in rete o altrove non conferisce ai medesimi natura pubblica. In altri termini, essi non sono liberamente utilizzabili, in particolare attraverso l'invio di informazioni di qualunque genere (anche se non specificamente a carattere commerciale o promozionale), senza un preventivo consenso[32] oltre, chiaramente, a un'idonea informativa sul trattamento dati, incluse modalità e finalità dello stesso ai sensi del 13 del Codice.
Sono noti quanto evidenti i molteplici profili dannosi dello *spamming*, in tal caso meritevole dunque anche della sanzione penale oltre che di quella amministrativa di cui agli artt. 161 e 162 comma 2 bis del Codice, rispettivamente per l'omessa o inidonea informativa all'interessato e l'omessa acquisizione di un consenso con i requisiti di cui all'art. 23 del Codice.
Infatti, come chiaramente sottolineato dall'Autorità, "*l'utilizzo spesso massivo della posta elettronica comporta una lesione ingiustificata dei diritti dei destinatari, costretti ad impiegare diverso tempo per mantenere un collegamento e per ricevere, come pure per esaminare e selezionare, tra i diversi messaggi ricevuti, quelli attesi*

---

[31] Cassazione, sez. III pen., sent. 15 giugno 2012 n. 23798, come commentata, *ex pluribus*, da Tripodi, *La Cassazione alla prova dello spamming, tra presunzioni e torsioni.*, in *www.penalecontemporaneo.it.*

[32] Fra i vari si distinguono il provvedimento generale del 29 maggio 2003 "*Spamming. Regole per un corretto uso dei sistemi automatizzati e l'invio di comunicazioni elettroniche*" (doc. web. 29840) e le nuove Linee guida del 4 luglio 2013, sopra citate.

o ricevibili, nonché a sostenere i correlativi costi per il collegamento telefonico (incrementati anche da messaggi di dimensioni rilevanti che rallentano tali operazioni), oppure ad adottare "filtri", a verificare più attentamente la presenza di virus, o a cancellare rapidamente materiali inadatti a minori specie in ambito domestico."

In particolare, con il comunicato stampa del 3 settembre 2003 «Lo *spamming* a fini di profitto è reato»[33], l'Autorità ha ribadito che, nell'ipotesi in cui il trattamento senza consenso fosse realizzato al fine di trarne un profitto, in corrispondenza dunque con una delle finalità contemplate nella previgente fattispecie di trattamento illecito di dati personali di cui all'art. 35 legge n. 675/1996, il trasgressore sarebbe andato incontro alla sanzione penale ivi prevista, laddove invece, in assenza di tale specifica finalità, sarebbe stato passibile di una semplice sanzione amministrativa pecuniaria.

Occorre evidenziare che, in relazione ad un'altra modalità promozionale automatizzata, l'invio di fax, il Garante è recentemente intervenuto, con le Linee guida in materia di attività promozionale e contrasto allo spam del 4 luglio 2013, a fornire alcune indicazioni e precisazioni, in via generale e astratta, sul trattamento dati effettuato mediante invio di fax indesiderati mediante piattaforme di società estere che, in caso di violazione degli obblighi del Codice (e in particolare di quello del consenso dell'interessato), può talora essere considerato quale spamming e integrare il reato ex 167.

Sulla base di istruttorie anche complesse, l'Autorità ha rilevato che lo spam via fax che proviene dall'estero solitamente è inviato da società straniere che offrono questo servizio di invio a utenti italiani (imprese, società,..) e che, come per il caso sopra riferito, utilizzano due distinte reti: la rete Internet, per l'invio dei fax nella tratta compresa tra il f*ax server* sito all'estero ed il *fax gateway* sito in Italia, e la rete pubblica telefonica italiana per la trasmissione dei fax da parte del *fax gateway* nella tratta compresa tra lo stesso e il terminale dell'utente.

Al riguardo, come già chiarito con il provvedimento 7 aprile 2011[34], l'Autorità ha ribadito che a tale tipo di trattamento si applica la disciplina del Codice, dato che, ai sensi dell'art. 5, comma 2, lo stesso è applicabile a qualsiasi soggetto che *"…impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione Europea…"*.

Pertanto, secondo il Garante, occorre individuare, in relazione alla fattispecie in questione, il soggetto titolare del trattamento con i relativi obblighi e nei confronti del quale il giudice ordinario, ex officio o previa trasmissione degli atti da parte del Garante, potrà ravvisare l'integrazione del reato ex art. 167 del Codice.

Ebbene, come stabilito dall'Autorità, a seconda del caso concreto, e in particolare del ruolo svolto nella scelta dei destinatari delle comunicazioni, nonché delle modalità e delle finalità del trattamento, il titolare sarà individuabile nell'impresa, nella società, nel soggetto che comunque si avvalga di tali piattaforme proprie di soggetti terzi oppure nel proprietario delle piattaforme se quest'ultimo le utilizza per svolgere attività promozionale per sé stesso.

---

[33] In *www.garanteprivacy.it.*

[34] *Ibidem,* cfr. doc. *web* n. 1810207.

8. La violazione di dati personali: c.d. data breach

Sempre nell'ottica del rapporto fra reati informatici e protezione dei dati, val la pena rilevare che l'accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615 ter c.p., può talora essere il reato informatico-presupposto per la realizzazione della violazione di dati personali (o "data breach"), di notevole impatto sulla disciplina del Codice nonché sulle *policy privacy* di alcune categorie di imprese.

Al riguardo, va subito evidenziato che, recentemente, in particolare con il decreto legislativo 28 maggio 2012, n. 69 in attuazione del vigente diritto europeo, è stato ulteriormente innovato il Codice, con l'introduzione delle violazioni di sicurezza nel settore delle comunicazioni elettroniche e dell'obbligo per i fornitori di servizi di comunicazione elettronica di comunicare al Garante e, in determinati casi, al contraente o alle eventuali terze parti interessate, le "violazioni di dati personali" .

L'art. 32 del Codice "Obblighi relativi ai fornitori di servizi di comunicazione elettronica accessibili al pubblico", nella sua attuale formulazione, impone al fornitore di adottare, anche attraverso altri soggetti cui sia affidata l'erogazione del servizio, "misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi e per gli adempimenti di cui all'articolo 32-bis".

Pertanto i soggetti che operano sulle reti di comunicazione elettronica devono garantire non solo "che i dati personali siano accessibili soltanto al personale autorizzato per fini legalmente autorizzati" (cfr. art. 32 comma 1-bis), ma che le misure tecniche e organizzative, che il fornitore di comunicazione elettronica deve adottare, siano adeguate al rischio esistente e garantiscano la protezione dei dati archiviati o trasmessi da una serie di eventi espressamente indicati, quali anche l'accesso o la divulgazione non autorizzati o illeciti.

Si segnala che il Garante con diversi interventi[35] ha chiarito che le violazioni contemplate attualmente nel Codice riguardano i soli servizi di comunicazione elettronica accessibili al pubblico (quali ad esempio il servizio telefonico o quello di accesso a Internet) e riguardano esclusivamente i fornitori di tali servizi.

L'art. 32-bis del Codice disciplina gli "Adempimenti conseguenti ad una violazione di dati personali" qualunque ne sia la causa, non limitandola ai casi in cui essa derivi da un reato informatico, valendo anche ad esempio per l'adozione di misure inappropriate o se causate da errore umano, e stabilisce l'obbligo, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico, di comunicare senza indebiti ritardi al Garante la violazione di dati personali da essi detenuti[36].

I fornitori dovranno comunicare l'avvenuta violazione anche ai contraenti o ad altre persone

---

[35] Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) - 4 aprile 2013 (Pubblicato sulla Gazzetta Ufficiale n. 97 del 4 aprile 2013) e la precedente deliberazione recante "Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali" (Del. n. 221 del 26 luglio 2012, in G.U. n. 183 del 7 agosto 2012).

[36] Il Regolamento UE n. 611/2013 del 24 giugno 2013 ha disciplinato le misure applicabili alla notifica delle violazioni di dati personali a norma della direttiva 2002/58/CE del Parlamento europeo e del Consiglio relativa alla vita privata e alle comunicazioni elettroniche. Il regolamento è entrato in vigore il 25 agosto 2013 negli ordinamenti giuridici degli Stati membri UE naturalmente senza necessità di recepimento mediante atto normativo nazionale e contiene di fatto le medesime indicazioni già inserite dal Garante nel citato provvedimento del 4 aprile 2013.

interessate nei casi in cui dalla violazione possa derivare pregiudizio ai dati personali o alla riservatezza di questi (art. 32-bis, comma 2). Questa comunicazione non è dovuta se il fornitore ha dimostrato al Garante di aver utilizzato misure "che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate al momento della violazione" (art. 32-bis, comma 3).
Resta ferma la possibilità per l'Autorità, qualora vi siamo presumibili risvolti negativi delle violazioni, di obbligare il fornitore ad effettuare questa comunicazione, ove lo stesso non vi abbia già provveduto (comma 4).
Appare così evidente che il principio su cui si basa la disciplina di cui agli articoli 32 e 32-bis del Codice è il rapporto esistente tra evento dannoso e danno al contraente o ai terzi interessati.
Diviene così essenziale che i fornitori effettuino una preliminare individuazione dell'insieme dei dati personali trattati e dei rischi nei quali gli stessi possono incorrere.
Questa individuazione permette ai fornitori di organizzare le misure di sicurezza necessarie a prevenire le possibili violazioni ed a intervenire con tempestività qualora questi dovessero verificarsi.
È stato giustamente rilevato dallo stesso Garante nel provvedimento citato che si tratta di valutazioni simili a quelle che i fornitori erano tenuti ad compiere ai fini della redazione del Documento programmatico sulla sicurezza, in virtù di preciso obbligo *ex lege* poi soppresso[37].
Va evidenziato peraltro che il legislatore comunitario è consapevole del fatto che l'interesse degli utenti ad essere informati sulle violazioni di sicurezza che coinvolgono i loro dati personali non si limita al settore delle comunicazioni elettroniche. Ed infatti, proprio in questa ottica di tutela, lo schema di riforma della disciplina comunitaria in materia di protezione dei dati prevede un'estensione generalizzata dell'obbligo di notifica delle violazioni dei dati personali a tutti i titolari pubblici e privati.

9. L'estensione del campo applicativo del d.lgs. 231/2001 ai delitti del Codice mediante il recente decreto legge del 14 agosto 2013

La materia in questione ha tratto sviluppi inaspettati con il recente intervento del Governo mediante il decreto legge del 14 agosto 2013, "*Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province*"[38][1], e in particolare con il comma 2 dell'art. 9, che tuttavia in fase di conversione in legge da parte del Parlamento non è stato confermato, venendo soppresso.

---

[37] Il decreto-Legge "Disposizioni urgenti in materia di semplificazione e sviluppo" del 03/02/2012, n. 5 (pubblicato in Gazzetta Ufficiale n. 33 del 09/02/2012), abrogando la lettera g) del comma 1 dell'art. 34 del Codice, ha eliminato l'obbligo di predisporre e aggiornare il documento programmatico sulla sicurezza (DPS), nonché di riferire nella relazione accompagnatoria di bilancio in merito alla sua stesura.

[38] [1] pubblicato nella G.U. n.191 del 16 agosto 2013.

In particolare, il comma 2 dell'art. 9 del detto decreto modificava l'articolo 24-*bis* del decreto n.231/2000, estendendo la sanzione già prevista in capo all'ente (in particolare la sanzione pecuniaria da cento a cinquecento quote) anche ad altri reati, peraltro frequentemente ricorrenti nella vita quotidiana nonché nella prassi giudiziale, quali l'indebito utilizzo, falsificazione, alterazione e ricettazione di carte di credito o di pagamento[39][2], nonché ai delitti in materia di violazione della protezione dei dati personali previsti dal d.lgs. 196/2003**,** e cioè le fattispecie di trattamento illecito dei dati, che comprende quelle richiamate dall'art.167 di falsità nelle dichiarazioni o di notificazioni al Garante e di inosservanza dei provvedimenti del Garante.
Mediante questa innovazione, tali delitti, seppur per il breve periodo di tempo (compreso fra il 16 agosto e il 9 ottobre 2013) in cui la norma ha avuto efficacia, sono entrati a far parte del catalogo dei reati- presupposto della responsabilità delle società a norma del d.lgs. 231/2001.
Sulla tale norma occorre formulare alcune inevitabili riflessioni. In particolare, si può osservare che, se l'introduzione dei reati di frode informatica e di contraffazione di carte di credito non avrebbe comportato per le aziende importanti conseguenze sotto il profilo operativo, quella dei delitti in materia di protezione dei dati personali senz'altro avrebbe avuto grande impatto, soprattutto per la configurazione della responsabilità degli enti per l'illecito trattamento dei dati, trattandosi di una violazione potenzialmente in grado di interessare l'intera platea delle società commerciali soggette al decreto n. 231/00[40][4], e quindi anche per il connesso obbligo di adozione di modelli organizzativi finalizzati ed evitare la commissione dei reati presupposto della responsabilità dell'ente.
In assenza di tali modelli preventivi, o anche quando essi siano stati predisposti ma siano ritenuti dal giudice inadeguati rispetto allo scopo preventivo o anche rispetto alla complessità dell'impresa per la quale sono stati congegnati, la norma soppressa prevedeva che, qualora i vertici dell'impresa avessero commesso uno dei delitti previsti in materia di protezione dei dati personali, la medesima impresa sarebbe stata soggetta ad una sanzione da 100 a 500 quote, e quindi di importo potenzialmente rilevante dato che una quota singola può variare da un minimo di 258 fino a un massimo di 1.549 euro.
La possibile gravosità della novella per le imprese si comprende ancor meglio se si considera anche che, per i reati commessi dagli apicali, il decreto legislativo n. 231/2001 prevede una presunzione relativa di responsabilità dell'ente, con inevitabili dubbi di compatibilità con l'art. 27 Cost., che impone, in ambito penale, una presunzione di innocenza fino a prova contraria e con l'art. 24 Cost., relativamente al diritto alla difesa che siffatto tipo di responsabilità non pare ben garantire.
Comunque, a prescindere dai possibili profili di illegittimità costituzionale della norma (poi soppressa) che era possibile rilevare considerando la difficoltà ad armonizzare la stessa con i principi di tassatività e frammentarietà delle fattispecie penali, data l'assimilabilità di tale responsabilità "amministrativa" a quella penale, non può negarsi che l'eventuale impatto dell'estensione della legge 231 ai delitti del Codice sarebbe stato senza dubbio rilevante. Infatti, avrebbe costretto le società, che intendessero salvaguardarsi da siffatta responsabilità, ad un significativo sforzo, in termini di risorse umane ed economiche, di analisi dei processi interni e di adeguamento degli

---

39 [2] di cui all'art. 55 comma 9 d.lgs. 231/2007.

40 [4] Di questo avviso è la Suprema Corte di Cassazione, con la recente relazione III/01/2013 del 22/8/2013, tesa a fornire una prima interpretazione sulle novità apportate dal d.l. n. 93/2013: cfr. Iorio, *Privacy, responsabilità da 231*, in *Il Sole 24 Or*e, ins. 27 agosto 2013.

stessi[41][5]. E non può certo escludersi che qualche impresa, premurosa nel rispettare la legge, nelle more della conversione abbia già speso inutilmente risorse umane e materiali, proprio al fine di avviare un pronto adeguamento di sistemi e procedure interne all'obbligo di legge che ha poi perso efficacia.
Peraltro, non può non rilevarsi l'atteggiamento non del tutto coerente del legislatore che, da un lato, ha semplificato gli oneri aziendali, sopprimendo, come detto, anche l'obbligo del documento programmatico sulla sicurezza, che pur risultava senz'altro utile all'ideazione e gestione di una *privacy policy* conforme al Codice nonché al controllo e monitoraggio del trattamento dei dati personali e dall'altro, con la norma non confermata, ha deciso di imporre di fatto, per poi ripensarci e tornare sui propri passi, l'adozione di un modello organizzativo teso a prevenire la commissione dei delitti previsti dallo stesso Codice.

10. Attualità del tema privacy e computer crime e recenti sviluppi

In un mondo, dove è divenuto di fondamentale importanza che i cittadini ivi compresi gli utenti di servizi di telecomunicazione abbiano il controllo dei propri dati e quindi di poter decidere quali informazioni comunicare, con chi comunicarle e per quali finalità. L'irrompere di strumenti sempre nuovi quali le *app* rende necessario individuare corrette modalità di gestione delle misure di sicurezza a protezione dei dati personali.
Diviene così indispensabile che l'utente riceva, all'interno delle *app*, informazioni chiare e comprensibili sui dati raccolti, prima che abbia inizio la raccolta effettiva di tali dati.
Questo consente agli utenti di avere la possibilità di consentire o meno l'accesso a informazioni personali, quali l'ubicazione o gli indirizzi presenti in rubrica.
In tale contesto, nella recente Dichiarazione di Varsavia sulla "appificazione" della società[42] è stata rilevata l'importanza, nella messa a punto delle *app*, di dare esecuzione al principio di minimizzazione delle sorprese: niente elementi nascosti, nessuna raccolta di informazioni effettuata in modo occulto e non verificabile. Ne discende che gli sviluppatori di *app* devono garantire il rispetto dei principi sulla protezione dei dati esistenti nei vari Paesi del mondo e devono tenerne conto fin dalle fasi iniziali di messa a punto delle *app*, apportando tanche benefici e accrescendo la fiducia dell'utente. Nella Dichiarazione è evidenziato che gli sviluppatori devono inoltre stabilire con chiarezza quali informazioni siano necessarie per il funzionamento dell'*app*, e devono garantire che non siano raccolti dati personali ulteriori senza il consenso informato dell'utente anche quando

---

41 [5] Comunque, si può condividere, al contempo, quanto sostenuto da Ferrara, *Privacy e 231*, in *www.abirt.it*, 04/09/2013, secondo il quale l'effettivo impatto della recente riforma legislativa poteva ritenersi ridotto se si fosse applicata con adeguato rigore la vigente normativa del decreto 231/001 ("*se il Sistema 231 è un sistema di Gestione del rischio e di responsabilità delle aziende . . . ed è efficacemente implementato, dovrebbe coprire tutti gli aspetti impattanti, derivando da ciò il fatto che una preventiva corretta ed efficace analisi dei rischi analizza tutti gli item operativi e legislativi verificandone la copertura e le azioni messe in atto o da intraprendere per aumentare la compliance e le attua secondo principi ormai assodati e propri di sistemi consolidati come la ISO 27001 (PDCA- Plan, Do, Check, Act.*").

42 Conferenza Internazionale delle autorità di protezione dei dati tenutasi a Varsavia il 24 settembre 2013.

vengano utilizzati codici o *plug-in* forniti da terzi, ad esempio da reti di distribuzione pubblicitaria. Che il tema sia oggetto di studio e di interventi a livello internazionale è dato anche dal fatto che anche ENISA ha pubblicato uno studio relativo ai rischi posti dagli *smartphones* in termini di sicurezza, con riguardo in particolare alle applicazioni utilizzabili e scaricabili attraverso tali dispositivi[43]. Lo studio formula anche una serie di raccomandazioni rivolte agli utenti, evidenziando la necessità di maggiore sensibilizzazione e, d'altro canto, alcune funzionalità insite negli *smartphones* che consentono di per sé una migliore tutela dei dati personali (lettori *smart card*, funzioni di *backup* e *recovery*, possibilità di cifratura rafforzata, ecc.).

Un altro documento di ENISA[44] prende invece esame gli acquisti *online (online shopping*), passando in rassegna i principali rischi (dal *phishing* al furto di identità o allo *spam*) e formulando raccomandazioni rivolte sia agli utenti sia ai gestori di servizi di *shopping online*.

Fondamentale, anche in questo caso, la sensibilizzazione e la conoscenza dei propri diritti; ENISA menziona gli strumenti, ivi compresi quelli giuridici che già esistono a tutela degli utenti e dei consumatori e invita anche i gestori (di carte di credito e servizi *online*) ad un rigoroso rispetto dei principi di protezione dati e trasparenza. Ad analoghi risultati è pervenuta la FTC che ha pubblicato un Report con cui evidenzia le molte carenze in termini di trasparenza e sicurezza delle *app* rivolte a minori rese disponibili sul mercato della telefonia mobile (in particolare da Apple e Google, ma non solo) per quanto riguarda la raccolta e la circolazione di dati personali[45].

---

[43] Smartphone security: Information security risks, opportunities and recommendations for users http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport

[44] How to shop safely online http://www.enisa.europa.eu/publications/archive/how-to-shop-safely-online/at_download/fullReport

[45] La sintesi del Report è rinvenibile in rete: http://www.ftc.gov/opa/2012/02/mobileapps_kids.shtm;
Nel settore delle app è di estremo interesse anche il documento di Enisa, utilizzato anche dal WP29 per il parere sul medesimo tema: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/appstore-security-5-lines-of-defence-against-malware/at_download/fullReport

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 146-157

Il reato informatico nella prassi giudiziaria: le linee guida internazionali per il contrasto ai nuovi fenomeni criminali.

Eugenio Albamonte

Abstract: Una delle principali caratteristiche della criminalità informatica è la sua dimensione transnazionale. Ciò impone che, per un adeguato contrasto, gli Stati si dotino di uno strumentario di diritto penale sostanziale e processuale che, oltre ad essere adeguato alla qualificazione giuridica delle condotte ed allo svolgimento efficace delle indagini, sia il più possibile uniforme. Infatti l'omogenietà delle norme è il primo fondamento di una proficua cooperazione giudiziaria tra gli Stati. Ma oltre ad una disciplina normativa comune è necessario che si addivenga ad una interpretazione quanto più condivisa delle norme, soprattutto quando l'operazione dell'interprete consiste nel dare una qualificazione giuridica a condotte criminali sempre mutevoli e connotate da una elevata tecnicità. Questo è l'ambito in cui opera il Cybercrime Convention Committee (T-CY) istituito dalla Convenzione di Budapest presso il Consiglio d'Europa, dal quale pervengono linee guida particolarmente utili a chi, nel nostro Paese, è impegnato nello studio delle nuove forme di criminalità informatica.

Parole chiave: phishing, bombing, botnet, DoS e DDoS attack, Convenzione di Budapest, interpretazione delle norme incriminatrici, linee guida internazionali, criminalità informatica transnazionale, strumenti di cooperazione giudiziaria internazionale.

1. Premessa.

La Convenzione di Budapest per il contrasto al Cybercrime[1] ha adottato una tecnica di tipizzazione delle fattispecie incriminatrici che non riproduce pedissequamente i fenomeni criminali, riscontrati

[1] La Convenzione sul *Cyber Crime*, firmata a Budapest il 23 novembre 2001 ed entrata in vigore l'1 luglio 2004, è stata ratificata dall'Italia con la legge 18 marzo 2008 n. 48 (GU n.80 del 4-4-2008 - Suppl. Ordinario n. 79) *entrata in vigore il 5-4-2008*.

Articolo pervenuto il 10 ottobre 2013, approvato il 30 dicembre 2013

nella prassi giudiziaria ed investigativa delle attività di contrasto ma individua, secondo una tecnica di tipizzazione radicata nell'esperienza della codicistica italiana, una serie di fattispecie penalmente illecite caratterizzate dalle modalità della condotta, finalità perseguite ed evento realizzato. Di modo che, nella Convenzione e nelle norme che le hanno dato recepimento nell'ambito degli ordinamenti nazionali, non troveremo riscontro esplicito e diretto alle modalità specifiche attraverso le quali la criminalità concretamente opera: non troveremo cioè riferimenti a prassi criminali molto frequenti nell'esperienza quotidiana quali il phishing, il bombing, i botnet, lo spamming, in quanto si è ritenuto preferibile focalizzare l'attenzione sulle condotte criminali piuttosto che sulla tecnologia da questi utilizzata.

La scelta assunta dai compilatori della Convenzione ha l'innegabile pregio di fornire strumenti sanzionatori che, non essendo finalizzati a fotografare e qualificare giuridicamente le mutevoli fenomenologie dell'illecito cibernetico, non sono condannati a cadere in desuetudine e divenire inutilizzabili quando le tecniche di commissione degli illeciti dovessero mutare ed evolversi. Offrono, quindi, strumenti di qualificazione giuridica sempre attuali. Al contempo, la tecnica di normazione prescelta, presenta il difetto di non consentire l'immediata riconduzione ad una unica fattispecie incriminatrice delle condotte illecite rilevate nella prassi. L'interprete dovrà esercitare impegno e pazienza nella ricerca e nell'individuazione della fattispecie astratta che meglio si attaglia a qualificare giuridicamente le condotte illecite accertate; ponendo sempre attenzione alla circostanza che quasi mai una sola fattispecie incriminatrice è idonea ad assumere in se l'intero disvalore della condotta che, nella maggior parte dei casi sarà, invece, sussumibile sotto due o più fattispecie astratte al fine di ricomprenderne tutti gli elementi costitutivi, secondo le regole del concorso formale di reati o del reato continuato.

Se da un lato l'operazione interpretativa finalizzata a qualificare giuridicamente le condotte criminali appare complessa e produttiva di risultati non sempre omogenei, l'esigenza sottesa alla Convenzione di Budapest è certamente quella di rendere omogenei i sistemi sanzionatori nazionali, al fine di facilitare la cooperazione giudiziaria, volta al contrasto di fenomeni criminali che presentano una eminente connotazione trans-nazionale. In questo ambito uno dei principi cardine della collaborazione internazionale è quello della *reciprocità*, ovvero il presupposto della comune qualificazione penale della condotta criminale da perseguire. Diventa quindi di centrale importanza che, non solo tutti i Paesi aderenti si dotino di un omogeneo sistema sanzionatorio ma che siano anche omogenei i canoni interpretativi che consentono di qualificare illecitamente le diverse condotte complesse nelle quali si estrinsecano le prassi criminali più ricorrenti.

Propri alla standardizzazione dei canoni interpretativi tendono le linee guida adottate periodicamente dal Cybercrime Convention Committee (T-CY) istituito presso il Consiglio d'Europa in virtù dell'art. 46 della Convenzione e finalizzato a darle attuazione, ad arricchirne e potenziarne i contenuti, a favorire lo scambio di informazioni e di esperienze attuative tra gli Stati aderenti. In particolare le linee guida costituiscono l'espressione del comune intendimenti delle parti del trattato circa le modalità concrete di darvi attuazione, superando, attraverso una condivisa interpretazione delle sue norme (e delle norme di recepimento dei singoli stati) le ricadute negative che potrebbero verificarsi, sul piano della cooperazione giudiziaria, per effetto della differente interpretazione di ciò che sia o meno qualificabile come reato in base alla convenzione.

Sul piano del diritto nazionale le linee guida, pur non assumendo alcun valore normativo e tanto meno vincolante per l'interprete, offrono un valido strumento di ausilio nell'attività di

interpretazione delle norme e di qualificazione giuridica dei fatti di reato, che presenta il pregio dell'uniformità ed il prestigio culturale proveniente, oltre che dall'elevata qualificazione tecnico giuridica della sua fonte, anche dall'attenzione e dalla completezza con le quali sono redatte.
Le principali linee guida adottate e diffuse sino ad ora riguardano: il furto d'identità ed il phishing, i DDoS attacks, le botnet e i malwere.
Altro tema di specifico approfondimento da parte del T-CY è quello dell'accesso trans frontalieri ai dati contenuti in computers e sistemi informatici; si tratta di un argomento di centrale importanza nella definizione delle prassi investigative e giudiziarie, che coinvolge direttamente l'impiego degli strumenti di cooperazione giudiziaria internazionale e riverbera i sui effetti sul regime di utilizzabilità delle prove in dibattimento. Anche a tale argomento è dedicata una linea guida di recente adozione.

2.Furto di identità e phishing[2].

Il furto d'identità consiste in una condotta illecita che consente di ottenere ed usare, in modo fraudolento, senza il consenso del titolare ed a sua insaputa, dati e informazioni correlate all'identità personale della vittima. Nell'accezione più ampia del termine, il furto d'identità comprende sia l'acquisizione e l'uso di dati ed informazioni reali sia la creazione di dati e informazioni false pertinenti ad una persona non realmente esistente.
Questo tipo di informazioni quali ad esempio il nome, la data anagrafica, l'indirizzo ma anche credenziali di accesso che identificano l'utente presso computers o sistemi informatici e telematici (username, password ed altri codici di accesso) possono essere utilizzate per il compimento di un'ampia gamma di reati tra i quali molto frequenti sono le truffe operate ottenendo beni o servizi in nome di un'altra persona che ne è del tutto all'oscuro.
Si possono distingue concettualmente tre differenti condotte con ricadono nell'ambito di questa pratica criminale:

1) l'acquisizione di informazioni pertinenti l'identità altrui, ad esempio attraverso il materiale illecito impossessamento di atti o documenti che contengono tali dati, tramite l'accesso illecito a banche dati pubbliche o private o a computers di uso personale o attraverso il phishing;
2) la detenzione di tali dati e informazioni e la cessione a terzi;
3) l'uso dei dati identificativi al fine di assumere una differente identità e commettere reati (aprire conti correnti bancari, acquistare servizi o beni, intestare fittiziamente utenze telefoniche mobili ecc.)

Non tutti i sistemi giudiziari sanzionano penalmente tale condotta. Ad esempio il nostro codice penale sanziona l'utilizzo di tali dati quando viene effettuato per creare una falsa identità, sia essa realmente esistente o di fantasia; tale condotta integra il delitto di sostituzione di persona sanzionato dall'art. 494 c.p.. Quanto all'acquisizione di tali dati ed informazioni, tale condotta

[2] Linea guida T-CY (2013) 8 adottata con delibera del 9 th Plenary Meeting del 5 giugno 2013 pubblicata sul sito internet del Consiglio d'Europa (http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)8REV_GN4_id%20theft_V10adopted.pdf)

può essere sanzionata soltanto se effettuata attraverso modalità di per se illecite, ad esempio attraverso l'impossessamento di documenti d'identità o certificazioni altrui (nelle forme del furto, dell'appropriazione indebita, della sottrazione di corrispondenza ecc), ovvero tramite l'accesso abusivo a sistemi informatici o telematici protetti.

Anche la Convenzione di Budapest ha omesso di creare una fattispecie ad hoc, idonea a tipizzare la condotta in esame secondo le componenti costitutive attraverso le quali si manifesta nella pratica criminale, ancorché il furto d'identità è quasi sempre prodromico e strumentale alla commissione di altri gravi reati tra i quali, il più ricorrente è la frode informatica ovvero la truffa commessa attraverso sistemi informatici o telematici.

Anche se il furto di identità non è tipizzato quale condotta illecita, secondo le linee guida del T-CY, le relative condotte sono ugualmente perseguibili in tutti gli Stati aderenti. Vengono in primo luogo in considerazione le norme che sanzionano l'accesso abusivo e l'intercettazione abusiva di comunicazioni (ipotesi previste rispettivamente dagli artt. 2 e 3 della Convenzione e gli artt. 615 ter e 617 quater del codice penale), quando i dati vengano carpiti attraverso accesi illegali a computers o data base attuati mediante virus, phishing, volazione di protezione, keylogger ovvero attraverso l'intercettazione illegale di comunicazioni telematiche provenienti da sistemi che contengono dati personali. Alcune condotte materiali di acquisizione illecita di dati identificativi possono poi comportare il danneggiamento o la cancellazione di dati presenti nel computer, ovvero il danneggiamento di banche dati o sistemi, come sovente avviene in occasione dell'inoculamento di virus al fine di ottenere informazioni contenute in computers o banche dati (artt. 4 e 5 della Convenzione e gli artt. 635 bis e 635 ter e quater del codice penale). Le norme indicate appaiono particolarmente adatte a qualificare penalmente le condotte finalizzate all'acquisizione delle informazioni e dei dati relativi all'identità personale.

La detenzione ed il traffico dei dati identificativi cade, invece sotto la sanzione di norme che incriminano la detenzione, commercializzazione, cessione di programmi informatici destinati principalmente alla commissione di reati ovvero di password, codici di accesso o altri analoghi mezzi che consentano di superare le procedure di sicurezza di computers e sistemi. Queste condotte sono qualificate dall'art. 6 della Convenzione e, nel codice penale italiano, dagli artt. 615 quater e 615 quinquies. Bisogna tuttavia evidenziare che tanto in ambito internazionale quanto nel nostro ordinamento le condotte illecite di detenzione non riguardano qualsiasi dato identificativo ma soltanto quelli che (come username e password) identificano l'utente rispetto ad un computer o ad un sistema per consentirne l'accesso.

Quanto all'utilizzo dei dati identificativi della persona, vengono evidenziate le norme che tipizzano la frode informatica (art. 8 della Convenzione e art. 640 ter del codice penale italiano) quando questa si realizza attraverso l'utilizzo di una falsa identità per trarre in errore altri utenti del web ovvero per interferire nel funzionamento di computers e sistemi al fine di ottenere un profitto economico realizzato mediante l'acquisizione di denaro o l'intestazione indebita di mezzi di pagamento (ad es. carte di credito) o di linee di credito, ovvero per ottenere beni o servizi.

All'esito della disamina delle fattispecie applicabili alle condotte di furto d'identità e phishing appare opportuno precisare che, tanto il sistema penale nazionale quanto il trattato in esame non attribuiscono rilievo criminale alla condotta di chi detenga o ceda a terzi, anche in numero consistente, dati identificativi delle persone diversi da user name, password e codici di accesso, per i quali si applica, appunto, l'art. 615 quater c.p.. Tuttavia tale condotta, a prescindere dalle modalità

di acquisizione dei dati, può trovare sanzione nell'art. 167 cod. privacy[3] e nelle fonti di omogeneo oggetto presenti nelle legislazioni nazionali.

3.Botnets[4]. Una botnet è una rete formata da dispositivi informatici collegati ad Internet e infettati da virus (malware), controllata da un'unica entità, il *botmaster*. A causa di falle nella sicurezza o per mancanza di attenzione da parte dell'utente e dell'amministratore di sistema, i dispositivi vengono infettati da virus informatici o trojan i quali consentono ai loro creatori di controllare il sistema da remoto. I controllori della botnet possono in questo modo sfruttare i sistemi compromessi per scagliare attacchi del tipo distributed denial of service (DDoS) contro qualsiasi altro sistema in rete oppure compiere altre operazioni illecite, in taluni casi agendo persino su commissione di organizzazioni criminali. I dispositivi che compongono la botnet sono chiamati bot (da roBOT) o zombie.

I malware creati per far parte di una botnet, non appena assunto il controllo del sistema, forniscono al proprio autore i dati relativi al sistema infettato. Per fare ciò spesso sfruttano i canali IRC (Internet Relay Chat). Tramite il canale di chat l'autore è in grado di controllare contemporaneamente tutti i sistemi infetti collegati al canale (i quali possono essere anche decine di migliaia) e di impartire ordini a questi. Per fare un esempio, con un solo comando potrebbe far partire un attacco DDoS verso un sistema a sua scelta.

Un altro sistema utilizzato dai botmaster per controllare i bot sono le reti peer-to-peer (tra queste è compresa la rete di skype). In questo caso la rete p2p viene usata come veicolo per le informazioni che il botmaster invia ai bot.

Le botnet vengono spesso utilizzate anche per altri scopi: questi virus sono spesso programmati in modo da spiare il sistema infetto e intercettare password ed altre informazioni utili. Possono anche offrire accesso alle macchine infette tramite backdoor oppure servizi proxy che garantiscono l'anonimato in rete.

Le botnet sono diventate ultimamente fonte di interesse per la criminalità organizzata. Sono infatti un sistema per guadagnare soldi in modo illegale. I botmaster vendono i servizi della botnet a clienti che vogliono compiere azioni illegali ma non ne hanno i mezzi. Tra le azioni che le botnet hanno a "catalogo" ci sono:

Denial of service: attacco massivo contro qualcuno

Spam: campagne di spam con lo scopo di vendere prodotti (spesso illegali)

Phishing: campagne di spam con lo scopo di carpire credenziali a scopo di furto, riciclaggio, ecc.

Anche per le botnet, come anticipato in premessa, non esistono norme incriminatici che, a livello di trattato o di legislazione nazionale, siano concepite al fine di sussumerne e tipizzarne gli elementi costitutivi. Tuttavia le botnet possono essere ricondotte a diverse disposizioni della Convenzione di Budapest in relazione alle finalità per le quali sono costituite ed utlizzate.

In primo luogo le botnet sono costituite mediante accesso illecito ad un computer o sistema e, a loro volta, possono essere utilizzate per accedere abusivamente ad un computer o sistema in violazione dell'art. 2 della Convenzione e dell'art. 615 ter c.p.; intercettano le comunicazioni

---

[3] Decreto legislativo del 30.06.2003 n° 196 , pubblicato in G.U. del 29.07.2003.

[4] Linea guida T-CY (2013) 6 E adottata con delibera del 9 th Plenary Meeting del 5 giugno 2013 pubblicata sul sito internet del Consiglio d'Europa http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2013_6REV_GN2_botnets_V7adopted.pdf

telematiche in violazione dell'art. 3 Convenzione e dell'art. 617 quater c.p.; inoltre la creazione della botnet di solito altera, danneggia o cancella dati contenuti nel computer zombie e viene sovente utilizzata per alterare, danneggiare e cancellare dati contenuti in computers oggetto di aggressioni portate tramite la botenet, in violazione dell'art. 4 della Convenzione e degli artt. 635 bis e 635 ter del codice penale, ovvero per danneggiare sistemi informatici e telematici quando le botnet vengono utilizzate per lanciare attacchi DDoS (art. 5 della Convenzione e art. 635 quater c.p.).

Norme di primario riferimento nel contrasto alle attività criminali commesse tramite botnet sono, senz'altro l'art. 6 della Convenzione e, nel codice penale italiano, gli artt. 615 quater e 615 quinquies. Infatti le stesse botnet possono essere considerate strumenti informatici creati ed utilizzati principalmente per commettere reati. I programmi utilizzati per la creazione di botnet ricadono sotto l'art. 615 quater c.p. in quanto costituiscono mezzi idonei all'accesso abusivo a sistemi informatici e telematici protetti da misure di sicurezza e la loro produzione, importazione, diffusione o cessione rientra tra le condotte sanzionate dall'art. 615 quinquies, trattandosi di programmi precipuamente finalizzati a dennaggiare siatemi informatici nonché i dati e programmi in essi contenuti.

Quanto alle finalità illecite perseguite tramite le botnet vengono in considerazione, tra le più frequenti rilevate nell'esperienza pratica, la falsificazione di documenti informatici contenuti in banche date pubbliche o private (art. 7 della Convenzione ed art. 491 bis c.p.), le frodi informatiche (art.8 della Convenzione e 640 ter c.p.), la diffusione di materiale pedopornografico (art. 9 della convenzione e 600 ter co. 3° c.p.), la violazione delle norme sul diritto d'autore (art. 10 della Convenzione).

4. DDoS[5].

La sigla DoS di denial of service si traduce letteralmente in *negazione del servizio*. Si tratta di un malfunzionamento dovuto ad un attacco informatico in cui si esauriscono deliberatamente le risorse di un sistema informatico che fornisce un servizio, ad esempio un sito web, fino a renderlo non più in grado di erogare il servizio.

Gli attacchi vengono abitualmente attuati inviando molti pacchetti di richieste, di solito ad un server Web, FTP o di posta elettronica saturandone le risorse e rendendo tale sistema "instabile", quindi qualsiasi sistema collegato ad Internet e che fornisca servizi di rete è soggetto al rischio di attacchi DoS. Inizialmente questo tipo di attacco veniva attuato da "hacker", come gesto di dissenso etico nei confronti dei siti web commerciali e delle istituzioni. Oggi gli attacchi DoS hanno la connotazione decisamente più "criminale" di impedire agli utenti della rete l'accesso ai siti web vittime dell'attacco.

Una variante di tale metodologia criminale è il DDoS (Distributed Denial of Service) dal

[5] Linea guida T-CY (2013) 9 adottata con delibera del 9 th Plenary Meeting del 5 giugno 2013 pubblicata sul sito internet del Consiglio d'Europa http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)10REV_GN5_DDOS%20attacks_V7adopted.pdf

funzionamento identico ma realizzato utilizzando numerose macchine attaccanti che insieme costituiscono una botnet. Gli attaccanti, per evitare di essere individuati e per avere a disposizione un numero sufficiente di computer per l'attacco, infettano precedentemente un numero elevato di computer con dei virus o worm che lasciano aperte delle backdoor a loro riservate. I computer che sono controllati dall'attaccante vengono chiamati *zombie*. Quando il numero di *zombies* è ritenuto adeguato, o quando viene a verificarsi una data condizione, i computer infetti si attivano e sommergono il server bersaglio di richieste di connessione. Con l'avvento della banda larga il fenomeno dei DDoS sta assumendo proporzioni preoccupanti, dato che attualmente esistono milioni di persone dotate di una connessione ad internet molto veloce e permanente ma con scarse o nulle conoscenze e contromisure riguardanti la sicurezza informatica.
Tra le modalità più ricorrenti con le quali vengono condotti gli attacchi DoS e DDoS si riscontrano, nell'esperienza investigativa, l'invio di un numero superiore di e-mails rispetto a quelle che il server del servizio di posta elettronica possa ricevere, ovvero l'invio di richieste non corrette o di richieste superiori a quelle che un sistema computerizzato possa simultaneamente elaborare.
Tra le norme che vengono in considerazione per la qualificazione giuridica di queste condotte si evidenziano, in particolare, quelle che sanzionano il danneggiamento di dati, programmi o sistemi (artt. 4 e 5 della Convenzione e 635 bis e 635 ter e quater del codice penale), nonché l' art. 617 quater c.p. che sanziona specificamente le condotte di impedimento ed interruzione delle comunicazioni relative ad un sistema informatico o telematico, ovvero intercorrenti tra più sistemi, effetto che, nella maggior parte dei casi, questi attacchi informatici sono preordinati a conseguire.

5. Malwere[6].

Il termine malware indica genericamente un qualsiasi software creato con il solo scopo di causare danni più o meno gravi ad un computer, ai dati degli utenti del computer, o a un sistema informatico su cui viene installato. Si conoscono molte categorie di malware, anche se spesso questi programmi sono composti di più parti interdipendenti e rientrano pertanto in più di una classe. Tra questi i più frequenti sono Virus: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti; Worm: il loro scopo è rallentare il sistema con operazioni inutili o dannose; Trojan horse: software che contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore, per diffondersi devono essere consapevolmente inviati alla vittima; Backdoor: consentono un accesso non autorizzato al sistema su cui sono in esecuzione; Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato, le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente; Dialer: questi programmi

[6] Linea guida T-CY (2013) 11 adottata con delibera del 9 th Plenary Meeting del 5 giugno 2013 pubblicata sul sito internet del Consiglio d'Europa http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)12rev_GN7_Malware_V4adopted.pdf

si occupano di gestire la connessione ad internet tramite la normale linea telefonica, possono essere utilizzati in modo illecito, modificando il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente; Hijacker: questi programmi si appropriano di applicazioni di navigazione in rete (soprattutto browser) e causano l'apertura automatica di pagine web indesiderate; Keylogger: sono dei programmi in grado di registrare tutto ciò che un utente digita su una tastiera o che copia e incolla rendendo così possibile il furto di password o di dati che potrebbero interessare qualcun altro.
I malwere vengono utilizzati dalla criminalità informatica per la sottrazione di dati (che vengono copiati ed inviati a terzi all'insaputa del loro titolare), per modificare dati, per danneggiare i sistemi informatici, compresi quelli che controllano infrastrutture critiche, per cancellare dati o bloccarne l'accesso. Le nuove forme di malware possono essere utilizzate per sottrarre indebitamente denaro o per bloccare l'erogazione di beni e servizi pubblici, come l'elettricità o l'acqua. Il loro numero e la varietà, unite alla loro rapida evoluzione ed obsolescenza non consentono di classificarli al fine di raggiungere una loro tipizzazione sanzionatoria. La Convenzione di Budapest ha quindi evitato deliberatamente di sanzionare specificamente le varie forme di malwere, anche soltanto limitandosi alle tipologie più ricorrenti, al fine di evitare la rapida perdita di attualità delle norme ivi contenute. Tuttavia è possibile ricondurre anche i malwere sotto specifiche disposizioni della Convenzione avendo riguardo alla funzionalità ed ai danni prodotti dai malwere che sono, invece, suscettibili di catalogazione e di tipizzazione normativa.
Anche in questo caso vengono in considerazione le norme, alle quali si è più volte già fatto riferimento in precedenza[7], che sanzionano l'accesso abusivo, l'interruzione e l'intercettazione di comunicazioni telematiche, le varie forme di danneggiamento aventi ad oggetto dati, programmi o sistemi, le norme che sanzionano la disponibilità e la cessione a terzi di programmi realizzati al fine di accedere illegalmente a computer e sistemi protetti ovvero al fine di danneggiarli, i programmi concepiti per l'alterazione e la falsificazione di informazioni presenti in banche dati pubbliche o private, i malware specificamente progettati per recare un danno economico e conseguire un profitto tramite l'interferenza sul funzionamento di computers o sistemi.

6. Accesso transfrontaliero ai dati.

L'art. 32[8] della Convenzione di Butapest è dedicato proprio a disciplinare l'accesso transfrontaliero ai dati presenti all'interno di un computer o sistema informatico. La norma prevede due ipotesi:
a) l'accesso ai dati disponibili al pubblico e rinvenibili su open sources (fonti aperte) (art. 32 a);

---

[7] Ci si riferisce principalmente agli artt. 2, 3, 4, 5, 6, 7, 8 della convenzione ed alle corrispondenti norme incriminatici del codice penale nazionale.

[8] **Article 32 – Trans-border access to stored computer data with consent or where publicly available**
A Party may, without the authorisation of another Party:
a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

b) l'accesso a dati non pubblici presenti in un computer o sistema collocato sul territorio di una Stato membro effettuato utilizzando un computer presente sul territorio di un altro Stato aderente al trattato (art. 32 b).

La previsione contenuta nell'art. 32 lett. a) non presenta problemi o particolartità. Infatti come ogni altro utente del web, anche la polizia giudiziaria e l'autorità giudiziaria possono, nell'ambito di indagini e procedimenti, accedere alle informazioni ed ai dati pubblicamente disponibili nel web, a prescindere dal luogo in cui sia collocato il server che li ospita e senza dover ricorrere a strumenti di cooperazione giudiziaria. Sarà poi ciascun ordinamento nazionale a disciplinare l'utilizzabilità investigativa e giudiziaria del dato e dell'informazione così acquisita.

Meno agevole appare l'applicazione dell'art. 32 lett. b) della Convenzione che prevede l'ipotesi in cui lo Stato che sta svolgendo le indagini voglia accedere, tramite un computer collocato sul proprio territorio nazionale, a dati presenti in un computer situato sul territorio di un altro Stato (aderente al trattato). Per l'ipotesi in esame la norme prevede la possibilità di accedere ed acquisire i dati senza ricorrere agli strumenti di cooperazione giudiziaria in tutti i casi in cui venga ottenuto il consenso, libero e legalmente valido, prestato dal soggetto titolare del diritto a rendere noto il dato (testualmente: consent of the person who has the lawful authority to disclose the data).

La previsione appare, ad un primo esame, particolarmente utile al fine di rendere più rapide ed efficaci le indagini per il contrasto alla criminalità informatica. Infatti accade molto frequentemente che dati rilevanti per le investigazioni siano conservati su server esteri, perché il soggetto che ne dispone ha intenzionalmente operato questa scelta (spesso al fine di ostacolare le indagini nei propri confronti), ovvero perché, in modo del tutto casuale o involontario, abbia fatto ricorso a servizi di raccolta ed immagazzinamento dei dati offerti da providers che, a loro volta utilizzano server esteri (si pensi, ad esempio, all'utilizzazione di servizi di posta elettronica offerti da provider che abbia all'estero i propri servers).

In questi casi poter accedere ai dati in questione senza utilizzare gli strumenti di cooperazione giudiziaria internazionale può avere l'effetto di semplificare ed accelerare l'iter dell'indagine giungendo più velocemente, ad esempio, all'acquisizione di elementi di prova utili ai fini di interrompere l'attività criminale in corso.

Peraltro l'applicazione di questa previsione normativa ben si coniuga con la sempre maggior disponibilità, da parte degli internet service providers e degli internet host providers, ad offrire collaborazione spontanea all'autorità giudiziaria impegnata nello svolgimento di indagini. Infatti, sempre più frequentemente, i soggetti che offrono servizi sul web adottano politiche aziendali di collaborazione con le autorità giudiziarie e di polizia di Stati diversi da quelli nei quali si collocano i rispettivi servers, rendendosi disponibili a fornire dati di rilievo investigativo in loro possesso, senza l'attivazione di strumenti di cooperazione giudiziaria internazionale. In base a tali politiche aziendali è solitamente previsto, infatti, che le informazioni ed i dati richiesti vengano forniti in base alla comunicazione diretta di una richiesta formale (solitamente proveniente dall'autorità giudiziaria straniera), ancorché, ovviamente, tale richiesta non assuma potere coercitivo o vincolante nei loro confronti in quanto emessa da uno Stato estero. In questi casi, quindi, la collaborazione viene resa pur non essendo il soggetto che la offre legalmente obbligato.

Il tema in esame è stato oggetto di un lungo dibattito nell'ambito dei lavori di redazione del testo della Convenzione. In particolare l'attribuzione ad uno degli Stati aderenti del potere di accedere a dati conservati sul territorio di un altro Stato, in modo unilaterale e senza ricorrere agli strumenti

di cooperazione giudiziaria internazionale, è stata una possibilità che, fin dal primo momento ha visto Paesi favorevoli e Paesi contrari. Alla fine il testo dell'art. 32, pur non fornendo una soluzione definitiva ad alcuni dei principali problemi che si pongono nel corso delle investigazioni sui crimini informatici transnazionali, ha raccolto un consenso unanime tra i Paesi che hanno partecipato alla redazione del testo della Convenzione. Peraltro, ancora oggi, alcuni degli Stati che non hanno aderito al trattato individuano questa norma quale ostacolo principale alla ratifica, assumendo che, per tale via, si consentirebbe ad uno Stato straniero di svolgere attività investigativa sul proprio territorio in violazione del principio di sovranità e rimanendo, perciò, contrari all'applicazione di questa norma nei loro confronti.

Il T-CY nel febbraio 2013 ha adottato linee guida anche in relazione all'art. 32 della Convenzione, al fine di favorire una interpretazione uniforme della norma da parte di tutti i Paesi aderenti al trattato e, per tal via favorirne l'omogenea applicazione, nella convinzione che, in attesa di ampliare l'ambito delle attività di libero accesso transfrontaliero ai dati, il pieno e più ampio utilizzo degli strumenti già previsti possa certamente giovare alla celerità ed efficacia delle attività di contrasto al cybercrime.

Il documento in esame si concentra, in particolare, su alcuni aspetti della fattispecie di cui all'art. 32 lett. b), chiarendone la portata applicativa:

a) in primo luogo l'art. 32 lett. b) consente l'accesso unilaterale ai dati immagazzinati in un computer situato sul territorio di un altro Stato aderente alla Convenzione, senza ricorrere agli strumenti di cooperazione giudiziaria. La possibilità conferita dall'art. 32 lett. b) è limitata ai Paesi aderenti al trattato e non si estende ai Paesi terzi. Ciò implica che tale fattispecie troverà applicazione solo quando sia noto il luogo geografico nel quale i dati siano conservati e tale luogo ricada sotto la sovranità di uno Stato aderente. Non è escluso che tale accesso diretto ai dati possa avvenire nel caso in cui questi siano custoditi in luoghi sconosciuti ovvero in Paesi terzi. In tali circostanze, secondo il T-CY, ciascuno Stato deve valutare autonomamente e sulla base del diritto nazionale, dei principi di diritto internazionale e delle relazioni intercorrenti tra gli Stati, se tale accesso unilaterale sia legittimo;
b) nel consentire l'accesso diretto ai dati, l'art. 32 lett. b) non solo esclude il ricorso agli strumenti di cooperazione giudiziaria internazionale ma non prevede, nemmeno, alcuna forma di comunicazione o notizia dell'attività in corso in favore dello Stato aderente sul cui territorio si trovino i dati. La comunicazione dell'attività investigativa non è preclusa, ma non è nemmeno obbligatoria, di modo che ciascuno Stato potrà effettuarla o meno pur rimanendo perfettamente legittima la procedura espletata;
c) l'art. 32 lett. b) prevede il consenso della persona titolare del diritto a rendere noto il dato. Tale consenso deve essere volontario e conforme alla legge. Ciò significa che non devono essere utilizzati mezzi di costrizione e che il consenso deve essere espresso da un soggetto che è titolare del diritto di disporre delle proprie situazioni giuridiche soggettive (quindi un soggetto adulto e capace). Sulle modalità di espressione del consenso e della sua documentazione con funzione di prova la Convenzione rimanda al diritto nazionale dello Stato che accede direttamente ai dati. Secondo le linee guida in esame il consenso non può essere reso anticipatamente ed in modo astratto. Ciò accade in tutti quei casi nei quali la persona che accede ad un servizio on line accetti i termini e condizioni del contratto di fornitura con il service provider ed ivi sia prevista la possibilità di comunicazione dei dati all'autorità giudiziaria in caso di abuso. Tale

adesione alle condizioni generali di contratto non costituirebbe consenso valido all'accesso ai dati custoditi dal service provider;

d) ogni qual volta l'art. 32 lett. b) fa riferimento alla legge quale parametro di legittimità di un atto o di un provvedimento[9], questa deve essere individuata nella legge vigente nel Paese che acquisisce direttamente i dati e, quindi, nella legge che delimita l'ambito legittima iniziativa dell'autorità giudiziaria o di polizia che svolge l'indagine nell'ambito della quale viene effettuato l'accesso e l'acquisizione transfrontaliera dei dati. Ciò in quanto, secondo le linee guida T-CY, non è possibile che, nel corso delle indagini, spesso governate da ragioni di urgenza, l'autorità procedente possa acquisire una conoscenza completa e puntuale delle norme vigenti nel Pease nel quale i dati sono custoditi. Rimane fermo, ovviamente, il rispetto dei diritti umani e dei principi di diritto internazionale ai quali rimanda l'art. 15 della Convenzione;

e) il profilo più difficile nell'interpretazione dell'art. 32 lett. b) è costituito dall'individuazione del soggetto titolare del diritto a rendere noto il dato; soggetto del quale l'articolo della Convenzione richiede il consenso affinché l'accesso e l'acquisizione diretta dei dati sia legittimo. Sul punto le linee guida T-CY offrono dei chiarimenti certamente utili ma non esaustivi. In premessa si ritiene che tale soggetto debba essere individuato in base alla legge applicabile – e quindi alla legge vigente nel paese che svolge le indagini- e in base alle circostanze del caso concreto. Tale soggetto può essere una persona fisica o una persona giuridica. Ad esempio, si chiarisce, il soggetto legittimato a prestare il consenso può essere il titolare di una casella di posta elettronica che è messa a disposizione da parte di un internet service provider che si avvale di servers collocati all'estero, ma anche un internet o cluod service provider estero, il quale potrebbe prestare legittimamente il consenso a fornire dati di terze persone da lui custoditi sui propri servers, se le condizioni generali di contratto sottoscritte dal cliente gli consentono di farlo;

f) anche la collocazione territoriale della persona legittimata ad esprimere il consenso costituisce un profilo rilevante e perciò esaminato dalle linee guida. Questa si può trovare nel territorio del Paese che svolge le indagini, e quindi sottoposta alla sua giurisdizione, ovvero nel Paese dove sono conservati i dati o, in fine in uno Stato terzo, e quindi sottoposta alla giurisdizione di uno Stato estero. La circostanza assume rilevanza al fine delle modalità attraverso le quali l'autorità che svolge le indagini possa contattare il soggetto interessato per acquisirne il consenso. Il C-TY ricorda che, secondo la legge nazionale di alcuni dei Paesi aderenti al trattato non è consentito un approccio diretto ai propri cittadini da parte di autorità giudiziarie o di polizia straniere; anzi, tale condotta configura una specifica ipotesi di reato a carico dell'autorità straniera procedente. In questi casi l'acquisizione del consenso non potrà che avvenire attraverso gli strumenti di cooperazione giudiziaria internazionale e con la collaborazione dello Stato che esercita la giurisdizione sul soggetto, persona fisica o giuridica, legittimato ad esprimere il consenso.

La portata applicativa dell'art. 32 lett. b) all'interno del nostro sistema processuale non è certo trascurabile; rilevanti sono le sue implicazioni, che investono sia lo svolgimento delle indagini preliminari che la formazione della prova nel corso del giudizio.

Certamente saranno acquisibili per via di accesso transfrontaliero i dati messi a disposizione della

[9] Ciò avviene con riguardo alle formule "lawful and voluntary consent" e "lawful authority", utilizzate nel testo dell'art. 32 lett. b).

vittima del reato o da persone informate sui fatti, dai quali è ragionevole prevedere la più ampia collaborazione.
Per i dati detenuti da soggetti terzi bisognerà, invece operare alcune distinzioni: se i dati sono nella titolarità esclusiva del terzo, si pensi ad esempio ai file di log conservati da un internet service provider e relativi all'accesso ai suoi servizi effettuato dall'indagato, il consenso prestato dal terzo (*id est* la sua disponibilità a fornirli materialmente) dovrà essere ritenuto condizione necessaria e sufficiente a legittimarne l'acquisizione al materiale d'indagine e l'utilizzazione quale prova nel giudizio. Differente è l'ipotesi in cui il terzo sia "contitolare" dei dati, ovvero che li detenga per conto del soggetto (ad es. l'indagato) che li ha affidati alla sua custodia. Si pensi all'ipotesi della casella di posta elettronica dell'indagato aperta presso un provider straniero. In questo caso bisognerà accertare, in base alle condizioni di contratto che regolano il servizio, se il provider possiede il potere giuridico di disporre dei dati. Tale positivo accertamento, tuttavia, sembrerebbe condizionare l'eventuale utilizzazione probatoria del dato in giudizio più che la sua acquisizione e valutazione per l'assunzione delle determinazioni nel corso delle indagini.
Più limitata appare la possibilità di accedere direttamente a dati nella disponibilità esclusiva della persona sottoposta alle indagini e collocati all'estero. Si pensi ad esempio all'ipotesi di dati contenuti in un computer che l'indagato detiene all'estero, ovvero al caso in cui sottoposto alle indagini sia un internet service provider con servers all'estero. In questi casi in assenza della collaborazione dell'indagato e del suo consenso, in base alla normativa sovranazionale vigente, non sarebbero esperibili forme di accesso diretto ai dati e sarebbe necessario ricorrere all'ausilio dello Stato estero dove il computer o i servers sono collocati, tramite gli strumenti di cooperazione giudiziaria internazionale.
Quanto agli strumenti investigativi utilizzabili, si deve ritenere che l'accesso transfrontaliero ai dati possa essere veicolato nelle forme giuridiche della perquisizione informatica, del sequestro o dell'ordine di esibizione a seconda delle finalità volta a volta perseguite. Sequestro ed ordine di esibizione saranno funzionali ad acquisire dati dei quali si conosce l'esistenza e la collocazione; la perquisizione informatica sarà utile, invece, in tutti i casi in cui ci si muova alla ricerca di dati rilevanti ma non già individuati per contenuto e collocazione. Nel primo caso si tratterà di apprendere il dato messo a disposizione dalla persona offesa, dal testimone o dal terzo, nel secondo caso di ricercare fra più dati ai quali si accede grazie alla disponibilità del titolare quelli di interesse investigativo; si pensi al caso in cui il cloud service provider consenta all'autorità inquirente di accedere all'intero data base che l'indagato ha creato presso di lui per ricercare ed acquisire i dati di interesse investigativo.

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 158-163

La Dematerializzazione delle Fonti di Prova

Marco Mattiucci

Abstract: la materia del Digital forensics ha alterato il concetto stesso di fonte di prova portandolo, negli ultimi anni, ad un livello di astrazione tale che lo rende difficilmente gestibile dal Codice di Procedura Penale. In questo lavoro si dettagliano proprio i vari livelli intermedi di oggetto virtuale che possono essere incontrati in una indagine tecnica di Polizia Giudiziaria con le relative influenze ai concetti di sopralluogo e sequestro nonché all'analisi forense.

The concept of evidence coming from the Italian laws is going to change because of Digital Forensics. This because digital pieces of evidence are not only physical but can include different kind of data at different levels of abstraction. This article is related to the several types of digital virtual objects we can have in a digital forensic analysis and to the consequences, from this point of view, for the police intervention in the scene of crime and for the idea of scene of crime itself.

Parole chiave: Digital Forensics, Cloud Forensics, Dematerializzazione, IAAS, Virtualizzazione, Codice di Procedura Penale, Sequestro, Reperto virtuale, Sopralluogo virtuale.

1. Premessa sulla Digital Forensics

La Digital Forensics è una neo-scienza che si è assestata a livello internazionale negli ultimi venti anni e in Italia sta raggiungendo la sta maturazione da circa dieci. Non sono mancati (e purtroppo non mancano) nel processo di crescita tutto italiano errori di impiego degli strumenti che la caratterizzano e cattive intepretazioni dibattimentali dei risultati esposti nei vari referti. Ciò nonostante la materia cresce in maniera inarrestabile e permea ormai le indagini civili e penali, nonché le aule dibattimentali ed i team aziendali per ogni tipo di questione, reato e caso investigativo.

La Digital Forensics è relativa l'identificazione, prelievo e preservazione (sulla scena del crimine) di sistemi e dati high tech (digitali nel senso elettronico del termine – caratterizzati dagli stati 0 ed 1 – cellulari, PC, Internet, ecc.) nonché validazione, analisi ed interpretazione degli stessi (in laboratorio) ed infine refertazione e presentazione dei risultati (in dibattimento).

La domanda fondamentale è perché ci debba essere un problema di impiego degli strumenti e dei risultati della digital forensics e ad un primo approccio la risposta potrebbe essere nell'implicita

Articolo pervenuto il 2 ottobre 2013, approvato il 30 dicembre 2013

complessità tecnica di settore, ma questa è una visione solo parziale della situazione.
La questione centrale, come vi vedrà in questo lavoro a seguire, è che la digital forensics ha intaccato alcuni concetti base ritenuti universalmente validi in ambito legale, i quali devono essere in qualche modo ricodificati o quantomeno riadattati all'inarrestabile evoluzione tecnologica del mondo digitale.

2. La Dematerializzazione

In generale il processo di dematerializzazione è stato largamente introdotto quando, anche la PA, ha cercato di trasformare l'enorme massa di documentazione cartacea in suo possesso in file su una memoria di massa digitale. A questo va aggiunto che si è cercato non solo di implementare l'archiviazione in tal senso, ma anche le procedure, spostando le attività umane su flussi descritti e contenuti in complessi database (archivi elettronici) e software basati su articolate reti di computer.
Risultati parziali di tale lungimirante lavoro di conversione sono evidenti negli ultimi anni, ma la loro parzialità è altrettanto evidente e si comprende anche che il completo processo di dematerializzazione, in Italia, impiegherà lunghi periodi a venire, lasciando ancora alla carta un centralissimo ed indiscutibile compito in qualsiasi ambito documentale e procedurale.
Uno dei motivi fondamentali di tale difficoltà di avanzamento è la mancanza di fiducia verso il digitale, che ha sicuramente mostrato la sua pervasività ed indispensabilità, ma ha parimenti evidenziato un'assoluta incapacità di gestire sicurezza, affidabilità e disponibilità dei dati:

a) **Sicurezza**: stabilire chi (identità) è autorizzato a fare cosa (attività) e con quali dati (informazioni) ed evitare che non autorizzati svolgano procedure o accedano a dati loro vietati. Non esiste ad oggi un sistema tecnico completamente sicuro per i sistemi digitali, soprattutto quando sono in rete, è indispensabile una politica di gestione della sicurezza che coinvolga anche le persone.
b) **Affidabilità**: garanzia che i dati registrati restino integri nel tempo. La maggior parte delle memorie digitali si danneggia con frequenza molto più alta della carta, che resta il supporto di memoria al momento più longevo.
c) **Disponibilità**: garanzia che i dati restino disponibili agli autorizzati quando questi lo richiedono. Spesso tra guasti di sistema, difficoltà di connessione, ecc. i dati, pur essendo presenti in una rete complessa, non sono disponibili.

Questi problemi appena elencati sembrano di natura puramente tecnica, ma così non è, essi sono dovuti alla difficoltà del direttivo di ogni ordine e grado di comprendere: (1) i nuovi concetti cui ci si può appoggiare nel mondo digitale per creare nuovi modi di lavorare e (2) la necessità degli ingenti investimenti che sicurezza, affidabilità e disponibilità richiedono.
Qualche esempio chiarificherà meglio i due punti esposti.
Per il punto (1), ad esempio, introdurre le email nel processo lavorativo è un buon punto di partenza ma evitare di gestire l'identificazione forte dei mittenti (es. PEC, Tracing) perché "costa troppo" e continuare ad inviare pratiche scannerizzate come se l'email fosse un fax, porta solo ad appesantire il sistema facendo percepire agli utenti che funziona male, inoltra si aprono le porte a possibili intrusioni dall'esterno (es. phishing).
Per il punto (2) è risaputo che in Italia sicurezza, affidabilità e disponibilità vengono percepiti come

costi sia dalle PA che dalle aziende e non come investimenti e quindi si cerca di "spenderci il meno possibile" conseguendo sistemi deboli e mediamente mal funzionanti che vengono rafforzati solo nelle aree in cui non se ne può fare a meno (es. aree riservate o critiche).
In definitiva non si può avere vera dematerializzazione se non c'è una revisione del processo lavorativo "umano", un cambio nei concetti alla base delle stesse attività e nell'atteggiamento del direttivo.

3. La Dematerializzazione nella Digital Forensics

Nella digital forensics i problemi appena visti per la dematerializzazione in generale, non solo esistono, ma sono rafforzati dalla pesantezza e rilevanza dell'attività considerata che è quantomeno un'indagine civile/penale. Ogni volta infatti che si devono affrontare questioni critiche in cui si rischiano grosse ripercussioni per degli errori è naturale irrigidirsi. Una delle prime risultanze è il pervasivo ed irremovibile uso della carta per la registrazione degli eventi e delle informazioni (verbali, referti, decreti, ecc.).
Questa *"imbalsamazione cartacea"* ed *"attaccamento a ciò che si può toccare con mano"* in cui i sistemi informatici assumono a malapena la valenza di fax e macchine da scrivere ("a malapena" in quanto al larghissimo impiego del fax, uno strumento assolutamente obsoleto, in ambito sia di PG che Procura o Uffici legali) rallenta i meccanismi di indagine e processuali, ma soprattutto cozza con nuovi aspetti inerenti i reperti che la digital forensics ha evidenziato e sta evidenziando.
Si può passare immediatamente a considerare l'aspetto centrale di tale faccenda mediante un esempio base di semplice e diretta comprensione.
Qualora un PC contenga nella sua memoria di massa (hard disk) alcuni dati di estremo interesse, per un'indagine di PG nei confronti del suo possessore, se ne può disporre il sequestro (fisico) per poi consentire ad un CT di svolgere un'analisi forense approfondita consegnandogli l'oggetto. La domanda però è perché disporre un sequestro fisico dello strumento quando NON si è interessati a tutto quello che contiene ma solo ad alcuni dati in esso registrati.
Una prima risposta potrebbe essere quella di copiare tutto il contenuto (dati) del PC (copia integrale bit-stream) per poi restituirlo all'avente diritto (a meno di particolari problematiche legali ovviamente).
Questo approccio è oggi largamente usato ma è solo una "pezza" di risoluzione basata sul riadattare un vecchio mondo fisico al nuovo mondo digitale. Basterebbe infatti copiare selettivamente dal PC solo quanto utile per le indagini/dibattimento e lasciare l'oggetto fisico nella disponibilità dell'avente diritto.
Quali sono le implicazioni di questo NUOVO modo di vedere il sequestro?

- difficoltà tecniche: non sempre è possibile selezionare quanto utile alle indagine e copiarlo istantaneamente;
- intrinseca irripetibilità: la copia selettiva sulla scena è palesemente non ripetibile in quanto il PC appena riutilizzato cambierà il suo contenuto.
- la copia selettiva ottenuta è l'unico reperto: ma cos'è una copia? Un insieme di dati, quindi un qualcosa di immateriale che va ad esempio depositato presso l'ufficio corpi di reato della competente procura.

In definitiva si è stabilito un nuovo concetto di sequestro virtuale in cui l'oggetto del sequestro non è la "cosa" ma il "dato". Depositare un dato presso un ufficio corpi di reato (l'esempio non è fatto a caso) non significa depositare l'hard disk o la pennetta USB che lo contiene, eppure ancora oggi, il verbale di deposito va a descrivere la memoria perché è un'evidenza fisica del sequestro. Il deposito dovrebbe avvenire parimenti in forma virtuale, ossia la procura o l'ufficio legale dovrebbe avere un server sicuro con un archivio in grado di ospitare la copia determinata sulla scena.
Non è infatti difficile capire che l'hard disk o la pennetta usata per ospitare la copia selettiva sul posto dei dati del PC è solo un mezzo, un involucro che contiene al suo interno un reperto (la copia) totalmente virtualizzato. Non va quindi depositato l'hard disk o la pennetta ma quanto contiene! Quella vista è una prima forma di dematerializzazione delle fonti di prova digitali ma è solo il primo passo, si può andare ben oltre.
Si ipotizzi infatti di rilevare su Internet un sito web palesemente illecito, esso è contemporaneamente fonte di prova del "suo" illecito e "scena del crimine" che si può replicare senza problemi in diversi punti della terra. Come procedere almeno ai rilievi? Come creare un minimo di evidenze dell'esistenza del sito e del suo contenuto/attività illeciti?
Mezzi tecnici assoluti in tal senso ad oggi non esistono. Si possono però gestire delle procedure abbastanza garantite, ad esempio:

- impiegare un PC preparato ad-hoc per la navigazione del sito così che non vengano introdotti elementi spuri nell'osservazione;
- riprendere video e foto del PC che naviga nel sito sia internamente (ci sono software che lo permettono) che esternamente (con una video camera);
- mettere sotto controllo la connessione del PC che naviga e quindi raccogliere tutto il flusso dati che a basso livello realizza il sito.

Il risultato di queste attività è un insieme disomogeneo di informazioni e dati informatici (descrizione del PC, video, foto, flussi, ecc.) che costituiscono l'UNICA fonte di prova, ottenuta in maniera ovviamente irripetibile, che evidenzia l'esistenza ed operatività del sito (il sito web potrebbe smettere di funzionare o mutare in qualsiasi momento).
Mentre nel caso del PC aprendo la sua copia selettiva era possibile visionarne i dati abbastanza agevolmente, in questo tipo di reperto virtuale i dati presenti nella fonte devono essere ricomposti in maniera tecnicamente complessa, al fine di ricostruire il sito web indagato.
Questo per dire che non solo si necessita del nuovo concetto di reperto virtuale ma che questo stesso concetto può essere considerato a diversi livelli: copia diretta, elementi per la ricostruzione ed altri che di seguito si va ad esaminare.
Il punto massimo di questo studio sul reperto virtuale e sulla dematerializzazione del reperto, lo si ha con i sistemi cloud. In breve un cloud system è un sistema che usa Internet come semplice rete di appoggio, combinando il lavoro di migliaia di server in tutto il mondo, ciò a determinare una serie di servizi. Per capire meglio, la famosa gmail.com, la google mail e/o lo stesso motore di ricerca google, non sono software nel senso classico del termine ma veri e propri servizi determinati da un gigantesco sistema cloud su Internet. La nostra impressione da utenti è che un solo software o computer risponda alle domande che poniamo a google o presenti le nostre email di gmail.com sullo schermo, ma in realtà un'infinità di differenti macchine stanno lavorando a nostra insaputa per rispondere alle impostate richieste.

Lo stesso problema del sito web di cui sopra si propone quando è necessario richiedere dei dati da un cloud (es. la posta di una casella di gmail.com) ma, come anticipato, si può passare ad un livello molto più alto.
Un cloud non è solo in grado di gestire servizi dati ma anche servizi di elaborazione. Ad esempio è possibile avere un proprio computer TUTTO sul cloud ed usarlo su un PC locale che però non ha nulla dei dati che si stanno trattando. Si accede al computer locale, poi si attiva il browser (Explorer/Firefox/Safari…) e si naviga su una pagina web in contatto con il cloud che presenta un nome utente ed una password. Scritti tali dati nasce dal browser un nuovo computer che risiede totalmente su Internet. Qualora si procedesse al sequestro del computer locale, ci sarebbe a malapena l'evidenza della navigazione Internet sul cloud, ma niente dei dati che l'utente stava manipolando.
Il computer virtuale su cloud o computer remoto è un intero sistema di elaborazione che NON esiste fisicamente ma solo virtualmente (è definito scientificamente macchina virtuale distribuita). Il suo sequestro può essere SOLO di natura virtuale ed il reperto che ne consegue è un insieme di dati che difficilmente potrà sussistere solo in un hard disk.
In altre parole NON è sempre possibile registrare questa fonte di prova su una nostra memoria locale, tale contenitore non è adeguato. L'unico modo di gestire la situazione è lasciare il computer virtuale nel cloud e chiedere al gestore del cloud di "congelarlo" lì dove si trova, ad esclusivo uso di PG ed AG e dei loro CT e periti (fatto che ricorda il sequestro con obbligo di custodia, se non fosse per il fatto che custode, oggetto custodito e sigilli/contenitore sono tutti immateriale e delocalizzati spazialmente).

4. Il Reperto Dematerializzato (virtuale) ed i suoi livelli

Riassumendo in maniera strutturata ed analitica gli esempi base riportati sopra, si può asserire che il reperto virtuale può sussistere almeno ai seguenti livelli:

1) copia selettiva o integrale di dati presenti su una memoria digitale fisica (es. hard disk, chievette USB, ecc.)
2) raccolta dati disomogenei su elementi che esistono in rete o su cloud (es. siti web, messaggi e caselle di posta elettronica, traffico intercettato, ecc.)
3) sistemi di elaborazione virtualizzati su cloud (es. computer remoto su cloud)

Nei primi due casi si può procedere a raccogliere i dati su una memoria locale di appoggio ed usare essa come "metafora" del reperto (che invece è solo l'insieme di dati) mentre nel terzo anche il contenitore del reperto è spesso virtuale, non potendo realmente e completamente copiare un computer virtuale da un sistema cloud ma solo congelarlo.
Alla domanda possono esistere ulteriori livelli di virtualizzazione del reperto? la risposta è sfortunatamente si. Il Cloud può ospitare intere infrastrutture completamente virtualizzate (denominati servizi IAAS) e quindi non ci sarebbe solo un computer virtuale ma un'intera rete locale o un'intera intranet. In questo senso si andrebbe a svolgere le indagini su una rete totalmente virtualizzata, non la si potrebbe "congelare" per intero, dato che potrebbe fornire servizi a migliaia di utenti e si dovrebbe eseguire tutta l'analisi forense nel cloud (realizzando di fatto ispezioni,

sequestri, ecc in un mondo non fisico). Questo crea un livello completamente innovativo di indagine che peraltro è internazionale, non soggetto a confini territoriali dato che il cloud sussiste su una rete (Internet) senza limitazioni di tale tipo.

5. Conclusioni

La dematerializzazioni delle fonti di prova è un'attività in corso da oltre dieci anni in Italia grazie alle necessità che la digital forensics sta progressivamente evidenziando. L'avanzata dei "reperti virtuali" è inarrestabile soprattutto a causa dei nuovi sistemi cloud ad oggi imperanti su Internet. Le difficoltà che a livello legale e tecnico tali categorie di reperti evidenzieranno nel repertamento ed analisi saranno crescenti al punto tale che creeranno delle strade senza uscita. L'unica possibilità è introdurre in ambito di PG e procedura penale queste nuove categorie completando quanto parzialmente ed indirettamente fatto dalla L.48/2008 (art. 244CPP ispezione virtuale, art. 247,352CPP perquisizione virtuale, art. 354 reperto virtuale).
Tali nuove categorie sconvolgono il panorama legale ed aprono tutta una serie di nuove disquisizioni dal punto di vista procedurale ma disconoscerle è ormai fattivamente impossibile.

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 164-180

Ruolo di Polizia Economico-Finanziaria della Guardia di Finanza a Contrasto dei Crimini Informatici

Alberto Reda

Abstract: La presa di coscienza delle gravi minacce derivanti dall'utilizzo illegale delle nuove tecnologie ha evidenziato la necessità di rafforzare il contrasto a conseguenti fenomenologie criminali in continua evoluzione. Tali fenomenologie interessano soprattutto le reti telematiche, in particolare la rete mondiale *Internet*, da cui l'economia nazionale ed europea dipendono fortemente e sulle quali sono compiuti illeciti il cui contrasto rientra a pieno diritto nella missione istituzionale della Guardia di Finanza quale polizia economica e finanziaria. Il Corpo interviene nel comparto attraverso due direttrici che, in linea con l'approccio unitario e trasversale che caratterizza l'azione del Corpo, sono in continuo contatto funzionale tra loro. Vi è la rete dei reparti territorialmente distribuiti sul territorio nazionale, con il compito di assicurare nei rispettivi ambiti, l'efficiente tutela degli interessi economici e finanziari; vi è poi quella dei Reparti Speciali, che si affiancano ai primi e che, istituiti per le investigazioni in specifiche materie, sono incaricati di realizzare direttamente, ovvero con azioni di supporto alle unità operative, moduli investigativi connotati da elevati *standards* qualitativi per i reparti territoriali.
Le iniziative avviate dalle unità operative della Guardia di Finanza si basano, oggi, sempre più su una stretta e continua interazione tra le diverse componenti del Corpo, nell'ottica di sviluppare sinergie che diano concreta attuazione a quell'approccio trasversale e multidisciplinare tipico della polizia economico-finanziaria. I moduli di intervento sono, quindi, contestualmente orientati a effettuare un monitoraggio della rete telematica per verificare l'esistenza di sacche di illegalità, intercettare i flussi finanziari sospetti e verificare la posizione fiscale dei soggetti investigati per l'eventuale tassazione dei proventi illeciti.

Parole chiave: Guardia di Finanza, Nucleo Speciale Frodi Tecnologiche, Reati Informatici, Polizia Economico-Finanziaria, Frodi Telematiche.

Articolo pervenuto il 2 ottobre 2013, approvato il 30 dicembre 2013

1. Introduzione

La Guardia di Finanza è una Forza di Polizia ad ordinamento militare, direttamente dipendente dal Ministro dell'Economia e delle Finanze, che ha come missione istituzionale il presidio delle libertà fondamentali della Costituzione economica. A seguito della revisione dei compiti operata dal legislatore nel 2001, le prerogative del Corpo sono state sensibilmente ampliate, passando dalla tutela prioritaria delle ragioni del prelievo alla più estesa funzione di polizia economico–finanziaria. Alla fine degli anni novanta infatti, alla luce del mutato scenario politico – economico e istituzionale emerse l'esigenza di riconsiderarne la struttura ordinativa e di riaffermare, in chiave più moderna e adeguata, il ruolo istituzionale del Corpo e la sua funzione di Forza di Polizia a competenza generale posta a difesa degli interessi economici e finanziari sia nazionali che dell'Unione Europea. A tal fine, il Governo fu delegato ad emanare:

- ex. Art. 27 della Legge 27 dicembre 1997, n. 449, un regolamento per la determinazione della struttura del Corpo, che definì i criteri base della riorganizzazione;
- ex. Art. 4 della Legge 31 marzo 2000, n.78, uno o più decreti legislativi per l'adeguamento dei compiti del Corpo in ordine al riordino della pubblica amministrazione come il D.Lgs. n. 68/2001 che adeguò i compiti d'Istituto ed assegnato al Corpo compiti di prevenzione, ricerca e repressione delle violazioni in materia di interessi economico-finanziari nazionali o dell'Unione Europea.

Nel dettaglio, il D.Lgs. n. 68/2001 ha assegnato alla Guardia di Finanza:

- funzioni di polizia finanziaria, a tutela del bilancio pubblico, delle regioni, degli Enti locali e dell'Unione Europea, sia dal lato delle entrate che delle uscite, esaltando la vocazione internazionale della Guardia di Finanza in adeguamento al carattere transnazionale delle fenomenologie criminali.
- compiti di polizia economica, allo scopo di tutelare il mercato dagli effetti distorsivi prodotti dall'infiltrazione della criminalità e dalle altre forme di concorrenza illecita;
- il concorso al mantenimento dell'ordine e della sicurezza pubblica ed alla difesa militare del Paese.

L'unitarietà delle attività investigative nel settore economico-finanziario costituisce tuttora imprescindibile elemento di efficienza ed economicità allargando le prerogative operative dell'Istituzione a tutti i settori e a tutte le materie correlabili, anche nel tratto a venire, con la tutela dell'Erario.

Le ragioni dell'evoluzione dei compiti istituzionali, rese ancor più attuali dalla perdurante crisi economica, sono di tutta evidenza: l'evasione fiscale, l'economia sommersa, le frodi sui finanziamenti pubblici, la criminalità organizzata, il riciclaggio, l'abusivismo finanziario, le truffe in danno dei risparmiatori, la contraffazione sono espressione di una minaccia unitaria, che impone una risposta altrettanto unitaria per essere veramente efficace.

Le proiezioni operative puntano a colpire nella loro globalità tutti i fenomeni che si connotano per la capacità di mettere a rischio, contemporaneamente, più interessi economico-finanziari, adottando tecniche investigative tipiche "di polizia".

Negli ultimi anni, la nascita di ulteriori minacce derivanti dall'utilizzo illegale delle reti telematiche e delle nuove tecnologie ed il ruolo che queste hanno assunto nelle dinamiche dei sistemi produttivi e

finanziari internazionali, hanno comportato la necessità per il Corpo di rafforzare il contrasto a tali fenomenologie che consentono a soggetti (in Rete assolutamente anonimi) di commettere ogni forma di illecito, ivi compresi quelli rientranti nella sfera di competenza della polizia economico-finanziaria. Si tratta di un ambito di intervento sempre più all'attenzione delle Istituzioni e Autorità nazionali e internazionali in ragione dello sviluppo della Rete, soprattutto di quelle che sono le sue intrinseche componenti (tecnologiche e/o economiche), quale opportunità di crescita e di trasformazione per un sistema socio-economico maturo, che sempre più spesso viene messa in discussione proprio da comportamenti della specie, capaci di minare irrimediabilmente il rapporto di fiducia tra operatori economici e cittadini/utenti.
Per tale ragione, la Guardia di Finanza è costantemente impegnata in attività di monitoraggio della rete Internet e di studio della fenomenologie criminali legate alle moderne tecnologie che vadano nel senso della tutela del buon andamento del mercato e del quieto vivere sociale, agendo sia sul piano della prevenzione e, laddove necessario, su quello della repressione, così da preservare in modo più efficace l'ambiente digitale nel suo insieme e di dare una maggiore fiducia all'intero sistema.
È questa un'attività che richiede, per la sua natura dinamica, la formazione continua del personale e la realizzazione di sistemi tecnologici ed applicativi informatici altamente prestanti, oltre che costantemente aggiornati e capaci di stare al passo con i rapidi processi evolutivi delle tecnologie e delle Reti, cui deve fare da complemento necessario lo studio e l'implementazione di metodologie operative che possano essere applicabili in ambito nazionale ed internazionale.

2. Organizzazione dei Reparti Speciali e delle Unità territoriali della Guardia di Finanza

Il Decreto del Presidente della Repubblica 29 gennaio 1999, n. 34, recante "Norme per la determinazione della struttura ordinativa del Corpo della Guardia di Finanza", ha ridisegnato la struttura generale e le linee di dipendenza dei comandi e reparti del Corpo, modificando, in parte, la Legge di ordinamento 23 aprile 1959, n. 189.
Ai sensi dell'art. 27, commi 3 e 4, della Legge 27 dicembre 1997, n. 449, il Corpo della Guardia di Finanza è costituito da:

- **Comando Generale**, con funzioni di alta direzione, pianificazione, programmazione, indirizzo e controllo delle attività del Corpo;
- **Comandi e Organi di esecuzione del servizio**, preposti all'espletamento delle attività istituzionali e variamente ripartiti a seconda che svolgano compiti di indirizzo e controllo delle attività operative (Comandi territoriali, con competenza interregionale, regionale e provinciale, Comandi speciali ed aeronavali), ovvero direttamente esecutivi del servizio (Nuclei di Polizia Tributaria, Nuclei Speciali, Gruppi, Reparti operativi minori, stazioni navali, sezioni operative navali e sezioni aeree);
- **Comandi, Istituti e Centri di reclutamento e di addestramento**, con il compito di curare la gestione e gli aspetti relativi al reclutamento, nonché di assicurare l'addestramento di base e la post-formazione del personale;

- **Comandi e Reparti di supporto tecnico, logistico e amministrativo**, costituiti per lo svolgimento di attività di supporto e di funzionamento a favore delle varie strutture organizzative centrali e periferiche.

Sul territorio operano "materialmente" i Reparti Territoriali, mentre, i Reparti Speciali che si affiancano ai primi, istituiti per le investigazioni complesse, multidistrettuali, ovvero extraterritoriali, in tutte le materie affidate al Corpo, sono incaricati di realizzare - direttamente, ovvero con azioni di supporto della componente territoriale – prodotti connotati da elevati standard qualitativi.
Il Comando dei Reparti Speciali, istituito alla sede di Roma, ha struttura e attribuzioni similari a quelli dei paritetici Comandi Interregionali.
Ha alle proprie dipendenze il Comando Tutela della Finanza Pubblica, il Comando Tutela dell'Economia, il Comando Unità Speciali, i quali, ai fini del controllo di gestione, costituiscono "centri di responsabilità di secondo livello", nonché il Reparto Tecnico Logistico e Amministrativo, alla sede di Roma.
Il Comando Tutela della Finanza Pubblica, assolve funzioni di comando, coordinamento e controllo dei Nuclei Speciali dipendenti:

- il Nucleo Speciale Entrate che ha competenza in materia di entrate del bilancio nazionale e degli Enti locali;
- il Nucleo Speciale Spesa Pubblica e Repressione Frodi Comunitarie - è competente a presidiare il segmento delle uscite (spesa pubblica, frodi al bilancio comunitario, bilancio nazionale e degli Enti locali);
- il Nucleo Speciale Pubblica Amministrazione, per le attività di collaborazione con l'Alto Commissario per la prevenzione ed il contrasto della corruzione e delle altre forme di illecito nella pubblica amministrazione, nonché referente della Guardia di Finanza nei rapporti con il Dipartimento della Funzione Pubblica;

Il Comando Tutela dell'Economia invece, ha funzioni di comando, coordinamento e controllo dei reparti dipendenti:

- il Nucleo Speciale di Polizia Valutaria, che presidia il segmento del mercato dei capitali, assolvendo funzioni di analisi, progettazione, direzione operativa ed esecuzione diretta del servizio. Nell'ambito delle competenze demandate, opera a tutela dei mercati finanziari, nei settori di servizio riguardanti il riciclaggio, i movimenti transfrontalieri di capitali, l'intermediazione finanziaria, l'usura, la disciplina dei mezzi di pagamento, il finanziamento al terrorismo, la tutela del risparmio e gli illeciti previsti dal testo unico delle leggi bancarie. Assicura, inoltre, le attività di collegamento con l'Ufficio Centrale Antifalsificazione Monetaria e altri Mezzi di Pagamento, presso il Ministero dell'Economia e delle Finanze. Il Nucleo dispone di due unità operative periferiche (Gruppi di Sezioni) alle sedi di Palermo e di Milano;
- il Servizio Centrale di Investigazione sulla Criminalità Organizzata (S.C.I.C.O.), riveste il ruolo di "servizio centrale" ai sensi dell'art. 12 della legge n. 203/1991, operando, in particolare, al fine di prevenire e reprimere le infiltrazioni criminali nel tessuto economico. Nelle materie di competenza sviluppa attività di analisi, elabora progetti operativi e svolge investigazioni, secondo le disposizioni in vigore nello specifico settore. Assicura, inoltre, il raccordo ed il collegamento informativo (come disciplinato dall'art. 12 della citata legge n. 203/1991 e dalle direttive vigenti in materia), nonché il supporto a favore dei reparti territoriali e dei "servizi

interprovinciali" nel contrasto ai delitti di criminalità organizzata.

Il Comando Unità Speciali assolve funzioni di comando, coordinamento e controllo nei confronti dei reparti dipendenti:

- il Nucleo Speciale Commissioni Parlamentari d'Inchiesta che collabora con le Commissioni Parlamentari d'Inchiesta;
- il Nucleo Speciale Privacy, costituisce il referente della Guardia di Finanza nei rapporti con l'Autorità Garante per la Tutela dei Dati Personali;
- il Nucleo Speciale Frodi Tecnologiche, opera direttamente, ovvero a supporto delle componenti speciale e territoriale, nel contrasto agli illeciti economico-finanziari perpetrati per via telematica;
- il Nucleo Speciale per la Radiodiffusione e l'Editoria, collabora con l'Autorità per la Garanzia nelle Comunicazioni, assicurando l'esecuzione e la direzione operativa delle attività di accertamento delle violazioni alla normativa in materia di radiodiffusione ed editoria;
- il Nucleo Speciale Tutela Mercati, presidia il segmento del mercato dei beni e dei servizi, svolgendo funzioni di analisi, progettazione ed esecuzione diretta del servizio. Assicura il corretto funzionamento delle relazioni economiche, a tutela dei consumatori e delle imprese, attraverso la prevenzione e la repressione dei reati che le possono compromettere (contraffazioni, frodi, ecc.) ed il supporto alle Autorità indipendenti (Autorità Garante della Concorrenza e del Mercato, Autorità per i Lavori Pubblici e per l'Energia e il Gas).

Infine, il Reparto Tecnico Logistico e Amministrativo dei Reparti, assicura il soddisfacimento delle esigenze di funzionamento e generali di caserma, nonché la gestione delle attività logistico-amministrative a favore dei reparti costituenti il comparto "speciale".

Proprio con riferimento all'azione di contrasto ai crimini informatici, nell'ultimo biennio, si è reso necessario uno specifico potenziamento organizzativo. Il Corpo ha pertanto rinforzato le proprie capacità operative nel comparto informatico, favorendo nell'ambito delle unità territoriali e delle varie componenti dei reparti speciali la costituzione, presso i Nuclei di Polizia Tributaria in sedi di Procura Distrettuale e presso i più impegnati Nuclei Speciali, di apposite articolazioni dedicate ai compiti di *Computer Forensics* e *Data Analysis*, cui sono stati assegnati militari avviati a specifici corsi di formazione che vengono annualmente tenuti presso la Scuola di Polizia Tributaria.

Questa rete di specialisti è in coordinamento funzionale con il rinnovato Nucleo Speciale Frodi Tecnologiche, secondo una logica che, con riferimento a indagini caratterizzate da elevato spessore tecnologico, multidistrettualità e/o sopranazionalità, pone quest'ultimo come punto di riferimento dei terminali sul territorio per quanto concerne il contrasto dei crimini informatici.

La consapevolezza dell'esistenza di gravi minacce derivanti dall'utilizzo illegale delle nuove tecnologie ha evidenziato la necessità di rafforzare il contrasto a conseguenti fenomenologie criminali in continua evoluzione. Tali fenomenologie interessano soprattutto le reti telematiche, in particolare la rete mondiale Internet, da cui l'economia nazionale ed europea dipendono fortemente e sulle quali sono compiuti illeciti il cui contrasto rientra a pieno diritto nella missione istituzionale della Guardia di Finanza quale polizia economica e finanziaria.

In particolare, l'adeguamento della struttura ordinativa del Nucleo Speciale Frodi Tecnologiche permette di:

- perseguire una maggiore efficacia dell'azione svolta dal Reparto valorizzandone la connotazione specialistica nel settore dell'innovazione tecnologica;
- potenziare la capacità di analisi dei fenomeni criminali, nonché il supporto tecnico-logistico ai

reparti territoriali impegnati nell'esecuzione di investigazioni per cui è necessario il possesso di particolari competenze nel campo informatico;
- conferire, in considerazione dei peculiari compiti istituzionali affidati al Corpo, una più incisiva propensione operativa del Reparto, avuto particolare riguardo ai contesti caratterizzati da più elevata complessità e/o sovranazionalità.

Il Nucleo, in luogo della precedente strutturazione in due sezioni operative, prevede ora, infatti, la presenza dei seguenti tre Gruppi ciascuno con due sezioni operative:
- il I, deputato a effettuare il monitoraggio della rete ai fini dello sviluppo e per l'avvio di attività operative anche da parte di altri reparti del Corpo in caso di reperimento di indizi sintomatici di illeciti economico-finanziari realizzati via web. L'articolazione svolge, altresì, attività di analisi operativa pianificando specifici progetti nei settori di competenza;
- il II, incaricato dell'ideazione, organizzazione ed esecuzione diretta di investigazioni nei settori di competenza istituzionale, nonché di fornire supporto tecnico-logistico ai reparti del Corpo impegnati sul territorio in investigazioni che richiedano, per la particolare delicatezza e rilevanza, il possesso di specifiche competenze nel campo informatico;
- il III, rivolto allo sviluppo di sistemi tecnologici e applicativi informatici di ausilio alle indagini, nonché allo studio e all'individuazione di metodologie operative maggiormente efficaci e, in quanto tali uniformemente applicabili in ambito nazionale. A tal fine, intrattiene le necessarie-relazioni istituzionali.

Ciò, in virtù del dinamismo fatto registrare dai fenomeni illeciti compiuti attraverso le tecnologie e la rete telematica mondiale e con diretto riguardo all'incidenza che questi hanno sui distinti segmenti della missione di polizia economico-finanziaria che l'ordinamento affida alla Guardia di Finanza in ambito nazionale e comunitario.
Al reparto sono quindi attribuiti compiti operativi, di supporto, di analisi, di studio e di formazione, nonché responsabilità nelle relazioni istituzionali di tipo operativo in tutti i settori di intervento rimessi alla competenza del Corpo dal Decreto Pisanu del 2006. Ci si riferisce, in particolare, alla tutela dei movimenti dei capitali e dei mezzi di pagamento; alla sicurezza della circolazione dell'euro; alla salvaguardia dei marchi, dei brevetti e della proprietà intellettuale, oltre che ai tipici comparti di polizia finanziaria quali quelli dell'evasione fiscale nel commercio elettronico e quello dei giochi e delle scommesse on line.

3. Economia digitale e linee di tendenza

Nel 2012 nel nostro Paese gli utenti *Internet* attivi sono stati circa 29 milioni e a dominare la scena sono stati proprio i dispositivi mobili. Questo è il fenomeno con cui ci dovremo confrontare.
Ciò è dimostrato anche dal fatto che, nell'anno passato, per la prima volta, nell'ultimo decennio, il mercato del PC ha chiuso in negativo, con un calo dell'1,2% sul 2011. È recentissima la notizia che vede, nei primi tre mesi del 2013, il fatturato di un grande produttore americano di PC (*Dell*) diminuire del 2%, mentre le vendite di quei dispositivi sono scese, nello stesso periodo, del 9%.
La ricerca sui "*Mercati Digitali Consumer e Nuova Internet*" presentata allo SMAU 2012 dalla *School of Management* del Politecnico di Milano, ha, inoltre, evidenziato come la diffusione di *Smartphone*,

Tablet e *Internet* TV esploderà nel corso dei prossimi 3 anni. Nel 2012, sul mercato italiano, sono, infatti, stati censiti, oltre 32 milioni di *Smartphone*, 2,9 milioni di *Tablet* e 2,5 milioni di *Internet* Tv, che cresceranno, secondo le stime, rispettivamente, a quasi 50 milioni, 12 milioni e 11 milioni entro il 2015.

Dovrà, inoltre, considerarsi che le nuove generazioni saranno sempre più attive sulla rete. Un recentissimo studio commissionato da *Eurispes* per il 2012 dimostra come, oggi, oltre il 23% dei ragazzi fra gli 8 ed i 12 anni naviga in Internet per un'ora al giorno, il 32% addirittura per circa 2 ore ed il 23% per oltre due ore al giorno. Ciò in misura sempre maggiore attraverso *smartphones* e *tablet* che sono nella loro disponibilità in maniera massiccia già a partire dai 9 anni di età.

Circa la vulnerabilità di questi sistemi mobili, è possibile attendersi che attraverso tali dispositivi potranno essere realizzati attacchi sempre più sofisticati ed aggressivi, dal momento che oltre ad avere ormai potenza di calcolo e di connettività di tutto rilievo, nella maggior parte dei casi non dispongono di protezioni *anti-malware* efficaci, anzi, spesso, sono gli stessi utenti a manometterli per sbloccarne alcune funzionalità avanzate, rendendoli ancora più vulnerabili.

Quasi sempre sono vissuti dagli utilizzatori come semplici "*gadget*", invece, consentono agli attaccanti di sfruttarne le avanzate caratteristiche peculiari (geolocalizzazione sopra tutte) per compiere nuovi tipi di crimini, anche molto insidiosi. In questo contesto, è opportuno sottolineare come l'elevata diffusione di tali *device*, tra i giovani ed i giovanissimi, porterà inevitabilmente ad un aumento dei reati perpetrati contro questa fascia di popolazione.

La portabilità e la comodità proprie di questi oggetti renderanno, inoltre, sempre più diffusi i casi di "*dual use*", cioè di utilizzo ibrido dello stesso dispositivo, tipicamente in ambito privato e *business*, introducendo vulnerabilità nuove e particolarmente complesse da gestire all'interno delle organizzazioni di tipo imprenditoriale e, di conseguenza, nelle relazioni di tipo economico.

Va aggiunto, poi, che il processo di educazione digitale dei cittadini appare ancora difficoltoso, lo stesso non si può dire per i *Cyber* criminali che escogitano, invece, metodi di offesa sempre più sofisticati ed aggressivi, in grado di influenzare i comportamenti degli utenti anche dal punto di vista psicologico, con danni apprezzabili per l'*Internet economy* nazionale.

Un esempio emblematico di come queste forme di criminalità possano influenzare il comportamento degli utenti è rappresentato dal virus conosciuto come "*ransomware*" apparso, anche nel nostro Paese, da oltre un paio di anni e capace di ingannare l'utente facendogli credere di essere incappato in un falso sequestro, da remoto, del PC da parte della Guardia di Finanza o di altra Forza di Polizia, a causa della presenza sullo stesso di contenuti illeciti a carattere osceno. Ovviamente, i finti agenti di Polizia, si premurano di rappresentare come con il pagamento, rigorosamente *on line*, di una "multa" possa essere risolto il problema evitando guai di natura giudiziaria.

Un attacco di questa natura, nei cui confronti, di recente, grazie alla cooperazione internazionale coordinata da Europol, è stata data una prima, importante, risposta, basato su una frode che, in linea teorica, sarebbe facilmente individuabile, dimostra, considerato l'alto numero di vittime coinvolte, come l'utilizzo di fattori offensivi, che fanno leva su vulnerabilità di tipo tecnologico, ma soprattutto culturali ed emotive dell'utente, possa produrre effetti dissuasivi importanti circa l'utilizzo dei servizi offerti dall'online, con ricadute negative sulla crescita dell'economia digitale, settore del quale, nelle generali condizioni di sofferenza della crescita in cui ci troviamo, non si può fare certamente a meno.

L'osservazione della realtà esterna ci permette, inoltre, di osservare come le più recenti sfide del

crimine informatico siano rivolte anche al mondo dei *Social Network*, che spingono l'utente ad esporre eccessivamente la propria identità digitale. Tale rischio aumenta in maniera esponenziale nei confronti degli utilizzatori di dispositivi mobili, posto che è più difficile distinguere una pagina *web* contraffatta su uno schermo di ridotte dimensioni.
Tutte le citate criticità sono acuite da specifici fattori, quali:

- la generale mancanza di *know-how* in materia di *Internet Technology* da parte dei responsabili aziendali;
- la bassissima consapevolezza degli utenti finali;
- la altrettanto bassa sicurezza intrinseca dei dispositivi mobili, che sono, ancora oggi, meno maturi dei PC e più difficilmente riconducibili all'interno delle *policy* e dei sistemi di controllo esistenti.

Un cenno, per l'importanza che riveste sotto vari profili, va fatto sulla necessità di incrementare in Italia, l'utilizzo dei mezzi di pagamento alternativi al contante. Ci si riferisce all'introduzione su larga scala di tecnologie che, già presenti in molti altri Paesi occidentali, consentono agli utenti di effettuare micropagamenti tramite dispositivi portatili.
Parliamo, nello specifico, della tecnologia NCF (*Near Field Communication*) che, applicata su telefonini e *tablet*, serve per effettuare piccoli pagamenti, definiti di prossimità, facendo passare il dispositivo a pochi centimetri di distanza dalla strumentazione abilitata. È, quindi, molto utile per pagare, ad esempio, il biglietto dei mezzi di trasporto pubblici.
Al momento i POS abilitati in Italia a ricevere pagamenti via NFC, che è attivo sui sistemi *Android*, sono solo il 10%, circa 170 mila su 1,7 milioni di apparati, anche se è in corso un piano di sostituzione dei vecchi POS con quelli di nuova generazione.
Rimanendo nella stessa categoria di applicativi, *Apple* e *Google* hanno puntato, invece, sulle applicazioni *wallet*, un portafoglio virtuale nel quale si registrano i dati delle proprie carte di credito che viene utilizzato al momento di pagare selezionando un'apposita *app*.
Esiste, poi, la possibilità di effettuare il pagamento soltanto fotografando il *QR*, un codice a barre leggibile da uno *smartphone*, oppure digitando sul telefonino un codice indicato dal POS del negoziante.
Alcune aziende offrono, infine, al cliente, al momento del pagamento on line, la possibilità di premere un tasto cd. "*My Bank*" per accedere, immediatamente, al proprio *home-banking* abituale e confermare l'acquisto in modo automatico inserendo le proprie *password*. Le maggiori banche italiane hanno previsto di fornire tale soluzione a imprese, Enti pubblici e clienti privati, in tutta Italia, già a partire dal 2013, anche per pagamenti in Europa.
Da ultimo, un cenno al cd. *Cloud*, servizio estremamente utile per l'utenza, poiché consente di disporre di banda e capacità di calcolo potenzialmente illimitate, rispetto al quale, però, al momento, dal punto di vista dell'*Enforcement*, non è possibile incidere concretamente nel caso in cui lo stesso venga utilizzato per massimizzare l'impatto della diffusione di *malware*, ovvero per ospitare, in maniera sicura materiale illegale.
Lo strumento Internet, come tutte le tecnologie innovative, è, comunque, una realtà incontestabile in termini di progresso e di democrazia. Basti pensare, ad esempio, alla quantità di informazioni che oggi troviamo liberamente sulla rete, anche di carattere giuridico, tecnico, societario, finanziario etc. etc.. La ricerca di queste informazioni fino ai primi anni '90 impegnava molta parte del nostro tempo ed era anche molto costosa visto che comportava l'impiego di maggiori risorse

umane e finanziarie. Un altro innegabile vantaggio si ritrova nella estrema facilità di comunicare e scambiarsi, in piena legalità, notizie, documenti o immagini. Come sempre, quindi, la patologia risiede nell'utilizzo illegale della tecnologia e non nelle capacità che questa ci offre.
Internet come fonte aperta rappresenta, inoltre, un'opportunità per gli Organismi di *Law Enforcement*, non sono rari, infatti, i casi investigativi risolti attraverso elementi trovati sulla rete.
Internet e la tecnologia possono, quindi, essere un formidabile ausilio per combattere i fenomeni criminali che infestano la Rete, a patto che, tra gli attori che operano nella legalità e per la legalità, si mantengano strette forme di collaborazione e cooperazione.
Ecco perché il Corpo, come ho già detto, ha tenuto, da sempre, una linea di collaborazione con le Istituzioni nazionali che hanno compiti di controllo, regolamentazione e prevenzione, tra le quali le *Autority* di riferimento, oltreché con le maggiori associazioni di categoria, come testimoniato dai numerosi Protocolli d'intesa in atto.
I Reparti del Corpo si avvalgono, così, nell'ambito della loro azione di ricerca, prevenzione e repressione degli illeciti di polizia economico/finanziaria commessi nel mondo virtuale, ovvero attraverso le nuove tecnologie, della conoscenza "dall'interno" che su tali fenomeni hanno i soggetti che operano istituzionalmente nel settore a tutela dei cittadini, delle imprese e dell'economia nazionale ed europea.
Dalla seconda metà dei primi anni duemila, il tema della *cyber-security* anche in campo economico ha acquisito una rilevanza crescente per l'Unione Europea. Non poteva essere diversamente, se si pensa che l'economia digitale europea ammonta, oggi, a oltre 500 miliardi di euro all'anno. Ne è dimostrazione, tra l'altro, il dinamismo delle Istituzioni europee, a vari livelli. Basti citare, sul punto, la costituzione nel 2004 dell'Agenzia Europea per la Sicurezza delle Reti e dell'Informazione (*European Network and Information Security Agency*, ENISA), la recente nascita dello *European Cybercrime Centre*, ovvero l'attenzione che OLAF, Europol e Commissione Europea (ove insiste anche, nell'Ufficio per l'Armonizzazione del Mercato Interno, l'Osservatorio Europeo sulle violazioni dei diritti di proprietà intellettuale) hanno messo sulla sicurezza economica e finanziaria delle imprese, dei cittadini e delle Pubbliche Amministrazioni.
In campo economico/finanziario gli interessi del *cyber-crime* sono, particolarmente, elevati verso settori quali le frodi bancarie, il furto di identità e di informazioni, la contraffazione, l'evasione fiscale sul commercio elettronico, la pirateria digitale ed i giochi e le scommesse *on line*. Ciò provoca danni patrimoniali ingenti ai privati in termini di minore occupazione, alle aziende minandone la capacità reddituale ed all'economia pubblica riducendo la base imponibile delle imposte dirette e indirette e, quindi, il gettito fiscale complessivo del Paese.
Quanto all'impatto del *cybercrime* sull'economia digitale, una ricerca *Norton* del 2012 valuta in 2.45 miliardi di euro il costo dei crimini informatici contro gli utenti *consumer* in Italia. Rispetto allo scorso anno, in linea con il forte sviluppo dei nuovi settori digitali, sono in aumento i casi associati ai *social network* e ai dispositivi mobili, mentre è diminuito il costo per ogni vittima (complessivamente sarebbero circa 9 milioni le persone colpite dal crimine informatico, su un totale di 28 milioni di utenti attivi in Italia).
Anche all'interno del mondo delle imprese l'argomento digitalizzazione, negli ultimi anni ha assunto un'importanza crescente. Esso rappresenta, infatti, da un lato un fattore fondamentale per aiutare la crescita delle aziende, dall'altro un possibile vantaggio nell'implementare strategie competitive, determinanti per oltrepassare questo periodo di stallo dell'economia europea, quali,

ad esempio, processi di riorganizzazione aziendale e di internazionalizzazione.
L'innovazione costituisce, infatti, un volano per superare il rallentamento dell'economia, creando nuove opportunità di occupazione, incrementando la crescita e le esportazioni (soprattutto grazie alla diffusione dell'*e-commerce*), fino ad influenzare positivamente la misura del PIL dell'intera Nazione.
Nel panorama europeo l'Italia si pone oggi come Paese inseguitore, con un ruolo dell'economia digitale ancora inferiore rispetto ad altre nazioni, quali Svezia, Gran Bretagna, Francia e Germania. Tuttavia il ruolo delle ICT nel nostro Paese è in espansione e, soprattutto, ripeto, rappresenta una via obbligata per la crescita, grazie alle enormi opportunità offerte da Internet per famiglie, imprese e Pubblica Amministrazione.
In Italia gli utenti attivi in ambito di *e-commerce* nel 2012 sono stati circa 28 milioni, il 9,2% in più rispetto al 2011. L'*audience online* nel giorno medio registra una crescita del 7,3%, con 13,8 milioni di utenti attivi. Il fatturato delle vendite online in Italia ha raggiunto complessivamente 11 miliardi di euro nel 2012[1]. Bisogna sottolineare, inoltre, come, sebbene, questo fenomeno abbia investito tutti i settori, un particolare impatto si sia avuto su abbigliamento, alimentare e turismo.
Nel 2009 il valore a livello mondiale dell'economia digitale poteva essere stimato, secondo *McKinsey*[2], in circa 1.672 miliardi di dollari, pari al 2,9% del PIL mondiale2. L'incidenza dell'economia digitale varia, tuttavia, significativamente a seconda dei Paesi considerati: negli Stati Uniti contava in quell'anno per il 3,8% del PIL, in Giappone per il 4%, in Cina per il 2,6%. In Europa, le quote appaiono comprese tra il 6,3% della Svezia e l'1,7% dell'Italia.
Malgrado l'impatto economico della digitalizzazione risulti ancora non elevato nel nostro Paese, le cifre sono in crescita: infatti, stime riferite al 2011, a cura di *Boston Consulting Group*, indicano in circa 32 miliardi di euro il valore dell'economia digitale in Italia, con un peso sul PIL pari al 2,5%. A parità di condizioni in termini di consumi privati, investimenti e spesa istituzionale, l'*Internet economy* varrà 59 miliardi di euro nel 2015, con un peso sul PIL pari al 3,3%, e una crescita media annua del 13% rispetto al 2009.
Sul punto l'Agenzia Digitale Italiana, ritiene che economia digitale ed *e-commerce* rappresentino delle leve di creazione di valore per il Paese sotto quattro fondamentali profili: il contributo alla crescita del PIL, la creazione di posti di lavoro, l'impulso alla crescita delle imprese ed il surplus di valore per i consumatori.
Di conseguenza, se da un lato il confronto con le altre economie avanzate evidenzia lo stato di arretratezza dell'Italia sul fronte della digitalizzazione, dall'altro tale arretratezza suggerisce come vi sia un ampio margine di miglioramento per la diffusione dell'internet economy nel nostro Paese

[1] Dati esposti nel rapporto "osservatori.net" del Politecnico di Milano.

[2] McKinsey Global Institute (2011), "Internet matters: The Net's sweeping impact on growth, jobs and prosperity". Lo studio prende in considerazione in particolare le 13 economie più importanti al mondo: Svezia, Germania, Regno Unito, Francia, Stati Uniti, Corea del Sud, Canada, Italia, Giappone, India, Cina, Brasile, Russia.

4. Esperienze operative

Entrando nel vivo dell'argomento, va innanzitutto ricordato come l'affacciarsi delle nuove tecnologie, da almeno due decenni, abbia consentito alle organizzazioni criminali di realizzare ulteriori ingenti profitti illeciti. I fenomeni relativi hanno ormai assunto dimensioni di rilievo anche sotto l'aspetto digitale.

Dovendo, anche per esigenze di spazio, limitare l'analisi delle esperienze sul campo si è scelto di fare riferimento, in particolare, a due contesti operativi molto sensibili, quali quelli della pirateria digitale e quello del "*gambling on line*" illegale che destano l'interesse delle organizzazioni criminali in considerazione dei forti profitti illeciti garantiti a fronte di investimenti in tecnologie e risorse.

Riguardo al primo ambito, dall'osservazione del contesto esterno di riferimento è emerso chiaro come le metodologie utilizzate per immettere in consumo contenuti digitali in violazione alle norme sul Diritto d'autore stiano gradualmente mutando. Infatti, secondo le informazioni fornite dalle maggiori associazioni di categoria, anche a livello internazionale, le abitudini dei cosiddetti «pirati» si stanno spostando dai tipici *peer to peer* o *Torrent* verso altre metodologie, ad esempio quella del *cyberlocker*, che non comporta una condivisione immediata dei *files*, essendo invece un servizio di archiviazione su Internet appositamente progettato per caricare contenuti che possono, poi, essere scaricati da altri utenti per mezzo di un indirizzo *web*.

Tale evoluzione, in un'ottica di forze di polizia, potrebbe in parte ascriversi alle numerose operazioni di polizia giudiziaria realizzate che hanno certamente determinato un effetto di deterrenza o quanto meno di freno verso i comportamenti illeciti, posto che diversi fra i più frequentati siti del nostro Paese sono stati fatti oggetto di specifiche azioni.

A prescindere dall'applicativo utilizzato per effettuare la condivisione di *files,* ancora oggi è possibile rendersi praticamente anonimi utilizzando particolari tecniche[3]. Si tratta comunque di modalità veramente efficaci soltanto quando si trasmettono *files* poco "pesanti" poiché il passaggio attraverso queste strettoie informatiche comporta un rallentamento dei flussi telematici.

Prima di ripercorrere le particolarità delle attività maggiormente significative dei nostri reparti, intendiamo ricordare come la Cassazione, a fattor comune, con la sentenza n. 49437 del 2009, abbia chiarito alcuni aspetti fondamentali per l'operatività in materia, colmando alcune delle difficoltà interpretative della disciplina vigente nel comparto. Ci si riferisce alle tematiche della responsabilità del sito *web* che mette in comunicazione gli utenti, i quali commettono l'illecito con l'attività di *uploading* e a quella della territorialità.

Riguardo alla prima, è stato chiarito che il titolare del sito *web* potrebbe essere considerato estraneo all'attività delittuosa solo se si limitasse a mettere a disposizione il protocollo di comunicazione, quale ad esempio quello *peer to peer,* per consentire la condivisione di *files* contenenti l'opera coperta da Diritto d'autore. Se, però, il titolare del sito non si limita a ciò, ma fa qualcosa di più, ossia indicizza le informazioni che gli vengono dagli utenti, che sono tutti potenziali autori di *uploading*, sicché queste informazioni (anche se ridotte al minimo, ma pur sempre essenziali perché gli utenti possano orientarsi chiedendo il *downloading* di quell'opera piuttosto che un'altra) sono in tal modo

[3] Servendosi di browser di navigazione con funzionalità di tipo *Tor* o, in buona sostanza, dei c.d. *server proxy* che con una serie di salti consentono di acquisire il proprio obiettivo nascondendosi dietro l'indirizzo IP (numero che identifica l'accesso di un computer sulla rete in un determinato momento) dell'ultimo *server proxy* utilizzato.

elaborate e rese disponibili nel sito stesso (ad esempio a mezzo di un motore di ricerca o con delle liste indicizzate), il sito cessa di essere un mero corriere che organizza il trasporto dei dati. C'è un *quid pluris*, in quanto viene resa disponibile all'utenza del sito anche un'indicizzazione costantemente aggiornata, che consente di percepire il contenuto dei *files* suscettibili di trasferimento. A quel punto l'attività di trasporto dei file si caratterizza come trasporto di dati contenenti materiale coperto da Diritto d'autore. Ed allora è vero che lo scambio di file avviene da utente ad utente, ma l'attività del sito web è quella che consente ciò e pertanto c'è un apporto causale a tale condotta che ben può essere inquadrato nella partecipazione imputabile a titolo di concorso di persone.

Quanto alla tematica della territorialità, la Cassazione ha confermato come la circostanza che l'*hardware* del sito non sia in Italia non esclude la giurisdizione del giudice penale nazionale, in ragione del disposto dell'articolo 6 del Codice Penale. Infatti, il reato di diffusione in rete dell'opera coperta da Diritto d'autore si perfeziona con la messa a disposizione dell'opera in favore dell'utente finale. Se si considerano gli utenti nel territorio dello Stato che accedono tramite *provider* ai vari siti e scaricano da altri utenti non localizzati opere coperte da Diritto d'autore, la condotta penalmente illecita di messa a disposizione in rete dell'opera stessa si perfeziona nel momento in cui l'utente in Italia riceve il *file* o i *files* che contengono l'opera. Quindi, pur essendo sopranazionale l'attività di trasmissione di dati a mezzo della rete Internet, vi è comunque nella fattispecie una parte dell'azione penalmente rilevante che avviene nel territorio dello Stato, ciò consentendo di considerare come commesso nel territorio dello Stato il reato di diffusione non autorizzata di opere coperte da diritto d'autore, limitatamente agli utenti in Italia.

I tre esempi di investigazione che abbiamo selezionato fanno riferimento ad attività condotte rispettivamente dai Nuclei di Polizia Tributaria di Bergamo e Cagliari e dalla compagnia di Agropoli e consentono una riflessione graduale e distintamente interessante sullo stato del diritto e della giurisprudenza nel contrasto al fenomeno della pirateria digitale *on line* nel nostro Paese.

Il primo esempio, assai articolato, concerne un'indagine del Nucleo di Polizia Tributaria di Bergamo, convenzionalmente denominata «*Pirate Bay*» dal nome del sito colpito, sviluppata tra il 2008 e il 2010. L'*input* iniziale è scaturito da una querela sporta dalla Federazione contro la Pirateria Musicale (FPM) a carico dei gestori del sito, attivo nello scambio di *files on line* con il sistema dei *torrents,* che ha avuto un picco massimo di 3 milioni di utenti connessi che scambiavano oltre 500 mila collezioni composte da svariati album musicali. Nello specifico, le attività di polizia giudiziaria del reparto hanno portato alla denuncia di undici soggetti, di cui quattro stranieri, per aver immesso a fine di lucro in Internet opere tutelate dal diritto d'autore. Nei confronti dei quattro soggetti, di nazionalità svedese, la Corte distrettuale di Stoccolma, il 31 gennaio 2008, ha a sua volta avviato un procedimento per violazione al Diritto d'autore, giunto alla condanna anche in secondo grado. Sotto il profilo giudiziario, la vicenda è risultata particolarmente interessante, in quanto il sequestro preventivo emesso dal Gip di Bergamo nell'agosto del 2008 - ai sensi dell'articolo 321 del Codice di Procedura Penale, anche a mente degli articoli 14 e 15 del Decreto Legislativo n. 70/2003 sul commercio elettronico, teso a far cessare la violazione del Diritto d'autore, veniva annullato nel successivo mese di ottobre dal Tribunale della città orobica e quindi definitivamente confermato con la citata sentenza della Suprema Corte del settembre 2009, che ha osservato come in realtà il provvedimento emesso dal Gip altro non fosse se non l'espressione di un potere inibitorio dell'autorità giudiziaria penale, contenente un ordine ai *providers* di precludere l'accesso alla rete informatica al solo fine di impedire la prosecuzione della perpetrazione del reato di cui all'articolo

171-*ter* comma 2, lett. a-bis.

Nello stesso filone, l'operazione denominata «*Colombo*», condotta sempre dal Nucleo di Polizia Tributaria di Bergamo, ha manifestato una particolarità, consistente nel fatto che il sito investigato non presentava *banners* pubblicitari, ma raccoglieva soltanto donazioni, allo scopo dichiarato di poter sostenere le spese di mantenimento del dominio e dell'infrastruttura che lo ospitava. Le indagini effettuate hanno consentito in questo caso di segnalare all'autorità giudiziaria cinque soggetti italiani che si sono serviti di false identità e di imprese di facciata per introitare i proventi illeciti, nonché di sottoporre a sequestro i conti correnti utilizzati per canalizzare i guadagni.

Il secondo caso, sviluppato dal Nucleo di Polizia Tributaria di Cagliari, riguarda l'operazione «*Last Paradise*» che ha interessato uno dei più grandi siti mondiali del falso multimediale, con circa 10 milioni di *torrents* attivi ed oltre 3 milioni di visite giornaliere da tutto il mondo. L'Italia era il terzo Paese per provenienza di utenti, alle spalle solo di India e Stati Uniti. Centinaia di migliaia di italiani accedevano, anche tramite i più noti motori di ricerca e *social network*, direttamente ai vari indirizzi IP senza alcun obbligo di registrazione e identificazione, e usavano regolarmente ogni giorno la piattaforma per scaricare in altissima definizione e qualità digitale musica, film, videogiochi e *software*. Il portale in questione aveva acquisito anche la fetta di mercato lasciata libera da un analogo sito, *BTJunkie*, già coinvolto in una precedente operazione, nell'ambito della quale era emerso tra l'altro come i gestori del sito avessero incassato, grazie ai numerosi *banners* pubblicitari presenti, guadagni per circa 3,5 milioni di euro l'anno. Il portale ospitava numerosi *banners* pubblicitari, producendo guadagni per i gestori, a livello mondiale, stimati in oltre 8,5 milioni di dollari all'anno.

In questa vicenda, successiva all'esperienza di Bergamo, si è intervenuti direttamente con l'ordine di inibizione emanato dal Pubblico Ministero titolare del procedimento penale, ai sensi degli articoli 14 e seguenti del Decreto Legislativo n. 70/2003. Si tratta di una scelta innovativa poggiata sulla norma di recepimento nel nostro ordinamento della Direttiva sul commercio elettronico, che prevede la possibilità per l'Autorità Giudiziaria o quella Amministrativa competente di "esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse".

In altre parole, il PM, ritenuto - sulla base di quanto emerso in sede di indagine – "concreto, attuale e consistente" il pericolo di reiterazione delle attività delittuose in materia di diritto d'autore, ha ordinato ai fornitori di servizi Internet e segnatamente a quelli operanti sul territorio dello Stato italiano, l'inibizione agli utenti ad accedere ai siti web identificati dallo specifico dominio e dal numero IP ad esso associato.

Si tratta, senza dubbio, di una soluzione all'avanguardia, che pur non essendosi ancora misurata sul piano della prassi giudiziaria (non risultano allo stato decisioni su eventuali ricorsi presentati in Cassazione) appare, nel concreto, la più efficace sul piano tecnico-giuridico, in quanto capace di impedire che i reati della specie vengano perpetuati, evitando un'irreparabile e gravissima compromissione del bene giuridico tutelato.

La terza operazione condotta dai finanzieri della compagnia di Agropoli ha portato alla custodia cautelare in carcere nei confronti di un soggetto conosciuto sulla rete con il *nickname* di «*Tex Willer*», al termine delle indagini scaturite dal sequestro, nel mese di novembre 2011, di cinque siti *web* appartenenti al *network* illegale *Italianshare*, con circa 300 mila utenti iscritti e 550 mila accessi mensili. Il catalogo era molto vasto, comprendendo prodotti cinematografici, libri e riviste, serie

tv, cartoni animati, videogiochi, *software* e musica. I siti appartenenti al *network* si presentavano come *forum*, finalizzati alla raccolta, indicizzazione e diffusione di materiale tutelato mediante diverse modalità che andavano dal classico *link* ai cosiddetti *cyberlockers*, alla fruizione in *streaming* di palinsesti e contenuti cinematografici o musicali, fino alla condivisione di collegamenti utili alle piattaforme *peer to peer* e *torrent*.

Rispetto alle vicende precedenti, quella in trattazione manifesta delle interessanti particolarità sotto il profilo tecnico e un elevato livello di trasversalità, essendo stati sviluppati contestualmente aspetti relativi alla violazione del diritto d'autore, tematiche connesse con la violazione della *privacy* e fenomeni di evasione fiscale.

Nello specifico, sotto il primo profilo va evidenziato come oltre all'inibizione dei siti *web*, operata attraverso la notifica a *Internet Service Provider* di un Decreto di sequestro preventivo disposto dal Gip di Vallo della Lucania - la cui efficacia è stata confermata dal tribunale del riesame di Salerno - è stato possibile, con la collaborazione del principale indagato, «scaricare» letteralmente l'intero contenuto dei siti, attuando fisicamente la misura ablativa sugli *hard disks* ottenuti. In questo modo si è reso, quindi, impossibile, anche interrogando DNS stranieri, ovvero utilizzando dei *server proxy*, raggiungere a livello planetario i siti inibiti.

Sotto il secondo aspetto, le indagini condotte hanno fatto emergere l'intero sistema messo in piedi dall'indagato che, nel corso del 2011, aveva venduto dietro compenso a diverse imprese operanti nel settore pubblicitario il *database* di utenti iscritti ai siti pirata, mettendo a disposizione i dati forniti in sede di registrazione, le *e-mail* e gli indirizzi IP dei 300 mila utilizzatori del *network* illegale, senza aver preventivamente acquisito il loro consenso e in violazione alle disposizioni previste a tutela della *privacy*.

Le indagini finanziarie svolte in Italia e all'estero nonché le attività investigative eseguite presso nove imprese clienti localizzate su tutto il territorio nazionale, hanno poi permesso di ricostruire minuziosamente il volume d'affari sviluppato dal 2007 al 2011, consentendo l'individuazione di basi imponibili non dichiarate per 700 mila euro e di IVA dovuta per circa 100 mila euro.

Il tema dei profitti illeciti è ricorrente. Sempre nel 2012, infatti, nell'ambito di un'operazione antipirateria scaturita dalla denuncia dei responsabili della Eagle Pictures SpA, la Guardia di Finanza di Milano ha stabilito che i gestori dei siti *web ItaliaFilm* e *Locandinehits*, grazie alla pubblicazione di *banners* pubblicitari, avevano avuto un guadagno superiore ai 3.500 dollari giornalieri, una cifra che supera gli 1,2 milioni di dollari in un anno.

La fantasia dei frodatori non ha però limiti: nel 2009, nell'ambito dell'operazione denominata «*Jackal*», la nostra compagnia di Melegnano ha denunciato tre persone per aver scaricato e venduto *on line* illegalmente il brano «Domani», registrato dai più noti cantanti italiani per raccogliere fondi per la ricostruzione in Abruzzo.

Con l'operazione «*Inedito*» del 2011, la Guardia di finanza di Milano ha denunciato due soggetti che avevano messo in condivisione *on line* tre brani ancora inediti di una nota artista italiana. È recentissima, infine, l'operazione della Guardia di finanza di Novara denominata «*Music in black*».

Nell'occasione il reparto, dopo un controllo di *routine* nei confronti di un esercizio commerciale, essendo emerse incongruenze sul servizio relativo alla fornitura personalizzata di contenuti audio diffusi nel negozio, ha esteso gli accertamenti anche nei confronti del cosiddetto *music service provider*. L'attività ha consentito di scoprire come quest'ultimo, che aveva oltre 300 clienti, cui metteva illecitamente a disposizione più di 400 mila brani tutelati dal diritto d'autore, dichiarasse

alla SIAE e alla Società consortile fonografici, preposta alla raccolta dei cosiddetti diritti connessi alla diffusione di opere in pubblico, appena un decimo dei contenuti musicali diffusi. Il titolare dell'azienda è stato segnalato all'Autorità Giudiziaria per l'ipotesi aggravata prevista dall'articolo 171-*ter* della legge in materia di diritto d'autore e sono stati effettuati sequestri di materiali presso lo stesso e presso tutti i clienti sparsi sul territorio nazionale.

La nostra esperienza sul campo ci porta, quindi, a considerare, da un lato, come l'evoluzione della prassi giudiziaria trovi un essenziale punto di ancoraggio nei princìpi fissati dalla Corte di Cassazione con la citata sentenza del 29 settembre 2009 e, dall'altro, come sia fondamentale affrontare tali fenomeni in un'ottica di trasversalità, posto che gli stessi offendono contestualmente distinti interessi giuridicamente tutelati.

Nel campo della tutela del diritto d'autore, il Corpo opera anche con il Nucleo Speciale per la Radiodiffusione e l'Editoria - anch'esso alle dipendenze del Comando Unità Speciali - che collabora con l'Autorità per le garanzie nelle comunicazioni, assicurando l'esecuzione e la direzione operativa delle attività di accertamento delle violazioni, commesse anche su Internet, alla normativa in materia di radiodiffusione ed editoria.

In relazione, invece, al settore del *Gambling,* per rimanere sull'attualità, si fa riferimento ad un recente servizio della Guardia di Finanza sviluppato nell'ambito dell'operazione "Duemila sesterzi" che ha consentito il sequestro di circa 100 agenzie di gioco e punti scommesse gestite dalla camorra in diverse regioni del territorio nazionale. In coincidenza dell'enorme incremento delle illecite scommesse avvenuto in occasione dell'evento mondiale della *Confederation Cup* 2013, infatti, è stata portata alla luce una vasta rete telematica di scommesse su eventi sportivi di qualsiasi genere, parallela a quella legalmente autorizzata, completamente efficiente e in grado di pagare ingenti somme di denaro anche oltre la soglia prevista antiriciclaggio, senza lasciare apparentemente traccia.

L'operazione ha visto impegnati oltre 300 uomini del Comando Provinciale della Guardia di Finanza di Caserta, dei Reparti Speciali della Guardia di Finanza, del Servizio Centrale Investigazioni Criminalità Organizzata (SCICO) e del Nucleo Speciale Frodi Tecnologiche.

Le indagini per reati di associazione a delinquere finalizzata alla raccolta di scommesse clandestine, sfruttando l'ormai consolidata esperienza giudiziaria della D.D.A. di Napoli, hanno consentito il disvelamento della illecita collaudata rete telematica e organizzativa che, ormai in funzione da qualche anno, è stata completamente mappata grazie all'applicazione di innovative tecniche investigative informatiche, poste in essere dagli specialisti del Nucleo Speciale Frodi Tecnologiche.

La rete abusiva disarticolata, aveva prodotto, nel biennio 2012-2013, un giro di affari di oltre 10 milioni di euro di giocate consentendo lucrosi e soprattutto stabili guadagni all'organizzazione criminale. Inoltre, i gestori del sistema, al fine di aumentare ulteriormente gli illeciti guadagni, all'esito del risultato, attraverso l'alterazione di giocate precedentemente effettuate, simulavano l'esistenza di più vincitori rispetto a quelli reali e riducevano in modo fittizio la consistenza del montepremi visibile sulla rete, in tal modo truffando gli abusivi giocatori risultati effettivamente vincitori.

5. Conclusioni

Negli ultimi tempi abbiamo assistito ad una rapida evoluzione nell'utilizzo delle tecnologie collegate ad Internet che ha prodotto un costante aggiornamento dei modelli di interazione e, conseguentemente, di acquisizione dei servizi e dei beni da parte dei cittadini, delle imprese e delle Pubbliche Amministrazioni, affermando un nuovo modo di vivere, organizzare l'impresa, lavorare e governare la *res publica*.

Siamo di fronte ad una vera e propria esplosione sociale e culturale, oltre che tecnologica, di determinati fenomeni legati all'accesso *on-line* ai servizi.

Non a caso, il 23 gennaio scorso, con apposito Decreto del Presidente del Consiglio dei Ministri, è stato dato avvio ad una strutturata strategia nazionale in materia di sicurezza informatica, anche sotto il profilo economico. Ed anche l'Unione Europea non sta a guardare. Ad *Europol*, come accennato, è stato, infatti, affiancato il Centro europeo di *cybercrime*, l'EC3, che aiuterà gli Stati a combattere i criminali virtuali, anche collaborando con aziende, banche, centri di ricerca e Università.

Il *cybercrime* che, ovviamente, riguarda sia reati "endemici" del *web*, che reati tradizionali, per la realizzazione dei quali i primi ed il *web* sono soltanto uno strumento, sta diventando anche una delle espressioni della criminalità economica.

In questo contesto il Corpo, quale Forza di Polizia specializzata nel settore economico-finanziario, persegue, attraverso i propri reparti, il primario obiettivo di intensificare l'aggressione della ricchezza accumulata indebitamente dalle consorterie criminali che operano nei vari campi di interesse, in quanto costituente il frutto ovvero il reimpiego di proventi di attività illecite.

Tale azione di impulso ha comportato una maggiore reattività delle nostre articolazioni operative che oggi, ogni qual volta da indagini di PG concluse e in corso di svolgimento o dal controllo del territorio emergono indizi di reato costituenti presupposto per l'applicazione di misure ablative, propongono sistematicamente alle locali autorità giudiziarie provvedimenti quali il sequestro preventivo finalizzato alla confisca per equivalente e il sequestro per sproporzione.

Da questo punto di vista, risulta, ad esempio, particolarmente indicativa la circostanza che, nelle sole operazioni di servizio concluse nell'ultimo triennio nei confronti delle organizzazioni delinquenziali coinvolte in traffici di prodotti contraffatti, sono stati sequestrati dal Corpo proventi illeciti per quasi 270 milioni di euro.

Intendiamo, allora, sulla base di queste considerazioni, proporre una riflessione sull'opportunità di dare ancora più concretezza ed efficacia alla disciplina vigente, soprattutto con riguardo agli illeciti guadagni ottenuti, così come nel tempo è avvenuto nella materia della contraffazione, attraverso l'introduzione nel nostro Codice Penale dell'articolo 474-bis ad opera della Legge n. 99 del 2009.

Sul presupposto che i reati informatici a carattere economico/finanziario interessino principalmente piattaforme che solo in minima parte sono riconducibili al territorio nazionale, è d'obbligo un accenno alla tematica della collaborazione. In questo ambito esiste, come sappiamo, una rete giudiziaria attiva a livello europeo e una rete di punti di contatto prevista dalla Convenzione di Budapest sulla criminalità informatica, la cosiddetta 24/7, che consente ad oggi l'invio immediato di richieste di supporto. Quello che andrebbe molto migliorato sono i tempi di risposta che in un mondo quale quello virtuale, caratterizzato dalla volatilità delle informazioni, vanno resi certi ed ineludibili. È quindi necessaria, su questo punto, una netta presa di posizione da parte degli

organismi europei ed internazionali competenti.
Infine, chiudendo con le prospettive a breve, si vuole sottolineare come la Guardia di Finanza stia per mettere a disposizione dei nostri reparti il Sistema Informativo Anticontraffazione (SIAC) che consiste, in estrema sintesi, in una piattaforma tecnologica per le attività di consuntivazione, analisi e monitoraggio in materia di lotta alla contraffazione e alla pirateria.
Tutto ciò non può essere raggiunto se non anche con una continua azione di stimolo ed informazione nei confronti dei giovani. Solo così si potrà, infatti, far crescere nella collettività il senso di responsabilità e la consapevolezza verso i danni che comportamenti sbagliati possono portare ai cittadini, alle imprese, ed all'Erario, in termini di perdita di opportunità di lavoro, minore ricchezza e diminuzione degli introiti fiscali.

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 181-187

Una Specialità della Polizia di Stato che "insegue il futuro"

Antonio Apruzzese e Emanuela Napoli

Abstract: La polizia postale e delle comunicazioni è un reparto specialistico della Polizia di Stato che opera in prima linea nella prevenzione e nel contrasto della criminalità informatica. Tra le sue attività istituzionali vi è tra l'altro quella del contrasto della pedopornografia online, dei crimini informatici, della tutela delle infrastrutture critiche. Attualmente diversi sono i nuovi scenari operativi con i quali la Polizia postale e delle comunicazioni si confronta quotidianamente. Tra questi particolare attenzione merita il fenomeno delle nuove organizzazioni di criminali informatici e quello dei nuovi reati di odio sovente perpetrati attraverso la rete. Per ottenere risultati sempre più concreti in questo settore occorre che accanto all'attività delle Forze di Polizia si diffonda una cultura della legalità in rete, che può essere favorita anche attraverso una nuova idea di commissariato on line, il cui obiettivo principale sia quello di diventare un punto specialistico di riferimento per i frequentatori della rete.

Parole chiave: Servizio Centrale, Centro Nazionale per il Contrasto della Pedopornografia on line, Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

1. L'organizzazione e le competenze

La ragion d'essere della Polizia Postale e delle Comunicazioni si individua nel nuovo scenario epocale che, con l'avvento delle nuove tecnologie, ha reso la rete Internet un mezzo indispensabile per lo scambio di informazioni, l'accesso alle grandi banche dati, l'esecuzione di transazioni e disposizioni finanziarie, l'ideazione e creazione di nuove attività professionali.

La rapida diffusione dell'uso dei nuovi strumenti di comunicazione ha messo in evidenza i punti di debolezza della Rete, soprattutto riguardo alle problematiche di sicurezza.

In tale contesto la Polizia Postale e delle Comunicazioni, reparto specialistico della Polizia di Stato creato con la legge di riforma dell'Amministrazione della Pubblica Sicurezza, opera in prima linea nella prevenzione e nel contrasto della criminalità informatica, a garanzia dei valori costituzionali della segretezza della corrispondenza e della libertà di ogni forma di comunicazione.

Al vertice della struttura, il Servizio Centrale istituito con decreto ministeriale dell' 1 marzo

Articolo pervenuto il 2 ottobre 2013, approvato il 30 dicembre 2013

1998 come organo del Ministero dell'Interno per la sicurezza e la regolarità dei servizi di telecomunicazione e punto di riferimento nel coordinamento, nella programmazione e nella pianificazione operativa degli uffici periferici della specialità.
La sua organizzazione interna ricalca l'ampia tipologia dei fenomeni di criminalità informatica e garantisce, attraverso l'alta professionalità dell'équipe di coordinamento, un'efficace azione di raccordo con gli uffici territoriali.
Il Servizio, cui affluiscono tutte le informazioni rilevanti in materia di *cybercrime*, svolge inoltre azioni mirate:

- nell'analisi della sfera applicativa delle normative in materia di comunicazioni;
- nell'analisi criminologica dei fenomeni criminali legati all'utilizzo di strumenti hi-tech ("*High Tech Crime*");
- nell'individuazione delle strategie di contrasto ai fenomeni criminali generati da sistemi telematici e di elaborazione computerizzata dei dati;
- nella partecipazione a gruppi di lavoro istituiti presso organismi nazionali e internazionali;
- nella selezione e formazione del personale;
- nella collaborazione con il mondo accademico e gli operatori del settore della "*New Economy*";
- nella cooperazione con organi di polizia di Paesi stranieri.

Le diramazioni territoriali della Specialità

La Polizia Postale e delle Comunicazioni è presente in modo capillare sul territorio nazionale attraverso 20 Compartimenti e 80 Sezioni, i cui compiti istituzionali comprendono:

- la prevenzione e repressione dei crimini informatici;
- la tutela dei servizi postali, di bancoposta e di telecomunicazione;
- la prevenzione e repressione dei reati legati al commercio elettronico;
- il raccordo operativo con gli Ispettorati Territoriali del Ministero delle Comunicazioni nelle attività di controllo amministrativo di comune interesse;
- il concorso nel contrasto delle violazioni del diritto d'autore per quanto attiene agli aspetti telematici.

2. Le attività istituzionali

A) Contrasto della Pedopornografia *on line*

L'impegno della Polizia Postale e delle Comunicazioni nel contrasto alla Pedopornografia *on line* ed alle connesse forme di devianza si appalesa ogni giorno più complesso sia per la continua evoluzione delle tecnologie utilizzate per l'occultamento e la diffusione di immagini di abuso sessuale sui minori, sia per le nuove frontiere di rischio che interessano soprattutto le giovani generazioni sempre più diffusamente proiettate nei contesti dei social network.
L'attività di contrasto è sviluppata dalla II Divisione del Servizio Polizia Postale e delle Comunicazioni, all'interno della quale è incardinato il Centro Nazionale per il Contrasto della Pedopornografia *on line*, istituito con la legge n. 38 del 6 febbraio 2006.
Il C.N.C.P.O., oltre a coordinare operativamente l'attività investigativa dei vari uffici territoriali della Specialità, aggiorna costantemente una *black list* di siti con contenuti pedopornografici

collocati su macchine in territorio straniero e quindi sottratte alla diretta giurisdizione dello Stato per impedirne l'accesso dall'Italia.
Il Centro opera altresì in stretto contatto con tutte le realtà istituzionali e sociali operanti nel settore dell'educazione e della tutela dei minori.
In parallelo, anche nell'ambito di progetti europei, sono state avviate procedure di dialogo avanzato con Organizzazioni non governative e mondo dell'industria, per perseguire comuni strategie di contrasto ai fenomeni di rischio della Rete sfruttando avanzati settori di ricerca e di produzione di nuove tecnologie utili alle investigazioni.
All'interno del C.N.C.P.O. opera l'Unità di Analisi dei Crimini Informatici composta da un'equipe di psicologi della Polizia di Stato che, oltre a supportare le attività investigative in materia di pedofilia, è impegnata nell'analisi criminologica dei soggetti autori di reato che frequentano il web, concorrendo a rilevare situazioni di pericolosità in tema di sfruttamento di minori a mezzo internet.

B) Contrasto degli illeciti relativi al commercio elettronico, ai sistemi di pagamento elettronico e ai servizi bancari on line

Il sempre più diffuso ricorso alle vantaggiose forme di commercio elettronico ha visto fiorire una vasta rete di illeciti che impegna la Specialità per contrastare i ricorrenti episodi di frodi nelle transazioni *on line* e nell'utilizzo della moneta elettronica.
Un capitolo a parte meritano gli illeciti nel settore delle carte di credito intorno alle quali è fiorita una vera e propria industria criminale che tende a fare incetta dei preziosi dati e codici di utilizzo delle carte. Dai singoli casi di clonazione ai furti massivi dei riservati codici di utilizzo di intere banche dati, il fenomeno criminale ha finito con l'alimentare un prospero e florido mercato nero agevolmente accessibile nel mondo di internet.
In parallelo sta assumendo dimensioni sempre più vaste il business criminale connesso all'aggressione dei servizi bancari *on line*. Anche in questo caso a fianco di isolati episodi di sottrazione stanno emergendo sempre più frequenti casi di furti massivi di credenziali per l'utilizzo di conti bancari *on line*.
La spiccata pericolosità del fenomeno è connessa non solo alla rilevanza economica degli episodi predatori ma anche e soprattutto al rischio di diffusione incontrollata di sensazioni di insicurezza per l'utilizzo delle nuove tipologie di transazione.
La risposta della Polizia delle Comunicazioni, oltrechè nell'affinamento di sofisticate procedure investigative e nell'avvio di campagne di sensibilizzazione dell'utenza sulle tematiche della sicurezza informatica in genere e dell'utilizzo attento dei sistemi elettronici, è incentrata anche nella realizzazione di mirate strategie di collaborazione con il mondo bancario in generale per mettere a punto le più efficaci strategie di contrasto avanzato.

C) Il contrasto alle violazioni del diritto d'autore on-line

La Polizia delle Comunicazioni è impegnata a contrastare anche le violazioni del diritto d'autore interessanti la rete internet e il sistema delle comunicazioni in generale.
Particolare attenzione è prestata agli illeciti posti in essere da articolate organizzazioni criminali.
Positivi risultati in tal senso sono stati conseguiti nel contrasto di bande criminali che violano i sistemi di sicurezza connessi alle trasmissioni televisive a pagamento.

D) Contrasto al cyberterrorismo, del proselitismo on-line dei cosiddetti reati d'odio (xenofobia, razzismo, intolleranza politica, religiosa, sessuale)

La Specialità concorre con altri organi di Polizia specializzati in indagini tecniche di particolare complessità sui fenomeni di eversione e terrorismo, a livello nazionale e internazionale, qualora caratterizzati dall'utilizzo di strumenti informatici e di comunicazione telematica.

Con l'obiettivo di prevenire turbative e pericoli per l'ordine e la sicurezza pubblica la Polizia Postale e delle Comunicazioni provvede anche al costante monitoraggio della Rete per individuare l'illecito proselitismo di iniziative di carattere razzista, xenofoba, sessuofobica o comunque ispirate a reati di odio.

E) La cooperazione internazionale – Gruppo di contatto 24/7 in ambito G8

Presso il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche è istituito il Punto di Contatto italiano per le emergenze tecnico – operative connesse al verificarsi di episodi di criminalità informatica transnazionale, secondo quanto stabilito dalla Convenzione sul Cybercrime di Budapest il 23 novembre 2001.

Il Punto di Contatto opera 24 ore su 24 e 7 giorni su 7 all'interno della rete High Tech Crime costituita in ambito G8 e successivamente estesa al Consiglio d'Europa.

La rete, che collega ben 64 paesi, è finalizzata a realizzare sollecite forme di ausilio nelle investigazioni informatiche ed in particolare ad ottenere il "congelamento" dei dati informatici utili alle inchieste, nelle more della loro formale acquisizione.

F) La tutela delle Infrastrutture Critiche

Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.) è stato istituito presso il Servizio Polizia Postale e delle Comunicazioni, quale organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni, con decreto del Ministro dell'Interno del 9 gennaio 2008 in attuazione della legge 31 luglio 2005 n. 155.

Il Centro svolge attività di tutela dei sistemi telematici di istituzioni e amministrazioni pubbliche, enti con personalità giuridica pubblica o privata e aziende, operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute e delle acque, ovvero la cui attività, per ragioni di tutela dell'ordine e della sicurezza pubblica, sia riconosciuta di interesse nazionale dal Ministro dell'Interno, anche su proposta dei Prefetti - Autorità provinciali di pubblica sicurezza.

I servizi di protezione informatica sono erogati attraverso speciali collegamenti telematici dedicati tra il C.N.A.I.P.I.C. e le singole infrastrutture critiche realizzati sulla base di convenzioni stipulate con il Dipartimento della Pubblica Sicurezza.

3. I nuovi scenari operativi

Il nuovo fronte delle investigazioni per il contrasto alla pedopornografia sulla Rete Internet è comunque puntato a contrastare l'utilizzo da parte delle comunità pedofile dei nuovi sistemi di

anonimizzazione della navigazione.
Nel solco della sperimentata attività di tutela dei giovani sono state individuate nuove strategie investigative mirate, tramite adeguato utilizzo di agenti sottocopertura, a contrastare i ricorrenti episodi di adescamento sessuale.
Il cd *grooming*, secondo la corrente denominazione anglosassone, solo di recente espressamente previsto come fatto penale a seguito del recepimento nella normativa italiana della cd *Convenzione di Lanzarote*, si sta rivelando di notevole diffusione anche in connessione con le sempre più ampie frequentazioni dei social network da parte dei minori.
Un'attenzione particolare viene prestata continuamente per la pronta individuazione delle giovani vittime di abusi sessuali sparse nei più remoti angoli del pianeta che alimentano il vasto mercato della pedopornografia online.
Fruttuose sinergie tra il Servizio Polizia Postale e delle Comunicazioni e aziende di rilievo del settore hanno ad esempio consentito di affinare efficaci procedure tecniche che permettono di agevolare con ampi margini di precisione l'individuazione delle vittime da sottrarre al mercato criminale.
Altri progetti, avviati con il mondo scientifico e le Università, hanno consentito di individuare le speciali connotazioni tecniche che consentono di associare con scientifici margini di certezza le immagini digitali agli apparati di fotovideoripresa che le hanno prodotte.
Il significativo risultato scientifico sta concorrendo in maniera decisiva alla più puntuale individuazione dei soggetti che producono il materiale pedopornografico oltrechè alla identificazione delle vittime del fenomeno.
Il concreto reale business della criminalità informatica è oggi senza dubbio divenuto il furto di identità digitale su larga scala.
Agguerrite ed articolate organizzazioni criminali, quasi sempre caratterizzate da marcata transnazionalità, sono alla caccia del vero oro del nostro secolo costituito dai dati e dalle informazioni.
Oggetto delle continue "attenzioni" dei gruppi criminali non sono solo le grandi banche dati (i cd *big data center*) ma anche i singoli dispositivi digitali degli utenti della rete.
La ormai quasi globale interconnessione dei sistemi favorisce per altro verso illecite intrusioni informatiche in ambito pressochè mondiale.
L'enorme accumulo di dati nei mega depositi del cd *cloud computing* hanno d'altro canto amplificato a dismisura i rischi di sottrazioni massive di informazioni.
La particolare aggressività e pervasività dei nuovi "programmi malevoli", diffusi ormai su larga scala anche mediante utilizzo di enormi reti di computer (*botnet*) fuori dal controllo dei legittimi detentori e gestiti da vaste organizzazioni criminali, favoriscono in maniera determinante questa nuova imponente caccia all'oro.
La Polizia Postale e delle Comunicazioni sta sperimentando le più avanzate forme di contrasto in materia inserendosi nel complesso meccanismo che vede le bande criminali gestire nelle forme più sofisticate i nuovi portati della tecnologia fino a realizzare accumuli di risorse di enorme rilevanza con incalcolabili danni che si riversano su una moltitudine sempre più ampia di soggetti passivi.
Individuare e contrastare le *botnet*, inserirsi nella complessa filiera di realizzazione dei furti di identità digitale nelle varie fasi della produzione, diffusione e utilizzazione di virus informatici, porre così un freno all'oramai fiorente mercato nero *on line* di dati ed informazioni rubate di vario

tipo, costituiscono le più impegnative sfide della Polizia Postale e delle Comunicazioni.
Ruolo determinante assume in tale prospettiva la più alta specializzazione tecnica degli operatori acquisita con l'ausilio delle più avanzate e prestigiose realtà scientifico-accademiche e le migliori sinergie con i settori privati e pubblici interessati.
Da citare in tal senso le sempre più numerose convenzioni di partnership sottoscritte con gli enti pubblici e privati che gestiscono le infrastrutture critiche e strategiche in ambito nazionale e le intese operative incorse con gli operatori del mondo bancario per l'affinamento della tutela dei sempre più diffusi servizi di home banking e dei sistemi di moneta elettronica.
Anche nell'ambito di pianificati programmi adottati dall'Unione Europea la Polizia Postale e delle Comunicazioni sta sperimentando innovative forme di monitoraggio della rete per individuare precocemente i fenomeni di cd radicalizzazione (*radicalisation*).
I recenti più gravi episodi di violenza indotti da rancori di origine razzista, xenofoba, religiosa e sessuofobica portano infatti a intravedere come unica effettiva forma di efficace prevenzione la tempestiva individuazione di persone e gruppi che manifestano in rete evidenti propensioni verso derive violente ed irrazionali.

4. Le nuove campagne di avvicinamento alle giovani generazioni di naviganti e di educazione alla legalità. Verso una nuova idea di Commissariato On-line

Da tempo oramai la Polizia delle Comunicazioni è impegnata in campagne di sensibilizzazione all'uso consapevole della rete rivolte soprattutto alle giovani generazioni.
La preziosa esperienza maturata ha consentito di associare agli originari contenuti anche nuovi spunti che tendono a far pervenire ai giovani concreti messaggi in tema di vera e propria educazione alla legalità.
Il cybestalking, il cyberbullismo, le più variegate forme di condotte illecite trovano oggi infatti nella rete le più favorevoli condizioni di diffusione e propagazione.
Le nuove campagne di avvicinamento alle giovani generazioni vedono alleato indispensabile l'intero sistema scolastico con il quale si stanno definendo le più adeguate sinergie.
Di primaria importanza in una moderna ottica di prevenzione generale l'imminente lancio del nuovo portale del Commissariato di P.S. *on line*, che conservando tutte le prerogative di base di ausilio al cittadino, tenderà a divenire punto specializzato di riferimento per i frequentatori della rete.
Caratterizzato da innovativi sistemi di interattività con l'utente attraverso specifiche finestre di dialogo e direttamente collegato con il mondo dei social network vedrà tra i suoi interlocutori privilegiati soprattutto i più giovani ai quali saranno anche dedicati forum e dibattiti.
Specifici spazi di ascolto e confronto saranno anche previsti per gli utenti che versano in condizioni di particolare vulnerabilità ed emarginazione.
L'iniziativa contribuirà in forma determinante ad accentuare la generale sensibilizzazione verso le problematiche di sicurezza informatica in generale, primo fondamentale e sicuro antidoto contro le fenomenologie criminali informatiche.

A puro titolo esemplificativo, si riportano gli esiti di attività operativa in alcuni fra i principali settori di interesse della Specialità riferiti al primo semestre del corrente anno:

Contrasto alla Pedopornografia *on line*

ATTIVITÀ	2013
ARRESTI	33
DENUNCE	170
IDENTIFICAZIONE MINORI VITTIME DI ABUSI	14

Contrasto ai reati in danno dei servizi/sistemi di monetica e di home banking

ATTIVITÀ	2013
ARRESTI	31
DENUNCE	2.643

Tutela delle Infrastrutture Critiche

ATTIVITÀ	2013
ARRESTI	7
DENUNCE	14
ATTACCHI E INTRUSIONI RILEVATE	817

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 188-196

Il malware di stato

Corrado Giustozzi

Abstract: il notevole incremento dei fenomeni di criminalità "cyber" riscontrato in questi ultimi anni è dovuto alla maggior diffusione dell'utilizzo dei sistemi informatici e telematici ed alla presenza in essi di vulnerabilità, dovute a difetti di progetto o di implementazione, che adottando opportune tecniche possono essere sfruttate come varchi di sicurezza per penetrare le difese dei sistemi e prenderne il controllo. Recentemente però si sono avute diverse prove che le stesse tecniche vengono adottate anche da organizzazioni governative impegnate nella lotta al crimine o nello spionaggio, le quali utilizzano nelle proprie attività dei veri e propri *malware di stato* sulla cui liceità giuridica non tutti sono concordi.

Parole chiave: Skype, Flame, Stuxnet, worm, intercettazione, sabotaggio, malware di stato.

1. Premessa

I sistemi informatici e le reti di comunicazione, ed in primo luogo Internet, sono purtroppo intrinsecamente deboli per quanto riguarda la capacità di resistere ad attacchi mirati, finalizzati a carpire informazioni in transito fra i sistemi o elaborate su di essi, ad alterarne il funzionamento o a prenderne surrettiziamente il controllo. Questo stato di cose discende da un complesso insieme di concause interdipendenti, nelle quali tuttavia giocano un importante ruolo le motivazioni storiche: anche i sistemi più moderni sono infatti basati su architetture e paradigmi sviluppati in un passato nel quale i rischi tecnologici erano minori e non richiedevano l'adozione di robuste funzioni intrinseche di sicurezza e protezione.

A tale scomoda ma imprescindibile eredità del passato si aggiunge purtroppo l'aggravante che la crescente complessità costruttiva dei sistemi moderni, e la sempre maggiore rapidità con cui essi vengono sviluppati ed immessi sul mercato, certamente non gioca a favore di una loro maggiore sicurezza. Infatti tanto più un sistema è complesso e maggiori sono le possibilità che da qualche parte esso ospiti insidiosi ed imprevisti difetti di progetto o di realizzazione che, se scoperti da un malintenzionato esperto, possono essere sfruttati per condurre a termine con successo un attacco. E ciò è tanto più probabile se, come oggi quasi sempre accade, la frenesia di mandare sul mercato nuovi prodotti in tempi sempre più ristretti e a costi sempre più bassi fa sì che essi non vengano quasi mai verificati e collaudati a fondo prima di essere commercializzati e messi in esercizio.

Sono questi inevitabili difetti di progetto o di realizzazione a costituire da sempre le principali

Articolo pervenuto il 7 ottobre 2013, approvato il 30 dicembre 2013

vulnerabilità che, sfruttate dai cybercriminali mediante opportune e spesso assai sofisticate tecniche, consentono loro di attaccare con successo i sistemi delle proprie vittime.
Ultimamente però i criminali non sono più i soli soggetti ad aver imparato a sfruttare per il proprio tornaconto le diffuse vulnerabilità che caratterizzano le tecnologie del mondo moderno. Da qualche tempo infatti le medesime tecniche vengono utilizzate anche da Stati sovrani o organizzazioni statuali, per vari fini istituzionali e non: tipicamente come moderni ausili nell'azione di contrasto alla criminalità e al terrorismo, ma talvolta anche come strumenti occulti di *intelligence* o addirittura di sabotaggio nei confronti di organizzazioni o Paesi avversi. Ciò ha sollevato un certo dibattito sulla liceità e le implicazioni tecniche, etiche e giuridiche dell'utilizzo da parte di uno Stato di strumenti, quali il *malware*, di natura tipicamente offensiva e comunque associati storicamente ad azioni e scopi di natura criminale.

2. Intercettare Skype

È noto a tutti come uno dei più potenti, e più utilizzati, strumenti d'indagine a disposizione da molti anni delle forze dell'ordine sia la capacità di intercettare legalmente le comunicazioni telefoniche degli indagati. Proprio al fine di consentire alle forze dell'ordine un adeguato svolgimento delle indagini, praticamente tutti i Paesi del mondo prevedono l'obbligo legale per gli operatori telefonici, dietro rituale presentazione di un regolare mandato da parte delle competenti autorità, di fornire agli inquirenti o i dettagli sulle comunicazioni effettuate da un indagato (i cosiddetti "tabulati di traffico", più propriamente definiti "cartellini") o il contenuto stesso delle comunicazioni intercorse (l'intercettazione vera e propria).
I criminali, dal canto loro, cercano ovviamente di evitare che ciò avvenga, e sono dunque alla continua ricerca di sistemi o espedienti per comunicare eludendo il rischio di essere intercettati. Ciò è divenuto relativamente più facile da quando la diffusione di Internet ha messo in grado chiunque di accedere, oltretutto con grande semplicità tecnica e costi bassi, a canali di comunicazione facilmente proteggibili mediante l'uso di tecniche di crittografia forte, oppure non veicolati tramite i tradizionali canali delle compagnie telefoniche. In questo nuovo scenario il problema di continuare ad assicurarsi la possibilità di effettuare intercettazioni è diventato assai rilevante per le forze dell'ordine, sia dal punto di vista tecnico che da quello legale.
Già nei primi anni '90 dello scorso secolo l'FBI, preoccupata dal diffondersi di sistemi di crittografia computerizzata gratuiti ed estremamente potenti utilizzati per cifrare i messaggi di posta elettronica, in particolare PGP[1], indusse il Governo statunitense a varare una proposta di legge che prevedeva l'introduzione di un meccanismo obbligatorio di *key escrow*[2] in tutte le comunicazioni elettroniche fra privati, vietando nel contempo l'utilizzo ai cittadini di ogni forma di crittografia che non fosse

[1] L'acronimo sta per "Pretty Good Privacy". Si tratta di un programma scritto da Phil Zimmerman, un programmatore che all'epoca era un forte attivista per il diritto di parola e le libertà in Rete, il quale lo diffuse gratuitamente allo scopo di consentire a chiunque di proteggere le proprie comunicazioni elettroniche anche contro le autorità.

[2] Il termine indica in modo generico qualsiasi sistema atto ad indebolire deliberatamente un sistema di crittografia, fornendo ad una o più apposite autorità una sorta di "grimaldello" con cui, in caso di necessità, poter decifrare i messaggi anche contro la volontà dell'autore.

approvata dal Governo stesso. Tale proposta di legge non venne in effetti approvata a causa della fortissima protesta delle organizzazioni in sostegno dei diritti dei cittadini, ed il progetto fu definitivamente accantonato e mai più riproposto. Il problema tuttavia riemerge sempre più spesso, anche per via della maggiore disponibilità di tecnologie di comunicazione sicura ed alla crescente sensibilità dei governi soprattutto nei confronti delle minacce terroristiche. Così, più di recente, nazioni quali l'India e gli Emirati Arabi Uniti, per motivi di sicurezza nazionale, hanno imposto ad alcuni fornitori quali RIM (produttore dei noti *smartphone* BlackBerry, caratterizzati dall'utilizzo di una propria rete cifrata per lo scambio di messaggi) di consegnare al locale governo le chiavi di decifrazione dei sistemi crittografici utilizzati dai loro dispositivi, pena l'embargo commerciale totale nei confronti del loro prodotti.

Un ruolo cruciale in questo delicato panorama lo ha giocato negli ultimi anni Skype, il noto programma gratuito che consente a chiunque abbia un computer ed una connessione veloce alla rete di "telefonare" in qualsiasi parte del mondo tramite Internet a costo irrisorio o addirittura nullo. L'azienda omonima, fondata nel 2002 in Estonia ed acquistata prima da e-Bay (2005) e poi da Microsoft (2011), ha infatti conquistato in pochi anni la posizione di leader mondiale nelle comunicazioni VoIP[3] grazie al suo ben noto *client* disponibile su praticamente ogni piattaforma informatica esistente. Agli inizi del 2012 le statistiche accreditavano a Skype oltre 600 milioni di utenti registrati nel mondo, di cui mediamente oltre 40 milioni contemporaneamente attivi sul sistema in ogni momento del giorno e della notte.

Sviluppato da Niklas Zennström e Janus Friis, già autori del noto software per lo scambio in rete di file in modalità *peer to peer*[4] denominato Kazaa, Skype implementa una complessa architettura distribuita, basata su algoritmi e protocolli proprietari e non divulgati, la quale consente ai corrispondenti una comunicazione non solo efficace e gratuita ma anche estremamente sicura. In effetti Skype, almeno sino all'acquisizione da parte di Microsoft, grazie all'utilizzo combinato di crittografia forte e dell'architettura *peer to peer* risultava del tutto immune ai tentativi di intercettazione da parte delle forze dell'ordine: cosa di cui le organizzazioni criminali internazionali si erano accorte da molto tempo, utilizzandolo come strumento principale di comunicazione sicura per le loro attività illecite.

Questo stato di cose era aggravato dal fatto che la stessa azienda Skype, con sede legale in Lussemburgo, aveva sempre sostenuto di non poter fornire alle forze dell'ordine supporto alle intercettazioni neppure volendo: e non solo in quanto non era legalmente tenuta a farlo, non essendo una compagnia telefonica registrata, ma anche e soprattutto perché la natura stessa della comunicazione impediva perfino agli stessi gestori della rete di ricostruire i complessi flussi di traffico tra i vari nodi. Il traffico di Skype era infatti frammentato imprevedibilmente in una rete a topologia distribuita, complessa e dinamicamente variabile, che impiegava gli stessi *client* degli utenti finali per svolgere sia il ruolo di "nodi" ordinari che quello di "super-nodi" di gestione della

[3] La sigla sta per "Voice over IP", ed indica tutte quelle tecnologie e protocolli che consentono di veicolare comunicazioni vocali tramite la rete Internet.

[4] Ossia in modalità totalmente distribuita, nella quale i trasferimenti avvengono mediante contatto diretto tra i corrispondenti e non tramite un'infrastruttura centralizzata di *server dedicati* che archivino e distribuiscano i file da condividere.

rete stessa[5]. La mancanza di *server* di controllo centralizzati, e la modalità di scambio *peer to peer*, di fatto non consentivano di stabilire il percorso esatto di una data conversazione, rendendo quindi materialmente impossibile intercettarla sulla rete. Non a caso nel 2009 l'Agenzia europea per la cooperazione giudiziaria permanente Eurojust aveva fatto partire un'iniziativa ufficiale volta proprio ad approfondire il problema e tentare di identificare un approccio che, pur nell'imprescindibile rispetto dei principi giuridici e delle norme nazionali ed internazionali, consentisse tuttavia di superare gli ostacoli legali e tecnici all'intercettazione del VoIP, con particolare riferimento proprio a Skype.

In questo scenario complesso e delicato, nel quale per motivi sia tecnici che legali era impossibile far ricorso alla fornitura di prestazioni obbligatorie di intercettazione da parte del gestore, le forze dell'ordine di vari Paesi si erano mosse da tempo cercando modalità alternative da impiegare per ottenere gli stessi risultati. La soluzione identificata ed adottata da quasi tutte è consistita nell'utilizzo di particolari *spyware*, ovvero veri e propri software di spionaggio progettati per intercettare la comunicazione sul computer stesso dell'indagato, in particolare prima che questo la invii alla rete Skype.

Programmi del genere, sviluppati solitamente da aziende specializzate, sono concettualmente e tecnicamente equivalenti ai vari tipi di *malware* usualmente impiegati dai cybercriminali per carpire i preziosi dati delle proprie vittime: sono infatti costruiti in modo da installarsi nascostamente sul computer da tenere sotto controllo, agendo senza rivelare all'utente la propria presenza; comunicano tramite la connessione Internet, in modalità nascosta e protetta, con un centro remoto di comando e controllo che li gestisce; catturano ciò che viene digitato sulla tastiera, visualizzato sullo schermo o detto al microfono, ed inviano tali dati al centro remoto di controllo; possono cercare tra i file presenti sul computer "ospite" o su altri computer connessi in rete locale, ed inviarli al centro remoto di controllo; possono eseguire localmente comandi inviati dal centro remoto di controllo; dispongono di contromisure che li rendono in grado di nascondersi ai più diffusi antivirus; vengono veicolati, come i virus, mediante allegati di posta elettronica infetti; sfruttano le vulnerabilità, spesso non ancora note, dei sistemi operativi o degli applicativi per aggirare controlli e contromisure che potrebbero ostacolarli o inibirli.

In particolare gli strumenti sviluppati per intercettare Skype catturano i segnali vocali direttamente dai circuiti audio cui è collegato il microfono, e le pressioni dei tasti direttamente dai circuiti della tastiera, prima ancora che entrambi tali flussi di dati vengano elaborati dal programma Skype e quindi inviati in Rete cifrati in modo ineludibile; e trasmettono quindi tali dati all'autorità responsabile dell'intercettazione in modo separato e, ovviamente, protetto.

Concettualmente tali strumenti agiscono come le usuali *cimici*, o microspie per intercettazioni ambientali, che vengono fisicamente piazzate in casa dell'indagato; con la differenza che in questo caso si tratta di prodotti *software* che vengono installati surrettiziamente sul suo computer. Per tale motivo esse sono state oggetto in alcuni Paesi di un forte dibattito giuridico, in quanto non risultava immediatamente chiaro se esse potessero direttamente ricadere nelle previsioni generali che regolano le intercettazioni ambientali tradizionali.

Un caso importante a riguardo si ebbe in Germania nel 2011 quando il noto Chaos Computer Club

[5] In particolare, per tenere traccia della topologia dinamica della rete, della presenza dei client, dell'instradamento delle conversazioni.

di Berlino, venuto in possesso di una copia dello *spyware* utilizzato dalla Polizia federale tedesca sin dal 2009, prodotto dalla società DigiTask, ne pubblicò una dettagliata analisi tecnica mostrando come esso, oltre a consentire l'intercettazione audio, fosse in grado di prelevare file dal computer dell'indagato ed anche di catturare immagini dello schermo. Entrambe queste funzioni erano state largamente sfruttate dalla Polizia in almeno quattro Länder, benché non consentite dalla rigida normativa federale sulle intercettazioni[6]. L'analisi del CCC mostrò inoltre che il programma non disponeva di sufficienti misure di sicurezza che ne impedissero un utilizzo anomalo, e quindi poteva essere usato per compiere atti di spionaggio estesi ed abusivi quali prendere il controllo completo del computer posto sotto osservazione. Teoricamente era anche possibile che una terza parte estranea potesse prendere il controllo dello *spyware* sottraendolo a quello degli inquirenti, sfruttando così a proprio vantaggio la presenza del prodotto sul computer di un obiettivo sensibile! Ciò portò l'allora ministro della Giustizia, Sabine Leutheusser-Schnarrenberger, ad aprire un'inchiesta sull'uso del prodotto, il quale in seguito fu silenziosamente abbandonato dagli inquirenti e sostituito con altri in grado di fornire maggiori garanzie.

Più di recente anche altre nazioni si sono dotate, o hanno ammesso di fare uso, di *spyware* per condurre intercettazioni legali nei confronti di cittadini soggetti ad indagini penali; tra queste, oltre alla Germania, si annoverano almeno l'Olanda e l'Italia. Altre nazioni, come ad esempio la Spagna, stanno invece introducendo nel proprio codice penale modifiche che consentano l'uso di tali strumenti da parte della polizia[7].

Va infine sottolineato, per dovere di cronaca, che l'architettura interna della rete Skype è stata profondamente (e silenziosamente) modificata da Microsoft successivamente all'acquisizione dell'azienda, per la quale ha sborsato ben 8,5 miliardi di dollari. In particolare adesso i *supernodi* responsabili dell'instradamento del traffico non vengono più scelti dinamicamente fra i milioni di computer degli utenti finali collegati alla rete Skype, ma sono stati sostituiti da una gigantesca batteria di *server* centralizzati, ospitati in modo permanente in un *datacenter* appositamente predisposto da Microsoft. Il reale motivo che ha portato Microsoft ad attuare questo profondo mutamento non è noto, anche se l'azienda in un comunicato ufficiale lo ha genericamente attribuito ad un generale miglioramento delle prestazioni e dell'affidabilità della rete Skype; tuttavia è certo che uno dei suoi effetti collaterali è quello di consentire facilmente l'intercettazione delle comunicazioni tra gli utenti, le quali ora passano tutte per la nuova infrastruttura centralizzata gestita proprio da Microsoft. Ciò ha portato alcuni osservatori a ritenere che l'intera operazione di acquisto di Skype da parte dell'azienda di Redmond fosse stata nascostamente voluta e finanziata dal Governo statunitense, il quale ha potuto così assicurarsi in esclusiva la piena facoltà di intercettazione sulla più diffusa rete VoIP al mondo[8]. È interessante a tal proposito notare che, a distanza di un anno, questa tesi sembra aver trovato ampia conferma nelle recenti rivelazioni di Edward Snowden

---

[6] Si veda ad esempio questo articolo pubblicato on-line dalla BBC: http://www.bbc.co.uk/news/world-europe-15253259

[7] Si veda ad esempio questo articolo pubblicato on-line dal Corriere della Sera: http://www.corriere.it/tecnologia/13_giugno_07/spagna-proposta-di-introdurre-trojan-legali-per-spiare-i-sospettati_e737f1d4-cf57-11e2-b6a8-ee7758ca2279.shtml

[8] Si veda ad esempio questo articolo pubblicato on-line da Repubblica: http://www.repubblica.it/tecnologia/2012/05/29/news/skype_microsoft_ristruttura_la_rete_l_esperto_saranno_possibili_intercettazioni-36171851/?ref=search

nell'ambito di quello che è stato definito "caso DataGate", ovvero l'iniziativa generalizzata di monitoraggio di stato da parte del Governo USA nei confronti dei propri ed altrui cittadini con la complicità di operatori e provider statunitensi.

3. Sabotaggio e spionaggio

Rimanendo in questo ambito decisamente meno lecito e trasparente, la cronaca recente annovera anche almeno due casi noti nei quali specifici *malware* di origine certamente governativa sono stati utilizzati per effettuare azioni deliberate e sistematiche, rispettivamente di sabotaggio e di spionaggio, nei confronti di Stati sovrani o di loro organizzazioni governative. Gli approfondimenti e le rivelazioni successive alla scoperta di tali episodi hanno chiaramente mostrato come, pur nella ovvia mancanza di conferme ufficiali, vi sia una responsabilità diretta degli Stati Uniti almeno nel primo di essi[9], il quale è così già passato alla storia come il primo caso documentato di attacco condotto dagli USA contro un'infrastruttura critica di un altro Paese mediante l'impiego di sistemi *software* anziché di armi convenzionali.

Il primo di tali casi, quello del *malware* denominato Stuxnet, emerge nel giugno 2010 quando alcuni ricercatori dell'azienda VirusBlokAda identificano in medioriente un nuovo *worm* che si replica usando ben quattro vulnerabilità *zero-day*[10] di Windows, oltre a due già conosciute (la prima, denominata CPLINK, che affligge i collegamenti simbolici e l'altra utilizzata in precedenza dal noto *worm* Conficker). Già tale caratteristica appare piuttosto anomala: le vulnerabilità *zero-day* sono infatti "merce" rara e preziosa sul mercato dei cybercriminali. Di solito una sola è più che sufficiente per confezionare un *malware* estremamente efficace e distruttivo, in quanto certamente non troverà difese attive a contrastarla; l'impiego di ben sei vulnerabilità, di cui addirittura quattro non note in precedenza, è un chiaro segno che il *worm* è stato confezionato senza risparmio di mezzi, e soprattutto con l'obiettivo di non fallire a nessun costo il proprio bersaglio.

Un'altra caratteristica del tutto peculiare di Stuxnet consiste nel fatto che le parti più critiche del suo codice, ossia i due *device driver* che costituiscono il cuore del sistema, risultano autenticate mediante due firme digitali valide e regolari, generate da due certificati digitali realmente esistenti e validi appartenenti a due diversi produttori entrambi noti ed affidabili. Il *worm* appare quindi al sistema operativo come un prodotto legittimo proveniente da un fornitore qualificato, il che gli consente di installarsi senza richiamare l'attenzione dell'utente e di andare a modificare anche aree particolarmente delicate del sistema senza necessità di richiedere esplicitamente particolari autorizzazioni. Successive analisi riveleranno che i certificati utilizzati, subito revocati, sono stati sottratti ai legittimi proprietari[11] a loro insaputa e con modalità ancora oggi non identificate.

Una prima analisi del codice del *worm* mostra ben presto che esso non ha come obiettivo primario i sistemi Windows sui quali si diffonde: essi infatti vengono semplicemente sfruttati dall'intruso

---

[9] Si veda ad esempio questo articolo pubblicato on-line dal New York Times: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0

[10] Ossia vulnerabilità ancora non pubblicamente note, per le quali pertanto non esistono misure correttive.

[11] Si tratta di JMicron e Realtek, due note aziende produttrici di schede elettroniche aventi entrambe sede in un medesimo edificio nel complesso industriale Hsinchu Science Park a Taiwan.

al fine di consentirgli di propagarsi via rete alla ricerca del suo reale obiettivo. E si scopre che quest'ultimo è nientemeno che uno specifico sistema automatico di controllo industriale (SCADA) prodotto dalla Siemens. Risulta quindi evidente che non ci si trova di fronte al solito *malware* scritto in garage da un *hacker* qualunque bensì ad un prodotto industriale, molto sofisticato e certamente costoso. Essendo inoltre caratterizzato da compiti inusuali e straordinariamente precisi, ed indirizzato verso un bersaglio tecnologico estremamente specifico e poco diffuso, non può che essere stato sviluppato da un'organizzazione dotata di grandi mezzi tecnologici e cospicue risorse finanziarie, mossa per di più da una motivazione eccezionalmente forte e determinata.
Successivi approfondimenti sulle modalità di azione del *worm* e soprattutto sull'ambito geografico e tecnologico nel quale esso è stato rilevato (il 60% delle infezioni si trova in Iran) fanno prendere sempre più corpo all'ipotesi che il suo obiettivo sia quello di indurre malfunzionamenti ed eventualmente anche veri e propri danneggiamenti nelle centrifughe che costituiscono uno dei componenti critici dell'impianto di arricchimento dell'uranio situato a Natanz, in Iran, centro nevralgico del controverso programma nucleare iraniano fortemente avversato dagli Stati Uniti e da Israele. Si scopre in seguito che il *worm*, iniettato inizialmente nell'impianto tramite una chiavetta USB, avrebbe dovuto rimanere confinato entro il perimetro cibernetico dell'impianto stesso: ne uscì inavvertitamente quando un aggiornamento inviato dal centro di comando e controllo remoto introdusse un difetto nel suo codice, portandolo dapprima ad infettare involontariamente il computer portatile che un tecnico aveva collegato alla rete interna dell'impianto, e poi a diffondersi erroneamente all'esterno quando lo stesso tecnico, tornato a casa, usò il medesimo portatile per collegarsi ad Internet. Se non fosse stato per questo comportamento maldestro il *worm* non sarebbe stato scoperto se non dopo parecchio tempo, e molto probabilmente avrebbe rallentato il programma nucleare iraniano molto più di quanto non abbia potuto fare.
Il secondo caso è quello del *worm* denominato Flame, scoperto nel maggio del 2012 dai ricercatori dei laboratori Kaspersky chiamati, dopo una lunga triangolazione tra il CERT nazionale iraniano ed il CrySyS Lab dell'università di Budapest, ad investigare su strani incidenti avvenuti sui sistemi del Ministero del Petrolio dell'Iran. Già dalle prime analisi gli esperti di *malware* si accorgono di trovarsi di fronte ad un qualcosa ben diverso dai soliti virus o *worm*: Flame è infatti un oggetto estremamente sofisticato e complicato, un vero e proprio *"attack toolkit"* come lo definiscono essi stessi, progettato per svolgere con grande efficacia azioni sistematiche di spionaggio cibernetico. Parte del codice di cui è composto appare subito analoga a quella di Stuxnet, evidenziando una comune origine: sembra tuttavia più primitivo dell'altro, forse un suo predecessore; il che confermerebbe la tesi, sostenuta da Kaspersky, che Flame fosse in azione indisturbato addirittura dal 2010.
Da un punto di vista tecnico, Flame presenta molte caratteristiche degne di nota: innanzitutto è estremamente modulare, essendo composto da una ventina di moduli specializzati che possono essere caricati ed attivati in modo indipendente; è scritto in diversi linguaggi di programmazione tra cui l'insolito Lua, sviluppato presso un'università brasiliana ma insegnato soprattutto nelle università israeliane, il quale viene solitamente utilizzato per sviluppare videogiochi; impiega internamente un robusto *database* relazionale per organizzare in modo sistematico le informazioni catturate; adotta ben cinque algoritmi crittografici differenti per proteggere sé stesso, i propri dati e le proprie comunicazioni segrete; sfrutta due delle vulnerabilità *zero-day* usate da Stuxnet per installarsi sul computer vittima e diffondersi in rete verso altri computer; possiede sofisticate capacità *stealth* per sfuggire agli antivirus, ed è addirittura in grado di automodificarsi in presenza di antivirus noti.

Tutte queste caratteristiche rendono Flame un oggetto insolitamente complesso e voluminoso per essere un *malware*, oltre 20 MByte: secondo Kaspersky il suo codice è venti volte più complesso di quello di Stuxnet, e potrebbe volerci addirittura una decina d'anni per analizzarlo completamente.
Una delle caratteristiche più notevoli di Flame è che esso non solo è "firmato" come Stuxnet, ma addirittura appare alla vittima sotto forma di un regolare aggiornamento del sistema proveniente da Microsoft! In questo modo esso può installarsi automaticamente sfruttando gli stessi meccanismi di aggiornamento remoto di Windows, eludendo così ogni controllo di sicurezza. Tale risultato, spettacolare e terrificante allo stesso tempo, è stato ottenuto producendo un falso certificato digitale intestato a Microsoft, col quale il codice è stato firmato. Questa incredibile contraffazione è stata resa possibile sfruttando una sottile e prima sconosciuta vulnerabilità della Certification Authority interna al servizio di emissione delle licenze per il prodotto Terminal Services di Microsoft, la quale ha consentito di produrre una "collisione" sull'*hash* del certificato (di soli 512 bit). In pratica gli autori di Flame sono stati in grado di creare un certificato falso avente lo stesso *hash* del certificato legittimo, e quindi lo hanno potuto utilizzare al posto di quello vero per firmare il codice del *worm*: un risultato straordinario, reso possibile solo a fronte dell'impiego di una enorme potenza di calcolo per generare la collisione. Conseguenza di ciò è che Microsoft ha dovuto rapidamente modificare i servizi vulnerabili, ma anche imporre l'uso di certificati lunghi almeno 1024 bit per evitare il ripetersi in futuro di simili "inconvenienti".
Anche le azioni di spionaggio, per le quali il *worm* è stato esplicitamente progettato, vengono condotte da Flame in modo estremamente efficace. Oltre a monitorare completamente la macchina su cui risiede, catturando ad esempio ciò che viene digitato sulla tastiera, visualizzato sullo schermo o detto al microfono[12], esso è infatti in grado di effettuare ricerche intelligenti tra i file presenti sul computer ospite e su tutti quelli collegati alla medesima rete locale, per identificare e prelevare documenti aventi caratteristiche specifiche o contenuti predeterminati; è inoltre in grado di utilizzare una connessione Bluetooth, eventualmente disponibile, per collegarsi a smartphone o altri dispositivi presenti nelle vicinanze e carpirne i contenuti. Naturalmente può ricevere istruzioni dal centro di comando e controllo remoto che lo gestisce, ed è anche in grado di autocancellarsi in seguito alla ricezione di un apposito comando di "suicidio".
Al contrario di Stuxnet, sfuggito per errore al controllo dei suoi gestori, Flame dispone di meccanismi molto robusti che ne controllano rigorosamente la capacità di autoreplicarsi: ed in effetti non è mai stato scoperto *in the wild*, ossia "allo stato brado", ma sempre e solo su siti mirati. Pertanto la sua diffusione, in confronto a quella di altri *worm* che tentano di replicarsi il più possibile, è straordinariamente limitata: ne sono stati infatti trovati solo un migliaio circa di esemplari, di cui la maggior parte in Iran e il resto suddiviso tra Sudan, Siria, Libano, Arabia Saudita ed Egitto.
Gli obiettivi nei quali Flame è stato trovato sono per lo più costituiti da agenzie governative, ma vi sono anche diverse istituzioni educative (università, scuole) e aziende private. Sembra che nella maggior parte dei casi, ed in particolare sui bersagli iraniani, esso sia stato impiegato soprattutto per ricercare ed acquisire file di AutoCAD (un noto programma di ausilio alla progettazione industriale) e documenti PDF, evidentemente alla ricerca di piani costruttivi e diagrammi tecnici ritenuti di valore a fini di *intelligence*.

[12] Comprese le connessioni Skype.

4. Conclusioni

Nell'eterna rincorsa tra "buoni" e "cattivi" non è inusuale vedere gli uni adottare metodi degli altri e viceversa. Il problema semmai è identificare chi è il "buono" e chi è il "cattivo", visto che generalmente si considera che la tecnologia sia neutra in sé mentre la differenza, sul piano etico e legale, la facciano il modo in cui essa viene impiegata e gli obiettivi che tramite tale impiego si intende perseguire.

Ciò di cui recentemente si è avuta la conferma, qualora ve ne fosse stato bisogno, è che anche nel moderno e rutilante mondo *cyber* vigono le stesse consuetudini: e così strumenti tecnici tipicamente presenti nella cassetta degli attrezzi dei cybercriminali, come i *worm* e gli *spyware*, vengono utilizzati da agenzie governative per fini più o meno chiari o legittimi. Nulla di nuovo in termini concettuali: tuttavia il peculiare ambito nel quale tali iniziative si collocano fa sorgere, in seconda istanza, alcune questioni interessanti sulle quali sarà necessaria una profonda riflessione.

Innanzitutto i produttori di antivirus si sono posti il problema di come considerare gli *spyware* utilizzati a fini di polizia che i loro sistemi dovessero eventualmente riuscire a rilevare: sono essi da considerarsi agenti di minaccia ricolti contro l'utente locale o no? E soprattutto, l'utente dovrebbe essere avvisato della loro eventuale presenza o no? È vero infatti che un criminale non dovrebbe essere avvertito di un'attività di intercettazione in corso su di lui, ma gli antivirus non sono certamente in grado di distinguere la *finalità* perseguita da un eventuale programma di spionaggio da essi rilevato, il quale potrebbe anche essere un reale *malware* di natura criminale che agisce contro gli interessi di un utente in buona fede. Né è pensabile di poter dotare gli antivirus di un mezzo oggettivo e standardizzato per poter distinguere con certezza tra *malware* "lecito" ed "illecito": cosa che, oltre ad essere tecnicamente difficoltosa, sarebbe un vero e proprio controsenso! Nel dubbio, dunque, i produttori hanno per il momento scelto la politica dell'avviso a tutti i costi: hanno cioè stabilito che sia meglio rischiare di mettere in guardia un criminale avvisandolo della presenza di un possibile *spyware* di polizia, che rischiare di non avvisare un utente di una possibile frode ai suoi danni da parte di un *malware* di natura criminale. In quest'ottica starebbe eventualmente alla polizia riuscire a produrre *spyware* così sofisticati da non essere rilevati dagli antivirus, il che tuttavia porterebbe ad una insensata "corsa agli armamenti". Il dibattito è quindi aperto.

Un'altra questione riguarda l'inevitabile accesso da parte delle agenzie governative (o delle aziende specializzate che sviluppano per loro i *malware*) al mercato nero delle vulnerabilità *zero-day* necessarie per poter confezionare un prodotto in grado di installarsi sui sistemi vittima superando le barriere attive o passive da essi erette. Tale mercato è infatti tipicamente in mano ad organizzazioni criminali, che impiegano esperti *black-hat*[13] per scoprirle e rivenderle al miglior offerente, che di solito è a sua volta un'organizzazione criminale. L'ingresso sistematico in tale mercato di acquirenti governativi, per quanto sotto copertura, potrebbe portare a pericolose escalation nelle dinamiche della domanda e dell'offerta con effetti collaterali difficilmente prevedibili. Un fenomeno complesso, ancora tutto da analizzare.

[13] Ossia *hacker* "cattivi".

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 197-206

Opportunità e strategie psicologiche nel cybercrime

Isabella Corradini

Abstract: Quando la scena del crimine è il Web si assiste ad un ampliamento delle opportunità e dei pericoli e ad una diversa percezione dei rischi. Il crimine in Rete si manifesta in modalità cyber ma la sua natura essenziale è ben nota. Furti di identità, frodi, stalking, bullismo, terrorismo, vengono compiuti sfruttando le opportunità di Internet che, al contempo, ne amplifica gli effetti.

Parole chiave: Web, opportunità, cybercriminale, vittima, percezione del rischio, ingegneria sociale, furto di identità, frode.

1. Introduzione alla tematica

E' ormai un fatto globalmente condiviso che i cambiamenti prodotti dalla rivoluzione digitale influenzino anche i comportamenti adottati nel nostro quotidiano.

Pensiamo, ad esempio, a quante volte consultiamo la Rete per scegliere un ristorante, un cinema, un viaggio, verificare un indirizzo. Ancora, per curiosare su una persona appena conosciuta e valutare quanto questa sia popolare sul Web, oltre che tenere d'occhio quale sia la nostra reputazione in Rete. Senza contare che le e-mail e i social network sono ormai il principale nostro mezzo di comunicazione, sia in ambito lavorativo che nel privato.

Nell'attuale contesto *siamo costretti* ad essere "sempre connessi". Se così non fosse, ci sentiremmo degli esclusi (o lo saremmo realmente). Purtroppo, o a ragione, è la Rete il vero mondo, tanto che lo stesso termine che abitualmente utilizziamo, *virtuale,* è da ritenersi inadeguato: tutto quello che facciamo in Rete è *reale* e produce effetti concreti.

Ad essere sempre connesso è però anche il crimine che, scoperti i vantaggi dell'Information & Communication Technology (ICT), ha adattato il suo *modus operandi* in funzione delle opportunità offerte dalla Rete. Una volta compresi i suoi meccanismi, ha capito che questo strumento avrebbe potuto apportare un prezioso contributo, come quello, ad esempio, di favorire il rapido e costante reperimento delle informazioni su persone, istituzioni e organizzazioni. È più probabile incontrare una persona con più di un profilo sui social network che qualcuno del tutto privo!

Il crimine diventa cyber, ma la sua natura essenziale è ben conosciuta. Così il bullismo diventa

Articolo pervenuto il 7 ottobre 2013, approvato il 30 dicembre 2013

cyberbullismo, lo stalking *cyberstalking*, il terrorismo *cyberterrorismo*, e via dicendo. Alcuni di questi crimini producono un vero e proprio allarme sociale, come la pedofilia e il terrorismo. Altri, come furti di identità e frodi, sono meno ripugnanti ma altrettanto insidiosi e nocivi per chi ne cade vittima.
Come si è arrivati a tutto questo?
Data la vastità dell'argomento, in questo saggio si intende enfatizzare il tema delle opportunità offerte dalla Rete ai criminali. E' infatti innegabile che le tecnologie e Internet rappresentino una grande conquista per tutti, ma è altrettanto vero che è l'essere umano ad interagire attraverso tali strumenti.
Il tema del cybercrime, con le esigenze di sicurezza che ne conseguono, non può quindi essere affrontato adeguatamente se non si considera tale aspetto. C'è da chiedersi, ad esempio: quale ruolo riveste l'utente nel cadere vittima di furti di identità e frodi? O ancora: come valuta i rischi il cybercriminale? In questo breve saggio si offre una panoramica su tali elementi.

2. Opportunità nel cybercrime

Il panorama della criminalità di stampo cyber è ampio e variegato. In questo ambito è possibile individuare crimini compiuti per le più svariate motivazioni: da quella economica, che ne costituisce la maggioranza, a quella sessuale, come nel cyberstalking e nella cyberpedofilia; dalla motivazione ideologica, come nel caso dell'hacktivism, a quella economico-sovversiva, come nel caso del terrorismo.
Una cosa è certa: l'incremento delle opportunità offerte dalle tecnologie e dalla Rete ha amplificato gli effetti di certi fenomeni e ne ha favorito la realizzazione.
Se è vero, infatti, che l'opportunità fa l'uomo ladro, tale verità trova riscontro anche con riferimento al crimine cyber. *Le opportunità hanno un ruolo nell'origine di tutte le tipologie di reato:* tale affermazione costituisce uno dei dieci punti chiave della teoria dell'opportunità di Felson e Clarke[1] che, pur riferendosi a tipologie di reato differenti da quelli cyber, fornisce spunti interessanti per condurre un'analisi sul tema.
La fruibilità di informazioni su Internet è sicuramente un'opportunità che viene sfruttata per il compimento di reati: ad esempio, venire a conoscenza tramite un social network di un viaggio di vacanza che una data persona (o famiglia) farà alle Maldive può rappresentare un'opportunità ed uno stimolo per un ladro di appartamenti. Utilizzando poi Google Streetview è anche possibile avere una panoramica a 360° della zona prescelta, con tanto di dettaglio delle strade. Nei social network si condividono informazioni apparentemente innocue, che sono però di grande interesse per il cybercriminale; egli, infatti, attraverso un'attività di *intelligence* on line, le raccoglie e le utilizza per fini non certamente sociali.
Insomma si può progettare un crimine stando comodamente seduti davanti a un Pc connesso alla Rete.

[1] **Felson, M. and Clarke, R.V.** (1998) Opportunity Makes the Thief. Police Research Series Paper 98, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate. London: Home Office.

Peraltro sono le stesse vittime (o potenziali vittime) che, in modo inconsapevole, aggiornano il popolo Web sulle loro specifiche abitudini, impegni, vacanze, conoscenze. Ecco dunque verificarsi episodi come l'invio di fiori e regali non graditi da parte del cyberstalker alla persona oggetto del suo desiderio, o i tentativi di adescamento in Rete da parte del cyberpedofilo.
Si assiste allo sviluppo di una criminalità dai contorni inquietanti: da un lato reati a danno di ignari utenti della Rete, dall'altro reati ben congegnati a danno di specifiche persone o istituzioni.
I numeri nell'ambito cybercrime continuano a crescere, e richiedono un aggiornamento costante. Allo stato attuale si registra una crescita degli attacchi mirati alla sottrazione della proprietà intellettuale; particolarmente a rischio, inoltre, sembra essere il settore mobile[2]. In questo ambito, infatti, si evidenzia un aumento del malware[3] il cui scopo, nella maggior parte dei casi, è quello di sottrarre informazioni, come indirizzi di posta elettronica e numeri di telefono.
Considerate dunque le modalità e le tecniche con cui si può agire, le vittime del cybercrime appartengono ad un universo molto vasto, da utenti singoli a piccole imprese, da grandi organizzazioni ad enti ed istituzioni. Allo stesso modo la criminalità fa un uso più o meno organico e professionale delle tecnologie di volta in volta disponibili.
Anche la criminalità organizzata, ad esempio, ha imparato a sfruttare le opportunità della Rete. Grazie al superamento delle distanze fisiche estende i traffici internazionali, s'infiltra in settori come quello dell'e-commerce, si dota di esperti finanziari e informatici, si protegge nell'anonimato di Internet, alimenta i guadagni con minor rischi. Il *cyberlaundering*, vale a dire il riciclaggio di denaro sporco mediante la Rete, è solo l'evoluzione di un fenomeno già conosciuto.
Quanto mai attuale è dunque l'affermazione di Levy secondo il quale "Internet non cambia il concetto dello spazio e del tempo, ma cambia esattamente lo spazio e il tempo"[4].

3. Un esempio di opportunità nel cybercrime: il fenomeno delle frodi

Nell'analisi condotta dal punto di vista delle opportunità e motivazioni, di particolare interesse è il fenomeno delle frodi, la cui tendenza – stando ai dati – non è certo positiva.
La frode comprende tutte quelle condotte illecite volte a trarre in inganno in modo intenzionale al fine di ottenere un beneficio. Le componenti che delineano la frode - dall'intenzionalità all'inganno, dalla condotte alle conseguenze che ne derivano – riconducono all'essere umano e alla sua abilità di persuasione e di azione (nel caso del frodatore) o alla sua capacità di accorgersi della frode, e dunque di prevenirne gli effetti (nel caso della vittima).
Varie sono le frodi che possono essere realizzate in funzione dei diversi contesti e ambiti: aziendali, alimentari, fiscali, creditizie, telematiche, in ambito sanitario, ecc.

---

[2] Internet Security Threat Report (ISTR), 2013 - Volume 18 a cura di Symantec.

[3] Il "malware" (termine che deriva dalla contrazione dell'espressione inglese "malicious software") è quel software che ha come obiettivo l'alterazione del normale funzionamento di un dispositivo o sistema informatico e/o la sottrazione di dati sensibili o riservati

[4] *http://www.mediamente.rai.it/home/bibliote/intervis/d/dekerc05.htm*, Firenze, Mediart 1998

Indipendentemente dalle tipologie, è comunque importante sottolineare come il ricorso alle tecnologie abbia oggi portato ad una evoluzione del modus operandi o, comunque, ad una diversa modalità di progettazione delle stesse.
Tra queste, si segnala l'aumento delle frodi creditizie[5], caratterizzate dall'appropriazione indebita di dati personali con l'obiettivo di ottenere credito in modo illecito. La facilità con cui oggi è possibile raccogliere informazioni personali utilizzando i contesti digitali costituisce uno dei fattori che ne hanno facilitato l'incremento.
Nel settore bancario particolare attenzione viene dedicata alle frodi identitarie, così chiamate in quanto si manifestano come uno schema criminale in cui un soggetto ottiene indebitamente un beneficio economico attraverso l'utilizzo di identità falsa o contraffatta[6].
Le ricerche condotte su tale tipologia di frode mettono in luce la dimensione del problema. Un'indagine del 2012 di ABI Lab (Centro di Ricerca e Innovazione per la Banca promosso dall'ABI) e Ossif (Centro di Ricerca dell'ABI sulla Sicurezza Anticrimine) ha evidenziato l'aumento per gli utenti del rischio connesso al furto di identità, in parallelo all'incremento del numero di utenti che utilizzano l'Internet Banking e il Mobile Banking. Una ricerca condotta nel 2013 da OSSIF, Ournext e il Centro di Ricerca Themis, ha rilevato le principali modalità con cui le frodi identitarie vengono perpetrate[7].
Secondo tale ricerca, nello specifico ambito bancario la frode identitaria può realizzarsi attraverso la falsa rappresentazione di un profilo creditizio privato o giuridico, generato con l'alterazione, la sofisticazione o il furto di documenti anagrafici o reddituali.
La progettazione dell'azione fraudolenta è facilitata da una varietà di strumenti e pratiche per ottenere dati e informazioni sulla potenziale vittima: dall'utilizzo di strumenti tecnologici malevoli al trashing[8] fino ad arrivare all'impiego di tecniche più o meno sofisticate di ingegneria sociale (si veda paragrafo 5).

Dal punto di vista criminologico, l'analisi della frode rimanda a tre elementi tra loro correlati: *pressione*, *razionalizzazione*, *opportunità.*[9]
La *pressione* è intesa come spinta a compiere un atto illecito dettata da una serie di fattori contingenti quali, ad esempio, il peggioramento delle condizioni economiche (riduzione degli stipendi, aumento del costo della vita, etc.), o i vizi e le abitudini del frodatore (si pensi al gioco d'azzardo o all'esigenza di mantenere un tenore di vita al di sopra delle proprie possibilità).
La *razionalizzazione* è invece il meccanismo psicologico attraverso il quale l'autore della frode arriva a giustificarsi, adducendone le cause a situazioni a lui esterne, come la vendetta rispetto ad un sopruso che ritiene di aver subito o la rivalsa nei confronti di uno status quo ritenuto ingiusto.
Infine, l'*opportunità* è costituita da tutte quelle condizioni e circostanze favorevoli al compimento della frode, come la mancanza di sistemi efficaci di controllo, l'inadeguata percezione del rischio

---

5 Osservatorio del CRIF, Centrale Rischi Finanziari.

6 I. Corradini, S. Tortora, Ricerca a cura di Ossif, Ournext, Centro Ricerche Themis: *Analisi sulle frodi identitarie,* 2013.

7 Ibidem.

8 Pratica di ricercare e risalire ad informazioni attraverso il setacciamento dei rifiuti della vittima, come documenti reddituali, bollette, ecc.

9 Donald R. Cressey, Other People's Money, Montclair N.J: Patterson Smith, 1973.

da parte delle vittime, l'insufficiente sensibilizzazione sul tema.
Non è scontata l'ipotesi di una correlazione diretta tra crisi economica e aumento delle frodi, in quanto per tale analisi sarebbe necessario valutare una molteplicità di variabili. Senza cadere in una logica riduttiva, è comunque evidente che le difficoltà oggettive di trovare un impiego espongono molte persone a comportamenti inconsapevolmente imprudenti nei confronti di chi, sfruttandone le debolezze, promette lavori e offerte. Così l'invio di curriculum o la diffusione di profili personali nei social network agevola i criminali nella ricerca di dati personali e informazioni varie.
L'Associazione per la Difesa dei Consumatori e il Movimento Difesa del Cittadino hanno evidenziato dodici tipologie di frode e pratiche commerciali scorrette a danno dei giovani in cerca di lavoro[10]. Tra queste si segnalano iscrizioni a banche dati, corsi di formazione, borse di studio, falsi periodi di prova, trasferimento di denaro, catene di S. Antonio.
Queste frodi, oltre al danno economico che possono provocare in persone peraltro già in difficoltà, possono produrre degli effetti anche sotto il profilo psicologico, facendo sperimentare frustrazione per la delusione delle aspettative e un abbassamento della propria autostima.

4. I costi per il cybercriminale

Il cybercriminale è sempre più interessato alla nostra vita raccontata sul web perché la nostra identità è costituita in gran parte da abitudini e frequentazioni on-line. Ad attirare la sua attenzione sono i nostri dati personali (documenti d'identità, carte di credito, credenziali di conti bancari, ecc.) che, una volta carpiti, possono essere utilizzati e/o venduti.
Questo interesse, unito ad un'attività di valutazione dei rischi e dei costi, favorisce l'applicazione di condotte criminose via web.
Ricorrendo alla teoria economico-razionale di Becker[11] nel valutare i costi e i benefici dell'azione criminosa, è possibile evidenziare come nell'ambito del cybercrime i costi diretti (esempio l'organizzazione del reato) e indiretti (rischio di individuazione e condanna), siano certamente più ridotti se comparati alla realizzazione di un crimine tradizionale. Un conto, infatti, è compiere una rapina o una truffa ai danni di una struttura commerciale con tutto ciò che un simile reato comporta in termini di organizzazione: dai sopralluoghi alla scelta dei complici, delle strategie e dei mezzi da impiegare, ovviamente in funzione del target obiettivo. Altro è, invece, compiere una frode impiegando un computer per inviare e-mail costruite ad arte. In questo caso ci si affida a modalità di comunicazione persuasive, senza dover ricorrere necessariamente ad un'esposizione fisica e diretta con la vittima: questo aspetto va certamente considerato nel valutare il cosiddetto "passaggio all'atto" del criminale che può agire in modo "tecnomediato". Inoltre, la tecnologia dell'informazione rende possibile il contatto con un numero elevato di potenziali vittime e consente di agire in parallelo e con un costo unitario irrisorio.
In linea generale, nella criminalità targata cyber, si evidenzia un meccanismo di depersonalizzazione della vittima che favorisce la condotta illecita. Ad esempio, attacchi condotti verso persone

[10] *http://miojob.repubblica.it/notizie-e-servizi/notizie/dettaglio/giovani-in-cerca-di-lavoro-state-attenti-alle-truffe/4300448*

[11] Becker G. (1968), Crime and Punishment: an economic approach, The Journal of Political Economy 76.

giuridiche sono spesso giustificati dalla percezione di non colpire direttamente la persona fisica, ma l'organizzazione, come se ciò risultasse meno deprecabile[12].

Ad entrare in gioco sarebbero, dunque, i cosiddetti meccanismi di *disimpegno morale*[13], vale a dire quei dispositivi cognitivi interni in grado di permettere all'individuo di adottare condotte contrarie alle norme senza però sviluppare sentimenti di autocondanna. Questi meccanismi possono operare a diversi livelli, come rivedere il significato della condotta criminosa, modificare la rappresentazione della vittima, distorcere la relazione causa-effetto. Ad esempio, nel meccanismo di disimpegno morale *confronto vantaggioso*, la gravità dell'azione viene ridimensionata operando il confronto con condotte ritenute generalmente più gravi. Nell'*attribuzione di colpa* l'azione agita viene giustificata in quanto pienamente meritata dalla vittima. O ancora nella *disumanizzazione* la condotta viene favorita dal processo di "spersonalizzazione" della vittima, evitando così lo sviluppo dell'angoscia derivante dalla sofferenza causata.

L'adozione di questi meccanismi ben si sposa con alcune caratteristiche delle tecnologie informatiche, come il superamento dei vincoli spaziali e temporali e la possibilità di agire in modo anonimo ed evitando ogni contatto personale con la vittima.

Non è poi da sottovalutare la carente percezione della vittima riguardo l'impatto e le conseguenze di un crimine informatico rispetto al crimine tradizionale. Un conto, infatti, è subire gli effetti di uno scippo, che vanno ad investire sia la sfera fisica (per la modalità violenta con cui il reato si manifesta) sia quella psicologica. Altro, invece, è subire una frode informatica: in questo caso, infatti, oltre alla mancanza di un impatto fisico diretto, ci si accorge delle conseguenze – principalmente di natura economica – solo a seguito di controllo sul proprio estratto conto. Anche in questo caso, tuttavia, non sono da escludersi gli effetti psicologici, soprattutto se il malcapitato si trova a dover fronteggiare richieste di creditori e a dover dimostrare la propria estraneità rispetto ai fatti accaduti.

Alla luce di queste considerazioni è chiaro che gli effetti di questo straordinario connettore che è Internet sono tangibili.

Doveroso a questo punto rivedere il concetto di virtuale, pena il rischio di sottovalutare certi comportamenti che, anche se veicolati dalla tecnologia, sono in grado di produrre serie conseguenze alla persona[14].

5. La persuasione nel cybercrime: l'ingegneria sociale

L'evoluzione del cybercrime trova riscontro nelle modalità con cui ci si approccia alla vittima (o potenziale vittima): se prima la criminalità targata cyber si connotava soprattutto per le capacità tecniche, oggi a richiedere particolare attenzione sono le abilità persuasive e di comunicazione con le quali i cybercriminali tentano di agganciare il bersaglio per farlo cadere nella loro "Rete".

---

[12] I. Corradini, A. Petrucci. I nuovi scenari dello stalking. Da internet ai luoghi di lavoro. Themis Edizioni, Roma 2012.

[13] A. Bandura, C. Barbaranelli, G.V. Caprara, C. Pastorelli, *Mechanisms of moral disengagement in the exercise of moral agency*, Journal of Personality and Social psychology, 1996, 71, pp. 364-374.

[14] I. Corradini, A. Petrucci. *Op. Cit.*

Si pensi al furto d'identità, problema certo non nuovo, ma oggi facilitato dall'impiego di tecniche come il *phishing*, in cui false e-mail costruite ad arte hanno lo scopo di raggirare utenti inconsapevoli inducendoli a fornire dati personali, come la user-id e la password. Generalmente la falsa e-mail, attraverso la tecnica dello spamming, viene inviata ad un numero elevatissimo di destinatari con l'intento di "pescare" qualche malcapitato inconsapevole che, attratto dai contenuti, fornisce alcuni suoi dati personali.

Ad attrarre è il tono cortese ma insistente di queste e-mail che creano nell'utente una sensazione di urgenza al fine di indurlo a rispondere. I contenuti di questi messaggi possono comprendere la richiesta di fornire i dati per un aggiornamento tecnico al fine di migliorare la qualità dei servizi offerti, l'invito ad accedere al sito per ottenere un nuovo pin di sicurezza, o ancora un avviso di addebito che il cliente è invitato a verificare cliccando sull'indirizzo riportato e fornendo user-id e password. Oggi si assiste ad una varietà di contenuti volti ad attrarre il lettore.

In gran parte dei casi (almeno allo stato attuale) la forma comunicativa, le imprecisioni, gli errori di grammatica allertano l'utente che cestina il messaggio. Tuttavia, nonostante le campagne di sensibilizzazione e di attenzione poste al problema del phishing, non è raro trovare qualcuno che cade nella trappola, forse per debolezza, forse per fretta, forse perché sullo smartphone non riesce a ben comprendere qual è la reale pagina web a cui indirizza il messaggio.

C'è anche chi avanza l'ipotesi di caratteristiche di personalità in grado di favorire l' "abboccamento" a richieste di e-mail di phishing. Uno studio internazionale[15] si sofferma su indicatori comportamentali, cognitivi e percettivi in grado di favorire la vulnerabilità alle azioni di phishing. Sembrerebbe (il condizionale è d'obbligo poiché al momento della redazione di questo saggio la descrizione della ricerca non è ancora stata pubblicata) che le donne siano più propense a considerare come autentiche le mail di phishing, mentre le persone sospettose, introverse e chiuse alle novità siano più propense a classificare come phishing mail perfettamente autentiche.

È anche vero che per far fronte alle diffidenze sempre più crescenti dell'utente, i criminali più esperti vanno via via perfezionandosi nello stile comunicativo, nel linguaggio, nella modalità di costruzione delle frasi per catturare l'attenzione di chi le riceve.

Dal phishing si è passati allo *spear phishing*, modalità mirata e persuasiva con cui il cybercriminale tenta di agganciare la vittima. Si tratta di una tecnica basata sull'invio di e-mail che sembrano provenire da una persona o un'azienda di conoscenza, mentre in realtà sono inviate da persone intenzionate a sottrarre dati preziosi (password, dati carta di credito, ecc.). Alla base della strategia dello *spear phisher* c'è proprio il far credere che il mittente è un conoscente della vittima, alla quale indirizza messaggi personalizzati in modo da metterla a proprio agio, riuscendo così a carpire le informazioni desiderate. D'altronde, con tutti i profili disponibili on line, è oggi possibile reperire sul Web la maggior parte degli elementi necessari per agganciare la vittima.

Il furto d'identità è un problema che non va assolutamente sottovalutato, sia per i danni economici che per quelli di immagine che può produrre. Le conseguenze di un furto d'identità non hanno impatto soltanto sul privato cittadino, ma incidono anche sulle amministrazioni pubbliche. Basti pensare che il fisco statunitense ha stimato in 5 miliardi di dollari il costo totale delle frodi subite

---

[15] Kyung Wha Hong, Christopher M. Kelley, Rucha Tembe, Emergson Murphy-Hill, and Christopher B. Mayhorn, "Keeping up With the Joneses: Assessing Phishing Susceptibility in an E.Mail Task", anteprima risultati in http://www.hfes.org/Web/DetailNews.aspx?ID=312

nel 2011 per falsi rimborsi fiscali legati a furti d'identità[16].
Tuttavia, a parte l'impiego di e-mail , è anche possibile che il recupero delle informazioni possa avvenire per vie "tradizionali", ad esempio ricorrendo a telefonate ben congegnate e indirizzate a soggetti specifici. Anche in questo caso si agisce su meccanismi tipicamente umani: ricorrendo alle lusinghe, al fascino, alla simpatia, è possibile ottenere la fiducia di una persona inducendola a farsi dare le informazioni di cui si ha bisogno.
Queste strategie persuasive costituiscono il punto di forza del cosiddetto *social engineering*, l'**ingegneria sociale**, nel quale con l'inganno e la persuasione ci si finge qualcun altro per raggiungere l'obiettivo.
Il *social engineer* deve essere molto bravo a mentire e a nascondere la propria identità, così come deve essere abile nell'arte della persuasione per spingere la vittima a fornire le informazioni necessarie. Riguardo alle tecniche di persuasione la letteratura è molto ampia, soprattutto nell'ambito della psicologia sociale. In proposito, vale la pena citare i sei schemi psicologici che porterebbero la vittima a cedere e ad esaudire le richieste dell'interlocutore (Cialdini, 1984):

- la reciprocità (il dover contraccambiare ciò che si è ricevuto)
- la coerenza (si tende ad onorare gli impegni presi)
- la simpatia (difficilmente si diffida di chi si presenta in modo accattivante)
- l'autorità (di fronte a richieste poste da chi percepiamo come un'autorità si ha un atteggiamento deferente)
- la scarsità (più una cosa scarseggia più diventa desiderabile)
- la riprova sociale (si tende a fare ciò che fanno gli altri)

Queste tecniche sono paragonate dall'autore all'arte marziale del jujiztu, il cui principio consiste nello sfruttare la forza fisica dell'aggressore per rivoltargliela contro. Così, il persuasore sfrutta le debolezze umane e attraverso strategie psicologiche induce l'interlocutore a ricorrere alle euristiche, impedendogli un'analisi approfondita delle informazioni nel prendere una decisione.

6. Considerazioni conclusive

A fronte di un fenomeno in rapida estensione e in continua evoluzione, sempre più le organizzazioni, pubbliche e private, necessitano di metodologie e strumenti volti alla prevenzione.
E' a questo punto doveroso un cambio di approccio culturale. La prevenzione non può essere costruita esclusivamente mediante soluzioni tecnologiche; se così fosse, con le tecnologie oggi a disposizione, avremmo già da tempo risolto il problema "sicurezza" in tutti i campi.
Nel corso degli anni è andato diffondendosi lo stereotipo secondo il quale l'essere umano sarebbe l'anello più debole della catena della sicurezza. E' certamente vero che le persone hanno caratteristiche tali da condurle in certi contesti ad errori di valutazione. Ma tenuto delle sofisticate capacità intellettive degli esseri umani e della assoluta rigidità e mancanza di senso comune dei sistemi informatici è chiaro che le persone possono trasformarsi nel punto di forza della sicurezza. Ad oggi nonostante da più parti sia stato messo in luce il problema della scarso coinvolgimento

[16] *http://spectrum.ieee.org/riskfactor/telecom/security/this-week-in-cybercrime-taxrelated-id-thefts-hit-18m-in-2012/*

attivo e consapevole della persona rispetto ai pericoli della Rete, nella prevenzione l'approccio di elezione continua a privilegiare soluzioni squisitamente tecnologiche.

Per affrontare la criminalità targata cyber occorre invece lavorare in modo interdisciplinare, integrando soluzioni tecnologiche ai comportamenti umani.
Questo significa saper progettare dispositivi e sistemi informatici tenendo conto del fattore umano. Ed è altresì indispensabile adottare percorsi informativi e formativi basati non solo su argomenti di natura tecnica, ma volti alla conoscenza e all'approfondimento del comportamento umano nell'interazione con le tecnologie.

Bibliografia e sitografia

- bandura A., Barbaranelli C., Caprara G.V., Pastorelli C. *Mechanisms of moral disengagement in the exercise of moral agency*, Journal of Personality and Social psychology, 1996, 71, pp. 364-374.
- Becker G.S. (1968). *Crime and punishment. An economic approach*". In Journal of Political Economy, 76.
- Cialdini R. (1984). *Influence. The Psycology of Persuasion*. New York: Quill William Morrow and Company. Trad. It. *Le armi della persuasione*. Milano: Giuffrè, 2005 – terza edizione.
- Corradini I. (2013). *Frodi, sicurezza e informazione*. In ICT Security, maggio 2013, Tecna Editrice, Roma.
- Corradini I., Petrucci A. (2012). *I nuovi scenari dello stalking. Da internet ai luoghi di lavoro*. Themis Edizioni, Roma 2012
- Corradini I. (2012). Comunicazione al XXVI Congresso Nazionale della SIC (Società Italiana di Criminologia), Delitti e genere, Como, 25-27 ottobre. Titolo della relazione: *Autore e vittima nei crimini in rete. Le differenze nella percezione del rischio.*
- *Corradini I. (2012). Tecnologie e l'arte della persuasione: il social engineering*. In Information Security. Anno III, Gennaio-Febbraio 2012. Edizioni Edisef, Roma.
- *Corradini I. (2012). Crimini in Rete: + pericoli per la vittima, - rischi per il cybercriminale.* In Information Security. N. 1e -Anno III, settembre 2012. Edizioni Edisef, Roma.
- Corradini I. *Social network: dalla percezione del rischio dell'utente alla valutazione del rischio del cybercriminale*. Convegno Security Summit, 7 giugno 2012, Roma.
- Cressey Donald R. (1973). Other People's Money, Montclair, N.J, Patterson Smith.
- Felson, M. and Clarke, R.V. (1998) *Opportunity Makes the Thief*. Police Research Series Paper 98, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate. London: Home Office.
- ABI Lab e Ossif, Il fenomeno delle frodi identitarie in banca, Luglio 2012
- Marotta G. (a cura di) 2004. *Tecnologie dell'informazione e comportamenti devianti*. Milano: LED.
- Ponti G. (1990). *Compendio di Criminologia*. Milano:Raffaello Cortina.
- Symantec, Internet Security Threat Report (ISTR), 2013 - Volume 18.
  http://www.themiscrime.com
  http://www.symantec.com/it/it/security_response/publications/threatreport.jsp
  http://www.acfe.com/fraud-101.aspx

www.adiconsumverona.it/truffe-12-le-tipologie-di-frodi-a-danno-dei-giovani-in-cerca-di-lavoro/
http://spectrum.ieee.org/riskfactor/telecom/security/this-week-in-cybercrime-taxrelated-id-thefts-hit-18m-in-2012/
http://www.crif.it/News/Pubblicazioni/pages/Osservatorio-sulle-frodi-creditizie.aspx
http://www.mediamente.rai.it/home/bibliote/intervis/d/dekerc05.htm, Firenze, Mediart 1998

- miojob.repubblica.it/notizie-e-servizi/notizie/dettaglio/giovani-in-cerca-di-lavoro-state-attenti-alle-truffe/4300448
- Kyung Wha Hong, Christopher M. Kelley, Rucha Tembe, Emergson Murphy-Hill, and Christopher B. Mayhorn, "Keeping up With the Joneses: Assessing Phishing Susceptibility in an E.Mail Task", anteprima risultati in http://www.hfes.org/Web/DetailNews.aspx?ID=312

Rivista elettronica di Diritto, Economia, Management

N. 3 - 2013 · pp. 207-245

Cyber Security
Politiche Globali, Compliance Normativa, Logiche Organizzative e Modelli di Gestione

Claudia Ciampi

Abstract: Negli ultimi anni la criminalità informatica e la sicurezza informatica hanno assunto una crescente importanza, sia per la rilevanza nell'economia e nella sicurezza nazionale delle infrastrutture critiche informatizzate sia per l'interazione delle politiche che affrontano la protezione dei dati. L'obiettivo principale degli attacchi informatici, qualunque sia la modalità con la quale vengono realizzati, è la compromissione, il furto o l'uso improprio di dati e informazioni gestite da aziende pubbliche e private o scambiate da queste attraverso la rete. La Cyber Security è stata identificata tra i primi cinque "Più Probabili" rischi per lo sviluppo globale. La crescita dei rischi informatici aumenta la necessità per le aziende, sia nel settore pubblico che in quello privato, di attuare meccanismi interni reali ed efficaci per salvaguardare la protezione dei dati e delle infrastrutture ICT.

In recent years Cybercrime and Cyber Security are attracting increasing attention, both for the relevance of Critical Information Infrastructure to the national economy and security and the interplay of the policies tackling data protection. The main objective of cyber attacks, whatever the mode by which they are achieved, is the compromise, theft or misuse of data and information managed by Public and Private Companies or exchanged by them through the network. The Cyber Security has been identified as one of the the top five "Most Likely" risks to global development. The growth of cyber risks increases the need for Companies, both in the public and private sectors, to implement real and effective internal mechanisms to safeguard data protection and ICT Infrastructure.

Parole chiave: Sicurezza informatica, Sicurezza delle informazioni, Cybercrime, Cyber Security, Information Security Management System, Compliance, Politiche di sicurezza, Analisi dei rischi, Protezione dei dati, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27004, ISO/IEC 27005; ISO 31000, ITIL, COBIT,

Articolo pervenuto il 18 Ottobre 2013, approvato il 30 dicembre 2013

1. Contesto di riferimento

Gli ultimi anni sono stati caratterizzati da una crescente diffusione delle tecnologie dell'informazione e della comunicazione per questioni legate principalmente alla riduzione dei costi, all'interoperabilità ed alla standardizzazione. L'innovazione se da un lato introduce nuove opportunità, dall'altro espone a nuove minacce tecnologiche sempre più insidiose ed avanzate.

Utilities, energia, finanza, sanità, pubblica amministrazione, sistemi militari si affidano alla rete per funzionare in modo efficace. Queste reti sono costantemente attaccate da un numero crescente di sofisticate minacce informatiche.

L'aumento dei pericoli in grado di compromettere la sicurezza dei sistemi informatici e telematici, rappresenta un'inquietante rischio per lo sviluppo globale. Al progresso tecnologico ha infatti corrisposto una crescita costante ed inarrestabile delle attività compiute dai criminali informatici o "*Cybercriminals*" il cui obiettivo non è più quindi la notorietà, ma l'implementazione di un vero e proprio modello di business differente rispetto al passato, in quanto organizzato, il più possibile stabile ed in grado di sopravvivere nel tempo.

Oggigiorno si è in presenza di vere e proprie reti criminali gestite da soggetti motivati da profitti importanti e duraturi, derivanti prevalentemente dalla vendita di dati personali, dalle truffe online o dalle estorsioni e ricatti.

Queste reti criminali riescono, spesso anche agevolmente, ad eludere i sistemi di difesa basati sul riconoscimento di firme di attacco note o su analisi comportamentali. L'anonimato rende più accessibile i mercati underground online che alimentano l'economia sommersa e dove è possibile trovare con estrema facilità strumenti che servono per attaccare siti e sistemi informatici.

Questo nuovo modello di criminalità organizzata crea un'asimmetria evidente tra attaccanti e difensori: chi attacca ha a disposizione a basso costo e in modo anonimo un ventaglio di opzioni amplissimo; chi difende si deve confrontare con costi elevati e con una complessa navigazione tra norme nazionali e comunitarie.

I principali driver di rischio sono attualmente rappresentati dalla crescente diffusione, anche all'interno delle organizzazioni pubbliche e private, di Device evoluti (smartphone e tablet), dal ricorso all'utilizzo di Social Network ed a soluzioni di Cloud, dall'obsolescenza delle tecnologie delle reti di telecomunicazione associata all'incremento delle attività di social hacking, al cambiamento nelle strategie di attacco ed alla diminuzione del costo delle tecnologie utilizzate dai criminali informatici.

La crescita dei rischi di cybercrime aumenta la necessità per le aziende, sia nel settore pubblico che in quello privato, di attuare meccanismi interni reali ed efficaci per salvaguardare la protezione delle reti, dei sistemi e dei dati.

Tanto più i dati sono disponibili e viaggiano in tutto il mondo attraverso reti telematiche, quanto maggiori e crescenti sono i rischi di violazione degli stessi.

Le violazioni delle informazioni personali meglio note come "*Data Breach",* possono avere effetti negativi molto significativi sulle aziende pubbliche e private, con conseguenze devastanti sia in termini economici che, soprattutto, in termini di reputazione.

Ridurre al minimo i rischi informatici, garantendo la protezione dei dati e delle informazioni, la costruzione e il mantenimento di una buona reputazione ed assicurando la fiducia dei cittadini e dei consumatori, è diventato per le imprese operanti in tutti i settori un obiettivo primario ed

imprescindibile e non più un'opzione di scelta.
Nessun sistema informatico o telematico è probabilmente mai completamente sicuro; anche i sistemi più curati dal punto di vista della sicurezza possono poi rivelarsi vulnerabili. Quindi, quello che è possibile ottenere attraverso una corretta gestione della problematica è di rendere particolarmente difficili i tentativi di attacco, estremamente rapidi i tempi di risposta agli incidenti di sicurezza e favorire la condivisione delle informazioni per creare una rete di cooperazione in grado di contrastare sul nascere le minacce informatiche.
Nei successivi paragrafi si analizzeranno:

- da una parte, l'importanza e la portata mondiale delle tematiche connesse alla sicurezza informatica e le strategie messe in campo dall'Italia e dall'Unione Europea
- dall'altra i risvolti in termini organizzativi e gestionali che la trattazione della tematica impone alle realtà organizzative operanti nel settore privato e in quello pubblico.

2. La politica italiana nella lotta alle minacce cibernetiche

Il problema della sicurezza informatica è diventata una fonte di preoccupazione crescente per la società moderna ed è stato oggetto di attente analisi da parte di importanti attori internazionali (ad es.: Stati Uniti, Regno Unito, Germania, Francia, Olanda) dell'Italia e dell'Unione Europea.
L'Italia, ritenendo che la minaccia cibernetica costituisce un rischio per la sicurezza nazionale, il *24 gennaio 2013* con Decreto del Presidente del Consiglio dei Ministri recante "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*" ha formalizzato la sua strategia nel campo della "cyber security".
Con questo decreto il nostro paese si pone ai primi posti nella lotta alle minacce cibernetiche e nella protezione del spazio cibernetico o "cyber space" cominciando ad affrontare il problema con un approccio nazionale, strategico ed accentrato (laddove ad oggi la trattazione di questo tema era affidata prevalentemente ad enti pubblici o soggetti privati) e ponendo le basi per una cooperazione nazionale su più livelli, che coinvolga tutti gli attori pubblici nonché gli operatori privati interessati, ed internazionale sia in ambito bilaterale e multilaterale, sia con l'UE che con la NATO.
Lo "spazio cibernetico" è costituito "dall'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi"[1]. Vi sono dunque inclusi: internet, le reti di comunicazioni, i sistemi attuatori di processo e le apparecchiature mobili dotate di connessione di rete.
La "minaccia cibernetica" è il "complesso delle condotte che possono essere realizzate nello spazio cibernetico o tramite esso, ovvero in danno dello stesso e dei suoi elementi costitutivi, che si sostanzia in particolare, nelle azioni di singoli individui o organizzazioni, statuali e non, pubbliche o private, finalizzate all'acquisizione e al trasferimento indebiti di dati, alla loro modifica o distruzione illegittima, ovvero a danneggiare, distruggere o ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi".

[1] Articolo 2 lett. h) del D.P.C.M. 24.01.2013

La "sicurezza cibernetica" invece è la condizione per cui il cyber-space "risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi"[2].
Il decreto definisce "l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, indicando a tal fine i compiti affidati a ciascuna componente ed i meccanismi e le procedure da seguire ai fini della riduzione della vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi"[3].
La nuova strategia nazionale avrà, dunque, tre scopi principali: individuare le minacce, prevenire i rischi e coordinare una risposta in situazioni di crisi.
Sono tre i livelli d'intervento:

- il primo di indirizzo politico e di coordinamento strategico affidato al "Comitato interministeriale per la sicurezza della Repubblica (CISR)" che si occuperà della elaborazione di un Piano nazionale per la sicurezza dello spazio cibernetico. A sostegno del CISR nel suo compito, verrà istituita presso la Scuola di formazione del DIS un organo dedicato, cui affidare anche compiti funzionali alla promozione e diffusione di una cultura della sicurezza cibernetica;
- il secondo di supporto operativo ed amministrativo a carattere permanente affidato al "Nucleo per la Sicurezza Cibernetica" presieduto dal Consigliere Militare del Presidente del Consiglio, con funzioni di raccordo nei confronti di tutte le amministrazioni ed enti competenti per l'attuazione degli obiettivi e delle linee di azione indicate dalla pianificazione nazionale e che provvederà a programmare l'attività operativa a livello interministeriale e ad attivare le procedure di allertamento in caso di crisi;
- il terzo livello, di gestione delle crisi affidato al "Tavolo Interministeriale di Crisi Cibernetica", con il compito di curare e coordinare le attività di risposta e di ripristino della funzionalità dei sistemi, avvalendosi di tutte le componenti interessate.

Sul piano pratico, la Direttiva prevede anche l'istituzione di un Computer Emergency Response Team nazionale, accanto al già istituito CERT della Pubblica Amministrazione.
L'articolo 11 della Direttiva contiene, infine, indicazioni specifiche per gli operatori privati che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, e che gestiscono le infrastrutture critiche a livello nazionale ed europeo, il cui funzionamento si basa su sistemi informatici e di telecomunicazione. Questi dovranno:

- comunicare al Nucleo per la Sicurezza Cibernetica qualsiasi violazione significativa di sicurezza o all'integrità dei loro sistemi informatici utilizzando canali di trasmissione protetti;
- adottare le best practice e le misure finalizzate all'obiettivo della sicurezza cibernetica;

---

[2] Articolo 2 lett. I) del D.P.C.M. 24.01.2013

[3] D.P.C.M. 24.01.2013 - Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale

- fornire informazioni agli organismi di informazione per la sicurezza e consentono ad essi l'accesso alle banche dati d'interesse ai fini della sicurezza cibernetica di rispettiva pertinenza;
- collaborare alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalità dei sistemi e delle reti da essi gestiti.

La sicurezza dello spazio cibernetico, dunque, è articolata su componenti di natura politica, economica, normativa e tecnica, e le principali sfide per il futuro della cyber-security in Italia consisteranno nelle possibilità di partnership tra settore pubblico e privato, indispensabili per la protezione delle infrastrutture critiche estranee alle pubbliche amministrazioni.

3. La strategia europea sulla Cyber Security

Numerosi negli anni sono stati gli interventi UE rispetto al problema della sicurezza informatica intesa inizialmente come protezione dei dati gestiti dai sistemi informativi pubblici e privati, e dunque come valutazione dei rischi connessi alla gestione delle informazione e dei sistemi in quanto risorse di valore strategico per il governo del paese. Tra questi, si segnalano:

Directive 95/46/EC	The protection of individuals with regard to the processing of personal data and on the free movement of such data
Directive 97/66/EC	Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector
Brussels, 6.6.2001 COM(2001)298	Network and Information Security: Proposal for a European Policy Approach
Council Resolution 2002/C 43/02	Common approach and specific actions in the area of network and information security
Brussels, 19.4.2002 COM(2002) 173	Proposal for a Council framework decision on attacks against information systems
Directive 21/2002/CE	Common regulatory framework for electronic communications networks and services
Directive 22/2002/CE	Universal service and users' rights relating to electronic communications networks and services
Directive 2002/58/EC	The processing of personal data and the protection of privacy in the electronic communications sector
Brussels, COM(2006)51	A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"
Brussels, 08.03.2010 n.7120/10	Draft Internal Security Strategy for the European Union: "Towards a European Security Model"
Directive 2008/114/EC	The identification and designation of European critical infrastructures and the assessment of the need to improve their protection
Brussels, 25.1.2012 COM(2012)11	Proposal for a regulation of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data
Brussels, 7.2.2013 COM(2013) 48	Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union

Solo nell'ultimo decennio l'Unione Europea ha cominciato ad affrontare il problema in una dimensione strategica più ampia che ha portato alla "*Proposta di Direttiva riguardante le misure volte a garantire un livello elevato e comune di sicurezza delle reti e le informazioni in tutta l'Unione*" (cd. Direttiva

UE sulla Cyber Security)[4] presentata dal Parlamento Europeo e dal Consiglio d'Europa il *7 Febbraio 2013*.

Il percorso che ha condotto alla formulazione dell'attuale strategia europea sulla Cyber Security si basa principalmente sui seguenti documenti:

Brussels, 08.12.2003 n.15895/03	A secure Europe in a better world. European security strategy.[5]
Brussels, 10.12.2008 n.17104/08	Report on the Implementation of the European Security Strategy – Providing Security in a Changing World.[6]
Brussels, 30.03.2009 n.8375/09	Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.[7]
Brussels, 19.05.2011 n.10299/11	Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" (CIIP).[8]

La strategia sulla cyber security presentata con la Direttiva espone la visione complessiva dell'Unione europea sul modo migliore di prevenire e rispondere agli attacchi informatici ed è articolata in cinque priorità[9]:

- conseguire la resilienza informatica;
- ridurre drasticamente la criminalità informatica;
- sviluppare la politica di difesa e le capacità informatiche connesse alla politica di sicurezza e di difesa comune;

---

[4] Brussels, 7.2.2013 COM(2013) 48 final 2013/0027 (COD) - Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union.

[5] Brussels, 08.12.2003 n.15895/03 - "... increased European dependence – and so vulnerability – on an interconnected infrastructure in transport, energy, information and other fields [...] terrorist movements are well-resourced, connected by electronic networks, and are willing to use unlimited violence to cause massive casualties."

[6] Brussels, 10.12.2008 n.17104/08 – "Modern economies are heavily reliant on critical infrastructure including transport, communication and power supplies, but also the internet. [...] However, attacks against private or government IT systems in EU Member States have given this a new dimension, as a potential new economic, political and military weapon. [...] More work is required in this area, to explore a comprehensive EU approach, raise awareness and enhance international co-operation"

[7] Brussels, 30.03.2009 n.8375/09 – "Information and Communication Technologies (ICTs) are increasingly intertwined in our daily activities. Some of these ICT systems, services, networks and infrastructures (in short, ICT infrastructures) form a vital part of European economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures. They are typically regarded as critical information infrastructures (CIIs)1 as their disruption or destruction would have a serious impact on vital societal functions The risks due to man-made attacks, natural disasters or technical failures are often not fully understood and/or sufficiently analysed. Consequently, the level of awareness across stakeholders is insufficient to devise effective safeguards and countermeasures .[...] Cyber-attacks have risen to an unprecedented level of sophistication. Simple experiments are now turning into sophisticated activities performed for profit or political reasons. ....The huge number of viruses, worms and other forms of malware, the expansion of botnets and the continuous rise of spam confirm the severity of the problem. [...] The high dependence on CIIs, their cross-border interconnectedness and interdependencies with other infrastructures, as well as the vulnerabilities and threats they face raise the need to address their security and resilience in a systemic perspective as the frontline of defence against failures and attacks".

[8] Brussels, 19.05.2011 n.10299/11 – "Cyber security and the protection of critical information infrastructures are vital for people and companies to trust the Internet and other networks and are a key priority of the Digital Agenda for Europe".

[9] Brussels, 07.02.2013 IP/13/94 - EU Cyber Security plan to protect open internet and online freedom and opportunity.

- sviluppare le risorse industriali e tecnologiche per la sicurezza informatica;
- istituire una coerente politica internazionale del ciberspazio per l'Unione europea e sostenere i valori fondamentali dell'UE.

L'intento è quello di promuovere i valori europei di libertà e di democrazia affinché l'economia digitale possa svilupparsi in modo sicuro.
L'Unione Europea propone l'istituzione di una Commissione per la sicurezza delle reti e delle informazioni, il cui compito dovrà essere quello di agevolare la commissione nell'aggiornamento della direttiva.
È stato inoltre proposto l'obbligo di istituzione, in ogni paese membro, un'autorità competente in materia di Cyber Security, che dovrà impegnarsi nel controllo dell'applicazione della direttiva e ricevere le notifiche delle violazioni rilevanti.
La collaborazione fra gli stati membri dovrebbe essere favorita dall'attivazione di una rete di cooperazione volta allo scambio di informazioni fra le autorità nazionali competenti, la commissione europea ed altri enti europei impegnati in attività di security e contrasto della criminalità informatica.
Gli interventi previsti dalla proposta interessano le pubbliche amministrazioni, gli operatori di infrastrutture critiche e altre organizzazioni potenzialmente interessate da attacchi, come fornitori di servizi informativi, gestori di servizi di cloud, motori di ricerca, social network, e-commerce, enti responsabili di trasporti, ospedali e istituzioni finanziarie.
Secondo il "*Piano di sicurezza informatica dell'UE per tutelare l'internet aperta, la libertà e le opportunità nella rete*"[10], su questi soggetti ricadrà l'obbligo di segnalare ogni incidente e violazioni di sicurezza rilevanti alle autorità nazionali competenti, pena l'applicazione di sanzioni "effettive, proporzionate e dissuasive" nel caso d'incidenti di una certa gravità.
L'onere di notifica e quello di soddisfare criteri minimi per la gestione dei rischi, verrà anche esteso ad una moltitudine di altri servizi (finanziari, nel campo dei trasporti) che utilizzano infrastrutture critiche, nonché alle amministrazioni pubbliche.

4. Concetto e rilevanza della sicurezza informatica

Compresa l'attualità, l'importanza e la portata mondiale delle tematiche connesse alla sicurezza informatica, è importante definirne il concetto e capirne i risvolti in termini organizzativi e gestionali nel settore privato e pubblico.
Con il termine *Cyber Security* o "*Sicurezza informatica*", in via generale, si indica quella branca dell'informatica che si occupa della salvaguardia dei sistemi informatici e delle reti da potenziali rischi di acceso, utilizzo, modifica e distruzione sia accidentali che dolosi.
Nell'ultimo quindicennio il significato del termine si è andato evolvendo fino a coincidere con quello di "sicurezza dell'informazione".
Con il termine sicurezza delle informazioni o "*Information Security*" si intende la capacità di salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni, qualunque forma

[10] Brussels, 07.02.2013 IP/13/94

esse assumano e qualunque siano i mezzi con cui vengono condivise o memorizzate, e delle risorse utilizzate per il suo trattamento, contrastando efficacemente ogni minaccia sia di tipo accidentale sia di tipo intenzionale, ovvero riducendo al minimo i rischi attraverso l'individuazione, la realizzazione e la gestione di opportune contromisure di natura fisica logica ed organizzativa. Tale definizione trova riscontro sia nel settore privato che in quello pubblico[11], e gli obiettivi della sicurezza delle informazioni vengono generalmente espressi in termini di *Riservatezza*, *Integrità* e *Disponibilità* dei dati e delle risorse ICT.

Per riservatezza si intende la capacità del sistema informativo di garantirne l'accesso e l'utilizzo di dati e risorse solo da parte di utenti autorizzati, ovvero di assicurarne la"confidenzialità".

Garantire l'integrità significa poter fare affidamento su informazioni "accurate", "complete" "valide" e su risorse "attendibili".

Per disponibilità si intende, invece, la capacità del sistema informativo di garantire l'accesso ai dati, alle procedure ed alle risorse ogni qual volta richiesti dagli utenti autorizzati, quindi poter offrire garanzie di "continuità" dei servizi, di "scalabilità" ed "affidabilità".

Ove si considerino le informazioni in fase di trasmissione ai sopra citati requisiti, vanno aggiunti l'*Autenticazione*, ovvero la capacità del sistema di assicurare al destinatario di una comunicazione la corretta identificazione della fonte di provenienza ovvero la certezza dell'autenticità dell'identità dichiarata dal mittente ed il "*Non Ripudio*", ovvero la capacità del sistema di garantire che né il mittente né il destinatario di un messaggio possano negarne la trasmissione o la ricezione.

Ne consegue che una rete o un sistema informatico possono considerarsi "sicuri" soltanto rispetto alla loro capacità di resistere ad eventi imprevisti o ad atti illeciti o dolosi che compromettano la riservatezza, l'integrità e la disponibilità dei dati conservati o trasmessi, e dei relativi servizi forniti o accessibili tramite tale rete o sistema, o ne pregiudichino l'autenticità e la non ripudiabilità.[12]

Gli obiettivi dell'Information Security possono essere raggiunti attraverso l'implementazione di specifici meccanismi di protezione atti a soddisfare una serie di requisiti funzionali di sicurezza che si distinguono in:

- Funzioni di sicurezza fisica.
  - *Sistemi di Rilevazione Passiva*: funzioni di sicurezza che rilevano la presenza di situazioni logistiche anomale (ad es. incendio, allagamento, fumo), inviando uno specifico allarme ai centri di controllo senza attivare contromisure;
  - *Sistemi di Rilevazione Attiva*: funzioni di sicurezza che rilevano la presenza di situazioni logistiche anomale (ad es. incendio, allagamento, fumo), inviando uno specifico allarme ai centri di controllo ed attivando una specifica contromisura.
  - *Sistemi di Controllo Accesso Fisico*: funzioni di sicurezza che regolano l'accesso fisico in determinate aree riservate alle sole persone e mezzi autorizzati.
  - *Sistemi di Continuità di Alimentazione*: funzioni di sicurezza che garantiscono la continuità

[11] "Le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese. Questo patrimonio deve essere efficacemente protetto e tutelato al fine di prevenire possibili alterazioni sul significato intrinseco delle informazioni stesse. È noto infatti che esistono minacce di intrusione e possibilità di divulgazione non autorizzata di informazioni, nonché di interruzione e di distruzione del servizio" (Direttiva 16 gennaio 2002 del Presidente del Consiglio dei Ministri "Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali." G.U. 22 marzo 2002, n. 69)

[12] Regolamento (CE) 460/2004

dell'alimentazione elettrica ai sistemi informatici, almeno per il tempo sufficiente alla chiusura ordinata.

- *Infrastrutture*: accorgimenti specifici sugli edifici e disposizione dei locali al fine di garantire la sicurezza degli impianti (edifici antisismici, uscite di sicurezza dotate di sistemi di allarme, separazione ambienti a rischio, ecc…).

– Funzioni di sicurezza logica[13].
  - *Access Control:* funzioni di sicurezza che controllano il flusso delle informazioni tra processi e dell'utilizzo delle risorse da parte dei processi stessi, con l'obiettivo di assicurare solo agli utenti autorizzati l'espletamento delle operazioni di propria competenza. Tra tali funzioni vanno previste anche quelle di amministrazione dei diritti di accesso e loro verifica.
  - *Accounting:* funzioni di sicurezza che registrano e tracciano le azioni poste in essere da utenti o conseguenti all'esecuzione di processi, con l'obiettivo di assicurarne l'univoca ed incontestabile attribuzione.
  - *Accuracy:* funzioni di sicurezza che garantiscono il mantenimento delle corrette relazioni tra i dati e la non alterazione degli stessi in fase di trasferimento tra i diversi processi. Hanno lo scopo di identificare, segnalare e correggere qualunque tipo di modifica non autorizzata dei dati (alterazioni, cancellazioni ed inclusioni di nuove parti nei dati scambiati tra processi o passati da un oggetto all'altro). Tra queste rientrano anche quelle di identificazione ed eliminazione di Virus, nonché di analisi dell'integrità degli indici di un Data Base.
  - *Audit:* funzioni di sicurezza che registrano ed analizzano gli scostamenti, da soglie predeterminate, di determinati eventi che potrebbero rappresentare una minaccia alla sicurezza delle risorse. Hanno l'obiettivo di monitorare e controllare casi anomali o sospetti. Tali funzioni devono consentire l'identificazione selettiva e la correlazione delle azioni eseguite da uno o più utenti, e consentire l'Alert on-line o differito al superamento di soglie di sicurezza predefinite.
  - *Data Exchange:* funzioni di sicurezza che garantiscono la protezione dei dati durante la loro trasmissione sui canali di comunicazione mediante l'autenticazione del mittente, l'integrità e la riservatezza del contenuto del messaggio, il non ripudio del mittente e del destinatario.
  - *Identification e Authentication:* funzioni di sicurezza che verificano l'identità degli utenti che accedono a risorse controllate. L'identificazione e l'autenticazione devono essere effettuate prima di ogni ulteriore interazione tra l'utente e il sistema. Solo se l'operazione di identificazione e autenticazione sarà andata a buon fine, l'utente autorizzato potrà avere altre interazioni con il sistema. Tali funzioni si applicano anche alle interazioni tra processi applicativi e tra sistemi.
  - *Object Reuse:* funzioni di sicurezza che consentono il riutilizzo di spazi di memoria centrale o di massa, impedendo che ciò costituisca una minaccia alla riservatezza delle informazioni precedentemente registrate su tali supporti. Tra queste, anche quelle

[13] Riferimento alla classificazione riportata nello standard ITSEC - Information Technology Security Evaluation Creteria

di inizializzazione e cancellazione dei supporti asportabili e riusabili (ad es. nastri magnetici, dischetti, ecc.).

- *Reliability of Service:* funzioni di sicurezza che assicurano l'accesso e l'utilizzo delle risorse esclusivamente a utenti/processi autorizzati entro tempi prefissati.

– Funzioni di sicurezza organizzativa.
  - *Ruoli e Responsabilità:* definizione delle figure organizzative coinvolte negli aspetti di gestione della sicurezza, dei loro compiti e delle relative responsabilità.
  - *Politiche di sicurezza:* strutturazione di un sistema documentale di regole finalizzato ad indirizzare il governo della sicurezza in linea con le strategie e gli obiettivi definiti dall'organizzazione.
  - *Procedure di Gestione:* strutturazione di un sistema documentale rivolto agli addetti alla gestione della sicurezza informatica atto a descrivere le modalità operative di svolgimento delle attività di competenza.
  - *Procedure di Utilizzo:* strutturazione di un sistema documentale rivolto agli utenti dei sistemi informatici atto a descrivere le norme comportamentali e le modalità operative di utilizzo sicuro delle risorse informatiche.
  - *Formazione e Comunicazione:* pianificazione di attività finalizzate alla diffusione di conoscenze e competenze volte a migliorare i comportamenti organizzativi ed operativi degli addetti e degli utenti che operano sulle risorse informatiche.

La sicurezza delle informazioni può, dunque, essere conseguita mediante l'attuazione di un insieme adeguato di controlli fisici, logici ed organizzativi, comprese le politiche, i processi, le procedure, le strutture organizzative, le funzioni software e hardware.
Questi controlli devono essere stabiliti, attuati, monitorati, rivisti e migliorati, se necessario, per garantire che siano rispettati gli obiettivi di sicurezza e di business specifici dell'organizzazione[14].
In questa ottica la sicurezza deve essere quindi considerata "un processo, non un prodotto" [15] e va analizzata ed affrontata attraverso un approccio integrato (tecnologico ed organizzativo, organico, strutturato ed interdisciplinare) ovvero mediante la strutturazione di un processo continuo di analisi, condivisione delle informazioni, riduzione della vulnerabilità, gestione dei rischi, selezione ed attuazione di strategie e controlli, monitoraggio, rilevazione, reazione, recupero e mitigazione degli impatti.

5. L'importanza della Compliance Normativa

Il tema della sicurezza informatica è strettamente correlato a quello della compliance normativa o "*Regulatory Compliance*".
Alcuni dei comportamenti che costituiscono una minaccia alla sicurezza informatica, sono stati

[14] "Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met." (ISO/IEC 27002:2013).

[15] Schneier B., Sicurezza Digitale, Tecniche Nuove, Milano, 2001

infatti qualificati come condotte giuridicamente perseguibili dalle legislazioni degli Stati Membri (es. intrusioni da parte di hacker, introduzione di virus informatici, frodi informatiche, sabotaggi, spionaggio, modifica o cancellazione di dati/informazioni, attentati a sistemi informatici che supportano l'erogazione di servizi di pubblica utilità, abusi di privilegi, utilizzo a fini personali delle risorse informative aziendali, etc..).

La capacità di garantire la conformità normativa e quindi, di diminuire i "*Rischi di compliance*" correlati all'utilizzo delle tecnologie ICT ed assicurare adeguati livelli di riservatezza, integrità e disponibilità dei propri dati, applicazioni e servizi, è uno tra i principali fattori che spingono oggigiorno le organizzazioni ad adottare modelli organizzativi di gestione della sicurezza meglio noti come "*Information Security Management System*" [16].

In tal senso, è possibile delineare il seguente quadro normativo nazionale di riferimento che deve essere preso in considerazione, sia nel settore pubblico che privato, nell'ambito della definizione del sistema di gestione della sicurezza informatica:

Legge n.633/41	Protezione del diritto d'autore e di altri diritti connessi al suo esercizio
DLgs. n.518/92	Tutela giuridica dei programmi per elaboratore
Legge n.547/93	Modificazioni e integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica
DLgs. n.169/99	Tutela giuridica delle banche di dati
Legge n.248/2000	Nuove norme di tutela del diritto d'autore
D.P.R. n 445/2000	T.U. in materia di documentazione amministrativa
DLgs. n.231/2001	Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica
D.P.C.M. 16.01.2002	Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali
DLgs. n.68/2003	Attuazione direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione
DLgs. n.196/2003	Codice in materia di protezione dei dati personali
DLgs. n.259/2003	Codice delle comunicazioni elettroniche
DLgs. n.82/2005	Codice dell'amministrazione digitale
Legge 31.07.2005	Misure urgenti per il contrasto del terrorismo internazionale
DLgs. n.231/2007	Prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo
Prov. Garante Privacy 17.01.2008	Sicurezza dei dati di traffico telefonico e telematico
Legge n.48/2008	Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica e norme di adeguamento dell'ordinamento interno
D.P.C.M. 01.04.2008	Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività
Prov. Garante Privacy 13.10.2008	Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali
Prov. Garante Privacy 13.11.2008	Misure e accorgimenti relativamente alle attribuzioni delle funzioni di amministratore di sistema
D.P.C.M. 30.03.2009	Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici
Deliberazione n.45/2009	Regole tecnico per il riconoscimento e la verifica del documento informatico
DLgs. n. 235/2010	Modifiche ed integrazioni al Codice dell'amministrazione digitale

[16] ISO/IEC 27001:2013 - ISO/IEC 27002:2013

Prov. Garante Privacy 08.04.2010	Provvedimento in materia di videosorveglianza
Legge n.12/2012	Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica
Prov. Garante Privacy 26.07.2012	Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali
D.P.C.M. 24.01.2013	Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale

Particolare rilievo tra le normative sopra citate assume il *Decreto Legislativo del 30 giugno 2003 n.196*[17] "Codice in materia di protezione dei dati personali" poiché nell'ambito della tutela dei dati personali[18] prevede una serie di obblighi generali e specifici di sicurezza introducendo il concetto giuridico di "*Rischio*", di "*Misura idonea*" e di "*Misura minima*". [19] In via generale, il decreto stabilisce all'art. 31[20] che devono essere individuate idonee e preventive misure di sicurezza al fine di proteggere i dati dai rischi di distruzione (riconducibile agli obiettivi di sicurezza della disponibilità e dell'integrità), perdita (riconducibile all'obiettivo di sicurezza della disponibilità) e accesso non autorizzato (riconducibile agli obiettivi di sicurezza della confidenzialità, disponibilità ed integrità), trattamento non conforme o non consentito (riconducibile al controllo accessi e all'integrità dei programmi).
Le misure minime (artt. 33, 34, 35) garantiscono invece quello che la legge definisce il "livello minimo" di protezione dei dati e la loro adozione è "conditio sine qua non" per lo svolgimento delle attività di trattamento. Dette misure devono essere implementate secondo le modalità definite nel Disciplinare Tecnico allegato al Codice (Allegato B), si applicano sia ai trattamenti effettuati

[17] È importante tenere presente l'Europa sta definendo un nuovo Regolamento che avrà lo scopo di mettere "ordine e disciplina", in ottica prevalentemente "europeista", nell'impianto giuridico dei 27 stati membri in materia di privacy e data protection. Il Regolamento avrà portata generale ed andrà a sostituire la direttiva 95/46 CE. Per ciò che concerne l'ambito di operatività, la nuova soluzione normativa godrà di un'applicazione interna e di una esterna. La prima, fondata sulla qualificazione giuridica del regolamento comporta l'applicabilità di un corpus unitario di norme ai 27 stati membri dell'unione, senza che si renda necessario un previo percorso normativo di recepimento e di attuazione ad opera del legislatore interno. La seconda, invece, sancita dall'art. 3 comma 2 del neo-regolamento, implica un'estensione extraterritoriale della portata delle norme ivi contenute, le quali, pertanto, saranno efficaci anche al di fuori del territorio dell'unione, allorquando soggetti extracomunitari porranno in essere trattamenti di dati personali volti a controllare i comportamenti o ad offrire beni e/o servizi a cittadini europei.

[18] Art.4 1c lett.b) del DLgs. n.196/2003 "dato personale, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

[19] Il DLgs. n.196/2003 è stato modificato dal Decreto Legge 6 dicembre 2011 n.201 "Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici" che ha apportato variazioni all'art.4 c1 lett.b (definizione di dato personale) all'art.4 c1 lett.i (definizione di interessato al trattamento) e dal Decreto Legge 9 febbraio 2012 n.5 "Disposizioni urgenti in materia di semplificazione e sviluppo" che ha soppresso i paragrafi dell'allegato B da 19 a 19.8 (documento programmatico sulla sicurezza) e 26 (inserimento nella relazione accompagnatoria del bilancio d'esercizio, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza).

[20] Art.31 del DLgs. n.196/2003 – "Obblighi di sicurezza – I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalita' della raccolta".

nel settore privato che in quello pubblico.
Tra le misure minime riguardanti i trattamenti svolti con l'ausilio di strumenti elettronici il Codice riporta (art. 34 del DLgs. n.196/03) :

- utilizzo di un sistema di autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione ed utilizzo di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, ad accessi non autorizzati ed a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, e per il ripristino della disponibilità dei dati e dei sistemi;
- adozione di tecniche di cifratura o di codici identificativi per dati idonei a rivelare lo stato di salute o la vita sessuale, trattati da organismi sanitari;

Le misure minime relative ai trattamenti svolti senza l'ausilio di strumenti elettronici (art. 35 del DLgs. n.196/03) includono:

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- ed infine, previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Le conseguenze giuridiche derivanti dalla mancata identificazione ed implementazione delle misure idonee di sicurezza sono diverse da quelle connesse all'omessa attuazione delle misure minime.
Per le prime è prevista, nel caso di danno a terzi, una responsabilità oggettiva ex art. 2050 del cod. civ., mentre per le seconde l'applicazione di una sanzione penale (art. 169) consistente nell'arresto fino a 2 anni e di una sanzione amministrativa (art.162 c 2-bis) consistente nel pagamento di una somma da diecimila euro a centoventimila euro.
L'attuazione delle misure di sicurezza risulta fondamentale anche nell'ambito di alcune tutele previste dalla *Legge 23 dicembre 1993 n.547***.** Al riguardo, la legge tutela i sistemi dotati di misure di sicurezza tecnologiche e/o organizzative che esprimono la volontà di riservare l'accesso, la permanenza o l'utilizzo delle risorse informative al solo personale autorizzato.[21] La predisposizione delle misure di sicurezza da parte dell'organizzazione, quindi:

- è necessaria per la punibilità di alcuni comportamenti;
- manifesta la volontà dell'organizzazione di riservare l'accesso o la permanenza solo alle persone autorizzate;
- garantisce l'organizzazione, e coloro che ne hanno la responsabilità, dai rischi di coinvolgimento sia patrimoniale che penale per i fatti penalmente rilevanti tenuti da dipendenti o da terzi.

[21] Sentenza 21 aprile 2000 n. 6677/99 R.G.G.I.P., del Tribunale Penale di Roma, Ufficio GIP, Sezione 8°.

Alla luce delle disposizioni in materia di obblighi generali e specifici di sicurezza previste dal DLgs. n.196/2003, è facile identificare queste misure con quelle previste dal sopra citato decreto agli artt. 31, 33, 34, 35 ed all'Allegato B, quando il reato informatico riguarda informazioni, documenti, sistemi e comunicazioni contenenti e/o riguardanti dati personali.
Accanto al quadro giuridico generale sopra menzionato, è opportuno ricordare che in Italia sono presenti anche Normative Specifiche per il settore delle Pubbliche Amministrazioni[22] oltre a *Linee Guida* che hanno rilevanza come "Best Practice" nell'ambito della gestione della sicurezza informatica. Tra le Linee Guida e le Raccomandazioni si segnalano:

AIPA – 28.10.1999	Linee Guida per la definizione di un piano per la sicurezza
AIPA – 20.09.2001	Manuale dei livelli di servizio nel settore ICT
AIPA –Racc. n.1/2000	Sicurezza dei siti web delle PA
AIPA – 01.11.2001	Linee Guida per la sicurezza dei servizi in rete
Dir. MIT 11.06.2002	Linee guida del Governo per lo sviluppo della Società dell'Informazione
Dir. MIT 20.12.2002	Linee guida in materia di digitalizzazione dell'Amministrazione
DigitPA Quad. 23/2006	Linee Guida per la sicurezza delle pubbliche amministrazioni
DigitPA - 2013	Linee Guida per il Disaster Recovery delle Pubbliche Amministrazioni
Garante Privacy - 2012	Cloud Computing per imprese e pubblica amministrazione

6. Gli Standard internazionali per la gestione della sicurezza

Negli ultimi dieci anni il settore della sicurezza delle informazioni e dei sistemi è stato caratterizzato da un flusso continuo di evoluzioni e miglioramenti che hanno contraddistinto tutte le diverse componenti della disciplina ovvero quella tecnologica, quella organizzativa e di processo.
Un ruolo importante in questo processo evolutivo è stato svolto dai progressi fatti nel settore della "Governance della Sicurezza".
Grazie all'affermarsi della Società dell'Informazione, all'interno delle organizzazioni hanno assunto sempre maggiore rilievo quelli che oramai sono diventati i "*Sistemi di Gestione della Sicurezza delle Informazioni*" (o SGSI) e si è consolidata la prassi che vede nel ricorso all'utilizzo degli Standard Internazionali lo strumento migliore per affrontare in modo sistematico e strutturato il problema.
Il ricorso agli Standard Internazionali in materia di gestione della sicurezza, quale strumento maggiormente idoneo per affrontare e gestire efficacemente la tematica è anche esplicitamente

[22] Tra le Normative Specifiche per il settore delle Pubbliche Amministrazioni di particolare rilievo sono: Decreto MI 19 luglio 2000 - Regole tecniche e di sicurezza per carta d'identità e documento d'identità elettronici; D.P.C.M. 31 ottobre 2000 - Regole tecniche per il protocollo informatico; Decreto 9 dicembre 2004 – Regole tecniche di sicurezza relative alle tecnologie ed ai materiali utilizzati per la produzione della carta nazionale dei servizi; Deliberazione AIPA 11/2004 - Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali.

richiamato all'interno di alcune normative nazionali[23] e codificato a livello europeo[24].
Gli Standard Internazionali dell'Information Security sono documenti di riferimento emessi da enti normativi nazionali (come ad es. il British Standard Institute - BSI) o internazionali (come ad es. l'ISO) nati in risposta alla precisa domanda dei settori dell'industria, del commercio e delle amministrazioni statali, di definire un framework comune per valutare il livello di affidabilità di un sistema/prodotto ICT, e sviluppare ed implementare sistemi di gestione della sicurezza delle informazioni[25].

---

[23] Il D.P.C.M. del 16 gennaio del 2002 emanato dal Dipartimento per l'Innovazione e le Tecnologie (MIT) afferma che "[...] le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del paese". Questo patrimonio, dunque, deve essere adeguatamente protetto e tutelato al fine di prevenire possibili alterazioni sul significato delle informazioni stesse. "E' noto infatti che esistono minacce di intrusione e possibilità di divulgazione non autorizzata di informazioni, nonché di interruzione e di distruzione del servizio", ed assume "[...] importanza fondamentale valutare il rischio connesso con la gestione delle informazione e dei sistemi.". La Direttiva stabilisce i criteri per una prima autovalutazione sul grado di sicurezza tecnologica di ogni amministrazione e la capacità di garantire l'integrità e l'affidabilità dell'informazione pubblica attraverso quelle che la direttiva stessa definisce "credenziali di sicurezza conformi agli Standard Internazionali di riferimento". Il Comitato tecnico nazionale sulla sicurezza informatica e delle comunicazioni nelle pubbliche amministrazioni nella Proposta del marzo 2004, nell'ambito della certificazione ICT, promuove il ricorso agli Standard di sicurezza riconosciuti a livello internazionale, che "[...] rappresentano un mezzo importante per costruire la fiducia e la confidenza sia nei confronti di un'organizzazione che tra le varie parti coinvolte". In particolare la proposta fa riferimento a due standard ISO/IEC: lo standard ISO 15408, noto anche come Common Criteria for Information Technology Security, che "[...] fornisce le principali direttive per la valutazione e certificazione di prodotti e sistemi informatici"; lo standard ISO 17799 (oggi ISO/IEC 27002:2013 e ISO/IEC 27001:2013), che "[...] fornisce importanti indicazioni sulle misure organizzative da intraprendere, in un'azienda, per poter far fronte al problema della sicurezza informatica".

[24] La strategia di gestione della sicurezza Proposta dalla Commissione Europea già nella Comunicazione del 26 gennaio 2001 "*Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica*" comprendeva misure volte a: proteggere gli elementi critici dell'infrastruttura, mediante l'impiego di infrastrutture a chiave privata (PKI), lo sviluppo di protocolli sicuri; proteggere gli ambienti privati e pubblici mediante lo sviluppo di software di qualità, di 'firewall', programmi antivirus, sistemi di gestione dei diritti elettronici, crittazione; rendere sicura l'autenticazione degli utenti autorizzati, l'uso delle carte intelligenti, l'identificazione biometrica, le firme digitali, le tecnologie basate su ruoli. In quest'ottica, la Commissione nella successiva Comunicazione del 6 giugno del 2001 "*Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*" , aveva specificato che con la locuzione "sicurezza delle reti e dell'informazione" si deve intendere la "capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema". Il Consiglio dell'Unione Europea nella Risoluzione del 28 gennaio del 2002 "*Approccio comune e ad azioni specifiche nel settore della sicurezza delle reti 2002/C43/02*" aveva ulteriormente sottolineato che la sicurezza delle reti e dell'informazione consiste nell'assicurare la disponibilità di servizi e di dati: impedendo interruzioni o intercettazioni abusive delle comunicazioni; confermando che i dati trasmessi, ricevuti o archiviati sono completi e invariati; assicurando la riservatezza dei dati e proteggendo i sistemi da accessi non autorizzato e software maligni; garantendo, infine, l'affidabilità dell'autenticazione. Il Consiglio dell'Unione Europea aveva affermato inoltre che gli Stati membri "…. devono promuovere l'applicazione delle migliori pratiche in materia di sicurezza basate su dispositivi vigenti quali l'ISO/IEC 17799…"

[25] Nel documento "*Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione*" (marzo 2004) il Comitato tecnico nazionale sulla sicurezza informatica e delle comunicazioni nelle pubbliche amministrazioni ha riconosciuto negli attuali Standard Internazionali gli strumenti per la certificazione della sicurezza ICT. All'interno della proposta si scrive "… nel 1999 è stata adottata in tutte le sue tre parti dall'ISO/IEC la raccolta di criteri denominata Common Criteria che consente la valutazione e certificazione della sicurezza di prodotti e sistemi ICT. Tale adozione si è formalmente realizzata attraverso l'emanazione dello standard ISO/IEC IS 15408. L'anno successivo, questo stesso organismo internazionale ha fatto propria la prima parte di un altro standard di certificazione della sicurezza ICT sviluppato in Gran Bretagna, il ben noto BS7799 (diviso in parte 1 e 2) che nella versione ISO/IEC ha assunto prima la denominazione ISO/IEC 17799 (diviso sempre in parte 1 e 2) poi quella di ISO/IEC 27001 (framework per la certificazione) e ISO/IEC 27002 (linee guida per la strutturazione

Dunque, a seconda degli obiettivi da conseguire il contenuto degli Standard può riguardare principalmente le seguenti aree tematiche:
Tecnologie informatiche utilizzate per la difesa del patrimonio informatico:

TCSEC (1985)	Trusted Computer System Evaluation Criteria
ITSEC (1991)	Information Technology Security Evaluation Criteria
ISO/IEC 15408 (1999)	Common Criteria for Information Technology Security Evaluation

Organizzazione e gestione della sicurezza:

ISO/IEC 27000	"Information technology -- Security techniques – Information security management systems – Overview and vocabolari"
ISO/IEC 27001:2013	"Information tecnnology – Security techniques – Information security management systems – Requirements"
ISO/IEC 27002:2013	"Information technology -- Security techniques -- Code of practice for information security management"
ISO 31000:2009	"Risk management — Principles and guidelines"
ISO/IEC 27005:2011	"Information technology -- Security techniques -- Information security risk management"
ISO/IEC 27004-2009	"Information technology -- Security techniques -- Information security management – Measurement"
ISO/IEC 27000-1:2011	"Information technology -- Service Management – Service Management System Requirement"
ISO/IEC TR 1335-1:1996	"Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security"
ISO/IEC TR 1335-2:1997	"Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security"
ISO/IEC TR 1335-5:2001	"Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security"

Lo Standard ITSEC (*Information Technology Security Evaluation Criteria*) nasce nel 1991 come evoluzione dello Standard TCSEC più noto come "Orange Book"[26], e con l'obiettivo di fornire

del sistema) recentemente aggiornati nella versione del 2013. Lo standard ISO/IEC IS 15408 (Common Criteria) e lo standard ISO/IEC 27001, sebbene abbiano in comune la sicurezza ICT, hanno lo scopo di certificare cose ben diverse. Nel caso dei Common Criteria (in seguito denominati brevemente CC), infatti, oggetto della certificazione è, come già anticipato, un sistema o un prodotto ICT13, nel caso invece dell'ISO/IEC 27001 ciò che viene certificato è il processo utilizzato da un'organizzazione, sia essa una società privata o una struttura pubblica, per gestire al suo interno la sicurezza ICT (tale processo, come è noto, viene indicato nello standard con l'acronimo ISMS che sta per "Information Security Management System"). In altri termini, la certificazione ISO/IEC 27001 può essere considerata una certificazione aziendale, del tipo quindi della ben nota certificazione ISO 9000, ma specializzata nel campo della sicurezza ICT.

[26] Il problema della sicurezza dei sistemi operativi fu affrontato per la prima volta in maniera sistematica dal National Computer Security Center (NCSC) usa nella pubblicazione "Trusted Computer System Evaluation Criteria" (TCSEC, nota anche come "Orange Book"). Lo standard introduce i concetti di "politica della sicurezza", intesa come guida formale, esplicita e conosciuta alla esecuzione delle contromisure, di "contromisura" come atto di protezione dei beni adeguato al valore ed al livello di rischio cui gli stessi sono esposti, e stabilisce anche classifica delle contromisure. Dall'Orange Book nel 1991 è stata ricavata una rielaborazione adottata da alcuni paesi europei nota anche come "White Book" il cui nome ufficiale è ITSEC "Information Technology Security Evaluation Criteria". Poiché all'interno dell'Unione europea questo Standard non era l'unico documento adottato dai diversi paesi la CEE redisse nel 1991 un Manuale di riconoscimento delle diverse procedure noto come ITSEM "IT Security Evaluation Manual".

un framework per la valutazione e la certificazione delle funzionalità di sicurezza (tecniche e non tecniche) di:

- un sistema informatico, ossia una specifica installazione IT avente uno preciso scopo in un ambiente operativo completamente definito;
- un prodotto informatico, ossia un dispositivo hardware o un pacchetto software progettati per l'uso e l'installazione in una grande varietà di sistemi.

Nonostante le evidenti differenze tra sistemi e prodotti, lo Standard ITSEC prevede che entrambi siano valutati secondo gli stessi criteri, e che vengano al riguardo identificati dal termine TOE (*Target of Evaluation*). Il TOE, in ITSEC è dunque, l'oggetto della valutazione.

La certificazione è effettuata sulla base di un Security Target ovvero di un documento, definito dal committente, nel quale sono specificate le funzioni di sicurezza che devono essere soddisfatte dal TOE e riportate altre informazioni rilevanti, quali gli obiettivi di sicurezza del sistema/prodotto (in termini di riservatezza, integrità e disponibilità).

La descrizione delle funzioni di sicurezza costituisce la parte più importante del Security Target. Al riguardo lo Standard suggerisce l'ordinamento delle funzioni di sicurezza in 8 gruppi generici, "Generic Headings".

Nell'approccio ITSEC, l'operazione di valutazione del livello di sicurezza, intesa come affidabilità del sistema/ prodotto informatico, si pone due obiettivi fondamentali[27]:

- valutare l'efficacia delle funzioni di sicurezza, in termini di capacità del sistema/prodotto di contrastare efficacemente le minacce alle quali si ritiene sia esposta l'informazione dallo stesso elaborata o immagazzinata;
- valutare la corretta realizzazione delle funzioni di sicurezza e dei corrispondenti meccanismi.

Lo Standard definisce 7 livelli di valutazione dell'affidabilità del sistema/prodotto informatico che rappresentano, dunque, la capacità di quest'ultimo di realizzare le specifiche di sicurezza attraverso le funzioni sopra citate.

Lo Standard ISO/IEC 15408 (*Common Criteria for information technology security evaluation*), nasce dallo sforzo dei rappresentanti degli Stati Uniti, Canada, Francia, Germania, Olanda e Regno Unito, in collaborazione con l'ISO (International Organization for Standardization) di sviluppare uno standard internazionale di valutazione della sicurezza in ambito informatico.

L'obiettivo era quello di sostituire gli Standard TCSEC e ITSEC attraverso la definizione di nuovi criteri in grado di consentire il reciproco riconoscimento della valutazione dei prodotti di sicurezza. Nel 1996 fu rilasciata la versione 1.0 dei Common Criteria. Nell'ottobre 1998 si ebbe il rilascio della versione 2.0 (DIS 15408) che, ora con l'approvazione finale dell'ISO è divenuta a tutti gli effetti un International Standard (ISO/IEC 15408). A gennaio 1999 fu rilasciata una versione draft (v 0.6) della Common Evaluation Methodology avente lo scopo di armonizzare le modalità di valutazione da parte degli enti valutatori. Tale metodologia è alla base per il reciproco riconoscimento.[28]

I Common Criteria dunque, delineano regole e direttive comuni per gli sviluppatori e per gli enti

---

[27] Fonte: documento "Privacy: la sicurezza informatica nell'unione europea ed i criteri ITSEC" (Milano, 1997) del dott. Marco Maglio (reperibile sul sito www.privacy.it).

[28] Fonte: documento "Introduzione ai nuovi standard di sicurezza" dell' Ing. Luigi Baffigo (reperibile sul sito www.privacy.it).

di valutazione, e rappresenta una guida ed una fonte di consultazione per gli utenti degli stessi sistemi informatici.
Come per lo Standard ITSEC, il processo di certificazione della sicurezza di un sistema/prodotto informatico previsto dai Common Criteria si pone l'obiettivo di valutare un sistema/prodotto in base all'efficacia delle funzioni di sicurezza garantite ed alla corretta realizzazione delle stesse e dei corrispondenti meccanismi di sicurezza.
I livelli di valutazione previsti dai Common Criteria sono 7, vengono identificati con la sigla EAL (Evaluation Assurance Levels) e sono stati definiti in modo da essere confrontabili con gli equivalenti livelli dei TCSEC e ITSEC:

- EAL1 testato funzionalmente;
- EAL2 testato strutturalmente;
- EAL3 testato e verificato metodicamente;
- EAL4 progettato, testato e riveduto metodicamente;
- EAL5 progettato e testato in modo semi-formale;
- EAL6 verifica del progetto e testing semi-formali;
- EAL7 verifica del progetto e testing formali.

Il sistema dei Common Criteria utilizza i *Protection Profile* per la valutazione del sistema/prodotto informatico. Il Protection Profile è un documento che contiene l'insieme di requisiti di sicurezza, il loro significato e le ragioni per cui sono necessari, oltre che il livello EAL che il sistema/prodotto deve soddisfare. Esso descrive le condizioni ambientali, gli obiettivi ed il livello previsto per la valutazione della funzionalità e della garanzia, specificando le motivazioni delle scelte effettuate circa il grado di garanzia e di robustezza dei meccanismi di protezione. Il Protection profile è, dunque, l'input per il prodotto da valutare (TOE).
L'utilizzo di prodotti certificati, non solo è spesso richiesta dalle normative nazionali, ma offre numerosi benefici, tra cui la disponibilità di un documento delle specifiche di sicurezza dei sistema/prodotto (il *Security Target*), contenente sia la descrizione delle minacce che il prodotto è in grado di contrastare, sia l'esistenza di test e di verifiche effettuate, secondo metodologie documentate, da un ente indipendente.
Inoltre, oggigiorno le pubblicazioni relative ai Common Criteria rappresentano un valido strumento di supporto nelle attività di progettazione di infrastrutture di sicurezza informatica, ancorché non s'intenda sottoporle al processo di certificazione.
L'ISO/IEC 27001:2013 *(Standard for information security management systems)* è uno Standard di Gestione della Sicurezza delle Informazioni che deriva dallo standard BS 7799 sviluppato dal britannico British Standard Institute (BSI).
Il documento originario (la cui prima edizione venne rilasciata nel 1995 mentre la seconda nel 1999) si componeva di due parti: Parte 1 - BS7799-1:1999 "Code of practice for information security management"; Parte 2 - BS7799-2:1999 "Specification for information security management system".
La Parte 1 forniva delle indicazioni, ovvero dei suggerimenti non prescrittivi per proteggere il patrimonio informativo di un organizzazione, mentre la Parte 2 forniva (e fornisce ancora) le prescrizioni da seguire per il conseguimento della certificazione di sicurezza.
Successivamente, l'ISO ha adottato lo standard BS7799 come proprio, mediante una procedura non usuale (ancorché prevista dai regolamenti dell'ISO stessa) consistente nella dichiarazione

formale che lo standard, così com'era, era da considerarsi approvato e sottoscritto dall'ISO[29]. Nel 2005 la parte 2 è divenuta ISO/IEC 27001 e nel 2007 la parte 1 è divenuta ISO/IEC 27002.
Recentemente entrambi gli Standard sono stati aggiornati a seguito di sostanziali evoluzioni nei loro contenuti dando vita alle attuali versioni 2013.
Oggi, come all'origine la ISO/IEC 27001 costituisce lo schema di riferimento per il conseguimento della certificazione di sicurezza. Oggetto della valutazione è il processo utilizzato dall'organizzazione, ed indicato nello standard con l'acronimo ISMS che sta per "*Information Security Management System*", sia essa una società privata o una struttura pubblica, per gestire al suo interno la sicurezza ICT [30].
Per quanto attiene l'identificazione degli obiettivi di controllo e dei controlli da attuare nell'ambito del sistema, lo Standard ISO/IEC 27001 propone 35 obiettivi di controllo, 114 controlli in 14 aree/categorie più specificatamente dettagliate dalla ISO/IEC 27002.
I controlli presenti al'interno delle aree tematiche, consistono in pratiche, procedure o meccanismi in grado di gestire i rischi, attraverso la riduzione delle minacce e delle vulnerabilità, la limitazione dei possibili impatti e la trattazione degli eventi critici (reazione e ripristino in tempi brevi delle condizioni iniziali).
Lo Standard ISO/IEC 27002:2013 (*Code of practice for information security management*) fornisce le linee guida per la creazione di un sistema di gestione della sicurezza delle informazioni certificabile, prendendo in considerazione i più recenti sviluppi nell'applicazione dell'Information Processing Technology.
In particolare, l'ISO/IEC 27002:

- costituisce un framework di riferimento a livello internazionale, ovvero un insieme di principi e di linee guida, per la strutturazione di un Sistema di Gestione della Sicurezza delle Informazioni (*Information Security Management System* - ISMS);
- fornisce agli addetti ai lavori una metodologia di implementazione, controllo e gestione della sicurezza in modo da agire in accordo alle proprie strategie, individuare le *situazioni d'errore e comportarsi di conseguenza.*

La norma introduce nel campo della sicurezza il concetto di "*Sistema di Gestione*", quale strumento di controllo sistematico e ciclico dei processi legati alla sicurezza, tramite la definizione di ruoli, responsabilità, di procedure formali (sia per l'operatività aziendale che per la gestione delle emergenze) e di canali di comunicazione.
Un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) efficiente, efficace e conforme allo Standard l'ISO/IEC 27002 permette all'organizzazione di:

- comprendere i fattori interni ed esterni al contesto organizzativo che influenzano i fattori di rischio, le necessità e le aspettative delle terze parti interessate;
- rafforzare la leadership ed il coinvolgimento della Direzione per garantire al sistema di gestione di raggiungere i risultati prefissati;
- assicurare responsabilità ed autorità ai ruoli rilevanti nell'ambito della sicurezza delle informazioni;

---

[29] Fonte: White Paper "Introduzione agli standard di Sicurezza delle Informazioni ed Informatica" di Alessandro Bottonelli.

[30] In altri termini, la certificazione ISO/IEC 27001 può essere considerata una certificazione aziendale, assimilabile alla ben nota certificazione ISO 9000, ma specializzata nel campo della sicurezza ICT.

- definire processi di comunicazioni interni ed esterni pertinenti al sistema di gestione della sicurezza delle informazioni;
- implementare politiche, processi e procedure operative di sicurezza, in accordo con normative cogenti e best practice di riferimento;
- definire processi strutturati di verifica e trattamento dei rischi;
- gestire le aree aziendali a rischio, attraverso la selezione di opportuni controlli di sicurezza;
- mantenersi aggiornata su nuove minacce e vulnerabilità, e di affrontarle in modo sistematico;
- creare una cultura della sicurezza all'interno dell'azienda;
- monitorare e misurare le prestazioni del sistema;
- trattare incidenti e situazioni critiche, in ottica di prevenzione e di miglioramento continuo del sistema.

La strutturazione secondo lo Standard del Sistema di Gestione della Sicurezza delle Informazioni, si sviluppa attraverso l'identificazione degli obiettivi di controllo e l'attuazione dei controlli[31] previsti all'interno delle seguenti aree tematiche (in questo contesto, il termine "controllo" deve essere inteso in senso lato come "strumento di gestione"):

1. Politica della sicurezza dell'informazione (Information Security policy).
2. Organizzazione per la sicurezza (Organization of information security).
3. Responsabilità del personale (Human resource security).
4. Classificazione e controllo delle risorse (Asset management).
5. Sicurezza del personale (Human resources security security).
6. Controllo degli Accessi (Access control).
7. Sistemi di crittografia (Cryptography).
8. Sicurezza fisica ed ambientale (Physical and environmental security).
9. Gestione delle operazioni e delle comunicazioni (Communications and operations management).
10. Controllo degli accessi (Access control).
11. Sicurezza nelle operazioni (Operations security).
12. Sicurezza nelle comunicazioni (Communications security).
13. Sviluppo e manutenzione del sistema (System acquisition, development and maintenance).
14. Relazioni con i fornitori (Suppliers relations).
15. Gestione degli incidenti di sicurezza (Information security incident management).
16. Gestione della continuità operativa (Information security aspects of business continuity management);
17. Conformità normativa a leggi, regolamenti, contratti, etc.. (Compliance).

L'ISO/IEC TR 13335 [32] (*Information Technology – Guidelines of IT Security*) è un Technical Report il cui scopo è quello di fornire delle linee guida per un approccio sistematico alla gestione della sicurezza ICT, che consenta di raggiungere e mantenere il livello di confidenzialità, integrità e

[31] Lo schema del Decreto Legislativo 196/2003 "Codice in materia di protezione dei dati personali" ha preso spunto dallo Standard ISO/IEC 27002, ma mentre lo Standard prende in considerazione tutte le tipologie di informazione, la legge si applica solo ai dati personali.

[32] La serie ISO/IEC 13335 che fa parte dei GMITS (Guidelines for the Management of IT Security).

disponibilità definito dall'organizzazione all'interno degli obiettivi di sicurezza[33].
Tali indicazioni non riguardano solo gli aspetti di gestione della sicurezza ma anche le misure di dettaglio per l'implementazione e la manutenzione delle procedure. Quindi se gli Standard ISO/IEC 27001 e ISO/IEC 27002 si fermano al "perché" ed al "cosa", il TR 13335 fornisce molti elementi sul "come".
Il TR 13335 era originariamente diviso in cinque parti:

- Parte 1: Concetti e Modelli di IT Security (Concepts and Models for IT security);
- Parte 2: Gestione e Pianificazione della Sicurezza IT (Managing and Planning IT security);
- Parte 3: Tecniche di Gestione della Sicurezza IT (Techniques for the management of IT security);
- Parte 4: Selezione delle contromisure (Selection of Safeguards);
- Parte 5: Guida al management della Sicurezza di Rete (Management Guidance on Network Security).

Nel 2008 la Parte 3 e la Parte 4 sono divenuti ISO e formalizzate al'interno dell'attuale versione dello Standard ISO/IEC 27005:2011 (Standard for information security risk and management).
La norma, che ricalca i concetti della vecchia ISO Guide 73[34] e ne riusa la terminologia, fornisce delle linee guida sulla gestione del rischio legato alla sicurezza IT e supporta l'applicazione della norma ISO/IEC 27001:2013. Si divide in Valutazione (Assessment) e Trattamento del Rischio, l'Analisi ne è un sottoinsieme. Riporta dettagli precisi per ogni fase e numerosi esempi negli annex informativi.
La norma ISO/IEC 27005 non fornisce tuttavia alcuna specifica metodologia poiché è compito delle singole organizzazione definire un approccio adeguato al contesto di riferimento, in considerazione degli obiettivi di sicurezza che si intendono raggiungere.

7. Modelli di gestione della sicurezza

La Gestione della Sicurezza ICT è un processo ciclico (Information Security Management System o ISMS) il cui scopo fondamentale è, dunque, quello di attuare un ragionevole compromesso tra il costo della sicurezza e i costi della non sicurezza e, raggiungere e mantenere appropriati livelli di confidenzialità, integrità e disponibilità delle risorse del sistema informativo detenute dall'organizzazione nonché di autenticità e di non ripudio delle informazioni trasmesse.
Il modello processuale di gestione della sicurezza informatica trae origine dalle indicazioni fornite dagli attuali Standard internazionali di riferimento in tema di organizzazione e gestione della sicurezza (ISO/IEC 27001:2013, ISO/IEC 27002:2013 e ISO/IEC 27005:2008 ecc) e dalle Best

[33] Non trattandosi, dunque, di uno standard non esiste una certificazione ISO TR 13335. Le procedure ISO prevedono, infatti, l'emissione di un Technical Report in alcune circostanze in cui non si possa giungere alla definizione di uno standard vero e proprio o per mancanza di consenso o per la generalità dell'argomento. Il TR 13335 ricade in quest'ultima casistica (Fonte: White Paper "Introduzione agli standard di Sicurezza delle Informazioni ed Informatica" di Alessandro Bottonelli).

[34] ISO Guide 73:2009 (aggiornamento della ISO Guide 73:2002) - "Risk management"; Vocabulary; Guidelines for use in standards.

Practice di riferimento in materia. Tra queste ultime rilevano:

ITIL v3 - 2011	Information Technology Infrastructure Library
COBIT v5 - 2012	Control Objectives for Information and related Technology

Il Modello si scompone nelle seguenti fasi, ciascuna delle quali prevede lo svolgimento di una serie di attività:

- Fase 1: Definizione delle Politiche di sicurezza aziendali:
  - Individuazione degli Obiettivi di sicurezza aziendali;
  - Strutturazione del modello di gestione della security aziendale;
  - Individuazione dei Ruoli e delle Responsabilità;
  - Definizione di Criteri Generali e riferimenti di conformità.
- Fase 2: Analisi dei Rischi:
  - Individuazione e valorizzazione dei beni da proteggere;
  - Individuazione e valutazione degli Impatti, delle Minacce e delle Vulnerabilità cui i beni da proteggere sono esposti (Misura del Rischio);
  - Individuazione delle misure di sicurezza raccomandate e stima dei relativi costi.
- Fase 3: Gestione dei Rischi:
  - Gap Analysis tra le misure di sicurezza raccomandate e quelle già presenti in azienda;
  - Scelta della strategia di gestione del rischio.
  - Mappatura delle misure sui controlli di sicurezza previsti dalla 27001.
- Fase 4: Elaborazione del Piano per la Sicurezza:
  - Pianificazione degli interventi di sviluppo delle misure di sicurezza;
  - Definizione delle specifiche funzionali delle misure di sicurezza;
  - Analisi e studi di fattibilità.
- Fase 5: Definizione di Standard e Procedure di sicurezza:
  - Definizione degli standard e delle procedure specifiche per l'esercizio ed il monitoraggio delle misure di sicurezza.
- Fase 6: Progettazione, sviluppo ed implementazione delle misure di sicurezza:
  - Effettuazione di verifiche architetturali;
  - Realizzazione e collaudo delle misure;
  - Certificazione delle soluzioni;
  - Implementazione delle misure.
- Fase 7: Esercizio delle misure di sicurezza:
  - Gestione delle misure di sicurezza implementate in conformità agli standard ed alle procedure operative definite.
- Fase 8: Gestione degli incidenti:
  - Adozione di processi e strumenti di rilevazione, identificazione, analisi e risposta agli incidenti.
  - Definizione di processi e procedure di comunicazione ed escalation e livelli di autorità interni ed esterni.

- Fase 9: Gestione della Continuità Operativa:
  - Effettuazione di una Business Impact Analysis, definizione delle strategie ed attuazione delle soluzioni e delle procedure di Disaster Recovery;
  - Definizione di piani di Business Continuity.
- Fase 10: Monitoraggio:
  - Misurazione della efficacia del sistema;
  - Verifica continua della compliance del sistema.
  - Reporting;
  - Gestione delle criticità e proposte migliorative.
- Fase 11: Formazione:
  - Progettazione ed erogazione di Piani formativi mirati e differenziati per il personale (crescita del grado di consapevolezza, sensibilizzazione sulle problematiche di sicurezza informatica, sviluppo di specifiche competenze).
- Fase 10: Comunicazione:
  - Definizione ed erogazione di Piani di comunicazione per ciascuna delle fasi del processo di gestione della sicurezza informatica.

Definizione delle politiche di sicurezza

La salvaguardia del patrimonio informativo aziendale è una scelta strategica manageriale volta a consentire e favorire il raggiungimento degli obiettivi di business attraverso:

- la tutela delle risorse informative nel loro valore patrimoniale e reddituale;
- la garanzia della qualità del servizio, venendo incontro alla domanda di fiducia degli interlocutori sociali (stakeholders) interni ed esterni;
- la garanzia della continuità operativa, prevenendo l'interruzione del business anche in condizioni estreme.

Una politica di sicurezza, è una formale dichiarazione degli obiettivi (rientrano negli obiettivi anche la conformità alle normative nazionali, generali e di settore, in materia di sicurezza delle informazioni), delle linee guida strategiche e del modello logico, organizzativo e gestionale definiti per l'attuazione di tale strategia[35]. Tale documento deve, quindi, essere approvato dal Management aziendale, pubblicato e comunicato a tutti i dipendenti e costituisce la cd. *Corporate ICT Security Policy.* Accanto alle Corporate ICT Security Policy, che esprimono dunque gli obiettivi e le strategie di sicurezza aziendali, è possibile trovare anche le *Department ICT Security Policy e le System Specific ICT Security Policy* .[36] Le Department ICT Security Policy individuano i requisiti funzionali e le regole tecniche e procedurali relativamente a tutte le misure di sicurezza applicabili alle strutture che erogano i servizi di business e/o amministrativi. Le System Specific ICT Security Policy individuano invece le regole specifiche di gestione della misura di sicurezza selezionata.

---

[35] Standard ISO/IEC 27002:2005. Paragrafo 5.1 - Information Security Policy. "*Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations*. Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization."

[36] ISO/IEC TR 1335-2:1997 - "Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security"

Analisi dei rischi

Tutte le più accreditate metodologie internazionali di gestione della sicurezza informatica sono concordi nel considerare l'attività di analisi dei rischi come prerequisito per una progettazione razionale dei sistemi di protezione e quindi per una corretta individuazione dei controlli di sicurezza.

Le organizzazioni che intendono affrontare, dunque, in maniera adeguata ed efficace il problema dell'Information Security devono creare adeguati programmi di gestione delle minacce e delle vulnerabilità, in modo da tenere sotto controllo i rischi, reagire prontamente ad ogni specifico problema e risolvere rapidamente tutti gli incidenti quando si verificano.

Presupposto necessario alla scelta della migliore strategia di gestione della sicurezza è, quindi, la corretta conoscenza dei rischi specifici cui i sistemi informativi aziendali sono esposti. E' quindi essenziale essere in grado di identificare e valutare i rischi esistenti o potenziali e il loro possibile impatto sull'organizzazione in termini di perdite economiche, violazione normative, rallentamenti dell'operatività, perdita di immagine etc...

In questo fase entrano in gioco i concetti di Rischio, Minaccia, Danno e Vulnerabilità.

Rischio	Può essere considerato come la probabilità che delle minacce, sfruttando vulnerabilità intrinseche o estrinseche ai beni dell'organizzazione (informazioni, risorse hardware, risorse software, location, personale), producano impatti negativi sull'organizzazione, in termini di perdite economiche, violazione normative, rallentamenti dell'operatività, perdita di immagine etc...
Minaccia	Viene generalmente definita come un evento o una azione, di natura accidentale o deliberata che, sfruttando punti deboli o vulnerabilità di sistemi, applicazioni o servizi, risulta potenzialmente idonea a provocare effetti dannosi sull'organizzazione. Le minacce possono essere fisiche (insistono su aree, edifici, locali, uffici e sfruttano vulnerabilità dell'ambiente fisico), tecnologiche (insistono sulle infrastrutture ICT e sfruttano vulnerabilità di configurazioni o installazioni) organizzative (sfruttano vulnerabilità rappresentate dal mancato senso di appartenenza, responsabilità e professionalità da parte del personale).
Vulnerabilità	E' una condizione di debolezza nel sistema operativo, nelle procedure di sicurezza, nei controlli interni (tecnici, operazionali e/o gestionali) o nella loro implementazione che, se sfruttata da una minaccia, può compromettere la riservatezza, l'integrità e la disponibilità dei beni aziendali. Le vulnerabilità possono dipendere dalla mancanza di appropriati meccanismi di sicurezza o da deficienze nelle procedure di utilizzo da parte degli utenti, da carenze organizzative o di assegnazione di responsabilità, dalla collocazione geografica del sistema informatico (es. ubicazione in una zona altamente sismica), da errori sistemici presenti nell'hardware o nel software (es. errori di progettazione), da possibili malfunzionamenti accidentali dell'hardware.
Danno	E' la conseguenza negativa del verificarsi di un rischio o dell'attuarsi di una minaccia. Si può distinguere il danno in "tangibile" (danno monetario traducibile in una perdita economica diretta o indiretta) e "intangibile" (danno di immagine o comunque immateriale)[37], oppure in "Business Consequence" (frodi o attacchi informatici andati a buon fine), "Security Breach" (perdita di disponibilità, integrità, riservatezza dovuti ad un incidente, come un guasto agli elaboratori) e "Data breach" (perdita, distruzione o diffusione indebita dei dati a seguito di attacchi informatici o di eventi avversi, come incendi o altre calamità).

Impatto	E' un concetto presente nella maggior parte degli strumenti/metodologie di analisi dei rischi la cui definizione spesso si sovrappone a quella di danno. Alcuni strumenti/ metodologie associano il concetto di impatto a quello di misura o entità del danno, ma la definizione che accomuna la maggior parte di essi[38] vede l'impatto come effetto sull'organizzazione e sul suo business del verificarsi di una minaccia, quindi l'effetto reale del danno sul sistema. L'impatto in questa accezione deve tenere conto ad esempio anche di possibili responsabilità civili o penali.

L'Analisi dei rischi costituisce uno strumento mirato all'individuazione del quadro generale delle reali esigenze di sicurezza aziendali[39] e si articola nelle seguenti attività da compiersi in sequenza ordinata:

- Classificazione degli Asset, ovvero delle informazioni e delle risorse informatiche da proteggere, attraverso la loro valorizzazione. Le informazioni andranno valutate ai fini degli obiettivi di integrità, riservatezza e disponibilità previsti nella definizione delle politiche di alto livello. Le risorse informatiche andranno valutate ai fini degli obiettivi di disponibilità.
- Individuazione e valorizzazione delle minacce e delle vulnerabilità cui gli Asset sono potenzialmente esposti.
- Calcolo del profilo di rischio.
- Identificazione delle protezioni offerte dai controlli identificati dalla ISO/IEC 27001 (contromisure raccomandate).
- Gap Analysis, ovvero valutazione del livello di scostamento tra le contromisure consigliate e quelle esistenti o pianificate all'interno dell'azienda.

Gestione dei rischi

Secondo lo Standard ISO/IEC 27002 le aree di rischio da gestire vanno identificate in base alla politica per la sicurezza e al grado di assicurazione richiesto. Partendo dall'assunto che la sicurezza totale non esiste, la scelta della strategia di gestione del rischio ha due obiettivi:

- prioritizzare i rischi sulla base delle indicazioni fornite dalle politiche di sicurezza;
- individuare un livello di rischio accettabile per l'azienda (rischio residuo);
- selezionare i controlli maggiormente efficaci e dal costo ragionevole in grado di ridurre i rischi al livello considerato accettabile.

L'identificazione della migliore strategia di gestione del rischio risulta essere, dunque, correlata:

- ai costi sostenibili dall'azienda per ottimizzare il livello di sicurezza esistente;
- ai benefici derivanti dall'approntamento delle misure di sicurezza ottimali;
- all'accettazione di un livello di rischio residuo.

e deve avvenire attraverso:

- la pianificazione in accordo con il Management del piano d'investimento per la gestione

[37] "Security impacts can be tangible, such as fines, or intangible, like loss of reputation. Impact is defined as a consequence of an undesirable incident that can be caused deliberately or accidentally and affects the software. The consequences can result in destruction or damage of software artifacts or even in loss of confidentiality, integrity, or availability" (Standard ISO/IEC 21827).

[38] ISA, CRAMM, EBIOS, ISO21827, OCTAVE, RAF, SARA, SPRINT e CETRA

[39] La certificazione ISO/IEC 27001 si basa sui risultati di una formale analisi del rischio.

dei rischi, quindi l'individuazione dei piani di intervento prioritari;
- la valutazione dei vincoli di realizzazione dei piani d'intervento (vincoli di tipo temporale, ambientale, economici, etc..).

Selezione dei controlli di sicurezza

"… Un sistema di sicurezza può essere paragonato a una catena, composta da vari anelli, ciascuno dei quali influisce in modo determinante sulla sua resistenza. Come in qualsiasi catena, la forza del sistema di sicurezza corrisponde a quella del suo componente più debole…"[40].

Per ridurre o prevenire lo sfruttamento, da parte di una potenziale minaccia, di una vulnerabilità, intrinseca o estrinseca ai beni aziendali, si rende necessaria un'opera di controllo mediante l'applicazione di particolari contromisure protettive rappresentate da azioni, dispositivi, procedure o tecniche.

Con il termine contromisure si indicano, quindi, gli strumenti organizzativi e tecnologici in grado di contrastare e abbattere il livello del rischio, riducendolo ad un livello individuato come accettabile. Poiché il costo dei controlli di sicurezza deve essere appropriato rispetto al rischio cui deve far fronte un'organizzazione, risulta di fondamentale importanza la scelta del "cocktail" di strumenti più adeguato alle esigenze di business dei diversi servizi dell'organizzazione.

8. Logiche Organizzative per i presidi della sicurezza

L'attuazione del "Sistema di Gestione della Sicurezza delle Informazioni"[41] (SGSI), comporta la definizione di un'infrastruttura organizzativa che si renda responsabile della sicurezza delle informazioni in tutti i suoi aspetti [42] ed assicuri:

- la gestione ed il controllo dei processi e delle attività legate alla sicurezza (SGSI);
- la protezione delle risorse informative aziendali:
    - nei rapporti interni (dipendenti, collaboratori, consulenti, etc..);
    - nei rapporti con le terze parti (clienti, fornitori, partner, etc..);
    - nei casi di affidamento all'esterno delle attività di trattamento (outsourcing).

Di seguito vengono descritti i principali ruoli e le responsabilità previste dalle normative internazionali e dalla legislazione italiana in materia di gestione della sicurezza.

---

[40] Schneier B. - Sicurezza digitale, Tecniche nuove (Milano 2001)

[41] Information Security Management System (ISMS)

[42] Standard ISO/IEC 17799. Paragrafo 4.1 – *Organizational Security*. "Objective: To manage information security within the organization. A management framework should be established to initiate and control the implementation of information security within the organization. Suitable management fora with management leadership should be established to approve the information security policy, assign security roles and co-ordinate the implementation of security across the organization. If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when dealing with security incidents. A multi-disciplinary approach to information security should be encouraged, e.g. involving the co-operation and collaboration of managers, users, administrators, application designers, auditors and security staff, and specialist skills in areas such as insurance and risk management".

Il ruolo della Direzione

La Direzione, ha la responsabilità di definire gli obiettivi, le linee guida strategiche ed il modello logico-organizzativo di gestione della sicurezza aziendale.

In base alla vigente normativa nazionale in materia di protezione dei dati personali (DLgs. n.196/2003) tale ruolo coincide con quello del "*Titolare del trattamento dei dati*" cui spettano tutte le "… decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza" (art. 4 lett. f del sopra citato decreto).

Compito della Direzione è, dunque, quello di dar vita ad un'organizzazione di sicurezza, attraverso:

- la strutturazione del modello processuale dell'SGSI;
- l'assegnazione dei ruoli e delle responsabilità nell'ambito della gestione della sicurezza;
- la definizione delle politiche, delle linee guida, delle procedure e delle direttive in materia di protezione delle informazioni;
- la scelta della strategia e degli strumenti per la gestione dei rischi;
- il potere di controllo sullo stato di attuazione dell'SGSI.

Il Management divisionale e dipartimentale

Il Management di livello divisionale e dipartimentale, avendo conoscenza diretta del funzionamento dei propri dipartimenti e delle mansioni del personale, ha la responsabilità di contribuire alla formazione delle politiche di sicurezza, di partecipare ai processi di analisi e di controllo del rischio, all'analisi costi/benefici delle contromisure e al monitoraggio delle attività di sicurezza.

Tale figura può essere ricondotta al ruolo del "Contitolare del trattamento dei dati" cui può essere attribuito, su delega, il potere di controllo e di vigilanza spettante al Titolare del trattamento dei dati (DLgs. n.196/2003).

Il Management di livello divisionale e dipartimentale esercita generalmente il suo ruolo delegando parte dei propri compiti, pur condividendo la responsabilità, al Management operativo, agli specialisti di sicurezza, ai System Administrator ed agli Auditor.

Il Management operativo

Il Management operativo ha il compito di fornire informazioni operative al personale per pianificare, organizzare e monitorare il sistema di gestione della sicurezza, implementare le politiche, le linee guida, le procedure ed attuare i controlli di sicurezza.

Poiché è generalmente responsabile del processo/servizio con cui viene generato il dato, ed è il proprietario delle applicazioni utilizzate per la sua elaborazione (Proprietario delle Applicazioni/Dati) risulta essere il massimo responsabile della protezione delle informazioni e della sicurezza in generale. A lui verrà imputata ogni negligenza che abbia come conseguenza l'alterazione, la perdita o la divulgazione illecita delle informazioni.

Il suo ruolo coincide con quello del "Responsabile del trattamento dei dati" previsto all'art. 29 del DLgs. n.196/2003.

Il System Administrator

Il System Administrator ha il compito di sovrintendere alla gestione delle risorse dell'infrastruttura informatica (base dati, applicazioni, sistemi, rete) e di consentirne l'utilizzazione. A seconda delle risorse amministrate può ricoprire il profilo autorizzativo di: Domain/Server Administrator,

Account Administrator, Network Administrator, Security Adminidtrator, Backup Administrator, Application Administrator, Database Administrator e Local Administrator/Technical Support.
Generalmente è identificabile con il gestore delle reti/sistemi/applicazioni/dati, deve essere formalmente individuato ai sensi del Provvedimento del 27 novembre 2008 emanato dall'Autorità Garante per la protezione dei dati in materia di "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e relativamente agli aspetti di sicurezza è responsabile:

- della gestione e dell'adeguamento dell'infrastruttura informatica a livelli tecnologici tali da garantire la riservatezza, l'integrità e la disponibilità dei dati e dei servizi, dell'implementazione dei meccanismi di sicurezza;
- dell'implementazione e della gestione dei meccanismi di sicurezza secondo le politiche, gli standard e le linee guida che riguardano la sicurezza delle informazioni e la protezione dei dati;
- della gestione dei sistemi di user management secondo le politiche definite dall'organizzazione e nel rispetto dei requisiti di sicurezza definiti dalla normativa, della verifica del loro corretto utilizzo e sostituzione;
- dell'adozione e dell'aggiornamento di idonei sistemi antivirus da aggiornare periodicamente con cadenza almeno semestrale, e comunque ogniqualvolta l'aggiornamento si renda necessario garantendo sempre alle apparecchiature della rete le ultime firme disponibili dalla casa produttrice;
- della predisposizione del sistema di registrazione e conservazione di tutti i log dei sistemi antintrusione (Firewall, Proxy, IPS, IDS, ecc..) secondo le tempistiche e le modalità stabilite dalla normativa, in modo da assicurare, in caso di attacchi, la disponibilità e l'integrità delle informazioni dell'attaccante e garantire la possibilità di ricostruire ogni tentativo di intrusione e gestire l'evento;
- dell'implementazione delle politiche di registrazione e conservazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione, alle applicazioni e agli archivi elettronici effettuati dagli Utenti, assicurando che le registrazioni (access log) siano conservate secondo le tempistiche e le modalità stabilite dalla normativa, ed abbiano caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste;
- della pianificazione ed attuazione della strategia di backup e recovery di dati, applicazioni e sistemi;
- della validazione periodica dell'integrità dei dati e dei supporti (sia online sia di back up);
- della gestione e risoluzione dei guasti o del malfunzionamenti SW e HW legati ai sistemi informatici e telematici.
- del monitoraggio delle eventuali violazioni al sistema.

Gli Utenti

Gli utenti sono tutti gli individui che quotidianamente utilizzano, ai fini lavorativi, i programmi ed i dati elaborati dai sistemi aziendali.
La loro responsabilità consiste nell'utilizzare correttamente le applicazioni/dati secondo le prescrizioni dettate dal Management operativo per preservare la disponibilità, l'integrità e la riservatezza delle informazioni., nei limiti dell'autorizzazione e conformemente ai profili/privilegi

ad esso assegnati (lettura, scrittura e non cancellazione, modifica, etc.), ottenuta da questo ultimo. Detta figura coincide con quella dell' "Incaricato del trattamento dei dati" definito dal DLgs. n.196/2003 come la "… persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile" (art. 4 lett. h del sopra citato decreto).

9. La Certificazione ISO/IEC 27001:2013

Obiettivo della certificazione ISO/IEC 27001:2013 è quello di attestare che l'organizzazione ha definito un "Sistema di Gestione della Sicurezza delle Informazioni" (SGSI) conforme a quanto previsto dalla norma.
I benefici diretti conseguenti alla certificazione dell'SGSI risiedono nella:

- formale attestazione da parte di una terza parte fidata (il Certificatore) della conformità dell'organizzazione allo Standard ISO/IEC 27001;
- capacità del sistema di tutelare efficacemente il patrimonio informativo aziendale, attraverso:
    - l'attribuzione di specifici ruoli e responsabilità nell'ambito della gestione della sicurezza;
    - la gestione delle aree aziendali a rischio;
    - il presidio delle attività relative alla generazione di procedure di sicurezza e tracciamento di operazioni critiche;
    - la prevenzione e risoluzione di incidenti.

Indirettamente il conseguimento della certificazione comporta un aumento della fiducia di clienti, fornitori e partner con conseguente accrescimento sul mercato del vantaggio competitivo dell'azienda, ed infine l'attestazione di una situazione di conformità rispetto alle normative nazionali in materia di gestione della sicurezza delle informazioni.
Ai fini della certificazione, dunque, l'organizzazione deve strutturare un SGSI aggiornato, documentato e conforme a quanto previsto dalla norma.
Il modello definito dalla ISO/IEC 27001:2013 per la strutturazione del sistema propone un approccio per processi che consente di gestire il miglioramento continuo del sistema e di garantire nel tempo la sua adeguatezza e rispondenza agli obiettivi aziendali.
Mentre l'edizione 2005 della norma faceva esplicito riferimento al ciclo Plan-Do-Check-Act (PDCA[43]) come metodo per sviluppare e migliorare continuamente un SGSI, l'edizione 2013 non prescrive questo approccio ma ne consente comunque l'utilizzo così come quello di altri approcci.

---

[43] Standard ISO/IEC 27001:2005. Paragrafo 0.2 - *Process Approach*. "…This International Standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes…
*Plan (establish the ISMS)***.** Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS). Implement and operate the ISMS policy, controls, processes and procedures.
*Check (monitor and reviewthe ISMS)***.** Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS). Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS...."

In base al modello PDCA, nella fase "Plan", sono previste le seguenti attività:

- Definizione dell'ambito (Scope) di applicazione del sistema di gestione della sicurezza delle informazioni, in termini di caratteristiche dell'azienda, della sua collocazione, beni e tecnologia;
- Definizione delle politiche di sicurezza delle informazioni a livello corporate;
- Definizione di un approccio sistematico per l'analisi dei rischi;
- Identificazione e valutazione dei rischi;
- Individuazione delle misure di sicurezza raccomandate e gap analisys con quelle già presenti al'interno dell'organizzazione;
- Definizione della strategia di gestione delle aree di rischio individuate sulla base delle politiche di sicurezza e del grado di assicurazione richiesto (identificazione delle opzioni per il trattamento dei rischi: eliminazione, trasferimento, riduzione);
- Mappatura delle misure sui controlli 27001;
- Redazione di una dichiarazione di applicabilità (SOA – Statement of Applicability), che dovrà documentare gli obiettivi di controllo e i controlli selezionati, nonché esplicitare le motivazioni della loro selezione e registrare e motivare l'esclusione di qualsiasi controllo elencato nell'appendice A della ISO/IEC 27001:2013.

Nella fase "Do" del modello, sono previste:

- Formulazione di un piano operativo di trattamento dei rischi;
- Implementazione del piano;
- Implementazione delle contromisure selezionate;
- Svolgimento di programmi di informazione e formazione;
- Esercizio delle contromisure implementate;
- Adozione di procedure e di altre misure che assicurino la rilevazione e le opportune azioni in caso di incidenti relativi alla sicurezza.

La fase "Check" prevede:

- Esecuzione delle procedure di monitoraggio dell'SGSI;
- Esecuzione di revisioni per l'accertamento del rischio residuo;
- Conduzione di audit interni all'SGSI;
- Esecuzione di review al massimo livello dirigenziale dell'SGSI;
- Registrazione delle azioni e degli eventi che potrebbero avere impatti sulla sicurezza o sulle prestazioni dell'SGSI.

Infine, la fase "Act" del modello prevede:

- Implementazioni delle azioni migliorative dell'SGSI identificate;
- Implementazione delle azioni correttive;
- Comunicazione dei risultati;
- Verifica che i miglioramenti raggiungano gli obiettivi identificati alla loro base.

La norma contiene una Appendice A[44], all'interno della quale definisce i controlli da attuare per la protezione delle informazioni. In linea con quanto previsto dallo Standard ISO/IEC 27002 vengono proposti 35 obiettivi di controllo, 114 controlli in 14 aree/categorie che vengono di

[44] ISO/IEC 27001:2013 - Annex A "Reference control objectives and controls".

seguito riportati.

Politiche di sicurezza [45]

E' il primo dei controlli previsti dalla norma. La politica di sicurezza è un documento formale, approvato dal management aziendale, che fornisce le direttive, le linee guida ed il modello logico organizzativo e gestionale definiti dal Management per la sicurezza delle informazioni.
Deve essere pubblicata e comunicata, in modo appropriato, a tutti i dipendenti.
La politica di sicurezza deve contenere almeno:

- una breve descrizione degli obiettivi di sicurezza ovvero dei principi e delle normative (aderenza ai requisiti legislativi e contrattuali e Standard) cui il Management intende conformarsi;
- una definizione delle responsabilità per la sicurezza ICT;
- le linee guida di supporto per il raggiungimento degli obiettivi.

Deve essere regolarmente revisionata, ed in caso di cambiamenti particolarmente significativi, la revisione dovrà essere tale da garantirne l'adeguatezza. A tal fine dovrà essere individuato un responsabile per il mantenimento della politica di sicurezza.

Organizzazione della sicurezza delle informazioni [46]

In seno all'organizzazione devono essere definite ed assegnate le responsabilità per la gestione della sicurezza delle informazioni, affinché il problema venga affrontato con il giusto impegno ed attraverso un'adeguata allocazione delle risorse.
La sicurezza dell'informazione è infatti una responsabilità di business che deve essere condivisa da tutti i membri del Management aziendale.
L'organizzazione deve anche:

- operare una segregazione di ruoli e di responsabilità per evitare l'insorgere di conflitti e ridurre le opportunità di modifiche o manomissioni volontarie o accidentali degli asset aziendali;
- servirsi di esperti e specialisti della sicurezza per il coordinamento delle attività all'interno dell'organizzazione e stabilire appropriati contatti con le autorità competenti, e le forze dell'ordine;
- verificare l'adeguatezza e coordinare l'implementazione di specifici controlli di sicurezza per i nuovi sistemi;
- garantire la sicurezza nell'utilizzo dei Device (smartphone e tablet) e nel telelavoro.

Sicurezza delle risorse umane [47]

Obiettivo dei controlli è ridurre il rischio della commissione di errori umani, violazioni, frodi o uso improprio delle strutture dell'organizzazione. A tal fine è necessario che l'azienda:

- includa la sicurezza nella definizione delle responsabilità del lavoro attraverso:
    - lo screening del personale. All'atto dell'assunzione dovrebbero essere richiesti o

[45] ISO/IEC 27001:2013 - A.5 "Information Security policy".

[46] ISO/IEC 27001:2013 - A.6 "Organization of information security".

[47] ISO/IEC 27001:2013 - A.7 "Human resources security".

verificati l'identità, le referenze personali, il curriculum vitae, i titoli di studio, etc..
    - la stipula di accordi di riservatezza. I termini e le condizioni di impiego dovrebbero illustrare al riguardo diritti e responsabilità giuridiche.
- si accerti che la sicurezza sia parte della formazione del personale e quindi proceda ad un adeguata educazione ed addestramento del personale alla sicurezza, attraverso corsi di formazione sulle politiche, le procedure e gli strumenti inerenti la gestione della sicurezza;
- definisca provvedimenti disciplinari in caso di violazione delle leggi in materia di sicurezza.

Gestione dei beni [48]

Obiettivo dei controlli previsti in questa categoria è quello di assicurare un'adeguata protezione ai beni dell'organizzazione. Al riguardo la ISO/IEC 27001:2013 prevede che si proceda:

- all'inventario di tutti i beni (informazioni: database, documentazione, procedure, manuali d'uso, risorse SW - di base, applicativo, di sistema, tool di sviluppo,… - e HW - monitor, modem e strumenti di communication quali router e fax …), attraverso l'identificazione e la documentazione del responsabile e della classificazione di sicurezza;
- alla classificazione delle informazioni, attraverso:
    - la definizione di linee guida che identifichino i vari livelli dell'informazione (pubblica, riservata, segreta, personale, sensibili etc..);
    - la previsione dei controlli associati alle informazioni critiche aziendali;
    - la predisposizione di procedure inerenti l'etichettatura ed il trattamento (copia, archiviazione, trasmissione, distruzione) delle informazioni classificate in accordo con le linee guida.
- alla predisposizione di procedure di gestione dei supporti rimovibili in accordo con la classificazione delle informazioni affinché sia impedito l'accesso non autorizzato, la compromissione e la corruzione delle informazioni anche durante il loro trasporto.

Controllo degli accessi [49]

Obiettivo dei controlli previsti in questa sezione dalla ISO/IEC 27001:2013 è di assicurare la correttezza e la sicurezza delle operazioni connesse al trattamento delle informazioni.

Per quanto attiene la definizione delle regole per l'accesso alle informazioni ed ai sistemi di informazione è sempre opportuno stabilire policy del tipo: "è generalmente proibito se non esplicitamente permesso" piuttosto che "è permesso se non espressamente proibito" e procedere secondo le seguenti direttive:

- i diritti di accesso devono essere congruenti agli scopi lavorativi;
- ad ogni utente dovrebbe essere:
    - fornito un ID univoco, in modo da poter risalire alle relative responsabilità e l'indicazione scritta dei suoi diritti di accesso;
    - richiesto di firmare una dichiarazione di accettazione delle condizioni di accesso;
- deve essere mantenuta una registrazione di tutti gli utenti abilitati e devono essere definite

[48] ISO/IEC 27001:2013 - A.8 "Asset management".

[49] ISO/IEC 27001:2013 - A.9 "Access Control".

delle procedure per la verifica periodica del la correttezza delle registrazioni (raccomandato ogni 6 mesi per diritti di accesso utente e 3 mesi per privilegi speciali);
- si deve procedere all'immediata revoca dei diritto di accesso nel caso l'utente sia dimissionario o venga licenziato.

In merito alle regole per l'utilizzo della password deve essere richiesto all'utente di firmare una dichiarazione di assunzione di responsabilità in caso di comunicazione della password. Al riguardo tutto il personale dovrebbe essere avvertito di:

- non rivelare la password;
- evitare di tenerla scritta;
- cambiare la password ogni qualvolta si ritenga compromessa;
- selezionare password robuste (min. 8 caratteri, niente nomi, uso caratteri speciali,..);
- cambiare password ad intervalli regolari;
- bloccare il terminale quando non utilizzato.

Al fine di proteggere i servizi di rete, occorre controllare tutti gli accessi provenienti dall'interno e dall'esterno dell'infrastruttura informatica. Al riguardo:

- dovrebbe essere implementata una politica che regolamenti l'utilizzo della rete e dei servizi di rete ed indichi le procedure di autenticazione da implementare;
- tutte le connessioni esterne (es. dial up) dovrebbero prevedere meccanismi di autenticazione;
- tutte le porte diagnostiche dovrebbero essere controllate.

Al fine di prevenire accessi non autorizzati alle macchine, occorre prevedere apposite procedure di log on che:

- segnalino che l'accesso è consentito ai soli utenti autorizzati;
- limitino il numero di log on conclusi con insuccesso (raccomandato tre volte);
- traccino i tentativi falliti;
- stabiliscano un tempo ragionevole prima di poter re-iniziare la procedura di log on;
- visualizzino i tentativi di log on falliti;
- monitorino accessi ed attività (log event).

Relativamente all'attività di controllo dei log event occorre sottolineare che essa risulta di fondamentale importanza per la sicurezza del sistema e dovrebbe essere pianificata ed effettuata ad intervalli regolari.

Tutte le macchine dovrebbero essere temporalmente sincronizzate, al fine di dare attendibilità ai file di log.

Crittografia[50]

Obiettivo dei controlli è quello di assicurare un utilizzo appropriato ed effettivo dei sistemi di crittografia per garantire la confidenzialità, l'autenticità e l'integrità delle informazioni attraverso:

- la definizione e l'attuazione di una politica per l'utilizzo dei controlli crittografici;
- la definizione e l'attuazione di una politica sulla gestione sicura del ciclo di vita delle chiavi crittografiche.

[50] ISO/IEC 27001 - A.10 "Cryptography".

Sicurezza fisica ed ambientale [51]

I controlli previsti dalla ISO/IEC 27001:2013 in questa sezione sono diretti ad impedire l'accesso non autorizzato, il danneggiamento e l'interferenza all'interno del flusso delle informazioni, la perdita o il danneggiamento dei beni del sistema e l'interruzione delle attività economiche, la manomissione o il furto delle informazioni.

Al riguardo:

- il perimetro di sicurezza deve essere chiaramente definito:
  - l'accesso fisico alla struttura deve essere controllato tramite un'area di reception e consentito solo al personale autorizzato;
  - tutte le uscite di sicurezza del perimetro devono essere allarmate e tenute chiuse;
- i visitatori delle aree di sicurezza dovrebbero essere supervisionati, l'ora e la data dell'ingresso registrati e i diritti di accesso regolarmente controllati;
- le macchine fotocopiatrici e i fax devono essere ubicati all'interno del perimetro di sicurezza;
- gli uffici che ospitano terze parti devono essere fisicamente separati da quelli utilizzati dall'organizzazione;
- gli equipaggiamenti di sicurezza devono essere installati, adeguatamente protetti e mantenuti in modo da ridurre i rischi derivanti da minacce ambientali e fisiche, e dalle opportunità di accesso non autorizzato.

Sicurezza operativa [52]

Le procedure operative identificate per la gestione della sicurezza devono essere documentate e soggette a processo di manutenzione. Esse includono:

- istruzioni in caso di condizioni anomale, chi contattare in caso di necessità, riavvio del sistema e procedure di recovery, procedure di back up e di restore, etc..;
- operazioni di change management: identificazione e registrazione, valutazione degli impatti, procedura di approvazione, etc..

Gli ambienti di sviluppo devono essere separati da quelli di produzione. Le attività di test e di sviluppo, infatti, possono causare seri problemi all'ambiente operativo (ad es. cancellazioni involontaria dei file o system failure). L'ambiente di sviluppo deve essere dedicato anche in ragione del fatto che altrimenti esisterebbe la reale possibilità di introdurre codice non autorizzato o non testato. Quindi, compilatori ed editor non dovrebbero essere utilizzati in ambiente operativo e dovrebbero esistere differenti procedure di log on.

Per minimizzare il rischio della presenza di falle (bug) nei sistemi, devono essere definiti chiaramente i criteri per l'accettazione dei sistemi e per la verifica delle loro performance.

Onde assicurare l'integrità dei programmi utilizzati dall'azienda contro i danni derivanti da malicious software è necessario definire regole per l'utilizzo delle licenze (proibizione di software non autorizzato) di installazione di soluzioni antivirus, e procedure di controllo periodico delle macchine finalizzato alla ricerca di software sospetto/non autorizzato.

Onde assicurare l'integrità delle informazioni nella fase di conservazione, è necessario regolamentare

---

[51] ISO/IEC 27001:2013 - A.11 "Physical and environmental security".

[52] ISO/IEC 27001:2013 - A.12 "Operational security".

le attività di backup e restore attraverso la definizione di politiche e procedure che prevedano:

- l'archiviazione dei supporti in luoghi protetti;
- attività di test periodico dei backup;
- il periodo di mantenimento delle copie di back up.

Per prevenire il danneggiamento dei beni aziendali e l'interruzione dei servizi di business è necessario che l'esportazione delle informazioni, dei media (nastri, disk, cdrom, tc…), e della documentazione ad essi relativa venga autorizzata dell'organizzazione.

Onde evitare il rischio di perdite, modificazioni o scambio di informazioni e software tra organizzazioni devono essere:

- stabilite le responsabilità e le procedure per il controllo e la notifica delle trasmissioni/ricezioni;
- indicate le proprietà dei beni o il copyright sul software e sulla documentazione;
- protette le informazioni tramite tecniche crittografiche;
- stabilite procedure di sicurezza per il trasporto delle informazioni (es. trasporto in contenitori chiusi).

Sicurezza delle comunicazioni [53]

I controlli previsti in questa sezione sono diretti ad assicurare la protezione delle informazioni nelle reti e le strutture che supportano la loro elaborazione.

Al fine di salvaguardare le informazioni in fase di trasmissione e proteggere l'infrastruttura di rete:

- le responsabilità operative per la rete dovrebbero essere disgiunte da quelle per i sistemi;
- devono essere stabilite le responsabilità e le procedure per la gestione degli apparati in remoto;
- deve essere preservata l'integrità e la confidenzialità dei file che transitano in rete (ad esempio mediante l'utilizzo di sistemi di crittografia).

Devono altresì essere: definite politiche e procedure per regolamentare il trasferimento delle informazioni effettuato con ogni mezzo a disposizione dell'organizzazione; siglati accordi per garantire la sicurezza nello scambio delle informazioni tra organizzazioni e terze parti; proteggere adeguatamente le informazioni scambiate con la posta elettronica.

Acquisizione, Sviluppo e manutenzione dei sistemi [54]

I controlli previsti in questa sezione sono finalizzati a garantire la sicurezza dei sistemi in termini di acquisizione, sviluppo e manutenzione.

Al riguardo occorre che l'azienda stabilisca i requisiti di sicurezza ed i controlli da effettuare relativamente alle modifiche di sistema od all'acquisizione di nuovi sistemi.

Per quanto attiene i sistemi applicativi, occorre sia controllare i dati di input (out-of-range, caratteri invalidi, dati incompleti o inconsistenti) che verificare la rispondenza a questi ultimi dei dati di output.

Nel caso di aggiornamento dei sistemi operativi, le operazioni di "update" a librerie dovrebbero essere effettuate solo a seguito di debita autorizzazione e debitamente tracciate. Inoltre, il codice

[53] ISO/IEC 27001:2013 – A.13 "Communication security"

[54] ISO/IEC 27001:2013 - A.14 "System acquisition, development and maintenance".

dovrebbe essere scaricato nella macchina solo dopo avere dato evidenza dell'opportuno testing della procedura di accettazione.
Ogni volta si scambi il S.O. per installare una nuova release sarebbe bene svolgere tutti i test di "non regressione" al fine di appurare che il software applicativo non sia stato inficiato dalle modifiche.
Le modifiche a pacchetti software pre-confezionati sono altamente sconsigliate, poiché è necessaria l'autorizzazione del fornitore in assenza della quale la manutenzione del prodotto decade.
Infine, occorre garantire la protezione ed il controllo dei dati utilizzati nelle attività di testing.

Relazioni con i fornitori [55]
Il controllo ha l'obiettivo di assicurare la protezione dei beni dell'organizzazione quando questi sono resi accessibili ai fornitori. Al riguardo:

- devono essere concordati con il fornitore e documentati i requisiti di sicurezza associati all'accesso ai beni dell'organizzazione;
- tutti i requisiti di sicurezza delle informazioni devono essere stabiliti e concordati con ciascun fornitore che può accedere, processare, conservare, comunicare o fornire componenti dell'infrastruttura IT;
- gli accordi con i fornitori devono includere i requisiti di sicurezza delle informazioni per indirizzare i rischi associati all'outsourcing dei servizi e dei prodotti ICT.

Gestione degli incidenti relativi alla sicurezza delle informazioni [56]
L'attuazione del controllo consente di assicurare che qualsiasi fatto o debolezza inerente alla sicurezza delle informazioni venga prontamente comunicato al'interno dell'organizzazione in modo che possano essere presi tempestivi provvedimenti.
In tale contesto per incidente s'intende qualsiasi evento che impatta o minaccia di impattare sulla sicurezza delle informazioni, ovvero di uno o più sistemi o dispositivi informatici, intesa come la possibilità di comprometterne le proprietà di confidenzialità, integrità e disponibilità. Nella realtà organizzativa un incidente di sicurezza è generalmente identificabile come una violazione delle politiche di sicurezza o la minaccia che tale violazione si stia concretizzando.
L'organizzazione deve strutturare un processo di gestione degli incidenti di sicurezza in modo da garantire alla Direzione una visione precisa e puntuale dei rischi e delle perdite, oltre che un valido metodo di prevenzione.
Devono altresì essere definite le procedure per la gestione degli incidenti rilevanti ai fini della sicurezza delle informazioni in conformità alle vigenti normative nazionali. Tali procedure devono descrivere le finalità, le modalità, i criteri di utilizzo ed i tempi di tenuta dei log rilevanti ai fini della ricostruzione degli incidenti.
Aspetti relativi alla sicurezza delle informazioni nella gestione della Continuità Operativa[57]
Obiettivo del controllo è minimizzare gli effetti legati all'interruzione della continuità operativa attraverso il ripristino dei servizi critici in tempi accettabili.

---

[55] ISO/IEC 27001:2013 – A.15 "Suppliers relationship"

[56] ISO/IEC 27001:2013 – A.16 "Information security incident management"

[57] ISO/IEC 27001:2013 - A.17 "Information security aspects of business continuity management".

Al riguardo è necessario strutturare un sistema di gestione attraverso il quale si identifichino i rischi legati all'interruzione dei processi critici in termini di probabilità di accadimento e relativi impatti per l'organizzazione (sia in termini di danni che di tempi di recupero).
La valutazione di tali rischi deve essere effettuata attraverso l'espletamento di una formale Business Impact Analysys (BIA) ovvero di una attività finalizzata a valutare il potenziale impatto sul business dovuto ad un'interruzione della continuità operativa e/o dell'indisponibilità dei sistemi informatici.
I principali obiettivi della BIA sono:

- dimensionare il danno arrecato all'azienda a seguito di un'interruzione di processi ed applicazioni critiche, ovvero che risultano vitali per il mantenimento della missione aziendale;
- individuare quali applicativi e processi recuperare e ripristinare, definendo priorità e timing di recovery (RPO[58] e RTO[59]);
- valutare i costi potenziali di un evento avverso e/o disastro;
- ottimizzare il processo di definizione degli SLA in funzione della criticità dei processi/servizi IT.

Output di questo processo è il Piano di Continuità Operativa o "Business Continuità Plan" (BCP). All'interno del piano vengono operativamente trattati tutti gli eventi atti a compromettere la continuità operativa aziendale, onde garantire un'organizzata ed efficiente gestione delle conseguenze di un evento imprevisto ed assicurare il ripristino dei servizi critici entro i tempi definiti.

Nel Piano sono descritti:

- i ruoli e le responsabilità delle figure coinvolte nel piano;
- la classificazione degli eventi dannosi;
- le condizioni per l'attivazione delle singole procedure identificate nel piano;
- le procedure di emergenza da porre in essere per contenere i potenziali impatti al verificarsi di eventi dannosi;
- le procedure operative alternative;
- le procedure di ripristino successive all'evento;
- le liste di reperibilità.

Il piano deve essere oggetto di attività di manutenzione ed aggiornamento periodiche, e di rivalutazione a fronte di particolari accadimenti (ad es. cambio di strategia aziendale, cambio di sede aziendale, modifiche legislative, etc…).

Conformità [60]

Ultimo punto di controllo previsto dallo Standard ISO/IEC 27001:2013 riguarda la conformità

---

[58] RPO o "Recovery Point Objective" è uno dei parametri utilizzati nell'ambito delle politiche di disaster recovery per descrivere la tolleranza ai guasti di un sistema informatico. Esso rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso.

[59] RTO o "Recovery Time Objective" è il tempo necessario per il pieno recupero dell'operatività di un sistema o di un processo organizzativo calcolato in un contesto di analisi ed implementazione di politiche di disaster recovery dei sistemi informativi. È in pratica la massima durata, prevista o tollerata, del downtime occorso.

[60] ISO/IEC 27001:2013 - A.18 "Compliance".

normativa (leggi, regolamenti, contratti, etc..) ed alla politica di sicurezza.
Per quanto attiene la conformità normativa è necessario che l'azienda proceda all'identificazione di tutti i requisiti statutari, legislativi e contrattuali che devono essere esplicitamente definiti e documentati per ciascun sistema informativo. Al riguardo lo Standard fa esplicito riferimento alle normativa in materia di:

- Protezione della proprietà intellettuale (Copyright);
- Protezione dei dati personali (Privacy);
- Protezione dei sistemi informatici;
- Regole in materia di sistemi di crittografia;
- Protezione delle registrazioni aziendali.

10. Conclusioni

La gestione della sicurezza informatica, nonostante le numerose iniziative normative sia a livello nazionale che comunitario, continua ad essere nel nostro paese un tema residuale poiché all'interno delle organizzazioni non esiste ancora la percezione reale del valore economico dell'informazione e della sua vulnerabilità.
Gestire la sicurezza informatica in un'organizzazione complessa come può essere una pubblica amministrazione o una azienda privata è certamente un'attività che richiede una particolare attenzione ed un approccio multidisciplinare e consapevole che tenga conto, oltre che della tecnologia, anche del fattore umano e degli aspetti metodologici e di processo.
Capire bene il valore dell'informazione è il primo passo da compiere.
La forte crescita della mobilità dei dati in ambiente aziendale e l'utilizzo di Device evoluti aumenta l'esposizione ai rischi di sicurezza ed in particolar modo a quelli di violazione dei dati con conseguenze devastanti per le organizzazioni.
E' necessario altresì cambiare la mentalità dei dipendenti, dei consumatori e dei cittadini, che tendono a considerarsi semplici spettatori invece di attori responsabili, dando priorità all'educazione in materia di sicurezza.
Occorre integrare la sicurezza informatica all'interno delle principali aree amministrative e di business, con un conseguente incremento della visibilità e delle risorse.
Bisogna spingere verso un cambio di prospettiva della compliance che da passiva, imposta dalle normative e dalla legge, deve diventare attiva ovvero prodotta spontaneamente dalle organizzazioni attraverso la definizione di politiche di sicurezza. Al riguardo, i temi della privacy e della protezione dei dati personali devono essere affrontati con un approccio proattivo allo scopo di minimizzare i rischi ben aldilà degli obblighi di legge.
I rischi devono essere individuati e valutati non attraverso un approccio empirico bensì sulla base di metodologie internazionali, in grado di oggettivizzare i risultati rendendoli misurabili, credibili e confrontrabili.
I controlli di sicurezza devono essere selezionati in base ai risultati di una formale analisi dei rischi seguendo le indicazione fornite dagli Standard di organizzazione e gestione della sicurezza riconosciuti non solo a livello internazionale come standard di certificazione, ma anche dalle

normative comunitarie e nazionali come Standard di riferimento per la gestione della sicurezza informatica.
Reagire prontamente per ridurre i costi ed i rischi diventa un obiettivo imprescindibile e non più una opzione di scelta in un contesto nel quale le minacce cibernetiche alle reti, ai sistemi e ai dati si evolvono rapidamente con lo svilupparsi dei fenomeni tecnologici.