dell'Arma dei Carabinieri
Rassegna
Quaderno n. 12/2016

TESI DI LAUREA DEI FREQUENTATORI DEL 22° CORSO DI PERFEZIONAMENTO

Anno Accademico 2015-2016

Ammissione alla quotazione in borsa
(Ten. Matteo Alborghetti)

Cybercrime
Aspetti giuridici e strumenti di contrasto
ai reati connessi al cyberspace
(Ten. Giovanni De Liso)

Scuola Ufficiali Carabinieri, 2016

dell'Arma dei Carabinieri
Rassegna

Direttore Responsabile
Gen. D. Vittorio Tomasone

Redattore Capo
Col. Giuseppe Arcidiacono

Redazione
Lgt. Remo Gonnella
M.A. s.UPS. Alessio Rumori
Brig. Mario Pasquale
App. Sc. Lorenzo Buono

Direzione e Amministrazione
Via Aurelia, 511 - 00165 Roma - tel. 06-66394680
fax 06-66394746; e-mail:scufrassegna@carabinieri.it

Grafica, Fotocomposizione e Impaginazione
a cura della Redazione

Fonti iconografiche
Ministero della Difesa
Comando Generale dell'Arma dei Carabinieri
Scuola Ufficiali Carabinieri

Periodico trimestrale a carattere scientifico-professionale a cura della Scuola Ufficiali Carabinieri
Proprietà editoriale del Ministero della Difesa Iscritto nel Registro della Stampa del Tribunale di Roma
al n. 305/2011 in data 27-X-2011
Diffuso attraverso la rete internet sul sito www.carabinieri.it
dal Service Provider "BT Italia" S.p.A. Via Tucidide, 56 - 20134 Milano

PRESENTAZIONE

In quest'ultimo Quaderno del 2016 presentiamo due tesi di laurea di Ufficiali del 22° Corso di Perfezionamento.

Nel primo lavoro, "*Ammissione alla quotazione in Borsa*", il Ten. Matteo Alborghetti, attraverso una ricostruzione analitica della procedura, riferisce come la stessa rappresenti una scelta di notevole rilievo per il *management* di una società, le cui implicazioni sono non solo economiche ma anche organizzative.

La seconda tesi, dal titolo "*Cybercrime. Aspetti giuridici e strumenti di contrasto ai reati connessi al cyberspace*", del Ten. Giovanni De Liso, tratta gli elementi teorici e tecnici utili a comprendere il complesso mondo del *Cyberspace*, soffermandosi sugli aspetti fenomenologici, le questioni processuali legate al *Cybercrime*, sui principi di diritto processuale penale e sulle relative tecniche di indagine finalizzate al contrasto del fenomeno.

Gen. D. Vittorio Tomasone

AMMISSIONE ALLA QUOTAZIONE IN BORSA

Ten. Matteo Alborghetti

"La capacità di prevedere che alcune
cose non si possono prevedere è una
qualità molto importante"

Jean Jacques Rousseau

INDICE

Introduzione

La quotazione in borsa rappresenta una decisione che assume rilevanza strategica per un'impresa: non è soltanto un canale di finanziamento, un'opportunità di accesso a nuove risorse finanziarie; essa rappresenta l'inizio di un processo di riorganizzazione dell'assetto, di modifica dei rapporti sia interni (manager, dipendenti) che esterni (fornitori, clienti e sistema finanziario in generale); l'impresa cioè si apre al pubblico, nel senso che la sua attività assume interesse per una serie di soggetti ed è, inoltre, tenuta al rispetto di parametri in diversi settori, dalla trasparenza alla solidità economica.

Molte società si trovano, in un determinato momento del loro ciclo di vita, nella condizione di valutare l'ipotesi di quotarsi, spinte dall'esigenza di finanziare nuovi investimenti senza appesantire la propria struttura finanziaria con ulteriore indebitamento, di rafforzare la propria capacità competitiva, non solo sul piano economico strutturale, ma anche investendo in ricerca e sviluppo tecnologico, o nell'acquisto di nuovi macchinari e materiali.

La spinta alla quotazione in borsa può derivare anche dalla necessità di affrontare un ricambio generazionale nelle posizioni di gestione e direzione delle società, infatti in un mercato, ormai da anni, votato alla globalizzazione dei commerci e delle operazioni finanziarie, la borsa rappresenta la vetrina privilegiata per chi ha interesse a presentarsi e farsi conoscere a livello internazionale, in questo modo si può ottenere un deciso miglioramento dell'immagine e della redditività della società, senza trascurare l'attrazione che si esercita verso manager più qualificati, che offrono garanzie di serietà e professionalità.

La quotazione in Borsa si presenta come un'operazione complessa, per la numerosità di scelte che l'impresa deve affrontare, la ristrettezza dei tempi di realizzazione e la necessità di rispettare i vincoli e le procedure previste dalla normativa, in particolare il TUF, il Regolamento Emittenti e il Regolamento di Borsa.

La quotazione di una società comporta una molteplicità di benefici capaci di migliorarne le performance operative con risultati visibili nel medio-lungo termine, ma richiede anche sforzi di natura monetaria e non monetaria, in quanto presuppone un notevole cambiamento organizzativo, operativo e manageriale coerentemente con i requisiti richiesti.

Inoltre le società quotate sono sottoposte ad un ferreo controllo da parte del mercato e delle autorità a ciò preposte, cui devono fornire un flusso continuo di informazioni e giustificare eventuali scostamenti e anomalie.

Questo elaborato si pone come obiettivo la ricostruzione analitica della procedura di ammissione alla quotazione in Borsa seguendo la disciplina che è dettata nelle norme e nei regolamenti; dalla scelta di quotarsi fino alla fissazione del prezzo di mercato, passando attraverso le modifiche strutturali della società e le attività proprie di Borsa S.p.A. e Consob.

1
La Borsa Italiana

1.1 Evoluzione storica

Prima di esaminare il percorso di ammissione alla quotazione è necessario dar conto dell'evoluzione storica del mercato di borsa e della normativa che ne disciplina l'ammissione.

Il termine "Borsa" deriva dagli incontri che si svolgevano tra il 1450 e il 1500, nella casa dei mercanti Van Der Burse a Bruges, per determinare il valore delle merci, ci troviamo all'inizio del periodo chiamato capitalismo mercantile[1] che si protrarrà per tre secoli, fino al termine sancito dalla rivoluzione industriale e dalla pubblicazione del "Wealth of Nation" di Adam Smith[2].

Le prime Borse vere e proprie furono fondate ad Anversa nel 1531 e a Lione nel 1548, importanti snodi commerciali dei trasporti via mare e via terra, e per questo luoghi di passaggio obbligati per gli esercenti il commercio.

L'espansione del mercato di borsa si ebbe principalmente con il parallelo sviluppo di diffusione delle società per azioni del XVII secolo[3], si fondarono quindi le Borse di Siviglia, Londra, Parigi, e la loro funzione venne incrementata dall'espansione dei traffici, degli investimenti e dei debiti pubblici, situazioni che vennero favorite da diversi fattori come per esempio l'ampliamento e l'annessione delle colonie, la creazione e il consolidamento degli Stati.

L'esperienza italiana annovera la fondazione della borsa di Venezia nel 1630, di una borsa di commercio a Napoli nel 1778, preceduta di tre anni dalla Borsa di Trieste, che all'epoca sottostava all'impero Asburgico[4].

La Borsa di Milano venne fondata nel 1808[5], da quel momento lo sviluppo della struttura si accompagnò al percorso storico-sociale, passando dall'occupazione napoleonica a quella

---

1 John Kenneth Galbraith, *Storia dell'Economia*, Milano, Rizzoli, 1988, pag. 42

2 Adam Smith (1723-1790) con l'opera "Wealth of Nations" del 1776 chiuse il periodo del capitalismo mercantile, dando avvio alla serie degli economisti classici. L'opera si fonda sul concetto di lavoro, inteso come "fondo da cui ogni nazione trae le cose necessarie e comode della vita", in questo contesto Smith introduce la metafora della Mano invisibile, simbolo della Provvidenza, grazie alla quale la ricerca egoistica dell'interesse del singolo condurrebbe al benessere della società. In Smith la ricchezza deriva dal lavoro produttivo svolto e dalla capacità produttiva di tale lavoro.

3 La nascita della società per azioni, o più in generale della società di capitali, viene fatta risalire alle compagnie coloniali del XVII secolo, le esplorazioni e gli insediamenti necessitavano di ingenti finanziamenti e comportavano un alto rischio per l'investimento. Per incentivare tale tipologia di attività, fu concessa la separazione tra il patrimonio societario e il patrimonio dell'investitore, esponendo al rischio solo il denaro investito nella compagnia.

4 www.wikipedia.org/borsavalori.

austriaca, per poi rivestire un ruolo centrale nell'assestamento delle finanze del Regno d'Italia, sfiancato dagli sforzi economici sostenuti per l'unificazione.

Nel periodo precedente il primo conflitto mondiale il mercato italiano non fu in grado di essere determinante, questo sia per le stringenti regole poste dalle autorità, sia per gli scarsi sistemi di comunicazione, inoltre per la poca offerta di listini e offerte finanziarie, e la conseguente eccessiva dipendenza dai capitali stranieri.

Nel primo dopoguerra, come dopo l'unificazione, la borsa sostenne i costi della riparazione, offrì finanze alle grandi imprese e sopportò l'urto delle crisi economiche internazionali.

Nel 1932 la Borsa, dopo alcuni spostamenti, trovò la sua collocazione definitiva a palazzo Mezzanotte.

Nel periodo del boom economico anche la Borsa ritrovò l'espansione domestica che nel periodo fascista era stata limitata dalla costituzione di IMI e IRI[6], salvo poi vivere una fase di stagnazione dovuta allo scarso interesse dei governi all'investimento borsistico.

Nel 1997 tutte le piazze finanziarie italiane furono accorpate in un'unica società privata, Borsa Italiana[7] con sede a Milano, dal 2007 Borsa Italiana è entrata a far parte del London Stock Exchange Group[8], dando vita a quello che è oggi il mercato leader in Europa per scambi azionari e scambi di ETF, covered warrant, certificates e strumenti del reddito fisso[9].

In particolare, si occupa dell'ammissione, sospensione ed esclusione di strumenti finanziari e operatori dalle negoziazioni. Inoltre, Borsa Italiana gestisce e controlla le negoziazioni e gli obblighi di operatori ed emittenti.

---

5 La fondazione avvenne su impulso del napoleonico viceré del Regno d'Italia Eugenio di Beauharnais.

6 Lo stato "imprenditore" e la chiusura verso il mercato internazionale, per la ricerca dell'autarchia, portarono la borsa a perdere di importanza.

7 Borsa Italiana S.p.A. nasce con la privatizzazione del settore borsistico prevista con il d.lgs. 415/1996, l'unificazione rispose all'esigenza di creare una struttura altamente competitiva e accorpata, a scapito delle piazze di scambio minori che svolgevano una funzione prettamente regionale.

8 Il gruppo è costituito da Borsa Italiana e Borsa di Londra (London Stock Exchange), con 3.600 società quotate ha il volume di scambi maggiore in Europa, la fusione è avvenuta con la finalità di creare un soggetto finanziario in grado di attrarre capitali asiatici e medio-orientali. I maggiori azionisti sono: Borse Dubai (21%), *Qatar Investment Authority* (15%).

9 Strumenti finanziari, in particolare:
- ETF, *Exchange Traded Fund*, fondo d'investimento che si caratterizza per essere negoziato come un'azione, replica l'indice cui si riferisce con una gestione passiva;
- *Covered Warrant*, strumento consistente in un contratto di opzione che attribuisce la facoltà di sottoscrivere l'acquisto o la vendita di un'attività finanziaria ad un prezzo e ad una data scadenza;
- *Certificates*, titolo emesso da una banca, consiste in un pool di opzioni sia di acquisto che di vendita, scritte sul medesimo sottostante;
- Strumenti del reddito fisso, sono titoli con una cedola fissa dall'emissione fino alla scadenza con il rimborso del capitale.

Intermediari nazionali ed internazionali, collegati al mercato tramite un sistema di negoziazione completamente elettronico, garantiscono l'esecuzione degli scambi in tempo reale. Obiettivo principale di Borsa Italiana è sviluppare i mercati e massimizzarne la liquidità, la trasparenza, la competitività e l'efficienza[10].

In questo momento storico Borsa Italiana gestisce i seguenti mercati[11]:

- MTA, Mercato Telematico Azionario: rappresenta il maggior mercato azionario italiano, ovvero il mercato in cui si negoziano i titoli delle più importanti imprese italiane. È un mercato regolamentato che risponde ai migliori standard internazionali dove si negoziano azioni, obbligazioni convertibili, diritti di opzione e warrant. Al suo interno, il segmento STAR dedicato alle società che si impegnano a rispettare requisiti di eccellenza in termini di liquidità, trasparenza informativa e corporate governance;
- AIM Italia, è l'MTF dedicato alle piccole e medie imprese italiane che vogliono investire nella loro crescita;
- MIV, Mercato degli Investment Vehicles, è il mercato regolamentato creato per offrire con una chiara visione strategica, capitali, liquidità e visibilità ai veicoli d'investimento;
- MOT, Mercato Telematico delle Obbligazioni: nato nel 1994, è l'unico mercato obbligazionario regolamentato italiano;
- ExtraMOT, è il sistema multilaterale di negoziazione (MTF) nato per permettere a operatori ed investitori di ampliare la gamma di strumenti obbligazionari in cui investire;
- ExtraMOT Pro**,** è il Segmento Professionale del mercato ExtraMOT, nato per offrire alle PMI un primo accesso ai mercati dei capitali semplice e veloce;
- SeDex, è il mercato di Borsa Italiana nato nel 2004 per la negoziazione di Certificates e Covered Warrant, nel loro insieme denominati securitised derivatives;
- ETFplus, è il mercato italiano dedicato alla quotazione degli ETF, ETC, ETN e fondi aperti e leader in Europa per scambi e controvalore;
- IDEM**,** è uno dei maggiori mercati di derivati nel panorama europeo; scambia circa 150mila contratti al giorno, per un controvalore nazionale di 3,4 miliardi di euro;
- IDEX, Mercato italiano dei derivati energetici;
- AGREX**,** Mercato italiano dei derivati sul grano duro.

[10] www.Borsaitaliana.it.

[11] www.Borsaitaliana.it, dato aggiornato al 11 marzo 2016

1.2 Legge 272 e regio decreto 1068 del 1913

La regolamentazione circa l'ammissione alla quotazione subì diversi interventi, spesso lacunosi e contrastanti, tanto è vero che per giungere ad una disciplina organica si dovette attendere la L. 272 del 1913 e il regolamento di attuazione, r.d. 1068/13[12], che si ispirarono al modello francese, il quale aveva un'impostazione marcatamente pubblicistica della Borsa, ritenendo necessarie le ingerenze e i controlli degli organi pubblici.

L'attività di vigilanza fu alternativamente devoluta al Ministero dell'agricoltura, industria e commercio, e al Ministero del tesoro, il cui Ministro poteva disporre ispezioni e adottare i provvedimenti di volta in volta necessari per garantire il regolare svolgimento degli affari, e veniva supportato e riceveva consulenza dalla Deputazione di Borsa e dal Comitato direttivo degli agenti di Cambio[13]. La Deputazione era un organo collegiale nominato annualmente con decreto ministeriale, cui era riservato l'ufficio di sorvegliare l'andamento delle borse e far applicare le leggi e i regolamenti, mentre il Comitato, oltre le attività specifiche di controllo degli agenti e liquidazione delle insolvenze, aveva il potere/dovere di sostituirsi ai membri assenti della Deputazione, si evidenzia che entrambi gli organi erano investiti di funzioni pubbliche e considerati organi dell'apparato amministrativo.

L'art. 1 co. 1 della L. 272/1913 prevedeva l'istituzione della Borsa "con regio decreto su proposta della Camera di commercio competente"[14], la quale era inoltre titolare di poteri di controllo e amministrazione, tra i quali l'ammissione e la revoca della quotazione.

L'ammissione riceveva scarsa considerazione dal legislatore, il cui atteggiamento poco attivo nel settore era da rinvenire nel modesto grado di sviluppo e diffusione dei titoli mobiliari in quel periodo storico[15]. Per quanto riguarda i titoli del debito pubblico, quelli garantiti dallo stato, quelli emessi da comuni e province, l'ammissione avveniva di diritto[16], configurandosi come atto dovuto, invece per i titoli delle società commerciali per azioni, l'ammissione era

---

[12] Donato Ivano Pace, *Ammissione sospensione esclusione dai mercati regolamentati*, Milano, Giuffrè Editore, 2012, pag. 13-14.

[13] Art. 2 L 272/1913, "Le borse di commercio sono sottoposte alla vigilanza del Governo, delle Camere di Commercio, delle Deputazioni di borsa e dei Sindacati di mediatori. I ministri di agricoltura, industria e commercio e del tesoro possono in ogni tempo ordinare di concerto ispezioni alle borse di commercio e, sentita la Camera di commercio, emanare i provvedimenti reputati di volta in volta necessari, secondo le speciali condizioni del mercato, per il regolare andamento degli affari nelle singole borse".

[14] "Le borse di commercio sono istituite con regio decreto, su proposta della competente Camera di Commercio. Il decreto di istituzione indica per ciascuna borsa, secondo le proposte della Camera di Commercio, per quali specie di contrattazione sia istituita".

[15] G. Siciliano, *Cento anni di Borsa Italiana*, Bologna, 2001, pag. 13.

[16] Si intendevano ammessi di diritto: i titoli del debito pubblico, i titoli garantiti dallo stato, le cartelle di credito fondiario italiano, i titoli emessi dalle province e dai comuni, i titoli cambiari.

subordinata alla totale discrezionalità della Camera di commercio[17] competente e richiedeva, in particolare, tre requisiti (art. 12 L. 272/1913):

- Capitale sociale non inferiore a seicentomila lire;
- Approvati dai soci e pubblicati i bilanci degli esercizi di due annualità;
- Le società dovevano avere un rappresentante dei titoli nella città sede della Borsa.

Il procedimento di ammissione era così disciplinato[18] negli artt. 3,12 L. 272/1913 e 27-29 r. d. 1068/1913:

- La società presentava la domanda deliberata dal consiglio di amministrazione alla Camera di commercio, la quale, dopo una prima analisi, ne curava la pubblicità e informava il Ministero;
- L'ammissione era disposta dalla Camera di commercio, decorso un mese dalla pubblicazione della domanda, previo parere favorevole della Deputazione di borsa e del Comitato direttivo degli agenti di cambio;
- La decisione di ammissione doveva essere comunicata il giorno seguente al Ministero per la approvazione;
- Se entro dieci giorni non veniva emesso un provvedimento contrario (che non necessitava di motivazione), la approvazione si intendeva concessa.

Durante i dieci giorni di attesa l'ammissione era provvisoriamente esecutiva e in caso di sopraggiunto provvedimento negativo venivano fatti salvi gli effetti medio-tempore prodotti.

1.3 Gli interventi degli anni Settanta e Ottanta

Una novità di rilievo si ebbe con la L. 216 del 1974 e il seguente d.p.r. 138/75, con cui si trasferirono alla CONSOB "la titolarità dei poteri e delle attribuzioni per l'organizzazione e il funzionamento delle borse, nonché l'ammissione dei titoli alla quotazione spettanti alle Camere di commercio, alle Deputazioni di borsa, ai Comitati direttivi degli agenti di cambio"[19].

---

[17] La discrezionalità prevedeva che anche in presenza dei requisiti minimi previsti dalla legge non vi era l'obbligo di ammettere a quotazione il titolo, la relativa decisione era comunque rimessa agli organi preposti. In particolare, poi, i provvedimenti di diniego non dovevano essere motivati (art. 29 co. 2 r.d. 1068/1913).

[18] Donato Ivano Pace, *Ammissione sospensione esclusione dai mercati regolamentati*, Milano, Giuffrè Editore, 2012, pag. 22-23.

[19] Art. 1 co. 1 d.p.r. 138/1975, "La titolarità dei poteri e delle attribuzioni relativi all'organizzazione ed al funzionamento delle borse valori, nonché all'ammissione dei titoli a quotazione spettanti alle Camere di commercio, industria, artigianato e agricoltura, alle Deputazioni di borsa, ai Comitati direttivi degli agenti di cambio e ai loro presidenti, designati nel presente decreto come organi locali di borsa, è trasferita alla Commissione nazionale per le società e la borsa".

Successive produzioni normative, in particolare la L. 49 del 1977, posero la CONSOB come organo di vigilanza delle negoziazioni di beni mobiliari parallele alla borsa[20].

La CONSOB divenne titolare della funzione di vigilanza, che si esprimeva in ampi poteri:

- Regolamentari, tramite l'emanazione dei regolamenti speciali di borsa, l'individuazione dei requisiti di ammissione, i contenuti del prospetto informativo e le modalità di pubblicazione;
- Informativi e ispettivi;
- Di intervento, adottando provvedimenti definiti dalla legge e, in via generale, i provvedimenti necessari per assicurare il regolare svolgimento degli affari;
- Di ammissione, sospensione ed esclusione dalla quotazione.

Con riferimento all'ammissione alla quotazione va sottolineato che la L. 216 del 1974 e il d.p.r. 138/75 delinearono una disciplina organica nei settori dell'ammissione e della permanenza, materie cui il sistema previgente si era interessato marginalmente[21].

In particolare l'ammissione e l'esclusione dalla quotazione spettavano alla CONSOB, l'ammissione poteva avvenire a domanda o d'ufficio.

Dinanzi all'istanza di ammissione si aprivano tre possibili esiti[22]:

- Ammissione del titolo, previo parere della Deputazione di borsa e del Comitato direttivo degli agenti di cambio, se sussistenti i requisiti e adempiuti gli obblighi informativi;
- Rigetto della domanda per mancanza dei requisiti, e comunque se l'ammissione risultasse contraria all'interesse pubblico;
- Non ammettere a quotazione e non rigettare la domanda immediatamente, ma subordinare l'ammissione a condizioni particolari.

La CONSOB poteva adottare provvedimenti di sospensione o revoca, sia per sopraggiunta carenza di requisiti, sia per situazioni specifiche previste dalla legge o per esigenza di tutela del pubblico risparmio.

---

[20] Tali contrattazioni, contraddistinte da forti fenomeni speculativi che più volte ne misero in discussione l'affidabilità, furono assoggettate al potere di CONSOB per quanto atteneva il compito di autorizzare, regolamentare e vigilare sullo svolgimento delle pubbliche riunioni del mercato ristretto per la negoziazione dei titoli non ammessi alle quotazioni ufficiali nelle borse valori.

[21] Donato Ivano Pace, *Ammissione sospensione esclusione dai mercati regolamentati*, Milano, Giuffrè Editore, 2012, pag. 35.

[22] A differenza di quanto stabilito dalla L. 272/1913 e dal r.d. 1068/1913, tutti i provvedimenti adottati da CONSOB, ammissione, esclusione, sospensione e revoca, dovevano essere motivati.

La riforma del 1974-1975 segnò inoltre il passaggio da una situazione in cui gli organi di borsa svolgevano una funzione di polizia, tesa ad assicurare l'ordinato funzionamento del mercato e il regolare svolgimento delle negoziazioni, ad una funzione di salvaguardia degli interessi dei risparmiatori[23].

Tuttavia mentre nella parte relativa all'organizzazione e al funzionamento della borsa, la Deputazione, il Comitato e le Camere di commercio, continuavano a svolgere le loro funzioni, la parte relativa all'ammissione, sospensione e revoca trovava come soggetto esclusivo la CONSOB.

1.4 Legge 1 del 1991 e il d.lgs. 58 del 1998

Con l'intervento normativo del 1991 venne istituito a Milano un Consiglio di borsa[24], cui vennero trasferiti i poteri delle Camere di commercio, delle Deputazioni di borsa e dei Comitati direttivi degli agenti di cambio.

Un significativo cambiamento si è avuto in attuazione della direttiva 93/22/CE posta in essere con il d.lgs. 58/98, Testo unico delle disposizioni in materia di intermediazione finanziaria.

Il legislatore italiano si decise per la modifica dell'assetto sino ad allora vigente, dirigendosi verso una struttura di tipo privatistico[25], ciò per meglio affrontare le mutate esigenze di buon funzionamento e concorrenza richieste dagli operatori del mercato[26], una gestione pubblicistica avrebbe, infatti, appesantito il sistema, rendendolo poco competitivo e con poca attrazione verso gli operatori.

---

[23] La Costituzione, infatti, prevede all'art. 41 che "L'iniziativa economica privata è libera. Non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana. La legge determina i programmi e i controlli opportuni perché l'attività economica pubblica e privata possa essere indirizzata e coordinata a fini sociali", inoltre all'art. 47 "La Repubblica incoraggia e tutela il risparmio in tutte le sue forme; disciplina, coordina e controlla l'esercizio del credito. Favorisce l'accesso del risparmio popolare alla proprietà dell'abitazione, alla proprietà diretta coltivatrice e al diretto e indiretto investimento azionario nei grandi complessi produttivi del Paese".

[24] La sede principale fu istituita a Milano, quelle secondarie presso ogni borsa valori. Il consiglio aveva il compito di rappresentare tutte le componenti del mercato: Banca d'Italia, Agenti di cambio, Sim, Istituti di credito, Camere di commercio, e unificare le contrattazioni sul piano nazionale.

[25] G. Chesini, *La regolamentazione e l'organizzazione dei mercati degli strumenti finanziari*, Padova, 1999, pag.55.

[26] Donato Ivano Pace, *Ammissione sospensione esclusione dai mercati regolamentati*, Milano, Giuffrè Editore, 2012, pag. 52.

L'organizzazione e la gestione dei mercati sono passati da essere attività pubblicistiche ad essere oggetto di controllo da parte della CONSOB, soggetto pubblico[27].

Alcune competenze che prima erano esclusivo appannaggio di CONSOB furono poste in capo alla società di gestione del mercato, trovando la disciplina negli art. 61 e seguenti del TUF[28]:

- Le condizioni e le modalità di ammissione, esclusione e sospensione di operatori e strumenti finanziari;
- Le condizioni per le negoziazioni e gli obblighi degli operatori;
- Le modalità di diffusione e pubblicazione dei prezzi;
- Il potere di disporre l'esclusione, l'ammissione e la sospensione di operatori e strumenti finanziari.

Con questo intervento la distinzione tra competenze circa il funzionamento e l'organizzazione e quelle relative ad ammissione, esclusione, sospensione, venne meno, ritrovandosi accentrate nella società di gestione del mercato, che divenne il promotore regolamentare, nella visione per la quale " la collaborazione tra legislatore e operatore è l'unica soluzione, in un sistema globalizzato, per realizzare regole sufficientemente elastiche e, contemporaneamente, efficienti"[29].

Rimase comunque in capo a CONSOB la possibilità di adottare i provvedimenti necessari, anche sostituendosi alla società di gestione del mercato, in casi di necessità ed urgenza e per garantire il regolare e trasparente svolgimento degli affari, nonché la tutela dei risparmiatori.

1.5 La legge a tutela del risparmio 262/2005 e le direttive MIfid, Prospetti e *Trasparency*

Tra gli interventi a tutela del risparmio, va analizzata la L. 262/2005 che in merito alle competenze decisionali attribuisce a CONSOB:

- Il potere di veto sui provvedimenti di ammissione, esclusione, sospensione, adottati dalla società di gestione del mercato;

---

[27] La direzione intrapresa dal legislatore italiano, ossia quella tendente alla privatizzazione della borsa, non poteva non prevedere l'attività di vigilanza svolta da un soggetto pubblico, per preservare i risparmiatori e garantire il corretto svolgimento delle attività.

[28] Artt. da 61 a 77 del d.lgs. 58/1998 (TUF).

[29] M. C. Cardarelli, sub art. 14 (m), a cura di Nigro e Santoro, Torino, 2007, pag. 253.

- Il potere di ordinare al gestore l'esclusione o la sospensione di uno strumento finanziario.

Gli interventi del legislatore europeo nella materia[30] si sono avuti con la direttiva 2004/39/CE (MIfid)[31], attuata nel 2007, che ha previsto il potere delle autorità di vigilanza di imporre al gestore del mercato l'adozione di provvedimenti, ha previsto l'estensione dei provvedimenti di sospensione ed esclusione degli strumenti alle altre piattaforme degli stati membri per interventi delle autorità di vigilanza.

La direttiva 2003/71/CE (Prospetti) individua gli obblighi per il prospetto informativo e assegna alle autorità competenti, in caso di violazione della relativa disciplina, il potere di sospendere o escludere. La direttiva 2004/109/CE (Trasparency) introduce l'obbligo di comunicazione periodica e continua per gli emittenti già ammessi alla negoziazione.

1.6 ESMA

L'autorità europea degli strumenti finanziari e dei mercati (ESMA)[32], è l'organismo dell'Unione Europea che dal 2011 è preposto per la vigilanza del mercato finanziario, ed è partecipato dalle autorità nazionali di vigilanza, per il nostro paese la Banca d'Italia.

Viene creata insieme all'EBA[33], autorità bancaria europea, e all'EIOPA[34], autorità europea delle assicurazioni e delle pensioni aziendali e professionali, dopo lo scoppio della crisi economica che aveva visto alcune istituzioni economiche europee vacillare.

Tra i compiti dell'ESMA troviamo[35]:

- Assicurare il trattamento omogeneo degli investitori in tutta l'Unione;
- Promuovere la concorrenza per i fornitori di servizi finanziari;
- Rafforzare la cooperazione nel settore della vigilanza;
- Vigilare soggetti con portata paneuropea;
- Adotta misure di emergenza qualora sussista una condizione di crisi.

---

30 Donato Ivano Pace, *Ammissione sospensione esclusione dai mercati regolamentati*, Milano, Giuffrè Editore, 2012, pag. 62 e ss.

31 *Markets in financial instruments directive.*

32 *European security and market authorities.*

33 *European banking authority.*

34 *European insurance and occupational pensions authority.*

35 www.esma.europa.eu.

2
Il processo di quotazione

2.1 La decisione di quotarsi in borsa: vantaggi e svantaggi, scelta del mercato e costi

La quotazione in Borsa rappresenta una scelta chiave per il successo di un'azienda, decisione capace di creare valore non solo per gli azionisti ma anche per gli investitori e il mercato nel suo complesso[36].

Con riferimento alle esigenze dell'emittente la quotazione è spesso intesa come risposta a uno o più dei seguenti bisogni:

a) agevolare l'afflusso di nuovi capitali per finanziare rilevanti progetti imprenditoriali, nonché generare l'aumento della redditività aziendale, che generalmente si accompagna all'adozione più efficienti sistemi di gestione
b) diversificare le fonti di finanziamento per ridurre la dipendenza dell'impresa dal capitale di debito, aprendosi a un nuovo canale di finanziamento, e allargare la base di raccolta del capitale di rischio assicurandone, al contempo, il frazionamento del possesso presso gli investitori
c) rafforzare il proprio prestigio e la notorietà per godere di ricadute positive in termini di potere contrattuale e visibilità, sia sul mercato dei fattori produttivi che su quello dei beni e servizi prodotti;
d) migliorare il proprio standing creditizio al fine di ridurre il costo del capitale, anche e soprattutto di debito, sia per l'effetto diretto connesso alla minor leva finanziaria che si determina per la società che emette nuove azioni, sia per l'effetto indiretto della maggior disciplina nel governo aziendale imposta dalla necessità di rispettare le regole di corporate governance e di trasparenza verso il pubblico previste dal regolamento del mercato;
e) disporre di moneta di scambio per possibili future operazioni di fusione o acquisizione;
f) disporre di uno strumento addizionale di incentivazione e motivazione del management e dei dipendenti;

[36] M. De Ambroggi, *La quotazione in borsa*, Parma, Facoltà di economia, 2012.

g) ottenere una valutazione di mercato che esprima il risultato di un'attenta, continua e credibile attività di monitoraggio esterno sull'efficacia del management nella produzione di valore, consentendo di adottare in tempo utile le decisioni necessarie

Da tale lista si evince come la scelta di un'impresa di quotarsi risponda non solo ad una logica finanziaria, ma nella maggior parte dei casi venga dettata da considerazioni di natura strategica o di governo aziendale[37]:

- il prestigio e la notorietà derivante dalla quotazione rendono più agevole e meno costoso reclutare capitale umano di qualità, con particolare riferimento ai top manager, motivati dalla maggiore assunzione di responsabilità, estendere la rete dei rapporti commerciali con altre imprese, che vedono nell'impresa quotata un partner sicuro e affidabile, inoltre si arriva ad affermare il proprio brand nel pubblico dei clienti potenziali;
- la possibilità di emettere azioni quotate e scambiate quotidianamente permette all'impresa di impegnarsi in acquisizioni di altre società senza alterare il proprio equilibrio finanziario offrendo come mezzo di pagamento azioni proprie;
- la quotazione offre l'opportunità di concordare più attraenti piani di incentivazione del management basati su stock options[38], di promuovere l'azionariato dei propri dipendenti, di avere un riscontro immediato del giudizio del mercato sulle scelte intraprese dal management[39];

La quotazione può, però, anche servire a soddisfare esigenze proprie di coloro che sono già azionisti. La creazione di un mercato pubblico per i titoli azionari infatti permette loro di:

- diversificare la propria ricchezza, senza perdere il controllo sulla società, consentendo inoltre di rendere più facilmente liquidabili le partecipazioni degli azionisti;
- realizzare rilevanti capital gain, derivanti dalla differenza di prezzo tra il momento dell'acquisto e quello della vendita;
- favorire il passaggio generazionale, agevolando l'uscita degli eredi dell'originario imprenditore non interessati a proseguire nella conduzione dell'azienda.

---

[37] www.Borsaitaliana.it/quotarsiinborsa.

[38] Le stock option sono opzioni call (strumenti derivati in base al quale l'acquirente acquista il diritto, ma non l'obbligo, di acquistare un titolo ad un determinato prezzo d'esercizio) che danno il diritto di acquistare azioni di una società ad un determinato prezzo di esercizio.

[39] Spesso avviene che le operazioni di quotazione si risolvano con un giudizio del mercato nei momenti immediatamente successivi, la promozione o la bocciatura sancita dalla reazione del mercato sono indicatori che servono a delineare le possibili strategie future, o a rivedere quelle già intraprese.

Un caso particolare di quotazioni motivate dall'interesse dell'emittente a liquidare, in tutto o in parte, la sua quota è dato dalle privatizzazioni perseguite dallo Stato italiano o dai suoi enti locali[40].

[40] www.italianieuropei.it/leprivatizzazioniitalia, "L'avvio delle privatizzazioni fu imposto dal grave deterioramento dei conti delle aziende a partecipazione statale, soprattutto l'IRI e l'EFIM, in una fase in cui anche i conti dello Stato erano in condizioni non più sostenibili, dopo oltre un decennio di elevati disavanzi che avevano fatto lievitare il debito pubblico oltre il 120% del PIL. Le privatizzazioni furono accelerate dalla crisi di cambio del settembre 1992, che portò all'uscita della lira dallo SME e rese chiara la crisi di credibilità delle politiche finanziarie dell'Italia, e dall'esplodere degli scandali di tangentopoli, che portarono alla luce fenomeni estesi di dilapidazione di risorse pubbliche e di corruzione nelle aziende di proprietà dello Stato. Gli obiettivi del programma di privatizzazione furono indicati dal governo nel «Libro verde sulle partecipazioni dello Stato», presentato al parlamento nel novembre del 1992: l'aumento dell'efficienza aziendale; la creazione di una decina di gruppi industriali capaci di competere internazionalmente (politica industriale); lo sviluppo della proprietà azionaria diffusa, assicurando al contempo il controllo delle imprese privatizzate da parte di nuclei stabili di azionisti; la riduzione del debito pubblico. Il processo trovò solide basi in una serie coordinata di interventi legislativi. Così, apposite leggi disposero la trasformazione in società per azioni delle banche (legge 218/90) e delle altre imprese pubbliche (legge 359/92); istituirono il Fondo per l'ammortamento del debito pubblico (legge 432/93), nel quale avrebbero dovuto obbligatoriamente confluire i proventi delle privatizzazioni, ad esclusione di ogni utilizzo per il ripiano dei disavanzi correnti; abolirono il ministero delle partecipazioni statali, trasferendo al tesoro la proprietà delle partecipazioni pubbliche; identificarono nell'offerta pubblica di azioni la tecnica preferita di vendita e introdussero negli statuti delle società cedute la golden share e le liste di minoranza per la nomina degli amministratori (legge 474/94, estesa anche a società possedute da enti pubblici); istituirono autorità di regolazione per i mercati dei servizi di pubblica utilità ceduti a privati (legge 281/95 per l'energia e legge 249/97 per le comunicazioni). Nel giugno 1993 fu costituito presso il ministero del tesoro (oggi dell'economia e delle finanze, o MEF) un Comitato per le privatizzazioni, tuttora operante, il quale fu incaricato di fare proposte sui tempi delle operazioni, i metodi di collocamento e la scelta dei consulenti e dei sottoscrittori.
Il processo di privatizzazione - che aveva visto negli anni Ottanta solo le cessioni di Alfa Romeo a FIAT e di Lanerossi al gruppo Marzotto - iniziò con la vendita dell'IMI, dell'INA e delle tre banche di interesse nazionale di proprietà dell'IRI, quest'ultima importante perché allargò le basi finanziarie esterne al circuito pubblico per i successivi collocamenti azionari e creò meccanismi di disciplina più severi nell'erogazione del credito. L'uscita dello Stato dal settore bancario fu completata più tardi con la cessione della BNL (1998) e del Mediocredito Centrale (1999). Questi collocamenti seguirono la riforma della legislazione bancaria, con l'emanazione del Testo unico in materia bancaria e creditizia del 1993 la quale, eliminando la separazione tra credito a breve e credito a medio e lungo termine, aprì la strada all'affermazione anche nel nostro paese della banca universale.
La cessione di società di servizio entrò nel vivo con la vendita di Aeroporti di Roma, Telecom Italia (di proprietà dell'IRI, il cui controllo fu ceduto al mercato nel 1997), *tranches* successive del capitale di ENI (a partire dal 1995) ed ENEL (dal 1999), e Autostrade (1999). Furono anche cedute con successo le società industriali dell'IRI e le attività petrolchimiche dell'ENI; l'IRI venne posto in liquidazione nel giugno del 2000, dopo aver trasferito la proprietà dell'Alitalia e della RAI al ministero del tesoro. Collocamenti significativi sul mercato furono effettuati anche da enti pubblici locali, perlopiù mantenendo il controllo e un grado elevato di interferenza delle amministrazioni pubbliche nelle gestioni. Gli effetti di concorrenza Nel complesso, i processi concorrenziali nel mercato bancario presero vigore solo lentamente per il freno posto dalla Banca d'Italia fino ai primi anni del Duemila ai processi di aggregazione e all'acquisto di quote di controllo da parte di investitori stranieri. La concorrenza sul mercato dei servizi è aumentata nella telefonia, molto meno negli altri comparti, a causa della lenta evoluzione del quadro regolamentare pro-concorrenziale. I mercati dell'elettricità e del gas e dei trasporti ferroviari sono ancora largamente organizzati su base nazionale, ad esclusione dei concorrenti esteri, quelli degli altri trasporti pubblici e della distribuzione di energia e dell'acqua addirittura su base locale. La resistenza ad ulteriori liberalizzazioni è stata aumentata dal desiderio del tesoro e degli enti locali di conservare profittevoli fonti di dividendi, in una fase di crescenti restrizioni nei bilanci pubblici. Il tesoro è rimasto come azionista di maggioranza relativa nell'ENI e nell'ENEL; invece di incoraggiare l'abbassamento delle tariffe e gli investimenti in tecnologia, gli indirizzi del tesoro hanno privilegiato il pagamento di elevati dividendi. Nel caso delle autostrade e degli aeroporti, l'inadeguatezza del quadro regolamentare e la commistione di regimi pubblicistici e privatistici di gestione non hanno aiutato a

Anche durante il positivo ciclo di borsa di fine anni novanta, la spinta maggiore all'attività di mercato primario sull'azionario è venuta proprio dalle privatizzazioni[41] e dalle uscite degli operatori di private equity[42].

Marginale è, invece, sempre rimasto il ruolo delle IPO promosse da aziende familiari, spesso limitate nella capacità concorrenziale da ostacoli di gestione interna e mancanza di una mission definita e comunemente accettata.

Mentre le grandi banche d'investimento straniere trovano nei collocamenti nazionali una delle loro primarie aree d'affari, il sistema finanziario italiano rimane alquanto bank oriented[43]. Sia i grandi gruppi polifunzionali, sia le banche multiregionali non mostrano una spiccata propensione a sviluppare le attività di mercato, preferendo piuttosto continuare a concentrarsi sull'ottimizzazione delle attività di lending[44].

Così, sia l'attività promozionale alla quotazione svolta con insistenza da Borsa Italiana, nel perseguimento del proprio fine di lucro, e da soggetti istituzionali, per rendere competitive le imprese a livello internazionale , sia quella di ricerca e convincimento delle società svolta dai pochi intermediari focalizzati sull'erogazione dei servizi per il mercato azionario, non hanno

---

stabilire un quadro trasparente di formazione dei prezzi, mentre sono mancati i meccanismi tesi a verificare gli impegni di investimento e la qualità dei servizi per conto degli utenti. Nel complesso, dunque, il programma di privatizzazione italiano degli anni Novanta può essere giudicato un successo dal punto di vista delle somme raccolte, che hanno fornito oltre 120 miliardi di euro di introiti, ovvero quasi l'11% del PIL medio del periodo di riferimento. Successo pieno ha coronato anche la privatizzazione delle attività industriali, che hanno condotto nella quasi totalità dei casi all'aumento dell'efficienza e in molti casi significativi all'integrazione delle attività in validi gruppi internazionali. Si conferma, al riguardo, la minor efficienza delle gestioni pubbliche, sempre caratterizzate da costi unitari più elevati (soprattutto del personale) e da minor efficacia nelle scelte strategiche. I collocamenti di azioni in borsa hanno anche contribuito considerevolmente all'allargamento del nostro mercato di borsa: una dozzina delle società nel MIB30 e circa il 50% della capitalizzazione di borsa è rappresentato da società privatizzate. Infine, nonostante la percezione diffusa in senso contrario, l'evidenza empirica indica anche che le commissioni pagate per gli advisor e i collocamenti sono nel complesso risultate più basse o in linea con quelle di mercato".

41 G. Siciliano, Cento anni di Borsa Italiana, Bologna, 2001.

42 Il private equity è un'attività finanziaria tramite la quale un investitore istituzionale rileva quote di una società, sia tramite l'acquisto presso terzi già in possesso delle azioni, sia sottoscrivendo azioni di nuova emissione, portando nuovi capitali nella società.

43 Nei sistemi "bank oriented" le imprese fanno prevalentemente (non esclusivamente) ricorso al sistema bancario per ottenere capitali per il loro funzionamento. Ovviamente questi capitali sono di debito in quanto mezzi di terzi. Nei sistemi "market oriented", invece, le imprese fanno prevalentemente ricorso al mercato dei capitali per ottenere risorse finanziarie (prevalentemente azioni). L'esempio più rilevante è quello degli USA. Con un sistema bank oriented la maggior parte delle imprese restano private e non fanno ricorso al mercato dei capitali di rischio, ovvero il mercato azionario. Questo permette ai soci di avere sempre pieno controllo sull'impresa. Inoltre gli adempimenti burocratici per le imprese non quotate sono decisamente minori, così come sono meno le informazioni che per legge vanno rese pubbliche. I capitali di debito, inoltre, permettono risparmi fiscali e fino a certi limiti costano di meno dei capitali di rischio. Tuttavia, i capitali di debito provengono dalle banche, che possono essere più o meno propense a dare fondi, soprattutto ad imprese più rischiose. Inoltre, le banche possono mettere clausole restrittive e stabilire condizioni di erogazione dei fondi tutt'altro che favorevoli all'imprenditore.

44 www.economiauniparthenope.it/icostidellaquotazione.

evitato che il negativo ciclo di borsa e la scarsa propensione verso la quotazione si riverberasse sulle nuove quotazioni di imprese italiane.

Da quanto sopra illustrato emerge che la quotazione comporta numerosi benefici, non solo economici, che si traducono in una migliore efficienza e trasparenza della società, elementi in grado di produrre un plusvalore sicuramente ravvisabile nel medio-lungo termine.

È importante tuttavia che la società prenda in considerazione anche gli obblighi e gli aspetti potenzialmente critici che la quotazione può comportare. Questi fattori di criticità, variabili a seconda delle circostanze e delle caratteristiche dell'azienda coinvolta, sono:

- il titolo è maggiormente suscettibile alle condizioni del mercato, si perla infatti di prezzo fatto dal mercato o subito dall'imprenditore, in quanto può essere influenzato dalle azioni speculative e dalla congiuntura negativa della borsa[45], indipendentemente dalle scelte strategiche dell'azienda, la conseguenza di questa volatilità potrebbe essere la mancata corrispondenza tra i risultati dell'azienda e il valore di mercato del titolo;
- la quotazione rende necessario il robusto cambiamento di aspetti organizzativi, gestionali e manageriali. Ad esempio è necessario adeguare i sistemi informativi[46], i meccanismi operativi, adottare i principi di corporate governance[47], effettuare politiche di comunicazione ed eventualmente modificare la cultura del management;

---

[45] La variazione del titolo oltre ad essere influenzata dalle caratteristiche dell'azienda, quindi da fattori interni come la stabilità finanziaria e il raggiungimento di obiettivi trimestrali, risente molto dei fattori di influenza esterna, quali per esempio l'andamento complessivo del settore di operatività, nonché dell'azione speculativa degli operatori del mercato.

[46] Art. 97 TUF, Obblighi informativi, "Fermo quanto previsto dal Titolo III, Capo I, agli emittenti, agli offerenti, ai revisori contabili e ai componenti degli organi sociali degli emittenti e degli offerenti, nonché agli intermediari incaricati del collocamento si applicano, in relazione all'offerta, l'articolo 114, commi 5 e 6 e l'articolo 115 dalla data della comunicazione prevista dall'articolo 94, comma 1.

2. La Consob individua con regolamento quali delle disposizioni richiamate nel comma 1 si applicano, nei medesimi periodi, agli altri soggetti indicati nell'articolo 95, comma 2, nonché ai soggetti che prestano i servizi indicati nell'articolo 1, comma 6, lettera *e)*.
3. Gli emittenti sottopongono il bilancio d'esercizio e quello consolidato, eventualmente approvati o redatti nel periodo dell'offerta, al giudizio di un revisore legale o di una società di revisione legale iscritti nell'apposito registro.
4. Qualora sussista fondato sospetto di violazione delle disposizioni contenute nel presente Capo o delle relative norme di attuazione, la Consob, allo scopo di acquisire elementi conoscitivi, può richiedere, entro un anno dall'acquisto o dalla sottoscrizione, la comunicazione di dati e notizie e la trasmissione di atti e documenti agli acquirenti o sottoscrittori dei prodotti finanziari di cui alla presente Sezione, fissando i relativi termini. Il potere di richiesta può essere esercitato anche nei confronti di coloro per i quali vi è fondato sospetto che svolgano, o abbiano svolto**,** un'offerta al pubblico in violazione delle disposizioni previste dall'articolo 94.

[47] Con la locuzione corporate governance si intende l'insieme delle regole, di ogni livello, che disciplinano la gestione e la direzione di una società. Sono incluse le relazioni tra gli stakeholder, chi detiene un qualunque interesse nella società, nello specifico: gli azionisti (shareholders), il consiglio di amministrazione (board of directors) e il menagement, e gli obiettivi per i quali l'impresa viene amministrata.

- l'accesso al mercato espone l'azienda ad una continua valutazione da parte di investitori e soggetti esterni che inducono l'azienda a privilegiare le performance di breve periodo. Infatti l'andamento del titolo dipende dalla capacità dell'azienda di confermare, trimestre per trimestre[48], il raggiungimento dei propri obiettivi attesi;
- la necessità di effettuare fin dall'inizio previsioni molto accurate, elemento essenziale per fondare la credibilità dell'azienda e renderla appetibile agli investitori
- aumenta il grado di complessità e di burocrazia in quanto la società quotata deve rispettare molte regole a tutela delle minoranze, del conflitto d'interesse e dell'integrità dei mercati. Inoltre alcune decisioni importanti per la vita di una società, quali l'aumento di capitale o l'ingresso in un nuovo mercato[49], devono essere prese considerando necessariamente gli interessi di soggetti che non possono partecipare a tale decisione[50];
- al fine di evitare fenomeni di insider trading[51], la società deve diffondere tempestivamente al pubblico, alla Borsa italiana e alla Consob, informazioni rilevanti ai

---

[48] Si fa comunemente riferimento al trimestre come periodo di tempo decorso il quale le società quotate comunicano i dati relativi alle vendite, ai costi e agli utili prodotti, inoltre con la comunicazione periodica la società comunica le prospettive di crescita per il successivo trimestre e adempie agli obblighi informativi periodici.

[49] Si parla di:
- Aumento di capitale, come atto straordinario che si realizza o con la modifica del patrimonio netto (a pagamento) o con l'utilizzo di riserve/fondi disponibili (aumento gratuito). L'aumento ha luogo con l'emissione di nuovi titoli o con l'incremento del valore delle azioni già circolanti.
- Ingresso in un nuovo mercato, nel momento in cui l'impresa decide di affacciarsi in sistemi di negoziazione/contrattazione nuovi.

[50] Il riferimento è a quei soggetti che non possiedono una quota tale da prendere parte alle attività decisionali.

[51] Art. 184 TUF, Abuso di informazioni privilegiate, "È punito con la reclusione da uno a sei anni e con la multa da euro ventimila a euro tre milioni chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:
a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;
b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;
c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a).
2. La stessa pena di cui al comma 1 si applica a chiunque essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose compie taluna delle azioni di cui al medesimo comma 1.
3. Il giudice può aumentare la multa fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo".

fini dell'andamento della quotazione, realizzando una "full disclosure di informazioni in precedenza non pubbliche"[52];

- l'impresa deve sostenere elevati costi per l'ammissione alla quotazione in Borsa, variabili a seconda della dimensione del collocamento, dell'emittente e del settore di operatività. Tali costi sono numerosi e comprendono vari voci di spesa tra cui: costi del consorzio, spese legali, costi Borsa Italiana, costi Consob, stampa e pubblicazioni, altri costi;
- la quotazione comporta una ridefinizione dell'assetto proprietario dell'azienda (diluizione della proprietà[53]) con conseguente dispersione della quota di controllo degli azionisti esistenti, e rende necessaria la condivisione delle decisioni. Per questo motivo gli azionisti spesso non sono favorevoli all'apertura del capitale[54].

Chiarita la volontà di procedere alla quotazione, l'impresa deve scegliere innanzitutto il mercato regolamentato su cui far negoziare le proprie azioni, tale scelta fa riferimento "sia alla posizione geografica del mercato, sia alla tipologia del mercato"[55].

Analizzando la posizione geografica si evidenzia che il fattore "Paese" resta di gran lunga preponderante in questa scelta[56].

Nonostante il rapido processo di integrazione delle normative e delle prassi operative dei mercati, perseguito soprattutto dalle nazioni appartenenti all'Unione Europea, gli emittenti continuano a prediligere i mercati localizzati nel Paese in cui hanno sede[57].

La quotazione su mercati esteri presenta, infatti, sempre e comunque, maggiore complessità. L'emittente si trova, infatti, a "fronteggiare l'incertezza derivante dalla necessità di rispettare i canoni di una securities law e di una regolamentazione di borsa diversa da quella del proprio Paese, quindi meno nota e, soprattutto, non sempre coordinata e compatibile con il diritto societario domestico che ne disciplina l'attività sociale"[58].

---

52 M. De Ambroggi, *La quotazione in borsa*, Parma, Facoltà di economia, 2012.

53 M. De Ambroggi, *La quotazione in borsa*, Parma, Facoltà di economia, 2012.

54 Paolo Montalenti, *Trattato di Diritto Commerciale*, La Società Quotata, IV volume, Padova, CEDAM, 2004, pag. 89.

55 La scelta di quotarsi in borsa e l'impatto sull'azienda, corso di Gestione finanziaria delle imprese, Facoltà di Economia, LIUC.

56 Dati Istat nel periodo 2010-2015.

57 La decisione di quotarsi nei mercati con sede nel proprio paese di origine è dettata da una molteplicità di fattori, tra gli altri la locazione dei propri interessi commerciali e la minore complessità. Circa la quotazione su mercati esteri rimane esplicita la difficoltà di rapportarsi con autorità estere e leggi diverse, che dettano una disciplina spesso poco compatibile con l'assetto domestico.

58 www.economiauniparthenope.it/icostidellaquotazione.

Una ulteriore difficoltà alla scelta di una quotazione all'estero può derivare da possibili divergenze tra i principi contabili da rispettare nella redazione di bilanci annuali e relazioni periodiche, trimestrali e semestrali, secondo gli obblighi di disclosure applicati dalla borsa estera e quelli imposti, invece, dalla normativa domestica. Non di rado le imprese di grandi dimensioni optano per la quotazione sia su un mercato domestico, sia su uno o più mercati esteri, dando vita al cosiddetto "dual listing, o anche multiple listing"[59]. Di tale possibilità si avvalgono, in genere, società di grandi dimensioni, i cui interessi sono diffusi in più Paesi, e funge da antidoto al rischio di flowback[60]. Se il suo brand è più affermato all'estero che nel proprio Paese, l'emittente può preferire una quotazione su mercato estero (foreign listing), "nella speranza che la notorietà del marchio presso i consumatori aiuti ad assicurare il successo del collocamento dei titoli presso gli investitori"[61]. Altre considerazioni entrano in gioco, nella scelta del mercato su cui quotarsi, in particolare:

- la presenza di paragoni significativi nel mercato regolamentato, cioè l'esistenza di società già quotate che svolgano analoga attività può garantire una migliore conoscenza dell'attività da parte degli investitori, generando la fiducia e la credibilità necessarie per ottenere supporto;
- la portata dei listing requiriments, ossia degli obblighi che l'accordo di quotazione tra società di gestione del mercato ed emittente impone a quest'ultima di osservare, per ottenere prima l'ammissione, e poi la permanenza del titolo in Borsa. Tali obblighi riguardano la corporate governance della società, la disciplina informativa, l'equilibrio finanziario della società dato dagli ultimi bilanci in utile, la negoziabilità del titolo tramite un flottante minimo;
- le caratteristiche della società, se l'emittente è in grado di produrre utili stabili si orienterà verso il "Value Stock"[62]nell'MTA, quindi l'attività si svolgerà nei settori tradizionali, con buona redditività, sfruttando una posizione di mercato consolidata, se l'emittente è una società con alto potenziale di crescita si orienterà verso l'"High growth Stock"[63] nel Nuovo Mercato, inserendosi nei settori altamente tecnologici, con elevate prospettive di crescita e fabbisogni legati a programmi di sviluppo rapido.

---

59 www.borsaitaliana.it/quotarsiinborsa.

60 Con il termine flowback ci si riferisce alla naturale tendenza delle transazioni a concentrarsi su un unico polo di liquidità, in genere quello costituito dal mercato domestico.

61 www.economiauniparthenope.it/icostidellaquotazione.

62 Con Value Stock si intende una valorizzazione nella quale si tende al commercio ad un prezzo inferiore rispetto ai suoi fondamentali e quindi sottovalutati da un investitore.

63 Con High growth Stock si intende una crescita ad un tasso superiore rispetto alla media del mercato.

Oltre alla decisione inerente al mercato su cui quotare la propria impresa assume una notevole valenza strategica anche quella relativa a quale segmento scegliere.

Analizzando il Mercato Telematico Azionario, che risponde ai migliori standard internazionali ed è il mercato azionario più rilevante[64], si evidenzia la suddivisione in tre segmenti, ognuno dei quali con requisiti di ammissione diversi:

a) Blue Chip (FTSE MIB), che comprende le quaranta imprese maggiormente capitalizzate;
b) STAR (FTSE Italia STAR), capitalizzazione tra un miliardo di euro e quaranta milioni di euro, requisiti ulteriori;
c) Segmento Standard, capitalizzazione tra un miliardo di euro e quaranta milioni di euro, senza i requisiti ulteriori previsti dal segmento STAR.

L'obiettivo di Borsa Italiana è la creazione di un mercato, o segmento di mercato, che sia adatto alle esigenze di un determinato tipo di imprese e in grado di attrarre investitori con uno specifico stile di gestione e una certa capacità economica.

Il Mercato Telematico Azionario, subordinato a requisiti stringenti risponde alle esigenze di quotazione di aziende di media e grande capitalizzazione che intendono attrarre risorse da investitori privati e professionali. Tuttavia, alle imprese di media o piccola dimensione, intese come società con una capitalizzazione di mercato compresa tra un miliardo di euro e quaranta milioni di euro, in grado di distinguersi sia per un modello di governance più attento alle esigenze degli azionisti, a prescindere dalla quota detenuta, sia per una maggiore liquidità del titolo, è consentita la possibilità di richiedere l'accesso al segmento STAR caratterizzato da requisiti di quotazione più stringenti.

L'Alternative Investment Market Italia (Mercato Alternativo del Capitale), istituito nel 2008 al fine di favorire l'accesso al mercato di nuove realtà, è il mercato gestito da Borsa Italiana ed indirizzato alle PMI ad alto tasso di crescita.

L'AIM ha stimolato un crescente interesse tra le piccole e medie imprese, che rappresentano il tessuto imprenditoriale italiano, presentandosi come un modo agevole e poco costoso per finanziarsi, abbattendo la distanza che storicamente ha diviso le PMI dal mondo finanziario, e la ragione del successo di questo mercato è dovuta alla semplicità delle procedure della quotazione, che sono generalmente veloci nei tempi e poco costose.

Si tratta di un sistema multilaterale di negoziazione (MTF)[65], AIM non rientra nella categoria di mercato regolamentato disciplinato dalla direttiva MIfid[66], di conseguenza soggiace

[64] www.borsaitaliana.it/mta.

a due regolamenti principali: Regolamento Emittenti, Regolamento Nominated Advisers, i quali conferiscono ad AIM "quella flessibilità che consente alle piccole-medie imprese di accedere al mercato dei capitali in modo più semplice e a costi più contenuti rispetto ad MTA"[67].

L'ammissione all'AIM non richiede criteri minimi: non è richiesta una capitalizzazione minima o massima della società e non è prevista una soglia minima di azioni sul mercato in termini di flottante. Il processo di quotazione in borsa oltre ad essere articolato e complesso sotto il profilo procedurale, risulta economicamente dispendioso e stimato in circa il cinque per cento del controvalore complessivo dell'offerta[68], anche se "l'impegno profuso dalla società quotanda dovrebbe essere considerato come un investimento finalizzato al miglioramento della capacità dell'impresa di creare valore nel lungo periodo"[69].

I costi connessi alla quotazione possono essere ripartiti in tre grandi categorie:

- costi indiretti; si tratta dei costi indotti dall'acquisizione dello status di impresa quotata, che sono difficilmente quantificabili essendo connessi alle modifiche che la società di gestione del mercato richiede di apportare alla struttura e ai sistemi di gestione e controllo dell'emittente.
- costi diretti ed espliciti, ossia:
  a) le spese legate all'ingresso sul mercato regolamentato, rappresentate prevalentemente dai compensi corrisposti ai vari consulenti intervenuti nella quotazione, e dalle spese per Consob e Borsa Italiana. Alcuni di questi costi non sono negoziabili, come il compenso da corrispondere alla Consob, due per cento del controvalore dell'offerta, e a Borsa italiana, settantacinque euro per ogni 500mila euro di capitalizzazione con un minimo di diecimila euro e un massimo di 500mila euro, i quali sono legati esclusivamente alla dimensione complessiva dell'offerta. Le altre spese dipendono invece da una molteplicità di variabili rintracciabili nel tipo di offerta, nel controvalore del collocamento, nel metodo del collocamento, nell'importanza e riconoscibilità dell'emittente e nella reputazione del collocatore, dal momento che, tra i servizi resi all'emittente, figura quello di certificazione della qualità dei titoli emessi. La spesa quantitativamente più rilevante è la remunerazione

---

65 Glossario Borsa Italiana: Sistemi di contrattazione privati che offrono la possibilità di negoziare strumenti finanziari quotati presso una borsa, senza compiti di ammissione e informativa.

66 Vedi cap. 1 par. 1.5.

67 M. De Ambroggi, *La quotazione in borsa*, Parma, Facoltà di economia, 2012.

68 www.borsaitaliana.it/quotarsiinborsa.

69 Donato Ivano Pace, *Ammissione sospensione esclusione dai mercati regolamentati*, Milano, Giuffrè Editore, 2012, pag. 80.

corrisposta agli intermediari che organizzano il collocamento dei titoli[70], la quale è calcolata come percentuale del controvalore dell'emissione;

b) i costi legati alla permanenza nelle negoziazioni, legate alla certificazione dei bilanci ed alla gestione dell'informativa periodica. Sono previsti, poi, compensi periodici a Borsa Italiana e alla Consob, come il contributo annuale di vigilanza connesso all'ammontare di capitale sociale dell'emittente, e gestione dei titoli. Infine, si ricorda la remunerazione per lo specialist, laddove previsto.

- costi impliciti, legati al fenomeno dell'underpricing[71]che può essere considerato un costo connesso alla quotazione poiché esiste una diffusa evidenza dell'esistenza di una differenza positiva tra il prezzo fatto registrare dai primi scambi sul mercato secondario ed il prezzo del collocamento.

2.2 Quadro Normativo

Nel quadro normativo che disciplina il processo di quotazione, le società emittenti e le attività trovano dei riferimenti in diverse fonti di matrice primaria e regolamentare.

La normativa primaria relativa alla disciplina delle società emittenti è contenuta, nel Testo Unico delle disposizioni in materia di intermediazione finanziaria d. lgs. 58 del 1998 (TUF), e in

---

[70] Renzo Costi, Luca Enriques, *Trattato di Diritto Commerciale*, Il Mercato Mobiliare, VIII volume, Padova, CEDAM, 2004, pag. 234.

[71] In letteratura si suole identificare l'*underpricing* come quel fenomeno che si verifica quando il prezzo dei titoli in Ipo durante il primo giorno di negoziazione si posiziona sopra il suo valore all'atto del collocamento. Da oltre un ventennio gli economisti si confrontano con quello che è stato definito come il puzzle dell'underpricing delle IPOs. Uno dei primi studiosi a documentare in maniera sistematica il fenomeno dell'underpricing è stato Ibboston (1975): questi trova un underpricing medio dell'11,4% per le IPOs condotte negli anni Sessanta negli USA. Ritter (1984), invece, riporta un underpricing medio del 18,8% per circa 5000 IPOs condotte negli USA fra il 1960 ed il 1982. Nel tentativo di spiegare le ragioni del perché le società scelgano di quotarsi ad un prezzo più basso (in media) di quello che rifletterebbe il vero valore dei loro titoli, tanto da generare underpricing, gli economisti hanno dato vita ad un'ampia letteratura teorica e empirica. A seconda degli approcci, l'underpricing è visto come un mezzo per incentivare gli investitori ad aderire all'offerta (compensandoli per i rischi che con ciò essi si assumono), o come un mezzo per evitare eventuali controversie legali con gli azionisti o, ancora, per evitare il rischio di un loro disinteresse nei confronti del titolo. L'underpricing può anche essere visto come uno strumento idoneo a generare un eccesso di domanda dei titoli, creando in questo modo un azionariato largamente diffuso (attraverso la fissazione di lotti minimi ridotti) funzionale a rendere la società più difficilmente scalabile. Quasi tutti i modelli teorici sviluppati in letteratura per spiegare il fenomeno dell'underpricing nelle IPO si basano sull'ipotesi dell'esistenza di asimmetrie informative fra i vari soggetti coinvolti nel collocamento (l'impresa, la banca d'investimento, gli investitori esterni). È tuttavia possibile operare una distinzione fra modelli in cui l'underpricing è una strategia volontariamente perseguita dall'impresa emittente, e i modelli in cui l'underpricing è il risultato dell'interazione e delle relazioni contrattuali fra emittente e banca d'investimento.

particolare nella parte quarta del medesimo. Il TUF contiene le disposizioni generali in merito agli obblighi ed agli adempimenti connessi alla quotazione, alle Autorità di vigilanza e controllo ed ai relativi poteri.

L'attuazione delle previsioni di cui al TUF è affidata al potere regolamentare di Consob, che ha adottato a tale scopo il Regolamento n. 11971 del 14 maggio 1999, come successivamente modificato, con delibera Consob n. 15232 del 29 novembre 2005 (Regolamento Emittenti).

Tale Regolamento contiene la disciplina di dettaglio volta a concretizzare le disposizioni del TUF e specificare, tra l'altro, i poteri e le funzioni dallo stesso attribuiti a Consob.

Pertanto, si rileva come sia indispensabile, per la società che intenda intraprendere la strada della quotazione, il costante e accurato monitoraggio della attività di produzione svolta da Consob.

In terzo luogo, la disciplina del processo di quotazione è altresì contenuta all'interno del Regolamento dei mercati organizzati e gestiti da Borsa Italiana, deliberato dall'Assemblea di Borsa Italiana S.p.A. il 29 aprile 2005 e approvato dalla CONSOB con la delibera 15101 del 5 luglio 2005[72].

Una ulteriore fonte nell'ambito dell'ammissione alla quotazione è costituita dal d.lgs. 385 del 1993, ossia il Testo unico delle leggi in materia bancaria e creditizia (TUB).

Infine per quanto attiene gli aspetti fiscali della materia ci si riferisce al d.p.r. 917 del 1986, Testo unico delle imposte sui redditi (TUIR).

2.3 I soggetti del procedimento di quotazione

Il processo di quotazione vede coinvolti, nel corso del suo svolgimento, una serie di soggetti con compiti precisi:

- Il Global Coordinator è quel soggetto, banca o società di intermediazione mobiliare o altro intermediario finanziario, che assiste la società quotanda nel processo di offerta dei propri strumenti finanziari sul mercato, in particolare costituendo e coordinando il consorzio di collocamento dei titoli, dirigendo l'operazione di collocamento dei titoli stessi sul mercato e fornendo alla società ogni necessario supporto. L'attività inizia con

[72] L'approvazione del Regolamento di Borsa da parte della CONSOB avviene a norma dell'articolo 63 co. 1 l. b TUF.

uno studio sulla fattibilità dell'operazione, in caso lo studio si risolva positivamente il global coordinator funge da collegamento tra l'emittente, la società di gestione del mercato e la CONSOB, di conseguenza è presente in tutte le fasi di ammissione. Il global coordinator può rivestire anche il ruolo di advisor o sponsor della società.

- Lo Sponsor è quel soggetto, banca o intermediario finanziario, che collabora con l'emittente nella procedura di ammissione a quotazione, nonché nel periodo successivo all'ammissione alle negoziazioni dei titoli della società e si pone come garante nei confronti del mercato della qualità, dell'esattezza e della completezza delle informazioni fornite dalla società, a tal fine si impegna a pubblicare almeno due analisi finanziarie nel corso dell'anno circa le condizioni della società e analisi sintetiche su eventi rilevanti che coinvolgono la società. La sua nomina è resa obbligatoria nei casi stabiliti dall'art. 2.3.1 del Regolamento di Borsa[73].

[73] Articolo 2.3.1: "1. L'emittente deve procedere alla nomina di uno sponsor nei seguenti casi: a) quando intenda presentare a Borsa Italiana, ai sensi dell'articolo 2.1.2, comma 1, domanda di ammissione di strumenti finanziari di cui all'articolo 2.1.1, comma 1, lettera a) e d) comprese le azioni di Investment Companies, di Real Estate Investment Companies e di SIV, non avendo altri strumenti già ammessi alla quotazione da Borsa Italiana; b) quando, a seguito di gravi infrazioni a norme del presente Regolamento o di altri regolamenti o discipline applicabili, Borsa Italiana richieda che sia nominato uno sponsor per assistere l'emittente negli adempimenti dovuti.

2. In caso di operazioni di Reverse merger e nel caso di operazioni di aumento di capitale mediante conferimento in natura di attività di valore significativamente superiore all'attivo patrimoniale dell'emittente come calcolato ai sensi dell'articolo 117 bis TUF e del relativo Regolamento Consob previsto dall'articolo 117 bis comma 2, questo ultimo procede alla nomina di un solo sponsor ai soli fini del rilascio di dichiarazioni conformi a quanto previsto dall'articolo 2.3.4, comma 2, lettere c) e d). L'incarico di sponsor non può essere conferito al soggetto che si trovi nelle condizioni previste all'articolo 2.3.3 del Regolamento e specificate nelle Istruzioni. A tal fine lo sponsor deve rilasciare alla Borsa Italiana l'attestazione di cui all'articolo 2.3.3, comma 2, entro la data della nomina e comunque almeno 10 giorni di borsa aperta antecedenti la data del rilascio delle dichiarazioni. Tali disposizione non si applicano per le società quotate nel Segmento Professionale del mercato MIV.
3. Non è necessaria la nomina dello sponsor nel caso di domanda di ammissione alla quotazione di azioni rinvenienti da un'operazione di fusione di società quotate.
4. L'incarico di sponsor deve essere conferito non più tardi del momento di presentazione a Borsa Italiana della domanda di ammissione degli strumenti finanziari e per una durata tale da coprire almeno: a) un anno dalla data di inizio delle negoziazioni, nel caso in cui l'incarico sia stato conferito in relazione all'ammissione degli strumenti finanziari di cui all'articolo 2.1.1, comma 1, lettera a), comprese le azioni di Investment Companies, di Real Estate Investment Companies e di SIV; b) il periodo fino alla data di inizio quotazione nel caso di ammissione degli Regbit 03-10-2011 senza ev. Data di entrata in vigore: 3 ottobre 2011, 61 strumenti finanziari di cui all'articolo 2.1.1, comma 1, lettera d).
5. Nei casi di cui alla lettera b) del precedente comma 1 l'incarico dovrà avere durata pari ad almeno un anno.
6. La nomina dello sponsor è comunque dovuta nel caso di prima ammissione degli strumenti finanziari di cui all'articolo 2.1.1, comma 1, lettera a), comprese le azioni di Investment Companies, di Real Estate Investment Companies e di SIV.
7. Borsa Italiana può esentare l'emittente dall'obbligo di cui al comma 1 qualora le azioni di cui si chiede l'ammissione alla quotazione siano già quotate in un altro mercato regolamentato europeo o extracomunitario.
8. Per gli strumenti finanziari emessi da Borsa Italiana ai fini del presente articolo i riferimenti a Borsa Italiana devono essere intesi come riferiti a Consob e i riferimenti all'emittente come riferiti a Borsa Italiana, per quanto applicabile".

- Il Financial Advisor è il consulente che si occupa di assistere la società e lo sponsor nello studio di fattibilità del progetto di quotazione, nella redazione del prospetto informativo, nella definizione dei termini dell'offerta. Studia i mercati finanziari e prospetta le alternative migliori, spiegando costi, rischi, vantaggi, per ogni soluzione. La figura del consulente finanziario indipendente viene regolamentata nell'art. 18 bis d.lgs. 58/98[74].
- Lo Specialist è l'intermediario cui è affidato il compito di sostenere la liquidità del titolo e migliorare l'informativa al mercato; a tal fine egli deve esporre con continuità proposte di acquisto e vendita a prezzi che non si scostino tra loro di una percentuale superiore a quella stabilita da Borsa Italiana ed impegnarsi nella redazione di studi sull'Emittente. La sua nomina è oggi resa obbligatoria in determinate ipotesi sancite dall'art. 2.3.4 del Regolamento di Borsa[75].

---

[74] Art. 18 bis: "1. La riserva di attività di cui all'articolo 18 non pregiudica la possibilità per le persone fisiche, in possesso dei requisiti di professionalità, onorabilità, indipendenza e patrimoniali stabiliti con regolamento adottato dal Ministro dell'economia e delle finanze, sentite la Banca d'Italia e la Consob, di prestare la consulenza in materia di investimenti, senza detenere somme di denaro o strumenti finanziari di pertinenza dei clienti.

2. È istituito l'albo delle persone fisiche consulenti finanziari, alla cui tenuta, in conformità alle disposizioni emanate ai sensi del comma 5, provvede un organismo i cui rappresentanti sono nominati con decreto del Ministro dell'economia e delle finanze sentite la Banca d'Italia e la Consob.
3. L'organismo di cui al comma 2 ha personalità giuridica ed è ordinato in forma di associazione, con autonomia organizzativa e statutaria. Nell'ambito della propria autonomia finanziaria, l'organismo determina e riscuote i contributi e le altre somme dovute dagli iscritti e dai richiedenti l'iscrizione, nella misura necessaria per garantire lo svolgimento delle proprie attività.
4. L'organismo di cui al comma 2: a) vigila sul rispetto delle disposizioni di cui alle lettere d), e) e g) del comma 5; b) per i casi di violazione delle regole di condotta delibera, in relazione alla gravità dell'infrazione e in conformità alle disposizioni di cui al comma 5, lettera b), la sospensione dall'albo da uno a quattro mesi, ovvero la radiazione dal medesimo.
5. La Consob determina, con regolamento, i principi e i criteri relativi: a) alla formazione dell'albo previsto dal comma 2 e alle relative forme di pubblicità; b) all'iscrizione all'albo previsto dal comma 2 e alle cause di sospensione, di radiazione e di riammissione; c) alle cause di incompatibilità; d) alle regole di condotta che i consulenti devono rispettare nel rapporto con il cliente, avuto riguardo alla disciplina cui sono sottoposti i soggetti abilitati; e) alle modalità di tenuta della documentazione concernente l'attività svolta dai consulenti finanziari; f) all'attività dell'organismo, con specifico riferimento ai compiti di cui al comma 4; g) alle modalità di aggiornamento professionale dei consulenti finanziari.
6. Avverso le decisioni di sospensione o radiazione dall'albo assunte dall'organismo, ai sensi del comma 4, lettera b), è ammesso ricorso, da parte dell'interessato, dinnanzi alla Consob, entro i successivi trenta giorni e secondo le procedure dalla stessa determinate con regolamento. Avverso le delibere adottate dalla Consob ai sensi del presente comma è ammessa opposizione da parte dell'interessato alla corte d'appello; si applicano i commi 4, 5, 6, 7 e 8 dell'articolo 195 del presente decreto.
7. La Consob può richiedere all'organismo la comunicazione di dati e notizie e la trasmissione di atti e documenti con le modalità e nei termini dalla stessa stabiliti. La Consob può effettuare ispezioni e richiedere l'esibizione dei documenti e il compimento degli atti ritenuti necessari presso l'organismo.
8. In caso di inerzia o malfunzionamento dell'organismo la Consob ne propone lo scioglimento al Ministro dell'economia e delle finanze".

[75] Articolo 2.3.4: "1. Lo sponsor collabora con l'emittente nella procedura di ammissione degli strumenti finanziari, ai fini di un ordinato svolgimento della stessa.

2. Nel caso di ammissione alla quotazione degli strumenti finanziari di cui all'articolo 2.1.1, comma 1, lettera a), lo sponsor assume le responsabilità di seguito elencate, rilasciando per ciascuna di esse apposita dichiarazione a Borsa Italiana: a) attesta di avere comunicato a Borsa Italiana tutti i dati e i fatti di cui egli è venuto a conoscenza nel corso della propria attività e che dovrebbero essere presi in considerazione da Borsa Italiana stessa ai fini dell'ammissione alla quotazione, oltre a quelli già resi noti dall'emittente ai sensi dell'articolo 2.4.1, comma 2; b) assicura che l'organo amministrativo e l'organo di controllo sono stati adeguatamente informati in ordine alle responsabilità e agli obblighi derivanti dalle leggi e dai regolamenti in vigore e conseguenti all'ammissione alla quotazione degli strumenti finanziari della società stessa; c) dichiara di non essere venuto a conoscenza di elementi tali da far ritenere, al momento del rilascio della presente dichiarazione, che la società emittente e le principali società del gruppo ad essa facente capo non abbiano adottato al proprio interno un Sistema di controllo di gestione conforme a quello descritto dall'emittente nel Memorandum e che le eventuali criticità evidenziate dall'emittente non siano incompatibili con la casistica indicata da Borsa Italiana nelle Istruzioni. A tal fine, lo Sponsor si avvale delle verifiche di conformità condotte da una società di revisione o da altro soggetto qualificato individuato dallo sponsor e incaricato congiuntamente con l'emittente, in possesso di requisiti di professionalità e indipendenza; d) dichiara di essersi formato il convincimento che i dati previsionali esibiti nell'ambito del piano industriale, relativi all'esercizio in corso alla data di presentazione della domanda di quotazione, sono stati determinati dall'emittente dopo attento e approfondito esame documentale delle prospettive economiche e finanziarie dell'emittente e del gruppo ad esso facente capo. Qualora il giorno in cui è stata completata la documentazione da allegare alla domanda di ammissione alla quotazione sia successiva al 15 settembre, la dichiarazione deve estendersi ad almeno i primi sei mesi dell'esercizio successivo. Ai fini del rilascio della dichiarazione, lo sponsor potrà avvalersi di un'apposita verifica condotta da una società di revisione o da altro soggetto qualificato indicato dallo sponsor e accettato dall'emittente. L'attestazione di cui alla lettera a) deve essere prodotta a seguito della presentazione della domanda di ammissione e rinnovata due giorni prima del provvedimento di ammissione a quotazione. Nel caso di procedura di ammissione alla quotazione di azioni sulla base di un prospetto costituito da documenti distinti di cui all'articolo 2.4.9 del Regolamento, le dichiarazioni di cui ai punti precedenti devono essere prodotte a seguito della presentazione della richiesta di rilascio del giudizio di ammissibilità. L'attestazione di cui alla lettera a) deve essere rinnovata due giorni prima del rilascio del giudizio di ammissibilità nonché due giorni prima del provvedimento di ammissione a quotazione. La dichiarazione di cui alla lettera d) deve essere rinnovata in occasione della presentazione della domanda di ammissione. Qualora il giorno in cui è stata completata la documentazione da allegare alla richiesta di rilascio del giudizio di ammissibilità o alla domanda di ammissione alla quotazione sia successivo al 15 settembre, la dichiarazione deve estendersi ad almeno i primi sei mesi dell'esercizio successivo.
3. Nel caso di ammissione alla quotazione degli strumenti finanziari di cui all'articolo 2.1.1, comma 1, lettera a), diversi dalle azioni di Investment Companies, di Real Estate Investment Companies e di SIV, per i quali non sia stata presentata la domanda di cui all'articolo 2.2.3, comma 1, lo sponsor si impegna, altresì, per tutta la durata del proprio incarico e a partire dalla data di inizio delle negoziazioni: a) a produrre o a far produrre a proprio nome almeno due ricerche (come definite nell'articolo 65 del Regolamento approvato con delibera Consob n. 11971) all'anno concernenti l'emittente, da redigersi tempestivamente e secondo i migliori standard in occasione della pubblicazione dei risultati di esercizio e dei dati semestrali. Le ricerche devono essere diffuse al pubblico secondo le modalità e la tempistica stabilite nelle Istruzioni; b) a organizzare almeno due volte all'anno un incontro tra il management della società e gli investitori professionali, presenziando agli incontri medesimi.
4. Nel caso di ammissione alla quotazione di azioni di emittenti AIM Italia lo sponsor assume le responsabilità di cui al comma 2 del presente articolo, lettere a), b) e d), rilasciando per ciascuna di esse apposita dichiarazione a Borsa Italiana.
5. Nel caso di ammissione alla quotazione di azioni di emittenti Private Equity backed lo sponsor assume le responsabilità di cui al comma 2 del presente articolo, lettere a), b) e d), rilasciando per ciascuna di esse apposita dichiarazione a Borsa Italiana.
6. Nel caso di ammissione alla quotazione degli strumenti finanziari di cui all'articolo 2.1.1, comma 1, lettera d) e azioni di Investment Companies, di Real Estate Investment Companies e di SIV, lo sponsor assume le responsabilità di cui al comma 2 del presente articolo, lettere a), b), rilasciando per ciascuna di esse apposita dichiarazione a Borsa Italiana.
7. Nel caso di ammissione alla quotazione di azioni di Investment Companies e di Real Estate Investment Companies lo sponsor attesta che l'emittente dispone di una struttura organizzativa e di procedure idonee ad assicurare un'adeguata valutazione delle proposte di investimento o di disinvestimento nonché un

- L'Investor Relator è il soggetto incaricato della gestione dei rapporti con investitori e intermediari e può essere un soggetto interno o esterno alla società. Se le società appartengono al segmento STAR l'investor relator deve essere una figura interna, in modo da poter partecipare alle decisioni strategiche, mentre nelle aziende di grosse dimensioni si trova l'Investor Relation Department, costituito da diverse unità in modo da gestire i numerosi rapporti. Rappresenta la società presso la comunità finanziaria e deve far comprendere ai potenziali investitori il valore dell'azienda, si tratta di una figura indispensabile per alimentare la fiducia e mantenerla. Con lo sviluppo della "trasparenza aziendale"[76] come cultura di riferimento nell'ambito finanziario, il ruolo del Relator trova la sua naturale collocazione nell'azienda che si deve confrontare quotidianamente con i mercati, gli investitori istituzionali, gli analisti e tutti gli altri soggetti che frequentano il comparto finanziario.
- Il Listing Partner è il soggetto incaricato dalla società per l'accesso alla quotazione sul

---

efficace monitoraggio del rischio. In particolare, lo sponsor attesta che l'emittente dispone di una adeguata politica di gestione dei conflitti di interessi. Tale attestazione non è richiesta nel caso in cui l'emittente sia un intermediario finanziario sottoposto a vigilanza prudenziale. Lo sponsor attesta altresì che la professionalità, l'esperienza e la reputazione dei soggetti titolari di deleghe di gestione sono adeguate.

8. Nel caso di ammissione alla quotazione di azioni di SIV lo sponsor attesta che l'emittente dispone di una adeguata politica di gestione dei conflitti di interessi. Lo sponsor attesta altresì che la professionalità, l'esperienza e la reputazione dei soggetti titolari di deleghe di gestione sono adeguate.
9. Nel caso di ammissione alla quotazione di azioni rappresentative del capitale di un emittente che abbia deliberato un'operazione di fusione per incorporazione di una società quotata (incorporata) in società non quotata (incorporante), qualora l'incorporante non abbia altre significative attività oltre alla partecipazione nell'incorporata e presenti debito finanziario, non è richiesta la dichiarazione di cui al precedente comma 2, lettera c). La disciplina di cui al presente comma si applica anche nel caso in cui sia prevista, successivamente al perfezionamento della fusione, la distribuzione di riserve, da finanziarsi mediante ricorso ad indebitamento finanziario.
10. Nel caso di ammissione alla quotazione di azioni rappresentative del capitale di un emittente che abbia deliberato un'operazione di fusione per incorporazione di una società quotata (incorporata) in società non quotata (incorporante), qualora l'incorporante non abbia altre significative attività oltre alla partecipazione nell'incorporata e non presenti debito finanziario, non sono richieste le dichiarazioni di cui al precedente comma 2, lettere c) e d). La disciplina di cui al presente comma non si applica nel caso in cui sulla società quotata incorporata, in funzione o per effetto dell'operazione di fusione, gravino garanzie ovvero impegni o vincoli contrattuali idonei, anche in via potenziale, ad incidere in maniera rilevante sulla struttura finanziaria della stessa.
11. Nel caso di ammissione alla quotazione degli strumenti finanziari di cui all'articolo 2.1.1, comma 1, lettera a), diversi dalle azioni di Investment Companies, di Real Estate Investment Companies e di SIV, per i quali sia stata presentata la domanda di cui all'articolo 2.2.3 comma 1, gli obblighi di cui al comma 3 sono a carico dello specialista ai sensi dell'articolo 2.3.5.
12. Per gli strumenti finanziari emessi da Borsa Italiana ai fini del presente articolo i riferimenti a Borsa Italiana devono essere intesi come riferiti a Consob e i riferimenti all'emittente come riferiti a Borsa Italiana, per quanto applicabile".

[76] www.borsaitaliana.it/investorrelator.

mercato Expandi[77], con il compito di curare il collocamento delle azioni e verificare la sussistenza dei criteri di selezione, divenendo il riferimento per il processo di quotazione. Possono svolgere tale funzione, a norma del Regolamento di Borsa, banche, imprese di investimento nazionali, comunitarie ed extracomunitarie ed intermediari finanziari iscritti nell'elenco di cui all'articolo 107 del D. Lgs.1 settembre 1993, n. 385 TUB[78].

- La Società di Revisione è responsabile della certificazione dei bilanci della società al fine del collocamento degli strumenti finanziari dell'Emittente, per il rilascio delle comfort letters[79] relativamente al prospetto informativo e per le relazioni sul bilancio d'esercizio.
- I consulenti legali e fiscali hanno la funzione di assistere la società quotanda, nonché i soci e gli intermediari nel corso dello svolgimento del processo di quotazione, curandone i profili legali, fiscali e di contrattualistica. I consulenti dell'Emittente, in particolare, si occupano di "fornire assistenza nell'ambito dell'attività di due diligence legale e fiscale svolta sulla società preliminarmente all'accesso alla quotazione ed in generale nell'ambito delle problematiche legali e fiscali connesse all'operazione, di predisporre e redigere il prospetto informativo e la documentazione necessaria per la

---

[77] Il mercato Expandi nasce nel 2004, ospita imprese di minore dimensione. È un mercato destinato alle negoziazioni dei titoli non in possesso dei requisiti per l'ammissione alla quotazione di borsa. I principali requisiti di ammissione al mercato Expandi sono:
- capitalizzazione minima pari a un milione di euro;
- flottante minimo pari al dieci per cento (con controvalore minimo di 750mila euro);
- presenza di almeno due bilanci di cui l'ultimo certificato;
- possesso di adeguati indicatori economico-finanziari negli ultimi due esercizi.

[78] 1. La Banca d'Italia autorizza gli intermediari finanziari ad esercitare la propria attività al ricorrere delle seguenti condizioni: a) sia adottata la forma di società per azioni, in accomandita per azioni, a responsabilità limitata e cooperativa; b) la sede legale e la direzione generale siano situate nel territorio della Repubblica; c) il capitale versato sia di ammontare non inferiore a quello determinato dalla Banca d'Italia anche in relazione al tipo di operatività; d) venga presentato un programma concernente l'attività iniziale e la struttura organizzativa, unitamente all'atto costitutivo e allo statuto; e) sussistano i presupposti per il rilascio dell'autorizzazione prevista dall'articolo 19 per i titolari delle partecipazioni ivi indicate; e-bis) i soggetti che svolgono funzioni di amministrazione, direzione e controllo siano idonei, secondo quanto previsto ai sensi dell'articolo 110; f) non sussistano, tra gli intermediari finanziari o i soggetti del gruppo di appartenenza e altri soggetti, stretti legami che ostacolino l'effettivo esercizio delle funzioni di vigilanza; g) l'oggetto sociale sia limitato alle sole attività di cui ai commi 1 e 2 dell'articolo 106.
2. La Banca d'Italia nega l'autorizzazione quando dalla verifica delle condizioni indicate nel comma 1 non risulti garantita la sana e prudente gestione.
3. La Banca d'Italia disciplina la procedura di autorizzazione, i casi di revoca, nonché di decadenza, quando l'intermediario autorizzato non abbia iniziato l'esercizio dell'attività, e detta disposizioni attuative del presente articolo.

[79] Con il termine comfort letter si intende una certificazione che ha ad oggetto la revisione dei conti, dichiarazioni e rapporti usati in un prospetto, redatta da un revisore esterno e consegnata alla società che ne ha fatto richiesta.

richiesta di ammissione e l'offerta, di fornire assistenza nei rapporti con Consob e Borsa Italiana"[80]. Accanto ai consulenti della società quotanda si affiancano i consulenti del global coordinator, dello sponsor e del listing partner, che si occupano dello svolgimento della due diligence legale e fiscale sulla società e di assistere l'intermediario in ogni problematica legale e fiscale e nei rapporti con Borsa Italiana e Consob.

- La Società di Comunicazione ha il compito di organizzare tutte le comunicazioni obbligatorie e facoltative nella fase antecedente la quotazione, di conseguenza è responsabile dell'accoglienza del titolo da parte degli investitori tramite una efficace campagna pubblicitaria e di immagine. L'attività di gestione delle informazioni prosegue anche nella fase successiva alla quotazione con la cura e la gestione da parte della società di comunicazione del flusso di informazioni con la comunità finanziaria e con gli investitori.

2.4 Le fasi

Il processo di quotazione si svolge attraverso una serie di fasi che vedono protagonisti la società quotanda e i diversi soggetti di consulenza e intermediazione elencati prima, soggetti che sono chiamati a svolgere un preciso ruolo e ad effettuare una serie articolata di adempimenti.

Le predette fasi possono essere così schematizzate:

1 fase antecedente all'IPO ("Initial Public Offering"[81]).

2 fase IPO.

3 fase successiva all'IPO.

---

[80] www.economiauniparthenope.it/icostidellaquotazione.

[81] Un'offerta pubblica iniziale (dall'inglese *initial public offering*) è un'offerta al pubblico dei titoli di una società che intende quotarsi per la prima volta su un mercato regolamentato. L'impresa che promuove un'IPO può scegliere fra le seguenti modalità per offrire sul mercato una quota del proprio capitale azionario:
- offerta pubblica di sottoscrizione (OPS), ovvero la possibilità data agli investitori di sottoscrivere azioni di nuova emissione;
- offerta pubblica di vendita (OPV), ovvero l'alienazione di azioni già esistenti e possedute dagli attuali azionisti;
- offerta pubblica di vendita e di sottoscrizione (OPVS), ovvero lo sfruttamento congiunto delle due modalità precedenti.

3
Fase antecedente all'IPO

La prima fase, definita antecedente all'IPO, comprende tutti quegli adempimenti che precedono l'ammissione alla quotazione, e che consistono da un lato nei presupposti e requisiti che, secondo la normativa, debbono possedere le società ai fini dell'accesso alla quotazione nei diversi mercati e segmenti, dall'altro in quegli interventi e procedure necessari a garantire il soddisfacimento dei predetti requisiti.

3.1 Presupposti e requisiti generali per la quotazione nel MTA

La definizione dei presupposti e requisiti per l'accesso alla quotazione è affidata al Regolamento di Borsa Italiana e alla normativa in esso richiamata.

I mercati gestiti da Borsa Italiana consentono alla società di scegliere, in relazione alle proprie caratteristiche, il mercato più adatto a soddisfare le esigenze e gli obiettivi che la stessa si pone.

In particolare verranno analizzati i requisiti necessari per la quotazione nel Mercato Telematico Azionario (MTA) che è il più rilevante dal punto di vista del movimento di capitali e importanza dei soggetti, segmenti Standard, Blue Chip e Star, il Mercato Alternativo del Capitale (AIM), dedicato alle piccole-medie imprese con alto potenziale di crescita e i Sistemi Multilaterali di Negoziazione in generale.

Il Regolamento di Borsa stabilisce, in primo luogo, al Titolo 2.1, art. 2.1.3[82], che per l'accesso alla quotazione sui mercati regolamentati segmenti Standard e Blue Chip, nonché Star, siano rispettate una serie di condizioni generali per l'ammissione.

---

[82] Art. 2.1.3: "1. Le società e gli enti emittenti devono essere regolarmente costituiti e i loro statuti devono essere conformi alle leggi e ai regolamenti ai quali le società e gli enti stessi sono soggetti.
2. Gli strumenti finanziari devono essere:
   a) emessi nel rispetto delle leggi, dei regolamenti e di ogni altra disposizione applicabile;
   b) conformi alle leggi ed ai regolamenti ai quali sono sottoposti;
   c) liberamente negoziabili. Gli strumenti finanziari il cui trasferimento sia soggetto a restrizioni sono considerati liberamente negoziabili qualora la restrizione non comporti alcun rischio di perturbare il mercato;
   d) idonei ad essere oggetto di liquidazione mediante il servizio di liquidazione di cui all'articolo 69 del Testo Unico della Finanza ovvero, ove stabilito dalle disposizioni applicabili ai singoli comparti, attraverso omologhi servizi esteri sottoposti a vigilanza dalle autorità competenti dello Stato di appartenenza;
   e) idonei ad essere negoziati in modo equo, ordinato ed efficiente".

Tali condizioni riguardano, da un primo punto di analisi, la società emittente con la costituzione e lo statuto (comma 1), sotto un secondo profilo, gli strumenti finanziari emessi (comma 2).

Quindi, per quanto attiene al primo comma, la regolare costituzione della società avviene a norma dell'art. 2247 c.c. che recita "Con il contratto di società[83] due o più persone conferiscono beni o servizi per l'esercizio in comune di un'attività economica allo scopo di dividerne gli utili", tuttavia va evidenziato che per le società a responsabilità limitata e per le società per azioni vi può essere la costituzione per atto unilaterale di un unico socio fondatore secondo il dettato dell'art. 2328[84] c.c.

In questo secondo caso "la formazione dell'atto costitutivo non è da sola sufficiente a porre in essere la società, occorre altresì che si realizzi quella condizione di efficacia dell'atto costitutivo di società per azioni, che è l'iscrizione di questa nel registro delle imprese"[85].

Lo statuto è quell'atto che "regola la vita interna ed il funzionamento della società"[86], rispettando le norme del Codice Civile, inoltre "anche se forma oggetto di atto separato, costituisce parte integrante dell'atto costitutivo" secondo il dettato dell'art. 2328 co. 3 c.c.

---

[83] Si tratta di un negozio consensuale utilizzato dall'imprenditore al fine di organizzare l'attività d'impresa, rappresenta una forma professionale di esercizio collettivo dell'attività economica, indirizzata alla produzione ed alla divisione di utili, nel rispetto del criterio di economicità e dell'art. 2082 che recita "È imprenditore chi esercita professionalmente un'attività economica organizzata al fine della produzione o dello scambio di beni o di servizi.

[84] "La società può essere costituita per contratto o per atto unilaterale.
L'atto costitutivo deve essere redatto per atto pubblico e deve indicare:
1) il cognome e il nome o la denominazione, la data e il luogo di nascita o lo Stato di costituzione, il domicilio o la sede, la cittadinanza dei soci e degli eventuali promotori, nonché il numero delle azioni assegnate a ciascuno di essi;
2) la denominazione e il comune ove sono poste la sede della società e le eventuali sedi secondarie;
3) l'attività che costituisce l'oggetto sociale;
4) l'ammontare del capitale sottoscritto e di quello versato;
5) il numero e l'eventuale valore nominale delle azioni, le loro caratteristiche e le modalità di emissione e circolazione;
6) il valore attribuito ai crediti e beni conferiti in natura;
7) le norme secondo le quali gli utili devono essere ripartiti;
8) i benefici eventualmente accordati ai promotori o ai soci fondatori;
9) il sistema di amministrazione adottato, il numero degli amministratori e i loro poteri, indicando quali tra essi hanno la rappresentanza della società;
10) il numero dei componenti il collegio sindacale;
11) la nomina dei primi amministratori e sindaci ovvero dei componenti del consiglio di sorveglianza e, quando previsto, del soggetto al quale è demandato il controllo contabile;
12) l'importo globale, almeno approssimativo, delle spese per la costituzione poste a carico della società;
13) la durata della società ovvero, se la società è costituita a tempo indeterminato, il periodo di tempo, comunque non superiore ad un anno, decorso il quale il socio potrà recedere.
Lo statuto contenente le norme relative al funzionamento della società, anche se forma oggetto di atto separato, costituisce parte integrante dell'atto costitutivo. In caso di contrasto tra le clausole dell'atto costitutivo e quelle dello statuto prevalgono le seconde".

[85] Francesco Galgano, *Diritto Commerciale*, *Le società*, Bologna, Zanichelli, 2012, XVIII Edizione, pag. 171.

[86] www.misterfisco.it/statutosocietà.

In caso di contrasto tra le clausole dell'atto costitutivo e quelle dello statuto, prevalgono le seconde. Analizzando ora il secondo comma, con riferimento agli strumenti finanziari[87], questi devono essere:

a) emessi nel rispetto delle leggi, dei regolamenti e di ogni altra disposizione applicabile, il riferimento in questo caso è all'emissione, cioè all'operazione con cui si da inizio alla circolazione dei titoli;
b) conformi alle leggi ed ai regolamenti ai quali sono sottoposti, cioè modellati sulla base di quanto disposto;
c) liberamente trasferibili, quindi non necessitano di particolari autorizzazioni e non soggiacciono a limitazioni per l'alienazione;
d) idonei ad essere oggetto di liquidazione mediante l'apposito servizio di liquidazione, cioè rimborsabili.

---

[87] Art. 1 co. 2 d.lgs. 58/1998 "Per "strumenti finanziari" si intendono:
a) valori mobiliari;
b) strumenti del mercato monetario;
c) quote di un organismo di investimento collettivo del risparmio;
d) contratti di opzione, contratti finanziari a termine standardizzati («future»), «swap», accordi per scambi futuri di tassi di interesse e altri contratti derivati connessi a valori mobiliari, valute, tassi di interesse o rendimenti, o ad altri strumenti derivati, indici finanziari o misure finanziarie che possono essere regolati con consegna fisica del sottostante o attraverso il pagamento di differenziali in contanti;
e) contratti di opzione, contratti finanziari a termine standardizzati («future»), «swap», accordi per scambi futuri di tassi di interesse e altri contratti derivati connessi a merci il cui regolamento avviene attraverso il pagamento di differenziali in contanti o può avvenire in tal modo a discrezione di una delle parti, con esclusione dei casi in cui tale facoltà consegue a inadempimento o ad altro evento che determina la risoluzione del contratto;
f) contratti di opzione, contratti finanziari a termine standardizzati («future»), «swap» e altri contratti derivati connessi a merci il cui regolamento può avvenire attraverso la consegna del sottostante e che sono negoziati su un mercato regolamentato e/o in un sistema multilaterale di negoziazione;
g) contratti di opzione, contratti finanziari a termine standardizzati («future»), «swap», contratti a termine («forward») e altri contratti derivati connessi a merci il cui regolamento può avvenire attraverso la consegna fisica del sottostante, diversi da quelli indicati alla lettera f), che non hanno scopi commerciali, e aventi le caratteristiche di altri strumenti finanziari derivati, considerando, tra l'altro, se sono compensati ed eseguiti attraverso stanze di compensazione riconosciute o se sono soggetti a regolari richiami di margini;
h) strumenti derivati per il trasferimento del rischio di credito;
i) contratti finanziari differenziali;
j) contratti di opzione, contratti finanziari a termine standardizzati («future»), «swap», contratti a termine sui tassi d' interesse e altri contratti derivati connessi a variabili climatiche, tariffe di trasporto, quote di emissione, tassi di inflazione o altre statistiche economiche ufficiali, il cui regolamento avviene attraverso il pagamento di differenziali in contanti o può avvenire in tal modo a discrezione di una delle parti, con esclusione dei casi in cui tale facoltà consegue a inadempimento o ad altro evento che determina la risoluzione del contratto, nonché altri contratti derivati connessi a beni, diritti, obblighi, indici e misure, diversi da quelli indicati alle lettere precedenti, aventi le caratteristiche di altri strumenti finanziari derivati, considerando, tra l'altro, se sono negoziati su un mercato regolamentato o in un sistema multilaterale di negoziazione, se sono compensati ed eseguiti attraverso stanze di compensazione riconosciute o se sono soggetti a regolari richiami di margini".

3.2 Requisiti specifici per l'ammissione al segmento *Standard/Blue Chips*

Il Regolamento Borsa, al Titolo 2.2, si occupa poi di disciplinare le condizioni specifiche richieste per l'ammissione alla quotazione sui mercati predetti, che possono così sintetizzarsi:

1) Per quanto riguarda l'emittente, l'art. 2.2.1[88] del Regolamento di Borsa richiede, in linea

[88] Articolo 2.2.1: "1. Possono essere ammesse alla quotazione le azioni rappresentative del capitale di emittenti che abbiano pubblicato e depositato, conformemente al diritto nazionale, i bilanci anche consolidati degli ultimi tre esercizi annuali, di cui almeno l'ultimo corredato di un giudizio della società di revisione redatto secondo le modalità di cui all'articolo 156 del Testo Unico della Finanza o della corrispondente disciplina di diritto estero applicabile. L'ammissione alla quotazione non può essere disposta se la società di revisione ha espresso un giudizio negativo ovvero si è dichiarata impossibilitata a esprimere un giudizio.

2. Le società risultanti da operazioni straordinarie o che abbiano subito, nel corso dell'esercizio precedente a quello di presentazione della domanda o successivamente, modifiche sostanziali nella loro struttura patrimoniale devono produrre, a completamento di quanto previsto dal comma 1: - il conto economico pro-forma relativo ad almeno un esercizio annuale chiuso precedentemente alla data di presentazione della domanda di ammissione; - lo stato patrimoniale pro-forma riferito alla data di chiusura dell'esercizio precedente la domanda di ammissione qualora le operazioni straordinarie o le modifiche sostanziali siano avvenute successivamente a tale data; - gli ulteriori documenti pro-forma infrannuali specificati nelle Istruzioni. Qualora dalla redazione dei documenti pro-forma di cui al presente comma possa derivare l'inattendibilità oggettiva dei dati contabili contenuti negli stessi, Borsa Italiana, su richiesta motivata dell'emittente, si riserva di accettare ricostruzioni contabili storiche diverse.
3. I documenti contabili di cui al comma 2 devono essere accompagnati dalla relazione della società di revisione contenente il giudizio sulla ragionevolezza delle ipotesi di base per la redazione dei dati pro-forma, sulla corretta applicazione della metodologia utilizzata nonché sulla correttezza dei principi contabili adottati per la redazione dei medesimi atti. Analoga relazione deve essere rilasciata dalla società di revisione sulle ricostruzioni contabili storiche diverse dai dati pro-forma; eventuali limitazioni o impedimenti all'espressione del giudizio dovranno essere motivati.
4. I bilanci annuali di esercizio e consolidati e le situazioni contabili annuali che costituiscono la base dei dati pro-forma di cui al comma 2 devono essere assoggettati, per una parte largamente preponderante, a revisione contabile completa. In caso di impossibilità oggettiva, Borsa Italiana si riserva, su richiesta motivata dell'emittente, di accettare che solo una parte preponderante dei dati sia assoggettata a revisione contabile completa.
5. In via eccezionale, in deroga al comma 1, può essere accettato un numero inferiore di bilanci eventualmente integrati dalla documentazione di cui al comma 2 corredata da quanto previsto ai commi 3 e 4, ovvero, nel caso di emittenti che non abbiano mai pubblicato e depositato un bilancio annuale i documenti di cui ai commi 2, 3 e 4. Tale deroga deve in ogni caso rispondere agli interessi dell'emittente e degli investitori e questi ultimi devono disporre di tutte le informazioni necessarie per una valutazione dell'emittente e degli strumenti per i quali è richiesta l'ammissione.
6. La società emittente e le principali società del gruppo ad essa facente capo devono adottare un Sistema di controllo di gestione tale da consentire ai responsabili di disporre periodicamente e con tempestività di un quadro sufficientemente esaustivo della situazione economica e finanziaria della società e delle principali società del gruppo a essa facente eventualmente capo e tale da consentire in modo corretto:
   - il monitoraggio dei principali key performance indicator e dei fattori di rischio che attengono alla società e alle principali società del gruppo ad essa facente eventualmente capo;
   - la produzione dei dati e delle informazioni con particolare riguardo all'informazione finanziaria, secondo dimensioni di analisi adeguate alla tipologia di business, alla complessità organizzativa e alle specificità del fabbisogno informativo del management;
   - l'elaborazione dei dati finanziari prospettici del piano industriale e del budget nonché la verifica del raggiungimento degli obiettivi aziendali mediante un'analisi degli scostamenti A tal fine l'emittente redige un Memorandum, approvato dal proprio organo amministrativo, nel quale descrive il Sistema di controllo di gestione adottato dall'emittente e dalle principali società del gruppo ad esso facente capo. Il Memorandum deve descrivere in modo sintetico ma esaustivo, i componenti del sistema, i soggetti responsabili, i contenuti informativi con particolare riguardo agli indicatori utilizzati per il monitoraggio dei principali key performance indicator e fattori di rischio aziendale. Il Memorandum dovrà altresì indicare le eventuali aree

generale e salvo specificazioni ed eccezioni contenute nello stesso articolo, che l'emittente abbia provveduto alla pubblicazione ed al deposito dei bilanci, anche consolidati, degli ultimi tre esercizi annuali, di cui l'ultimo corredato da apposito giudizio della società di revisione[89], che, ai fini dell'ammissione alla quotazione, dovrà risultare positivo, poiché in caso di esito negativo o senza giudizio l'ammissione non verrà disposta.

2) Sotto il profilo dei requisiti degli strumenti finanziari oggetto della richiesta di

---

di criticità del Sistema presenti al momento della presentazione della domanda; l'emittente dovrà precisare in quale delle casistiche previste da Borsa Italiana nelle Istruzioni ricadano tali criticità.

7. L'emittente deve esercitare, direttamente o attraverso le proprie controllate e in condizioni di autonomia gestionale, una attività capace di generare ricavi. Borsa Italiana nel valutare la sussistenza delle condizioni di autonomia gestionale verifica che non vi siano ostacoli alla massimizzazione degli obiettivi economico-finanziari propri dell'emittente. Qualora Borsa Italiana ravvisi elementi potenzialmente idonei a ostacolare il conseguimento dell'autonomia gestionale, richiede che sia data al pubblico adeguata informativa all'atto dell'ammissione a quotazione ed eventualmente in via continuativa. Per le società controllate sottoposte all'attività di direzione e coordinamento di un'altra società non devono sussistere le condizioni che inibiscono la quotazione di cui all'articolo 37 del regolamento Consob 16191/2007 e successive modifiche e integrazioni. L'attivo di bilancio ovvero i ricavi dell'emittente non devono essere rappresentati in misura preponderante dall'investimento o dai risultati dell'investimento in una società le cui azioni sono ammesse alle negoziazioni in un mercato regolamentato.
8. Le società controllanti società costituite e regolate dalla legge di Stati non appartenenti all'Unione Europea devono rispettare le condizioni per la quotazione di cui all'articolo 36 del regolamento Consob 16191/2007 e successive modifiche e integrazioni.
9. Le società finanziarie il cui patrimonio è costituito esclusivamente da partecipazioni devono rispettare le condizioni di cui all'articolo 38 del regolamento Consob 16191/2007 e successive modifiche e integrazioni.
10. Fermo quanto previsto dai commi precedenti, le azioni delle banche popolari e delle società cooperative autorizzate all'esercizio dell'assicurazione possono essere ammesse a condizione che nello statuto dell'emittente: - sia previsto che le emissioni ordinarie di nuove azioni siano riservate all'ingresso di nuovi soci e si realizzino con l'assegnazione di una sola azione; - il periodo minimo di iscrizione richiesto per il riconoscimento del diritto di voto nelle assemblee non sia superiore a 90 giorni.
11. Le azioni delle società cooperative possono essere ammesse a condizione che: - l'atto costitutivo dell'emittente e/o la delibera di emissione delle azioni contenga specifiche previsioni atte a garantire la libera trasferibilità delle azioni emesse; - le previsioni dell'atto costitutivo dell'emittente e/o della delibera di emissione delle azioni siano conformi alle specifiche condizioni previste dalle disposizioni di legge in materia.
12. I requisiti di cui ai commi precedenti non si applicano per l'ammissione di azioni dello stesso emittente di categoria diversa rispetto a quelle già quotate.
13. L'emittente deve aver conferito l'incarico di revisione contabile dei bilanci a una società di revisione ai sensi dell'articolo 159 del Testo Unico della Finanza, salvo quanto previsto dalla corrispondente disciplina di diritto estero applicabile.
14. Nel caso in cui l'emittente sia stato oggetto di rating sul merito di credito da parte di un'agenzia di rating indipendente locale o internazionale nei 12 mesi antecedenti la domanda di ammissione, tale rating o il relativo aggiornamento, se pubblici, dovranno essere comunicati a Borsa Italiana. Tale informazione sarà diffusa al mercato nell'avviso in cui si stabilisce la data di inizio delle negoziazioni.
15. Per gli strumenti finanziari emessi da Borsa Italiana i requisiti di cui al presente articolo sono verificati dalla Consob.
16. Nel disporre l'ammissione alle negoziazioni di azioni ordinarie di emittenti le cui azioni ordinarie siano già ammesse su altri mercati regolamentati europei o extracomunitari, Borsa Italiana può derogare a quanto previsto dai commi precedenti anche tenuto conto, a titolo esemplificativo e non esaustivo, dell'appartenenza a primari indici finanziari internazionali o nazionali, della dimensione dell'emittente e del periodo di tempo da cui è ammesso alle negoziazioni".

[89] Sulla quale vedasi cap. 2 par. 3.

quotazione, con riferimento in particolare alle azioni, cioè, lo strumento più diffuso e accessibile, l'art. 2.2.2[90] richiede:

- una capitalizzazione di mercato prevedibile pari ad almeno quaranta milioni di euro;
- una sufficiente diffusione delle azioni, che si presume realizzata con la ripartizione delle azioni stesse fra il pubblico per almeno il 25% del capitale rappresentato dalla categoria di appartenenza.

Si denota, che per l'accesso al suddetto mercato è necessaria la nomina dello sponsor[91], secondo il dettato dell'art. 2.3.1, in quanto le azioni ricadono nella domanda di ammissione di strumenti finanziari di cui all'articolo 2.1.1, comma 1, lettera a.

---

[90] Articolo 2.2.2: "1. Ai fini dell'ammissione alla quotazione, le azioni devono avere i seguenti requisiti:
a) capitalizzazione di mercato prevedibile pari almeno a quaranta milioni di euro; Borsa Italiana può ammettere azioni con una capitalizzazione inferiore qualora ritenga che per tali azioni si formerà un mercato sufficiente;
b) sufficiente diffusione, che si presume realizzata quando le azioni siano ripartite presso gli investitori professionali oltre che presso gli investitori non professionali per almeno il 25% del capitale rappresentato dalla categoria di appartenenza; Borsa Italiana può, peraltro, ritenere sussistente tale requisito quando il valore di mercato delle azioni possedute dal pubblico faccia ritenere che le esigenze di regolare funzionamento del mercato possano essere soddisfatte anche con una percentuale inferiore a quella sopraindicata. Nel computo della percentuale:
1) non si tiene conto delle partecipazioni azionarie di controllo, di quelle vincolate da patti parasociali e di quelle soggette a vincoli alla trasferibilità delle azioni (lock-up) di durata superiore ai sei mesi;
2) non si tiene conto delle partecipazioni azionarie superiori al due per cento, salvo che Borsa Italiana, su istanza motivata dell'emittente, valutate la tipologia dell'investitore e le finalità del possesso, non accordi una deroga al riguardo. Il calcolo delle partecipazioni deve essere effettuato secondo i criteri indicati all'articolo 118 del Regolamento Consob 11971/99;
3) si tiene sempre conto di quelle possedute da organismi di investimento collettivo del risparmio, da fondi pensione e da enti previdenziali. Ai soli fini di tale disposizione, si ha riguardo anche agli OICR di diritto estero non autorizzati alla commercializzazione in Italia.
2. Borsa Italiana si riserva di ritenere adeguata la ripartizione presso i soli investitori professionali se il valore di mercato delle azioni possedute dagli investitori oppure il numero degli stessi faccia ritenere che le esigenze di regolare funzionamento del mercato possano essere comunque soddisfatte.
3. Nel disporre l'ammissione alle negoziazioni di azioni ordinarie di emittenti le cui azioni ordinarie siano già ammesse ovvero siano contestualmente ammesse alle negoziazioni in un mercato regolamentato europeo o extracomunitario o derivino da una scissione, fusione mediante costituzione di nuova società o altre operazioni assimilabili alle precedenti che coinvolgano società quotate in un mercato regolamentato, Borsa Italiana può derogare a quanto previsto dal precedente comma 1, lettera b). Tale deroga può essere accordata tenuto conto della diffusione delle azioni ordinarie.
4. Per le azioni di nuova emissione di pari categoria e medesime caratteristiche, ad eccezione del godimento, rispetto a quelle già quotate, non si applicano le previsioni di cui al precedente comma 1. Borsa Italiana potrà disporne l'ammissione a quotazione con separata linea, avuto riguardo all'entità e alla diffusione delle azioni emesse, nonché alla prevista durata di esistenza della separata linea.
5. Ad eccezione dei titoli azionari delle banche popolari e delle società cooperative autorizzate all'esercizio dell'assicurazione, non possono essere ammesse categorie di azioni prive del diritto di voto nelle assemblee ordinarie, se azioni dotate di tale diritto non sono già quotate ovvero non sono oggetto di contestuale provvedimento di ammissione a quotazione.
6. Le disposizioni di cui al comma 1, lettera b), del presente articolo non si applicano alle azioni di risparmio, per le quali la sufficiente diffusione dovrà essere tale da assicurare un regolare funzionamento del mercato.
7. Per gli strumenti finanziari emessi da Borsa Italiana i requisiti di cui al presente articolo sono verificati dalla Consob".

[91] Sul quale vedasi cap. 2, par. 3.

3.3 Requisiti specifici per il Segmento Star

Ad integrazione di quanto precedentemente indicato, il Regolamento di Borsa individua ulteriori requisiti che devono essere rispettati al fine dell'ammissione alle negoziazioni sul segmento Star in aggiunta a quelli previsti per il segmento Blue Chip/ Standard.

La quotazione sul segmento Star, infatti, consente alla società di beneficiare di una maggiore presenza di investitori istituzionali[92] e di una maggiore liquidità del titolo[93], di contro, l'accesso a tale segmento richiede una particolare attenzione da parte della società quotanda ai profili di trasparenza e governance, onde poter soddisfare i predetti requisiti.

L'art. 2.2.3[94] del Regolamento di Borsa detta infatti precise disposizioni in merito, prevedendo requisiti più stringenti per gli emittenti e per le azioni, e soprattutto precisi obblighi in materia di corporate governance.

---

92 Glossario Borsa Italiana, "alla categoria degli investitori istituzionali appartengono:
- gli organismi di investimento collettivo del risparmio (OICR), i fondi comuni di investimento mobiliari, immobiliari, speculativi e le Sicav;
- i fondi pensione;
- le compagnie di assicurazione.

L'attività svolta dall'investitore istituzionale può derivare da un mandato specifico, pertanto l'investimento avviene su base collettiva, come negli OICR e nei fondi pensione, oppure può derivare dall'intermediazione in senso stretto, come nel caso delle compagnie di assicurazione relativamente alle polizze vita".

93 Glossario Borsa Italiana, "l'attività più liquida è la moneta. Le altre attività (beni immobili, strumenti finanziari, depositi bancari) hanno ciascuna un grado di liquidità differente. Un'attività è tanto più liquida quanto minori sono i costi di transazione, la perdita di capitale che la conversione può comportare ed i tempi necessari per la conversione stessa.
Diversi sono i fattori che incidono sulla liquidità di uno strumento finanziario. Innanzi tutto, requisito necessario per la liquidità è la negoziabilità di uno strumento finanziario, a sua volta influenzata dalla trasferibilità dello stesso e quindi dalla sua circolazione nel mercato secondario successivamente all'emissione nel mercato primario, dalla standardizzazione e divisibilità del titolo, in modo da garantire il massimo accesso da parte degli investitori (un mercato è tanto più liquido quanto maggiore è il volume delle contrattazioni), e dal fatto che lo strumento sia quotato. La liquidità dipende anche dalla vita residua dello strumento finanziario (un titolo è tanto più liquido quanto più vicina è la sua scadenza) e dalla credibilità dell'emittente. Sotto quest'ultimo punto di vista il rischio emittente, legato proprio alla solvibilità dell'emittente, è un fattore di incidenza rilevante sulla liquidità di un titolo, sia esso un titolo di credito, come le azioni, o un titolo di debito, come le obbligazioni.
La liquidità di un'attività ed il rendimento di questa sono inversamente proporzionali: quanto più l'attività è liquida, tanto minore è il rischio che l'investitore non riesca a venderla facilmente. Contribuiscono alla liquidità di uno strumento l'ampiezza, lo spessore e l'elasticità del mercato nel quale esso è trattato".

94 Articolo 2.2.3: "1. All'atto della domanda di ammissione ovvero successivamente alla quotazione, l'emittente può richiedere per le proprie azioni ordinarie la qualifica di Star, secondo le modalità indicate nelle Istruzioni, rispettando le condizioni indicate nei commi seguenti. Borsa Italiana, verificata la sussistenza di tali condizioni, attribuisce la qualifica di Star, con l'Avviso in cui si stabilisce la data di inizio delle negoziazioni ovvero con successivo Avviso.
2. Al fine di ottenere la qualifica di Star, le azioni devono soddisfare i seguenti requisiti:
   a) devono avere una capitalizzazione di mercato, effettiva o prevedibile, non superiore alla soglia stabilita nelle Istruzioni ai sensi dell'articolo 4.1.2, comma 3, del Regolamento;
   b) devono avere una capitalizzazione di mercato, effettiva o prevedibile, non inferiore alla soglia stabilita nelle Istruzioni ai sensi dell'articolo 4.1.2, comma 3, del Regolamento;

c) devono essere diffuse presso gli investitori professionali oltre che presso gli investitori non professionali almeno per la percentuale di capitale stabilita nelle Istruzioni. Nel computo della percentuale si seguono le modalità di cui all'articolo 2.2.2, comma 1, lettera b). Si applica inoltre il comma 2 dell'articolo 2.2.2.

3. Al fine di ottenere e mantenere la qualifica di Star, gli emittenti devono:
   a) rendere disponibile al pubblico il resoconto intermedio di gestione entro 45 giorni dal termine del primo, terzo e quarto trimestre dell'esercizio. Gli emittenti sono esonerati dalla pubblicazione del quarto resoconto se mettono a disposizione del pubblico la relazione finanziaria annuale, unitamente agli altri documenti di cui all'articolo 154-ter, comma primo, del Testo Unico della Finanza entro 90 giorni dalla chiusura dell'esercizio;
   b) avere l'ultimo bilancio d'esercizio annuale corredato di un giudizio positivo della società di revisione;
   c) non avere l'attivo di bilancio ovvero i propri ricavi rappresentati, in misura preponderante, dall'investimento o dai risultati dell'investimento in una società le cui azioni sono ammesse alle negoziazioni in un mercato regolamentato;
   d) rendere disponibile sul proprio sito Internet il bilancio, la relazione semestrale, i resoconti intermedi di gestione, nonché l'informativa di cui all'articolo 114, comma 1, 4 e 5, del Testo Unico della Finanza e gli ulteriori elementi indicati da Borsa Italiana nelle Istruzioni. Le informazioni dovranno essere rese disponibili sul sito secondo il formato indicato da Borsa Italiana, anche in lingua inglese; le comunicazioni al pubblico di cui all'articolo 114, commi 1 e 4 del Testo Unico della Finanza nonché le eventuali integrazioni richieste da Consob ai sensi dell'articolo 114, comma 5 del Testo Unico della Finanza devono essere rese disponibili in lingua inglese contestualmente rispetto alle corrispondenti comunicazioni in italiano;
   e) aver pubblicato, nei termini previsti, i documenti contabili obbligatori sulla base delle disposizioni applicabili e non essere incorsi, nei precedenti 18 mesi, in violazioni di obblighi informativi formalmente accertati;
   f) non essere ammessi a procedure concorsuali e non avere società controllate ai sensi dell'articolo 2359 del codice civile ammesse a procedure concorsuali in misura superiore alla soglia stabilita nelle Istruzioni;
   g) non avere le proprie azioni ordinarie sospese dalle negoziazioni a tempo indeterminato;
   h) non incorrere in una delle situazioni previste dagli articoli 2446 e/o 2447 del codice civile;
   i) aver individuato all'interno della propria struttura organizzativa un soggetto professionalmente qualificato (investor relator) che abbia come incarico specifico la gestione dei rapporti con gli investitori;
   j) aver adottato il modello di organizzazione, gestione e controllo previsto dall'articolo 6 del decreto legislativo 231/2001;
   k) applicare, per quanto riguarda la composizione del consiglio di amministrazione nonché il ruolo e le funzioni degli amministratori non esecutivi e indipendenti, i principi e i criteri applicativi previsti dagli articoli 2 e 3 del Codice di Autodisciplina; Borsa Italiana definisce nelle Istruzioni criteri generali per la valutazione dell'adeguatezza del numero degli amministratori indipendenti. L'entrata in vigore della disciplina è subordinata all'esplicito assenso della Consob;
   l) applicare per quanto riguarda l'istituzione e il funzionamento dei comitati interni al consiglio di amministrazione i principi e i criteri applicativi previsti dall'articolo 5 del Codice di Autodisciplina;
   m) applicare per quanto riguarda la remunerazione degli amministratori i principi e i criteri applicativi previsti dall'articolo 7 del Codice di Autodisciplina;
   n) aver nominato un comitato per il controllo interno in conformità a quanto previsto dal principio 8.P.4. e dal criterio applicativo 8.C.3. del Codice di Autodisciplina;
   o) aver vietato con efficacia cogente ai componenti degli organi di amministrazione e di controllo, nonché ai soggetti che svolgono funzioni di direzione e ai dirigenti ai sensi del regolamento Consob n. 11971/99 (cosiddetto *internal dealing*) l'effettuazione - direttamente o per interposta persona - di operazioni di acquisto, vendita, sottoscrizione o scambio delle azioni o di strumenti finanziari ad esse collegate nei quindici giorni precedenti la riunione consiliare chiamata ad approvare i dati contabili di periodo. Non sono soggetti alle limitazioni gli atti di esercizio di eventuali stock options o di diritti di opzione relativi agli strumenti finanziari e, limitatamente alle azioni derivanti dai piani di stock options, le conseguenti operazioni di cessione purché effettuate contestualmente all'atto di esercizio. Le limitazioni non si applicano nel caso di situazioni eccezionali di necessità soggettiva, adeguatamente motivate dall'interessato nei confronti della società.

In caso di adozione di un sistema di amministrazione e controllo dualistico o monistico, si applicano i principi e i criteri applicativi previsti dall'articolo 12 del Codice di Autodisciplina.

4. La qualifica di Star è subordinata alla nomina di un operatore specialista incaricato di svolgere le funzioni di cui all'articolo 2.3.5 relativamente alle azioni ordinarie. Possono esercitare le funzioni di specialista gli operatori ammessi alle negoziazioni sul mercato. Non possono esercitare l'attività di specialista gli operatori che appartengono al gruppo cui l'emittente fa parte o che fa capo all'emittente. Qualora l'emittente abbia diverse tipologie di strumenti finanziari quotati può procedere alla nomina di un operatore specialista incaricato di svolgere le funzioni di cui all'articolo 2.3.5, comma 1, lettera a) anche relativamente a tali tipologie.
5. In caso di emittenti già quotati, al fine di ottenere la qualifica di Star è richiesto il rispetto del requisito economico indicato nelle Istruzioni.
6. Borsa Italiana, su richiesta motivata dell'emittente, può ritenere soddisfatti i requisiti di cui al comma 3, lettere k) e n), qualora il Consiglio di Amministrazione abbia deliberato di proporre all'Assemblea l'adeguamento a tali requisiti.
7. L'emittente si impegna a comunicare tempestivamente a Borsa Italiana la temporanea impossibilità di rispettare gli obblighi di cui ai commi 3 e 4 e le relative motivazioni.
8. Borsa Italiana può concedere una deroga al rispetto del requisito di presentazione entro 45 giorni del 4o resoconto intermedio di gestione di cui al comma 3, lettera a), in caso di comprovata impossibilità per l'emittente di rispettarlo, dandone comunicazione all'emittente e al pubblico entro quindici giorni dalla richiesta di deroga.
9. Borsa Italiana può richiedere alla società tutte le informazioni rilevanti ai fini della verifica degli obblighi di cui al comma 3.
10. Con la periodicità indicata nelle Istruzioni, Borsa Italiana con apposito Avviso può escludere dalla qualifica di Star le azioni per le quali non siano state rispettate le condizioni di cui ai commi 3 e 4, tenendo conto dell'importanza e della frequenza dei casi nei quali tali condizioni sono venute a mancare. Borsa Italiana può altresì escludere, con la periodicità indicata nelle Istruzioni, dalla qualifica di Star le azioni per le quali siano venute meno le condizioni di cui al comma 3, lettera e), dalla data di ammissione della società nel segmento Star. Con la medesima periodicità, Borsa Italiana può escludere dalla qualifica Star le azioni per le quali il flottante, calcolato secondo le modalità di cui all'articolo 2.2.2, comma 1, lettera b), sia sceso al di sotto della percentuale di capitale stabilita nelle Istruzioni. Dell'esclusione viene data notizia al pubblico.
11. Borsa Italiana verifica il rispetto del requisito di capitalizzazione di cui al comma 2, lettera a), secondo la periodicità indicata all'articolo 4.1.2 e può, con apposito Avviso, escludere dalla qualifica di Star gli strumenti finanziari la cui capitalizzazione sia divenuta superiore alla soglia stabilita, secondo la procedura stabilita all'articolo 4.1.2, salvo che la società chieda di rimanere nel segmento Star secondo quanto previsto nelle Istruzioni.
12. Borsa Italiana, anche in deroga alla periodicità indicata nelle Istruzioni, può escludere, con provvedimento motivato, dalla qualifica di Star le azioni delle società per le quali:
    a) si verifichino condizioni tali da pregiudicare la situazione economico finanziaria e/o patrimoniale dell'emittente o del gruppo ad esso facente capo, ivi incluse le situazioni previste dagli articoli 2446 e/o 2447 del codice civile
    b) quando le azioni sono sospese a tempo indeterminato
    c) sia comunicato al pubblico ai sensi dell'articolo 2.6.14 l'applicazione di provvedimenti di cui all'articolo 2.6.11. Il provvedimento è reso pubblico mediante Avviso di Borsa Italiana.
13. Borsa Italiana, anche in deroga alla periodicità indicata nelle Istruzioni, può escludere, con provvedimento motivato, dalla qualifica di Star le azioni di una società rispetto alla quale risultino essersi verificati fatti che siano in sostanziale contrasto con il pieno rispetto degli elevati standard caratteristici del segmento Star e che possano incidere negativamente sulla reputazione del Segmento. In tal caso, Borsa Italiana, su richiesta da parte della società, può attribuire nuovamente la qualifica di Star alle azioni della società di cui al paragrafo precedente, se è venuta meno la causa sottostante l'esclusione e ferma restando la sussistenza dei requisiti di cui all'articolo 2.2.3 del Regolamento. Tale richiesta può essere presentata anche prima che sia trascorso un anno dall'esclusione.
14. Le disposizioni di cui ai commi precedenti si applicano, nella sostanza, anche alle società di diritto estero. È fatta salva la facoltà di Borsa Italiana di stabilire, per singoli emittenti, tenuto conto degli ordinamenti cui sono assoggettati, modalità e termini diversi e/o ulteriori".

La qualifica di Star può essere richiesta dalla società sia all'atto della domanda di ammissione sia successivamente alla quotazione, secondo il modello di domanda riportato nelle Istruzioni al Regolamento.

Al fine di ottenere e mantenere la qualifica di Star, gli emittenti devono:

1. rendere disponibile al pubblico la relazione trimestrale entro quarantacinque giorni dal termine di ciascun trimestre dell'esercizio, salvo deroga concessa da Borsa Italiana in caso di comprovata impossibilità per l'Emittente;
2. avere l'ultimo bilancio d'esercizio annuale corredato di un giudizio positivo della società di revisione;
3. non avere l'attivo di bilancio ovvero i propri ricavi rappresentati, in misura preponderante, dall'investimento o dai risultati dell'investimento in una società le cui azioni sono ammesse alle negoziazioni in un mercato regolamentato;
4. trasmettere i dati di bilancio, nonché i dati trimestrali e semestrali, una volta approvati dal Consiglio di Amministrazione, a Borsa Italiana e comunicare tempestivamente eventuali modifiche apportate ai dati di bilancio dall'assemblea dei soci;
5. rendere disponibile sul proprio sito Internet il bilancio, la relazione semestrale, la relazione trimestrale, nonché l'informativa diretta a Consob e al pubblico relativa alle informazioni privilegiate, ossia informazioni di carattere preciso concernenti direttamente ed indirettamente gli emittenti che non siano state rese pubbliche e che se rese pubbliche potrebbero influire in modo sensibile sui prezzi degli strumenti finanziari (art. 114, comma 1 e 3[95] ed art. 181[96] del TUF) e gli ulteriori elementi indicati

[95] Art. 114: "1. Fermi gli obblighi di pubblicità previsti da specifiche disposizioni di legge, gli emittenti quotati comunicano al pubblico, senza indugio, le informazioni privilegiate di cui all'articolo 181 che riguardano direttamente detti emittenti e le società controllate. La Consob stabilisce con regolamento le modalità e i termini di comunicazione delle informazioni, ferma restando la necessità di pubblicazione tramite mezzi di informazione su giornali quotidiani nazionali, detta disposizioni per coordinare le funzioni attribuite alla società di gestione del mercato con le proprie e può individuare compiti da affidarle per il corretto svolgimento delle funzioni previste dall'articolo 64, comma 1, lettera b).

2. Gli emittenti quotati impartiscono le disposizioni occorrenti affinché le società controllate forniscano tutte le notizie necessarie per adempiere gli obblighi di comunicazione previsti dalla legge. Le società controllate trasmettono tempestivamente le notizie richieste.

3. Gli emittenti quotati possono, sotto la propria responsabilità, ritardare la comunicazione al pubblico delle informazioni privilegiate, al fine di non pregiudicare i loro legittimi interessi, nelle ipotesi e alle condizioni stabilite dalla Consob con regolamento, sempre che ciò non possa indurre in errore il pubblico su fatti e circostanze essenziali e che gli stessi soggetti siano in grado di garantirne la riservatezza. La Consob, con regolamento, può stabilire che l'emittente informi senza indugio la stessa autorità della decisione di ritardare la divulgazione al pubblico di informazioni privilegiate e può individuare le misure necessarie a garantire che il pubblico sia correttamente informato.

4. Qualora i soggetti indicati al comma 1, o una persona che agisca in loro nome o per loro conto, comunichino nel normale esercizio del lavoro, della professione, della funzione o dell'ufficio le informazioni indicate al comma 1 ad un terzo che non sia soggetto ad un obbligo di riservatezza legale,

regolamentare, statutario o contrattuale, gli stessi soggetti indicati al comma 1, ne danno integrale comunicazione al pubblico, simultaneamente nel caso di divulgazione intenzionale e senza indugio in caso di divulgazione non intenzionale.

5. La Consob può, anche in via generale, richiedere agli emittenti, ai soggetti che li controllano, agli emittenti quotati aventi l'Italia come Stato membro d' origine, ai componenti degli organi di amministrazione e controllo e ai dirigenti, nonché ai soggetti che detengono una partecipazione rilevante ai sensi dell'articolo 120 o che partecipano a un patto previsto dall'articolo 122 che siano resi pubblici, con le modalità da essa stabilite, notizie e documenti necessari per l'informazione del pubblico. In caso di inottemperanza, la Consob provvede direttamente a spese del soggetto inadempiente.
6. Qualora gli emittenti, i soggetti che li controllano e gli emittenti quotati aventi l'Italia come Stato membro d'origine oppongano, con reclamo motivato, che dalla comunicazione al pubblico delle informazioni, richiesta ai sensi del comma 5, possa derivare loro grave danno, gli obblighi di comunicazione sono sospesi. La Consob, entro sette giorni, può escludere anche parzialmente o temporaneamente la comunicazione delle informazioni, sempre che ciò non possa indurre in errore il pubblico su fatti e circostanze essenziali. Trascorso tale termine, il reclamo si intende accolto.
7. I soggetti che svolgono funzioni di amministrazione, di controllo o di direzione in un emittente quotato e i dirigenti che abbiano regolare accesso a informazioni privilegiate indicate al comma 1 e detengano il potere di adottare decisioni di gestione che possono incidere sull'evoluzione e sulle prospettive future dell'emittente quotato, chiunque detenga azioni in misura almeno pari al 10 per cento del capitale sociale, nonché ogni altro soggetto che controlla l'emittente quotato, devono comunicare alla Consob e al pubblico le operazioni, aventi ad oggetto azioni emesse dall'emittente o altri strumenti finanziari ad esse collegati, da loro effettuate, anche per interposta persona. Tale comunicazione deve essere effettuata anche dal coniuge non separato legalmente, dai figli, anche del coniuge, a carico, nonché dai genitori, i parenti e gli affini conviventi dei soggetti sopra indicati, nonché negli altri casi individuati dalla Consob con regolamento, in attuazione della direttiva 2004/72/CE della Commissione, del 29 aprile 2004. La Consob individua con lo stesso regolamento le operazioni, le modalità e i termini delle comunicazioni, le modalità e i termini di diffusione al pubblico delle informazioni, nonché i casi in cui detti obblighi si applicano anche con riferimento alle società in rapporto di controllo con l'emittente nonché ad ogni altro ente nel quale i soggetti sopra indicati svolgono le funzioni previste dal primo periodo del presente comma.
8. I soggetti che producono o diffondono ricerche o valutazioni, con l'esclusione delle società di rating, riguardanti gli strumenti finanziari indicati all'articolo 180, comma 1, lettera a), o gli emittenti di tali strumenti, nonché i soggetti che producono o diffondono altre informazioni che raccomandano o propongono strategie di investimento destinate ai canali di divulgazione o al pubblico, devono presentare l'informazione in modo corretto e comunicare l'esistenza di ogni loro interesse o conflitto di interessi riguardo agli strumenti finanziari cui l'informazione si riferisce.
9. La Consob stabilisce con regolamento:
   a) disposizioni di attuazione del comma 8;
   b) le modalità di pubblicazione delle ricerche e delle informazioni indicate al comma 8 prodotte o diffuse da emittenti quotati o da soggetti abilitati, nonché da soggetti in rapporto di controllo con essi.
10. Fatto salvo il disposto del comma 8, le disposizioni emanate ai sensi del comma 9, lettera a), non si applicano ai giornalisti soggetti a norme di autoregolamentazione equivalenti purché la loro applicazione consenta di conseguire gli stessi effetti. La Consob valuta, preventivamente e in via generale, la sussistenza di dette condizioni.
11. Le istituzioni che diffondono al pubblico dati o statistiche idonei ad influenzare sensibilmente il prezzo degli strumenti finanziari indicati all'articolo 180, comma 1, lettera a), devono divulgare tali informazioni in modo corretto e trasparente.
12. Le disposizioni del presente articolo si applicano anche ai soggetti italiani ed esteri che emettono strumenti finanziari per i quali sia stata presentata una richiesta di ammissione alle negoziazioni nei mercati regolamentati italiani".

[96] Art. 181: "1. Ai fini del presente titolo per informazione privilegiata si intende un'informazione di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari.

2. In relazione ai derivati su merci, per informazione privilegiata si intende un'informazione di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più derivati su merci, che i partecipanti ai mercati su cui tali derivati sono negoziati si aspettano di ricevere secondo prassi di mercato ammesse in tali mercati.

da Borsa Italiana. Le informazioni dovranno essere rese disponibili sul sito secondo quanto indicato da Borsa Italiana, anche in lingua inglese[97];

6. aver pubblicato, nei termini previsti, i documenti contabili obbligatori sulla base delle disposizioni applicabili e non essere incorsi, nei precedenti diciotto mesi, in violazioni di obblighi informativi formalmente accertati;
7. non essere ammessi a procedure concorsuali[98] e non avere società controllate ai sensi dell'art. 2359[99] c.c. ammesse a procedure concorsuali in misura superiore alla soglia stabilita nelle Istruzioni;

---

3. Un'informazione si ritiene di carattere preciso se:
   a) si riferisce ad un complesso di circostanze esistente o che si possa ragionevolmente prevedere che verrà ad esistenza o ad un evento verificatosi o che si possa ragionevolmente prevedere che si verificherà;
   b) è sufficientemente specifica da consentire di trarre conclusioni sul possibile effetto del complesso di circostanze o dell'evento di cui alla lettera a) sui prezzi degli strumenti finanziari.
4. Per informazione che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di strumenti finanziari si intende un'informazione che presumibilmente un investitore ragionevole utilizzerebbe come uno degli elementi su cui fondare le proprie decisioni di investimento.
5. Nel caso delle persone incaricate dell'esecuzione di ordini relativi a strumenti finanziari, per informazione privilegiata si intende anche l'informazione trasmessa da un cliente e concernente gli ordini del cliente in attesa di esecuzione, che ha un carattere preciso e che concerne, direttamente o indirettamente, uno o più emittenti di strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari".

97 L'utilizzo della lingua inglese si è reso necessario per consentire la comprensione di quanto viene pubblicato anche agli investitori stranieri.

98 Le procedure concorsuali sono una serie di procedure nelle quali, preso atto di uno stato di crisi di un'impresa commerciale, connotata da requisiti individuati di volta in volta dal legislatore, viene regolato il rapporto di tale impresa con il complesso dei suoi creditori, alla presenza di almeno un'autorità pubblica e di altri soggetti indicati in modo specifico e diversificato da procedura a procedura. Scopo principale di ognuno dei procedimenti di cui trattasi, comunque, è la drastica riduzione dell'autonomia imprenditoriale, mediante la sottrazione all'imprenditore della disponibilità dei beni, o addirittura dell'impresa stessa, ovvero mediante la nomina di un organo con funzioni di controllo sull'esercizio dell'attività, in vista di una risoluzione della crisi e/o della pari soddisfazione dei creditori dell'azienda interessata.
Il fallimento è la più nota delle procedure concorsuali individuate tutte dalla legislazione speciale ed è disciplinato, in particolare, dal Regio Decreto 16 marzo 1942, n. 267 (cosiddetta *Legge Fallimentare*, in breve "l.fall."), come significativamente modificato, di recente, dal D.Lgs. 9 gennaio 2006, n. 5. La Legge Fallimentare disciplina, altresì, il concordato preventivo (titolo III l.fall.), l'amministrazione controllata (titolo IV l.fall.) e la liquidazione coatta amministrativa (titolo V l.fall.). Per quanto concerne i rapporti tra quest'ultima e il fallimento, l'art. 2 l.fall., dopo aver chiarito che spetta alla legge determinare quali imprese sono soggette alla liquidazione coatta amministrativa, i casi per le quali essa può essere disposta e l'autorità competente a disporla, precisa che le imprese soggette a liquidazione coatta amministrativa non sono soggette al fallimento, a meno che sia la legge stessa a prevedere in senso opposto.

99 Art. 2359: "Sono considerate società controllate:
1) le società in cui un'altra società dispone della maggioranza dei voti esercitabili nell'assemblea ordinaria;
2) le società in cui un'altra società dispone di voti sufficienti per esercitare un'influenza dominante nell'assemblea ordinaria;
3) le società che sono sotto influenza dominante di un'altra società in virtù di particolari vincoli contrattuali con essa.

Ai fini dell'applicazione dei numeri 1) e 2) del primo comma si computano anche i voti spettanti a società controllate, a società fiduciarie e a persona interposta; non si computano i voti spettanti per conto di terzi.
Sono considerate collegate le società sulle quali un'altra società esercita un'influenza notevole. L'influenza si presume quando nell'assemblea ordinaria può essere esercitato almeno un quinto dei voti ovvero un decimo se la società ha azioni quotate in borsa".

8. non avere le proprie azioni ordinarie sospese dalle negoziazioni a tempo indeterminato;
9. non incorrere in una delle situazioni previste dagli artt. 2446[100] e/o 2447[101] c.c. (riduzione del capitale sociale per perdite e riduzione del capitale sociale al di sotto del limite legale);
10. aver individuato all'interno della propria struttura organizzativa un investor relator che abbia come incarico specifico la gestione dei rapporti con gli investitori.

Per quanto concerne i requisiti delle azioni, per quotarsi sul segmento Star è necessaria una capitalizzazione di mercato prevedibile compresa tra quaranta e mille milioni di euro e la collocazione sul mercato del trentacinque per cento del capitale[102].

---

[100] Art. 2446: "Quando risulta che il capitale è diminuito di oltre un terzo in conseguenza di perdite, gli amministratori o il consiglio di gestione, e nel caso di loro inerzia il collegio sindacale ovvero il consiglio di sorveglianza, devono senza indugio convocare l'assemblea per gli opportuni provvedimenti. All'assemblea deve essere sottoposta una relazione sulla situazione patrimoniale della società, con le osservazioni del collegio sindacale o del comitato per il controllo sulla gestione. La relazione e le osservazioni devono restare depositate in copia nella sede della società durante gli otto giorni che precedono l'assemblea, perché i soci possano prenderne visione. Nell'assemblea gli amministratori devono dare conto dei fatti di rilievo avvenuti dopo la redazione della relazione.
Se entro l'esercizio successivo la perdita non risulta diminuita a meno di un terzo, l'assemblea ordinaria o il consiglio di sorveglianza che approva il bilancio di tale esercizio deve ridurre il capitale in proporzione delle perdite accertate. In mancanza gli amministratori e i sindaci o il consiglio di sorveglianza devono chiedere al tribunale che venga disposta la riduzione del capitale in ragione delle perdite risultanti dal bilancio. Il tribunale provvede, sentito il pubblico ministero, con decreto soggetto a reclamo, che deve essere iscritto nel registro delle imprese a cura degli amministratori.
Nel caso in cui le azioni emesse dalla società siano senza valore nominale, lo statuto, una sua modificazione ovvero una deliberazione adottata con le maggioranze previste per l'assemblea straordinaria possono prevedere che la riduzione del capitale di cui al precedente comma sia deliberata dal consiglio di amministrazione. Si applica in tal caso l'articolo 2436".

[101] Art. 2447: "Se, per la perdita di oltre un terzo del capitale, questo si riduce al disotto del minimo stabilito dall'articolo 2327, gli amministratori o il consiglio di gestione e, in caso di loro inerzia, il consiglio di sorveglianza devono senza indugio convocare l'assemblea per deliberare la riduzione del capitale ed il contemporaneo aumento del medesimo ad una cifra non inferiore al detto minimo, o la trasformazione della società".

[102] Il flottante rappresenta la parte del capitale sociale effettivamente in circolazione sul mercato azionario. Nel computo di questa quota non si tiene conto delle partecipazioni azionarie di controllo, di quelle vincolate da patti parasociali e di quelle soggette a vincoli alla trasferibilità (come clausole di lock-up) di durata superiore ai 6 mesi; al contrario, rientrano nel computo le azioni possedute da organismi di investimento collettivo del risparmio, da fondi pensione e da enti previdenziali.
Borsa Italiana S.p.A. richiede alle società specifici requisiti in termini di flottante minimo per l'ammissione a quotazione: si richiede un flottante minimo pari al 25% del capitale per le azioni negoziate nei segmenti di Borsa e del 10% per le azioni negoziate su Expandi. Un'ulteriore soglia è poi prevista per il Segmento Titoli con alti requisiti, lo STAR nel quale confluiscono le aziende a media capitalizzazione, o cosiddette "medium cap" (titoli con capitalizzazione compresa tra quaranta milioni e un miliardo di euro). In tale segmento si obbligano le aziende a quotarsi con un flottante iniziale pari al 35% della capitalizzazione post-quotazione.
Una volta ammessa a quotazione, la società deve mantenere il requisito relativo al flottante; infatti, la carenza di negoziazioni sul proprio titolo può comportare la revoca dell'ammissione a quotazione. Le azioni con un flottante di poco superiore al 25% e caratterizzate da bassi volumi di scambio sono dette titoli sottili.

L'art. 2.2.3 prevede inoltre il potere di vigilanza di Borsa Italiana sulle informazioni fornite dalla società ed il potere di escludere dalla qualifica di Star le azioni per le quali nel semestre precedente non siano state rispettate le condizioni sopra viste, tenendo conto dell'importanza e della frequenza dei casi nei quali tali condizioni sono venute a mancare.

Inoltre, rivestono particolare evidenza gli obblighi in tema di corporate governance. Ossia:

- avere come membri del Consiglio di Amministrazione amministratori non esecutivi indipendenti, in base ai criteri indicati all'art. 2.2.3, comma 3, lett. k del Regolamento di Borsa e dalle relative Istruzioni, il cui numero e autorevolezza siano tali da garantire che il loro giudizio abbia un peso significativo nell'assunzione delle decisioni consiliari;
- avere nominato un comitato per il controllo interno, composto da amministratori non esecutivi, la maggioranza dei quali indipendenti, con le funzioni indicate nel Codice di Autodisciplina delle società quotate[103] (art. 2.2.3, comma 3, lettera l) del Regolamento di Borsa), e, in particolare, con funzioni consultive e propositive nei confronti del Consiglio di amministrazione nelle materie indicate dal Regolamento stesso;
- legare parte significativa della remunerazione degli amministratori esecutivi e degli alti dirigenti al raggiungimento di obiettivi prefissati e/o a risultati economici conseguiti dalla società, oppure nominare un apposito comitato al fine della formulazione di proposte per la remunerazione, secondo quanto disposto dall'art. 2.2.3, comma 3, lettera m) del Regolamento di Borsa.

Per l'ottenimento della qualifica Star è infine necessario nominare, oltre che lo Sponsor, uno Specialist.

[103] Glossario Borsa Italiana, Il Codice di Autodisciplina delle società quotate è stato redatto nel 1999 dal Comitato per la Corporate Governance promosso da Borsa Italiana e contiene raccomandazioni che costituiscono un modello di "best practice" per l'organizzazione ed il funzionamento delle società quotate italiane. Le raccomandazioni del Codice non sono vincolanti, ma le società quotate devono, in conformità alle Istruzioni al Regolamento di Borsa Italiana, tenere informati sia il mercato sia i propri azionisti in merito alla propria struttura di governance e al grado di adesione al Codice. A tal fine, le società quotate sono tenute alla pubblicazione di una apposita relazione, in occasione della pubblicazione dei dati di bilancio, che viene messa a disposizione dell'assemblea dei soci e contestualmente trasmessa a Borsa Italiana, che la mette a disposizione del pubblico. Il Codice ha per oggetto, fra gli altri, i seguenti temi: ruolo del consiglio di amministrazione; composizione del consiglio di amministrazione; presenza di amministratori indipendenti; trattamento delle informazioni riservate; procedure di nomina degli amministratori e loro criteri di remunerazione; comitato per il controllo interno; operazioni con parti correlate; rapporti con gli investitori istituzionali e con gli altri soci.

3.4 Requisiti per i Sistemi Multilaterali di Negoziazione

I Sistemi Multilaterali di Negoziazione sono "sistemi di contrattazione privati che offrono la possibilità di negoziare strumenti finanziari quotati presso una Borsa, senza compiti regolamentari di ammissione e informativa"[104]

La disciplina è dettata dall'art. 77 bis TUF, che in particolare evidenzia il ruolo di Consob nella gestione di questi sistemi.

Al comma 1 Consob viene investita del potere regolamentare per la determinazione dei requisiti minimi di funzionamento dei sistemi multilaterali di negoziazione, inclusi gli obblighi dei loro gestori in materia di:

a) processo di negoziazione e finalizzazione di operazioni;
b) ammissione di strumenti finanziari;
c) informazioni fornite al pubblico e agli utenti;
d) accesso al sistema;
e) controllo dell'ottemperanza da parte degli utenti delle regole del sistema.

Il comma 2 attribuisce a Consob poteri in merito alla permanenza degli strumenti finanziari, in particolare:

a) chiedere ai soggetti che gestiscono un sistema multilaterale di negoziazione l'esclusione o la sospensione degli strumenti finanziari dalle negoziazioni sul sistema multilaterale di negoziazione;
b) chiedere ai soggetti che gestiscono un sistema multilaterale di negoziazione tutte le informazioni che ritenga utili ai fini della esclusione o sospensione di strumenti finanziari;
c) vigila, al momento dell'autorizzazione e in via continuativa, che le regole e le procedure adottate dai sistemi multilaterali di negoziazione siano conformi alle disposizioni comunitarie.

Il comma 3 sancisce che la Consob richiede la sospensione o l'esclusione di uno strumento finanziario dalle negoziazioni in un sistema multilaterale di negoziazione nei casi in cui tale strumento finanziario sia ammesso alle negoziazioni in un mercato regolamentato e sia stato oggetto di provvedimento di sospensione o esclusione da parte di autorità competenti di

[104] Glossario Borsa Italiana.

altri Stati membri[105], salvo che ciò possa causare danni agli interessi degli investitori o all'ordinato funzionamento del mercato

Di seguito l'elenco dei Sistemi Multilaterali di Negoziazione autorizzati da Consob[106]:

Elenco dei Sistemi Multilaterali di Negoziazione "MTF"		
Denominazione società	**Denominazione"MTF"**	**Codice MIC[107]**
E-MID SIM SPA	E-MIDER	EMDR
E-MID SIM SPA	E-MID Repo	EMIR
EuroTLX SIM SPA	EUROTLX	ETLX
HI-MTF SIM SPA	HI-MTF	HMTF
	HI-MTF "Order Driven"	HMOD
BORSA ITALIANA SPA	AIM ITALIA - MERCATO ALTERNATIVO DEL CAPITALE	XAIM
	EXTRAMOT	XMOT
	BORSA ITALIANA TRADING AFTER HOURS	MTAH
MTS SPA	BOND VISION CORPORATE	SSOB

Per ognuno di questi sistemi la relativa società di gestione ha adottato un regolamento che disciplina anche i requisiti di ammissione.

3.5 Requisiti specifici per l'*Alternative Investment Market*

A differenza dei mercati regolamentati, AIM Italia stabilisce solo alcuni requisiti minimi di ammissione[108]:

- il requisito fondamentale è la continua presenza del Nomad[109], sia nella fase di pre-ammissione che in quella successiva all'ammissione

[105] Direttiva 2004/39/CE (MIfid), vedasi par. 1.5.
[106] www.consob.it/mercati/sistemi.
[107] Market identification code.
[108] www.borsaitaliana.it/AIMitalia.
[109] Il Nomad è una figura centrale per AIM Italia. I Nomad devono essere ammessi da Borsa Italiana e sono iscritti in un apposito registro. Può essere una banca d'affari, un intermediario o una società che opera prevalentemente nel settore corporate finance; deve valutare l'appropriatezza della società ai fini dell'ammissione al mercato, supportarla nel mantenere un profilo adeguato di trasparenza informativa nei confronti degli investitori, stimolare l'attenzione da parte della società al rispetto delle regole derivanti

- non è prevista una dimensione minima o massima della società in termini di capitalizzazione
- flottante minimo del dieci per cento[110]
- nessun requisito particolare in tema di corporate governance
- nessuno specifico requisito economico-finanziario

È il mercato stesso, grazie alla figura del Nomad, a definire la dimensione ideale delle società che concretamente verranno ammesse al mercato, il flottante che sarà opportuno collocare per garantire adeguata liquidità al titolo e i presìdi in termini di governance per tutelare gli azionisti di minoranza.

Il Nomad nel corso degli incontri preliminari valuterà il potenziale apprezzamento della società da parte degli investitori, in base al generale contesto di mercato, al settore di appartenenza, al track record, alle prospettive di crescita e consiglierà la società in merito all'opportunità di intraprendere il processo di quotazione.

In fase di ammissione, la società deve predisporre soltanto il documento di ammissione, che riporta le informazioni utili per gli investitori relative all'attività della società, al management, agli azionisti e ai dati economico-finanziari.

Una volta quotata, la società non deve presentare i resoconti trimestrali di gestione, ma solo il bilancio e la relazione semestrale e non deve pubblicare altra documentazione per effettuare aumenti di capitale successivi.

3.6 Procedure preliminari alla quotazione

La fase antecedente all'IPO è caratterizzata dallo svolgimento, da parte della società quotanda, di una serie di operazioni e valutazioni dirette all'integrazione dei presupposti necessari alla quotazione, che si apre con il lancio dell'operazione da parte del Consiglio di

---

dall'essere quotata su AIM Italia, massimizzandone i benefici. I principali compiti del Nomad, così come previsti dai regolamenti di AIM Italia, sono:

1. effettuare la due diligence descritta nel Regolamento AIM Italia al fine di valutare se la società è appropriata per l'ammissione sul mercato;
2. gestire il processo di quotazione, coordinando il team di consulenti, definendo la tempistica e guidando la società nella redazione del documento di ammissione;
3. dare consulenza all'impresa, una volta quotata, circa gli adempimenti previsti dal Regolamento emittenti. Il Nomad assiste la società quotata su AIM Italia per tutto il periodo di permanenza sul mercato.

[110] Vedasi nota 101.

Amministrazione della società[111] per terminare con la predisposizione di tutta la documentazione da presentare all'esterno onde avviare la procedura di quotazione vera e propria, nella fase di IPO.

3.6.1 Fase preliminare

La decisione di intraprendere la strada della quotazione parte normalmente dalla presentazione da parte del management della società quotanda al Consiglio di Amministrazione del progetto di quotazione, corredato da apposito studio di fattibilità.

Una volta che il Consiglio abbia deliberato sulla richiesta di ammissione a quotazione, si procede alla convocazione della Assemblea ordinaria, o, se previsto un aumento di capitale, straordinaria[112].

Successivamente, la società opera il cosiddetto beauty contest, ossia il processo finalizzato alla scelta dei consulenti chiamati ad assistere la società nel corso dello svolgimento del procedimento di quotazione, ed al termine del quale si procede alla nomina dello sponsor, degli studi legali e fiscali, delle società di revisione e degli altri consulenti.

Si tratta di una fase che richiede "particolare attenzione da parte della società quotanda, che dovrà tenere conto, nell'operare tale scelta, sia dei fattori oggettivi, legati ad esperienza e competenza del consulente rispetto al costo, sia soggettivi, in termini di fiducia e spirito collaborativo nella relazione con il management e gli attuali consulenti della società stessa"[113].

---

[111] Nell'organizzazione aziendale il consiglio di amministrazione (spesso abbreviato CdA) è l'organo collegiale al quale è affidata la gestione delle società per azioni e delle altre società la cui disciplina è modellata su quella delle società per azioni. Un organo analogo, a volte con lo stesso nome, si trova anche in altri enti non aziendali, come ad esempio le università.
I membri del consiglio di amministrazione sono detti amministratori (*directors* nei paesi anglosassoni); nella maggior parte degli ordinamenti non devono essere necessariamente soci.

[112] La legge determina espressamente le competenze dell'assemblea straordinaria, le quali sono inderogabili e non dipendono dal modello di gestione e controllo adottate dalla società.
Essa in particolare delibera sulle seguenti materie:
- scelta di quali amministratori abbiano la rappresentanza societaria (art. 2365 c. 2 c.c.);
- nomina, sostituzione, revoca e determinazione dei poteri dei liquidatori (art. 2365 c. 1 c.c.);
- modificazioni dello statuto (art. 2365 c. 1 c.c.);
- Adeguamento dello statuto alle norme di legge (art. 2365 c. 2 c.c.);
- Trasferimento della sede sociale purché in ambito nazionale (art. 2365 c. 2 c.c.);
- Istituzione o soppressione di sedi secondarie (art. 2365 c. 2 c.c.);
- Aumento di capitale (art. 2443 c.c.);
- Decisione di non emettere certificati azionari (art. 5 RD 239/1942);
- Emissione di azioni a favore dei prestatori di lavori o di strumenti finanziari per i dipendenti delle società controllate (art. 2349 c. 2 c.c.);
- Emissione di obbligazioni convertibili (art. 2420 ter c.c.);
- Fusioni, scissioni e trasformazioni (art. 2365 c. 1 c.c.);
- Fusioni con società interamente possedute o possedute almeno al 90% (art. 2365 c. 2 c.c.).

[113] www.economiauniparthenope.it/icostidellaquotazione.

Avvenuta la nomina dei consulenti, si procede alla "riunione di lancio"[114] dell'operazione, occasione nella quale il management della società si incontra, per la prima volta, con tutti i consulenti incaricati, e si procede all'assegnazione delle rispettive responsabilità e alla pianificazione dei tempi e dei passaggi della procedura.

3.6.2 Due diligence e documentazione

Successivamente, occorre procedere alla effettuazione della cosiddetta attività di due diligence sulla società quotanda, che consiste in un complesso di attività, condotte dai consulenti coinvolti nella redazione del Prospetto Informativo[115], dirette all'analisi approfondita della società sotto vari profili, ivi incluso il profilo legale, economico, di business e finanziario, al fine di verificare la fattibilità della quotazione ed assumere tutte le informazioni necessarie ai fini della redazione del Prospetto Informativo stesso.

Si tratta di una procedura molto complessa che vede coinvolti in primis i consulenti legali e fiscali e la società di revisione e che richiede alla struttura amministrativa ed al management della società quotando un notevole impegno e collaborazione fine di agevolare la ricerca ed il reperimento delle informazioni necessarie.

In questa fase si procede anche alla stesura del Prospetto Informativo, documento ufficiale di sollecitazione del pubblico risparmio, la cui redazione è resa obbligatoria dall'art. 113[116] del TUF e il cui contenuto è regolato dall'art. 94, co. 2[117] del TUF, e che viene redatto,

---

[114] Francesco Galgano, *Diritto Commerciale*, *Le società*, Bologna, Zanichelli, 2012, XVIII Edizione, pag. 434.

[115] Documento necessario affinché gli investitori possano formarsi un fondato giudizio sulla situazione patrimoniale, economica e finanziaria dell'emittente e sull'evoluzione della sua attività.

[116] Art. 113: " 1. Prima della data stabilita per l'inizio delle negoziazioni degli strumenti finanziari comunitari in un mercato regolamentato l'emittente o la persona che chiede l'ammissione alle negoziazioni pubblica un prospetto. Si applicano gli articoli 94, commi 1, 2, 3, 4, 5, 8, 10 e 11 e 94-bis, commi 1, 2, 3 e 5 anche nei confronti della persona che chiede l'ammissione alle negoziazioni.

2. Qualunque fatto nuovo significativo, errore materiale o imprecisione relativi alle informazioni contenute nel prospetto che sia atto ad influire sulla valutazione degli strumenti finanziari e che sopravvenga o sia rilevato tra il momento in cui è approvato il prospetto e quello in cui inizia la negoziazione in un mercato regolamentato deve essere menzionato in un supplemento del prospetto.
3. La Consob:
   a) determina con regolamento le modalità e i termini di pubblicazione del prospetto e di eventuali supplementi dettando specifiche disposizioni per i casi in cui l'ammissione alle negoziazioni in un mercato regolamentato sia preceduta da un'offerta al pubblico;
   b) determina con regolamento la lingua da utilizzare nel prospetto per l'ammissione alle negoziazioni di strumenti finanziari;
   c) può individuare con regolamento in quali casi non si applica l'obbligo di pubblicazione del prospetto previsto al comma 1;
   d) disciplina l'obbligo di depositare presso la Consob un documento concernente le informazioni che gli emittenti hanno pubblicato o reso disponibili al pubblico nel corso di un anno;
   e) stabilisce le condizioni per il trasferimento dell'approvazione di un prospetto all'autorità competente di un altro Stato membro;

f) esercita i poteri previsti negli articoli 114, commi 5 e 6, e 115 nei confronti dell'emittente, della persona che chiede l'ammissione alle negoziazioni e degli altri soggetti indicati in tali disposizioni;
g) può sospendere l'ammissione alle negoziazioni in un mercato regolamentato per un massimo di dieci giorni lavorativi consecutivi per ciascuna volta se ha ragionevole motivo di sospettare che le disposizioni del presente articolo e delle relative norme di attuazione sono state violate;
h) fermo restando il potere previsto nell'articolo 64, comma 1-bis, lettera c), può chiedere alla società di gestione del mercato la sospensione in via cautelare, per un periodo non superiore a dieci giorni lavorativi consecutivi, delle negoziazioni in un mercato regolamentato in caso di fondato sospetto di violazione delle disposizioni del presente articolo e delle relative norme di attuazione;
i) fermo restando il potere previsto nell'articolo 64, comma 1-bis, lettera c), può chiedere alla società di gestione del mercato di vietare le negoziazioni in un mercato regolamentato in caso di accertata violazione delle disposizioni del presente articolo e delle relative norme di attuazione;
l) informa l'autorità competente dello Stato membro d'origine, qualora, quale autorità competente dello Stato membro ospitante, rilevi che siano state commesse violazioni degli obblighi incombenti all'emittente in virtù dell'ammissione degli strumenti finanziari alle negoziazioni in un mercato regolamentato;
m) adotta, dopo averne informato l'autorità competente dello Stato membro d'origine, le misure opportune per tutelare gli investitori, se, nonostante le misure adottate dall'autorità competente dello Stato membro d'origine o perché tali misure si rivelano inadeguate, l'emittente persevera nella violazione delle disposizioni legislative o regolamentari pertinenti. Dell'adozione di tali misure ne informa al più presto la Commissione europea;
n) rende pubblico il fatto che l'emittente o la persona che chiede l'ammissione alle negoziazioni non ottempera ai propri obblighi.

4. Alla pubblicità relativa ad un'ammissione di strumenti finanziari alla negoziazione in un mercato regolamentato si applica l'articolo 101.
5. Al prospetto di ammissione alle negoziazioni in un mercato regolamentato si applicano gli articoli 98 e 98-bis".

[117] Art. 94: "1. Coloro che intendono effettuare un'offerta al pubblico pubblicano preventivamente un prospetto. A tal fine, per le offerte aventi ad oggetto strumenti finanziari comunitari nelle quali l'Italia è Stato membro d' origine e per le offerte aventi ad oggetto prodotti finanziari diversi dagli strumenti finanziari comunitari, ne danno preventiva comunicazione alla Consob allegando il prospetto destinato alla pubblicazione. Il prospetto non può essere pubblicato finché non è approvato dalla Consob. Nel caso di offerta al pubblico di quote o azioni di Oicr chiusi per le quali l'Italia è lo Stato membro d'origine, il prospetto è pubblicato quando si è conclusa la procedura prevista dall'articolo 43 o dall'articolo 44 e dalle relative disposizioni di attuazione.

2. Il prospetto contiene, in una forma facilmente analizzabile e comprensibile, tutte le informazioni che, a seconda delle caratteristiche dell'emittente e dei prodotti finanziari offerti, sono necessarie affinché gli investitori possano pervenire ad un fondato giudizio sulla situazione patrimoniale e finanziaria, sui risultati economici e sulle prospettive dell'emittente e degli eventuali garanti, nonché sui prodotti finanziari e sui relativi diritti. Il prospetto contiene altresì una nota di sintesi la quale, concisamente e con linguaggio non tecnico, fornisce le informazioni chiave nella lingua in cui il prospetto è stato in origine redatto. Il formato e il contenuto della nota di sintesi forniscono, unitamente al prospetto, informazioni adeguate circa le caratteristiche fondamentali dei prodotti finanziari che aiutino gli investitori al momento di valutare se investire in tali prodotti.
3. Il prospetto per l'offerta di strumenti finanziari comunitari è redatto in conformità agli schemi previsti dai regolamenti comunitari che disciplinano la materia.
4. L'emittente o l'offerente può redigere il prospetto nella forma di un unico documento o di documenti distinti. Nel prospetto composto di documenti distinti, le informazioni richieste sono suddivise in un documento di registrazione, una nota informativa sugli strumenti e i prodotti offerti e una nota di sintesi.
5. Se è necessario per la tutela degli investitori, la Consob può esigere che l'emittente o l'offerente includa nel prospetto informazioni supplementari.
6. Se l'offerta ha ad oggetto prodotti finanziari diversi dagli strumenti finanziari comunitari il cui prospetto non è disciplinato ai sensi dell'articolo 95, comma 1, lettera b), la Consob stabilisce, su richiesta dell'emittente o dell'offerente, il contenuto del prospetto.
7. Qualunque fatto nuovo significativo, errore materiale o imprecisione relativi alle informazioni contenute nel prospetto che sia atto ad influire sulla valutazione dei prodotti finanziari e che sopravvenga o sia rilevato tra il momento in cui è approvato il prospetto e quello in cui è definitivamente chiusa l'offerta al pubblico deve essere menzionato in un supplemento del prospetto.

secondo gli schemi previsti dal Regolamento 809/2004/CE (art. 24 co.2 Reg. Emittenti), dallo sponsor insieme con i consulenti legali e fiscali e con il management della società quotanda.

Nel Prospetto Informativo vengono riportati i dati raccolti sulla base delle analisi svolte nel corso della due diligence relativi alla condizione economico finanziaria della società, relativi alla posizione della società rispetto alla concorrenza, al management, ad obiettivi e strategie della società stessa.

Vengono inoltre analizzati ulteriori fattori quali: forza lavoro, fornitori, clienti, creditori, e contratti, nonché strumenti finanziari, parti correlate ed operazioni poste in essere con le stesse.

Il Prospetto Informativo è finalizzato infatti a garantire la più ampia informativa e trasparenza rispetto al mercato.

---

8. L'emittente, l'offerente e l'eventuale garante, a seconda dei casi, nonché le persone responsabili delle informazioni contenute nel prospetto rispondono, ciascuno in relazione alle parti di propria competenza, dei danni subiti dall'investitore che abbia fatto ragionevole affidamento sulla veridicità e completezza delle informazioni contenute nel prospetto, a meno che non provi di aver adottato ogni diligenza allo scopo di assicurare che le informazioni in questione fossero conformi ai fatti e non presentassero omissioni tali da alterarne il senso.
9. La responsabilità per informazioni false o per omissioni idonee ad influenzare le decisioni di un investitore ragionevole grava sull'intermediario responsabile del collocamento, a meno che non provi di aver adottato la diligenza prevista dal comma precedente.
10. Nessuno può essere ritenuto civilmente responsabile esclusivamente in base alla nota di sintesi, comprese le eventuali traduzioni, salvo che la nota di sintesi risulti fuorviante, imprecisa o incoerente se letta insieme ad altre parti del prospetto oppure che essa, quando viene letta insieme con altre parti del prospetto, non contenga informazioni chiave che aiutino gli investitori nel valutare se investire nei prodotti finanziari offerti. La nota di sintesi contiene inoltre una chiara avvertenza a tale riguardo.
11. Le azioni risarcitorie sono esercitate entro cinque anni dalla pubblicazione del prospetto, salvo che l'investitore provi di avere scoperto le falsità delle informazioni o le omissioni nei due anni precedenti l'esercizio dell'azione".

4
Fase di IPO

Conclusa la prima fase del procedimento, destinata all'attività preparatoria: delibere e attività necessarie a soddisfare i requisiti richiesti, nomina dei consulenti, due diligence, si avvia la fase esecutiva del processo, che consiste[118]:

- nella predisposizione della documentazione da presentare a Borsa Italiana e Consob a corredo della domanda di ammissione a quotazione e nella relativa istruttoria;
- nella attività di marketing che precede il collocamento, allo scopo di suscitare l'interesse verso il titolo e concorrere alla determinazione del prezzo;
- nella fase di conclusione del processo, nella quale ha luogo il bookbuilding, la fissazione del prezzo definitivo, il collocamento ed eventuale sollecitazione e l'avvio delle negoziazioni.

L'attività svolta in tale fasi è puntualmente regolata dal TUF e dal Regolamento Emittenti, oltre che dal Regolamento di Borsa e relative Istruzioni.

4.1 Domanda di ammissione a quotazione davanti a Borsa Italiana S.p.A.

4.1.1 Presentazione della domanda

Contestualmente agli adempimenti connessi alla procedura di autorizzazione alla pubblicazione del prospetto e alla sollecitazione all'investimento degli strumenti finanziari oggetto dell'offerta da svolgersi con Consob (art. 52 co. 1[119] Reg. Emittenti), "l'Emittente presenta domanda di ammissione alla quotazione a Borsa Italiana, società di gestione dei mercati, che dovrà accertare la sussistenza di tutte le condizioni ed i requisiti richiesti dalla normativa di riferimento"[120].

[118] www.economiauniparthenope.it/icostidellaquotazione.

[119] Art. 52 co. 1: "Ai fini della pubblicazione del prospetto di ammissione alle negoziazioni, l'emittente o la persona che chiede l'ammissione trasmette alla Consob, ai sensi dell'articolo 113, comma 1, del Testo unico, la comunicazione prevista dall'articolo 94, comma 1, del Testo unico, sottoscritta dal legale rappresentante e corredata del prospetto medesimo e degli altri documenti indicati nell'Allegato 1I".

[120] Donato Ivano Pace, *Ammissione sospensione esclusione dai mercati regolamentati*, Milano, Giuffrè Editore, 2012, pag. 154.

Seguendo il disposto dell'art. 2.4.1[121] del regolamento di Borsa, la domanda, sottoscritta dal legale rappresentante[122] dell'Emittente o dal soggetto munito dei necessari poteri (co. 4), redatta in duplice copia secondo l'apposito modello riportato nelle Istruzioni al Regolamento di Borsa[123], deve essere inoltrata a Borsa Italiana dall'Emittente, previa delibera dell'organo competente[124] (co. 1), e deve indicare la documentazione prodotta in allegato, anch'essa espressamente indicata nelle predette Istruzioni (co. 2).

La domanda deve riferirsi a tutti gli strumenti finanziari facenti parte della stessa emissione. L'Emittente deve precisare se analoga domanda è stata presentata in un altro mercato regolamentato o se lo sarà nel termine di dodici mesi (co. 3).

4.1.2 Istruttoria di Borsa Italiana S.p.A.

L'art. 2.4.2 del regolamento di Borsa disciplina il ruolo di Borsa Italiana S.p.A., in particolare al comma 1 recita "Entro due mesi dal giorno in cui è stata completata la documentazione da allegare alla domanda, Borsa Italiana delibera e comunica all'Emittente

---

[121] Articolo 2.4.1: "1. Salvo quanto disposto all'articolo 2.4.7, la domanda, redatta secondo l'apposito modello riportato nelle Istruzioni, deve essere inoltrata a Borsa Italiana dall'emittente, previa delibera dell'organo competente, in conformità con le modalità indicate nelle Istruzioni stesse.
2. Borsa Italiana indica nelle Istruzioni la documentazione da produrre a seguito della presentazione della domanda di ammissione.
3. La domanda deve riferirsi a tutti gli strumenti finanziari facenti parte della stessa emissione. L'emittente deve precisare se analoga domanda è stata presentata in un altro mercato regolamentato o se lo sarà nel termine di dodici mesi.
4. La domanda deve essere sottoscritta dal legale rappresentante dell'emittente o dal soggetto munito dei necessari poteri e presentata, congiuntamente allo sponsor nei casi di cui all'articolo 2.3.1, comma 1, lettera a), presso il competente ufficio di Borsa Italiana. Borsa Italiana comunica all'emittente nonché alla Consob la completezza della domanda allorché completa della documentazione di cui al comma 2.
5. Fino alla data di inizio delle negoziazioni, ogni annuncio, avviso, manifesto e documento, che l'emittente intenda rendere pubblico, relativo alla domanda di ammissione ed alle caratteristiche degli strumenti finanziari oggetto della domanda stessa, deve essere preventivamente comunicato a Borsa Italiana e deve menzionare che è in corso la procedura per l'ammissione.
6. Ai fini dell'ammissione a quotazione di strumenti finanziari di nuova emissione, fungibili con quelli già quotati, nonché per le azioni di nuova emissione, di pari categoria e aventi le medesime caratteristiche ad eccezione del godimento di quelle già quotate, l'emittente informa Borsa Italiana secondo le modalità e i termini indicati nelle Istruzioni perché questa possa provvedere in merito.
7. Per gli strumenti finanziari emessi da Borsa Italiana ai fini della domanda di ammissione di cui al presente articolo i riferimenti a Borsa Italiana devono essere intesi come riferiti a Consob e i riferimenti all'emittente come riferiti a Borsa Italiana".

[122] Art. 1387 c.c.: "Il potere di rappresentanza è conferito dalla legge ovvero dall'interessato";
Art. 2384 c.c.: "Il potere di rappresentanza attribuito agli amministratori dallo statuto o dalla deliberazione di nomina è generale".

[123] Reg. Borsa, Titolo IA.1, Domanda di ammissione alla quotazione e documentazione da allegare, Modelli di domanda.

[124] "La decisione di quotarsi, quale che sia il modello societario prescelto, non debba essere deliberata in sede straordinaria, ma possa essere adottata dall'assemblea ordinaria, ricadendo, come è noto, nella competenza di quest'ultima tutte le deliberazioni che non possono essere ricomprese fra quelle di competenza dell'assemblea straordinaria", Michele de Mari, *La quotazione di azioni nei mercati regolamentati: profili negoziali e rilievo organizzativo*, Torino, Giappichelli Editore, 2004, pag. 72.

l'ammissione o il rigetto della domanda, dandone contestuale comunicazione a Consob. Con il provvedimento di ammissione viene altresì stabilito il comparto nel quale verrà negoziato lo strumento finanziario, nonché il quantitativo minimo di negoziazione, ove previsto".

Il termine è di un mese se la domanda è stata presentata da un emittente AIM Italia.

Il termine di due mesi può essere interrotto da Borsa Italiana che ne da comunicazione, per una sola volta, qualora sia necessario assumere nuove informazioni e documenti, per i quali Borsa Italiana fissa un termine.

In questo caso, a partire dalla data del ricevimento della relativa documentazione, decorre nuovamente il termine di due mesi per l'ammissione o il rigetto della domanda (co. 2).

L'efficacia del provvedimento di ammissione ha validità di sei mesi ed è in ogni caso subordinata al deposito del prospetto di quotazione presso Consob (co. 3).

L'ammissione si perfeziona allorché Borsa Italiana, accertata la messa a disposizione del pubblico del prospetto informativo, stabilisce la data di inizio delle negoziazioni e il segmento di mercato nel quale verrà negoziato lo strumento finanziario e ne informa il pubblico mediante proprio Avviso (co. 4), trasmesso anche ad almeno due agenzie di stampa.

Borsa Italiana deve essere tempestivamente informata di ogni fatto nuovo, suscettibile di influenzare in modo significativo la valutazione degli strumenti finanziari, che si verifichi nel periodo intercorrente tra la data del provvedimento di ammissione e la data di inizio delle negoziazioni. Borsa Italiana, valutati tali fatti e qualora lo richieda la tutela degli investitori, potrà procedere alla revoca del proprio provvedimento (co. 5).

4.1.3 Rigetto della domanda

Borsa Italiana, sulla base della documentazione ricevuta e delle informazioni di pubblico dominio, può respingere la domanda di ammissione alle negoziazioni se:

- le caratteristiche dello strumento finanziario siano tali da far ritenere che non possa aver luogo la formazione di un mercato regolare;
- avendo altri strumenti finanziari già ammessi alle negoziazioni, l'Emittente non adempie agli obblighi derivanti dalla ammissione;
- vi siano dati e fatti idonei a pregiudicare gravemente la situazione e l'andamento della gestione dell'Emittente. A tal fine, Borsa Italiana farà principalmente riferimento all'esistenza di rilevanti controversie o procedimenti giudiziali, anche in sede penale, alla pendenza di rilevanti accertamenti fiscali;

- la situazione dell'Emittente, al momento dell'ammissione a quotazione della società, sia tale da rendere l'ammissione contraria all'interesse degli investitori.

Su questo ultimo punto Borsa Italiana farà principalmente riferimento alla presenza di gravi squilibri nella struttura finanziaria.

Verranno valutati per esempio[125]:

- se la posizione finanziaria netta è stata influenzata da operazioni di rinuncia a crediti da parte di terzi o da aumenti di capitale/versamenti a fondo perduto;
- l'esistenza di pattuizioni di condizioni atipiche o inusuali nell'incasso di crediti o nel pagamento di debiti di natura commerciale.

4.2 Il procedimento davanti a Consob

Preliminarmente va segnalato che entro cinque giorni dal ricevimento della comunicazione di ammissione alla quotazione da parte di Borsa Italiana, CONSOB può:

- vietare l'esecuzione della decisione di ammissione degli strumenti finanziari e degli operatori dalle negoziazioni se, sulla base degli elementi informativi in suo possesso, ritiene la decisione contraria alle finalità di cui all'art. 74, comma 1, del TUF, "La Consob vigila sui mercati regolamentati al fine di assicurare la trasparenza, l'ordinato svolgimento delle negoziazioni e la tutela degli investitori e può adottare ogni misura per garantire il rispetto degli obblighi previsti dal presente Capo";
- chiedere a Borsa Italiana tutte le informazioni che ritenga utili ai fini dell'esercizio del potere di veto di cui al precedente punto;
- chiedere a Borsa Italiana l'esclusione o la sospensione degli strumenti finanziari e degli operatori dalle negoziazioni.

4.2.1 Il prospetto di quotazione

Ai sensi dell'art. 113[126] del TUF, l'Emittente, prima della data stabilita per l'inizio delle negoziazioni degli strumenti finanziari in un mercato regolamentato, deve pubblicare il prospetto informativo, redatto nella fase di "due diligence"[127].

---

[125] www.economiauniparthenope.it/icostidellaquotazione.

[126] Vedasi nota 111.

[127] Vedasi paragrafo 3.2.2.

A tal fine, l'Emittente o la persona che chiede l'ammissione alle negoziazioni su un mercato regolamentato trasmette a Consob domanda di autorizzazione alla pubblicazione del prospetto[128], sottoscritta dal legale rappresentante e corredata del prospetto medesimo e degli altri documenti indicati nell'Allegato 1I del Regolamento Emittenti[129].

Con il prospetto di quotazione devono essere fornite al pubblico determinate informazioni, individuate dalla legge in generale (art. 94 TUF) e specificate da Consob.

La pubblicazione del prospetto rappresenta una condizione per il completamento della procedura di ammissione a quotazione e costituisce uno strumento informativo che deve essere messo a disposizione per la tutela dei potenziali investitori nella fase iniziale dell'offerta al pubblico (IPO).

"Il prospetto può essere costituito da un unico documento o da più documenti distinti, in tal caso conterrà un documento, detto "di registrazione", una nota informativa sugli strumenti finanziari e una nota di sintesi"[130].

4.2.2 Istruttoria di Consob

L'istruttoria di Consob sul prospetto si svolge entro venti giorni lavorativi dalla data in cui Borsa Italiana comunica l'ammissione della società alla quotazione.

Il termine di venti giorni si riferisce all'ipotesi in cui la società che chiede l'ammissione alla quotazione non abbia altri strumenti finanziari già quotati o comunque diffusi tra il pubblico (art. 8 co. 3 Reg. Emittenti).

---

[128] Presentata contemporaneamente alla domanda di ammissione a quotazione presso Borsa Italiana, vedasi nota 115 sull'art. 52 co. 1 Reg. Emittenti.

[129] Documentazione da allegare alla domanda di autorizzazione alla pubblicazione del prospetto di quotazione di azioni, "Alla domanda di autorizzazione alla pubblicazione del prospetto di quotazione di azioni deve essere allegata la documentazione di seguito indicata:
a) copia della delibera dell'organo competente che ha approvato la presentazione della domanda di quotazione;
b) copia dello statuto vigente dell'emittente;
c) copia dei bilanci degli ultimi tre esercizi, anche consolidati, ove redatti, nonché degli ulteriori documenti indicati al punto 3, Tavola 1, Sezione IA.1.1 delle Istruzioni al Regolamento di ammissione emanato dalla Borsa Italiana S.p.A., ove non già contenuti nel prospetto di quotazione;
d) prospetto di quotazione, firmato in originale dal legale rappresentante e dal presidente dell'organo di controllo dell'emittente, redatto secondo le modalità previste nell'Allegato 1B;
e) dichiarazione dell'emittente e, ove presente, dello sponsor/listing partner, che attesti che il prospetto di quotazione contiene tutte le informazioni rilevanti di cui all'articolo 94, comma 2, del Testo Unico;
f) in caso di richiesta, ai sensi dell'art. 10 del regolamento, di trasmissione del certificato di approvazione della Consob alle autorità competenti di altri Stati membri della UE, la traduzione della nota di sintesi nella lingua ufficiale degli Stati ove la sollecitazione è prevista, ove richiesta da tali Stati".

[130] www.borsaitaliana.it/prospetti.

Il termine di venti giorni si riduce invece a dieci nel caso in cui l'Emittente abbia altri strumenti finanziari già quotati o diffusi, o abbia già effettuato offerte al pubblico (art. 8 co.2 Reg. Emittenti).

Qualora CONSOB ritenga necessario acquisire documenti o informazioni supplementari, ne farà richiesta nei termini sopra visti; l'Emittente avrà 10 giorni (co. 2) o 20 giorni (co. 3) di tempo per consegnare quanto richiesto, a pena di improcedibilità, e i termini per l'istruttoria decorreranno dal momento della consegna della documentazione supplementare.

In merito alle funzioni di controllo svolte da CONSOB sul prospetto, queste si dividono in due categorie:

a) la legittimità dell'operazione
b) controllo di veridicità del contenuto

La prima funzione si riferisce al caso in cui Consob si convinca dell'illegittimità dell'operazione, in questa situazione Consob procederà ad autorizzare la pubblicazione del prospetto subordinandola all'inserimento di questo convincimento.

La Consob si è spesso arrogata il potere di esercitare il controllo di legittimità, "incontrando le critiche della dottrina, ad avviso della quale tale controllo è riservato all'autorità giudiziaria".[131]

La seconda funzione riguarda la corrispondenza tra quanto scritto nel prospetto e la situazione reale.

Se da un lato non è possibile che si sviluppi un controllo dettagliato su ogni informazione, poiché questo implicherebbe un intralcio burocratico insormontabile, dall'altro lato "il principio di buon andamento della P.A. (sancito dall'art. 97[132] Cost.) impone alla Consob di procedere ad una valutazione di non palese falsità o incompletezza sulla base delle informazioni in suo possesso, di pubblico dominio o di agevole verificabilità"[133].

---

[131] Renzo Costi-Luca Enriques, *Trattato di Diritto Commerciale*, Il Mercato Mobiliare, VIII volume, Padova, CEDAM, 2004, pag. 77.

[132] Art. 97: Costituzione "Le pubbliche amministrazioni, in coerenza con l'ordinamento dell'Unione europea, assicurano l'equilibrio dei bilanci e la sostenibilità del debito pubblico.
I pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione.
Nell'ordinamento degli uffici sono determinate le sfere di competenza, le attribuzioni e le responsabilità proprie dei funzionari.
Agli impieghi nelle pubbliche amministrazioni si accede mediante concorso, salvo i casi stabiliti dalla legge".

[133] Renzo Costi-Luca Enriques, *Trattato di Diritto Commerciale*, Il Mercato Mobiliare, VIII volume, Padova, CEDAM, 2004, pag. 77-78.

4.2.3 Pubblicazione del prospetto

Quando si parla di "autorizzazione alla pubblicazione del prospetto" ci si trova di fronte ad un provvedimento autorizzatorio che rimuove un limite all'esercizio di un diritto, in particolare ci si riferisce alla libertà di iniziativa economica, sancita dall'art. 41[134] della Costituzione.

Di conseguenza "l'autorizzazione alla pubblicazione del prospetto è uno strumento di polizia e non di governo del mercato"[135].

La pubblicazione del prospetto avviene prima della data fissata per l'ammissione a quotazione (art. 113 co. 1 TUF)

Qualora non sia stato possibile inserire nel prospetto tutti i dati, particolarmente quelli relativi al prezzo e alla quantità di strumenti oggetto di offerta, è possibile pubblicare avvisi integrativi (art. 94 co. 7, art. 113 co. 2 TUF).

Ai sensi dell'art. 56 (co.1) del Regolamento Emittenti, il prospetto è reso pubblico mediante deposito presso Consob dell'originale e di una copia riprodotta su supporto informatico, nonché messo a disposizione del pubblico alternativamente:

- mediante inserimento in uno o più giornali a diffusione nazionale o a larga diffusione (lettera a);
- in forma stampata e gratuitamente, nella sede della società di gestione del mercato o nella sede legale dell'Emittente (lettera b)
- in forma elettronica nel sito web dell'Emittente e nel sito degli intermediari che provvedono al collocamento degli strumenti finanziari, compresi gli organismi incaricati del servizio finanziario (lettera c);
- in forma elettronica nel sito web della società di gestione del mercato (lettera c).

Il prospetto ha una validità di dodici mesi, a partire dalla data della sua approvazione (art. 10 co. 1 Reg. Emittenti).

La validità presuppone peraltro che il prospetto venga integrato tempestivamente ogni qual volta intervengano fatti nuovi o si accerti l'esistenza di errori materiali o inesattezze che possano influire sulla valutazione dello strumento finanziario oggetto di quotazione, in questo scenario si provvede alla redazione di un supplemento al prospetto, soggetto anch'esso all'autorizzazione di Consob che viene rilasciata entro sette giorni (art. 7 co. 6 Reg. Emittenti).

---

[134] Vedasi nota 23.

[135] Renzo Costi, Luca Enriques, *Trattato di Diritto Commerciale*, Il Mercato Mobiliare, VIII volume, Padova, CEDAM, 2004, pag. 80.

Il supplemento è pubblicato utilizzando almeno le stesse modalità adottate per il prospetto (art. 9 co. 8 Reg. Emittenti).

Sono inoltre previsti nell'art. 57 co. 1 del Regolamento i casi di esenzione dall'obbligo di pubblicare un prospetto:

a) azioni che rappresentino, in un periodo di dodici mesi, meno del 10% del numero delle azioni della stessa categoria già ammesse alla negoziazione nello stesso mercato regolamentato;
b) azioni emesse in sostituzione di azioni della stessa categoria già ammesse alla negoziazione nello stesso mercato regolamentato, se l'emissione di queste nuove azioni non comporta un aumento del capitale emesso;
c) valori mobiliari offerti in occasione di un'acquisizione mediante offerta pubblica di scambio, a condizione che sia disponibile un documento contenente informazioni considerate dalla Consob equivalenti a quelle del prospetto, tenendo conto degli adempimenti previsti dalla normativa comunitaria;
d) valori mobiliari offerti, assegnati o da assegnare in occasione di una fusione o scissione, a condizione che sia disponibile un documento contenente informazioni considerate dalla Consob equivalenti a quelle del prospetto, tenendo conto degli adempimenti previsti dalla normativa comunitaria;
e) azioni offerte, assegnate o da assegnare gratuitamente agli azionisti esistenti e dividendi versati ad azionisti esistenti sotto forma di azioni della stessa categoria di quelle per le quali vengono pagati tali dividendi, a condizione che dette azioni siano della stessa categoria delle azioni già ammesse alla negoziazione nello stesso mercato regolamentato e che sia reso disponibile un documento contenente informazioni sul numero e sulla natura delle azioni, sui motivi e sui dettagli dell'offerta;
f) valori mobiliari offerti, assegnati o da assegnare ad amministratori o ex amministratori o dipendenti o ex dipendenti o consulenti finanziari abilitati all'offerta fuori sede da parte del loro datore di lavoro o da parte dell'impresa controllante, di un'impresa controllata, collegata o sottoposta a comune controllo, a condizione che detti strumenti finanziari siano della stessa categoria dei valori mobiliari già ammessi alla negoziazione nello stesso mercato regolamentato e che sia reso disponibile un documento contenente informazioni sul numero e sulla natura degli strumenti finanziari, sui motivi e sui dettagli;

g) azioni derivanti dalla conversione o dallo scambio di altri strumenti finanziari o dall'esercizio di diritti conferiti da altri strumenti finanziari, a condizione che dette azioni siano della stessa categoria delle azioni già ammesse alla negoziazione nello stesso mercato regolamentato;

h) valori mobiliari già ammessi alla negoziazione in un altro mercato regolamentato a condizione che:

   1) tali valori mobiliari o valori mobiliari della stessa categoria siano stati ammessi alla negoziazione in tale altro mercato regolamentato da oltre 18 mesi;

   2) per i valori mobiliari ammessi per la prima volta alla negoziazione in un mercato regolamentato dopo la data di entrata in vigore della direttiva 2003/71/CE, l'ammissione alla negoziazione in tale altro mercato regolamentato sia stata associata ad un prospetto approvato e messo a disposizione del pubblico a norma della disciplina comunitaria;

   3) ad eccezione dei casi in cui si applica il punto 2), per i valori mobiliari ammessi per la prima volta alla quotazione dopo il 30 giugno 1983, il prospetto di quotazione sia stato approvato in base ai requisiti di cui alla direttiva 80/390/CEE o alla direttiva 2001/34/CE;

   4) gli obblighi in materia di informazione e di ammissione alla negoziazione in tale altro mercato regolamentato siano stati soddisfatti;

   5) la persona che chiede l'ammissione di un valore mobiliare alla negoziazione in un mercato regolamentato in virtù della presente esenzione metta a disposizione del pubblico un documento di sintesi in lingua italiana;

   6) il documento di sintesi di cui al punto 5) sia messo a disposizione del pubblico, secondo le modalità di cui all'articolo 56;

   7) il contenuto del documento di sintesi sia conforme a quanto previsto dall'articolo 5, comma 3. Tale documento deve indicare inoltre dove può essere ottenuto il prospetto più recente e dove sono disponibili le informazioni finanziarie pubblicate dall'emittente in conformità dei suoi obblighi in materia di informazione e di ammissione alla negoziazione;

i) valori mobiliari diversi dai titoli di capitale emessi da o che beneficiano della garanzia incondizionata e irrevocabile di uno Stato membro dell'Unione Europea o emessi da organismi internazionali a carattere pubblico di cui facciano parte uno o più Stati membri dell'Unione Europea;

j) valori mobiliari emessi dalla Banca Centrale Europea o dalle banche centrali nazionali degli Stati membri dell'Unione Europea;

k) valori mobiliari diversi dai titoli di capitale emessi in modo continuo o ripetuto da banche a condizione che tali valori mobiliari:

   1) non siano subordinati, convertibili o scambiabili;

   2) non conferiscano il diritto di sottoscrivere o acquistare altri tipi di valori mobiliari e non siano collegati ad uno strumento derivato;

   3) diano veste materiale al ricevimento di depositi rimborsabili;

   4) siano coperti da un sistema di garanzia dei depositi a norma degli articoli da 96 a 96-quater del decreto legislativo 1° settembre 1993, n. 385.

m) valori mobiliari emessi, al fine di procurarsi i mezzi necessari al raggiungimento dei propri scopi non lucrativi, da associazioni aventi personalità giuridica o da enti non aventi scopo di lucro, riconosciuti da uno Stato membro.

4.2.4 Sollecitazione all'investimento

Con la domanda di autorizzazione alla pubblicazione del prospetto di quotazione può essere comunicato a Consob, ai sensi dell'art. 94, comma 1, del TUF, che si intende effettuare una sollecitazione[136] relativa agli strumenti finanziari oggetto della domanda.

In tal caso, il prospetto di quotazione, se contiene le informazioni riguardanti la sollecitazione, vale anche come prospetto informativo per la sollecitazione.

Dalla data della comunicazione di cui all'art. 94 del TUF e fino ad un anno dalla conclusione della sollecitazione, all'Emittente che effettui una sollecitazione finalizzata alla quotazione in un mercato regolamentato si applicano, in relazione al mercato di quotazione, le disposizioni concernenti gli obblighi di informazioni a Consob previsti nei del Regolamento Emittenti.

---

[136] Glossario Borsa Italiana, "Ogni offerta, invito a offrire o messaggio promozionale, in qualsiasi forma rivolti al pubblico, finalizzati alla vendita o sottoscrizione di prodotti finanziari (secondo l'articolo 1 del Testo Unico sull'Intermediazione Finanziaria). La sollecitazione all'investimento è disciplinata dagli articoli 94 e seguenti del Testo Unico sull'Intermediazione Finanziaria (TUF). Nel regime giuridico precedente l'emanazione del TUF si faceva riferimento al concetto di "sollecitazione del pubblico risparmio". La finalità principale della disciplina della sollecitazione all'investimento è realizzare una forma di tutela del "risparmio inconsapevole", ossia non necessariamente proveniente da operatori professionali, attraverso la trasparenza delle operazioni proposte. La trasparenza delle operazioni proposte è da intendersi come disponibilità di informazioni che, per qualità e quantità, possano considerarsi adeguate al fine della formulazione di un giudizio fondato sul profilo di rischio-rendimento dell'investimento proposto. Lo strumento concretamente utilizzato a tal fine è rappresentato dalla diffusione di un prospetto informativo contenente alcune informazioni riguardo il proponente l'operazione e le modalità di svolgimento della stessa".

4.3 Il collocamento dei titoli sul mercato

Esaurita la fase istruttoria e ottenuta l'ammissione della società a quotazione da parte di Borsa Italiana e l'autorizzazione alla pubblicazione del prospetto informativo da parte di Consob, la società e i propri consulenti "si dedicano all'attività necessaria al collocamento dei titoli sul mercato, nella quale assume particolare rilievo il marketing presso potenziali investitori"[137], che ha lo scopo di sondare l'interesse del mercato per il titolo e conduce alla determinazione del prezzo di collocamento.

Questa attività può descriversi, in sintesi, come segue:

- Formazione del consorzio di collocamento;
- Pre-marketing e road show;
- Bookbuilding e fissazione del prezzo;
- Assegnazione dei titoli/Sollecitazione all'investimento;
- Stabilizzazione del titolo.

4.3.1 Formazione del consorzio di collocamento

Il global coordinator costituisce il consorzio di collocamento a cui è affidato il compito di raccogliere le dichiarazioni di interesse sui titoli, di raccogliere gli ordini relativi ai titoli e di allocare gli strumenti finanziari tra i sottoscrittori una volta conclusa la fase di raccolta ordini.

Esistono tre diverse tipologie di consorzi[138] che contraddistinguono per in funzione degli impegni assunti dagli intermediari:

- il consorzio di collocamento semplice, dove ogni intermediario facilita il collocamento di una parte dei titoli, senza assumere impegni precisi, e percependo una commissione di sportello;
- il consorzio di collocamento di garanzia, che funge da garante del collocamento, eventualmente sottoscrivendo i titoli non collocati presso il pubblico degli investitori dopo la chiusura del periodo di offerta;
- il consorzio di assunzione a fermo, dove gli intermediari sottoscrivono direttamente l'emissione prima ancora di procedere al collocamento e incassano la differenza tra prezzo di sottoscrizione e prezzo di offerta al pubblico.

[137] www.economiauniparthenope.it/icostidellaquotazione.
[138] www.borsaitaliana.it/consorzi.

Nello svolgimento della attività di collocamento, ciascuno dei soggetti coinvolti esercita un ruolo; in particolare, "il ruolo del global coordinator si svolge, nell'interesse del mercato, assumendo responsabilità per la società di fronte ad esso; l'advisor opera solo ed esclusivamente nell'interesse della società, fornendo servizi di consulenza per tutti gli aspetti legali, fiscali e strategici necessari per realizzare la quotazione; il lead manager dirige il consorzio di collocamento; mentre i co-manager, anch'essi membri del consorzio di collocamento, garantiscono eventualmente il collocamento dei titoli presso il pubblico"[139].

4.3.2 Pre-marketing e road show

Uno dei compiti del global coordinator è collocare la parte di titoli riservata agli investitori istituzionali, generalmente di importo maggiore di quella destinata al pubblico.

Questa fase dell'attività riveste particolare importanza perché concorre alla determinazione del prezzo di collocamento[140].

A tale riguardo, si procede ad una iniziale attività di pre-marketing[141], nella quale il global coordinator avvia contatti con investitori istituzionali, trasmettendo agli stessi una presentazione dell'operazione e chiedendo ai destinatari di manifestare il loro interesse verso il titolo, comunicando i quantitativi di titoli che sarebbero disposti ad acquistare ed i prezzi che sarebbero disposti a pagare.

Questa attività preliminare conduce all'identificazione di una fascia di prezzo, che è influenzata anche dalla situazione del mercato, dalla presentazione dell'operazione, dalle ricerche pubblicate dalle altre banche, che contengono valutazioni indipendenti dell'operazione.

---

[139] www.economiauniparthenope.it/icostidellaquotazione.

[140] Glossario Borsa Italiana, "Il prezzo di collocamento è il prezzo stabilito dall'emittente per la vendita del titolo sul mercato primario. Tale prezzo può essere determinato in maniera univoca dall'emittente (o dal consorzio di collocamento), come nel caso delle operazioni di collocamento retail, oppure può scaturire da un'asta tra operatori istituzionali, come nel caso di operazioni di collocamento riservate ad investitori istituzionali, oppure nel caso dei Titoli di Stato. Il prezzo di collocamento è spesso considerato sinonimo di prezzo di emissione in quanto, nella maggior parte dei casi, il collocamento di uno strumento finanziario avviene contestualmente alla sua emissione. Tuttavia possono esistere differenze tra i due prezzi nel caso in cui il collocamento presso il pubblico retail avvenga in un momento successivo rispetto alla data di emissione. Tipicamente ciò può avvenire nel caso in cui l'emittente si sia avvalso di un consorzio di assunzione a fermo in cui gli intermediari (membri del consorzio) hanno acquistato i titoli all'atto dell'emissione (pagando il prezzo di emissione) per poi collocarli sul mercato soltanto in un periodo successivo (al prezzo di collocamento)".

[141] Prima del collocamento del titolo sul mercato.

Ad esito di questi contatti il global coordinator, insieme alla società e agli azionisti della stessa, è in grado di determinare con maggiore precisione il range[142] di prezzo per il collocamento e il prezzo massimo.

Questa forbice di prezzo sarà naturalmente influenzata da altri fattori[143]:

- i risultati recenti della società;
- le sue prospettive di sviluppo;
- il metodo di valutazione della società;
- le aspettative degli azionisti;
- gli opposti interessi dei vari soggetti coinvolti, il global coordinator, da un lato, e i manager, dall'altro, cercheranno di mantenere basso il prezzo di collocamento, il primo per rendere maggiormente conveniente l'adesione al consorzio di collocamento, i secondi per accrescere la convenienza dell'offerta;
- la presenza di altre emissioni nello stesso periodo;
- la situazione generale della borsa, del settore in cui opera l'Emittente.

Successivamente alla determinazione del range di prezzo, si dà inizio al "road- show", cioè alla presentazione vera e propria della società agli investitori istituzionali, agli esperti e alla stampa di settore, che prevede anche il coinvolgimento del management della società.

La prima tappa del roadshow è, parlando di imprese italiane, sempre Milano, che è ovviamente la piazza finanziaria più importante.

La tappa milanese è quindi quella di maggiore rilevanza, con una folta presenza di analisti e gestori italiani che, per forza di cose, sono i più interessati e con ogni probabilità finiranno per essere i principali acquirenti.

Comunque, in tutti i casi il roadshow prevede sempre delle tappe all'estero, considerando che, in tempi di "globalizzazione" dei mercati, è normale per le società quotate avere una compagine societaria con una folta presenza straniera.

La tappa per eccellenza è Londra, che è la piazza finanziaria europea principale; seguono Parigi e Francoforte, anch'essi mercati finanziari molto importanti.

In aggiunta, possono esserci altre destinazioni che cambiano a seconda della presenza di clienti importanti in quel paese, dell'attività della società oppure dell'esito del pre-marketing, che potrebbe aver individuato investitori particolarmente interessati in una certa zona.

---

[142] Range: differenza e oscillazione tra il prezzo massimo e il prezzo minimo registrato durante una seduta. È un parametro che serve per calcolare e valutare la volatilità del titolo.

Il roadshow tradizionale, con tappe europee, ha di solito una durata di sette-dieci giorni, che possono raddoppiare nel caso in cui si ricomprendano anche tappe nord-americane. Da un punto di vista pratico, le presentazioni della società possono essere fatte ad una platea nutrita (anche cinquanta tra analisti e gestori), come nel caso della tappa di apertura normalmente fatta a Milano, oppure più spesso, consistere in lunch presentation fatti a un numero più ristretto di interlocutori (sei-otto)[144].

4.3.3 Bookbuilding e fissazione del prezzo

A seguito del road-show, il global coordinator raccoglie gli ordini e le manifestazioni di interesse all'acquisto e, sulla base di questi elementi, può giungere ad una determinazione ancora più precisa del prezzo di collocamento del titolo, che sarà applicato anche all'offerta al pubblico.

Riassumendo, la determinazione del prezzo di collocamento è il risultato di quattro fasi distinte:

- una fase di pre-marketing per sondare l'interesse sul titolo da parte di investitori istituzionali e giungere alla determinazione della "forbice" di prezzo iniziale proposta dal CDA sulla base della valutazione[145] della società secondo "i metodi finanziari e dei multipli di mercato"[146];

---

[144] La scelta di effettuare il road-show tramite una seduta di presentazione ad una platea numerosa piuttosto che organizzare diversi incontri con gruppi ristretti di potenziali investitori si inserisce nel quadro delle scelte strategiche, concordate tra management e global coordinator. In linea di principio la presentazione ad una platea numerosa è appannaggio di quelle società che hanno già dimostrato in passato la validità delle operazioni finanziarie, e che quindi vengono precedute da resoconti positivi che sono in grado di attirare numerosi investitori. La presentazione a piccoli gruppi avvantaggia le società di nuova quotazione, che con questo strumento sono in grado di delineare nel dettaglio il progetto finanziario e operare un convincimento che di fronte a numerosi investitori rischierebbe di vanificarsi. La tappa di apertura è, di solito, proposta ad una platea nutrita, in modo da ottenere il massimo risalto tra gli investitori e i media.

[145] La valutazione di un'azienda consiste in un processo finalizzato alla stima del suo valore tramite l'utilizzo di uno o più metodi specifici. La valutazione propedeutica ad un'operazione di quotazione in borsa ha l'obiettivo di contribuire al processo di pricing dei titoli da collocare presso gli investitori. Dalla razionalità con cui viene condotto l'intero processo dipende il successo dell'operazione e in gran parte l'immagine della società quotanda nei confronti della comunità finanziaria e di tutti gli altri stakeholder.

[146] www.borsaitaliana.it/pubblicazioni/guidaallavalutazione, Il metodo dei multipli di mercato presuppone che il valore di una società si possa determinare assumendo come riferimento le indicazioni fornite dal mercato per società con caratteristiche analoghe a quella oggetto di valutazione. Il metodo si basa sulla determinazione di multipli calcolati come rapporto tra valori borsistici e grandezze economiche, patrimoniali e finanziarie di un campione selezionato di società comparabili. I moltiplicatori così determinati vengono applicati, con le opportune integrazioni, alle corrispondenti grandezze della società oggetto di valutazione, al fine di stimare un intervallo di valori, qualora la società non sia quotata, o verificare se essi siano in linea con quelli espressi dal mercato, qualora sia negoziata su mercati borsistici. L'applicazione di tale criterio si articola nelle fasi di seguito descritte.
I) Determinazione del campione di riferimento. Data la natura di tale metodologia, risulta fondamentale l'affinità (da un punto di vista industriale e finanziario) tra le società incluse nel campione di riferimento e la società da valutare. L'impossibilità pratica di identificare società omogenee sotto ogni profilo induce a

- la fase di road show, consistente nella presentazione della società agli investitori, al fine di conoscere l'interesse per il titolo, il quantitativo da acquistare e il prezzo che gli investitori sarebbero disposti a pagare;
- la fase di raccolta degli ordini presso gli incaricati del collocamento[147] (bookbuilding) che restringe ulteriormente la banda di prezzo sulla base delle aspettative dei soggetti interessati;
- la fissazione del prezzo di collocamento in base alle risultanze del bookbuilding.

4.3.4 Assegnazione dei titoli

Si procede ad assegnare i titoli ai membri del consorzio di collocamento, secondo i criteri di ripartizione predeterminati all'atto della costituzione del consorzio.

Nel caso sia prevista la sollecitazione al pubblico, i membri del consorzio procedono poi all'offerta, che sarà di vendita (OPV)[148] in caso siano offerti titoli già precedentemente emessi, o di sottoscrizione (OPS)[149], nel caso siano offerti titoli di nuova emissione.

---

determinare i tratti più significativi per la definizione del paniere di confronto e a selezionare di conseguenza le aziende comparabili in relazione agli attributi prescelti.
II) Scelta dei multipli significativi. I principali multipli impiegati nella valutazione d'azienda sono di seguito elencati: - EV/EBITDA: rapporto tra Enterprise Value (capitalizzazione di mercato più posizione finanziaria netta) e margine operativo lordo; - EV/EBIT: rapporto tra Enterprise Value e reddito operativo; - Price/earning (P/E): rapporto tra prezzo dell'azione e utile netto per azione; - EV/OFCF: rapporto tra Enterprise Value e flusso di cassa operativo; - EV/Sales: rapporto tra Enterprise Value e fatturato dell'azienda. I multipli costruiti utilizzando grandezze contabili più influenzate da politiche di bilancio e fiscali sono soggetti al rischio di distorsione e possono condurre a risultati fuorvianti; fra tutti, il P/E risente maggiormente di tali fattori (oltre a risentire del diverso livello d'indebitamento). Per questa ragione, nella prassi vengono effettuate alcune rettifiche e normalizzazioni o in alternativa si ricorre a multipli calcolati con poste meno discrezionali (ad esempio, EV/ EBITDA rispetto a EV/EBIT). L'utilizzo dell'EV/Sales, invece, è sempre meno frequente ed è confinato a casi di società con margini negativi o in fase di turnaround.
III) Calcolo dei multipli prescelti per le società rappresentate nel campione. In genere i multipli vengono calcolati sulla base dei dati finanziari dell'anno corrente e di quello successivo, tuttavia è possibile scegliere periodi temporali diversi, in funzione della specifica realtà aziendale e del contesto di valutazione.
IV) Identificazione dell'intervallo di valori dei multipli da applicare alla società oggetto di valutazione. La scelta dell'intervallo da applicare avviene in base a considerazioni qualitative e quantitative circa la comparabilità delle società che compongono il campione.
V) Applicazione dei multipli. I ratio così ottenuti sono applicati alle quantità economiche, patrimoniali e finanziarie della società oggetto di valutazione, al fine di determinare un intervallo di valori.

147 Vedasi par. 4.3.1.

148 OPV, acronimo di Offerta Pubblica di Vendita, con questa scelta il Consiglio di Amministrazione della società che ha deciso di quotarsi in Borsa mette in vendita una parte della proprietà mediante il rilascio sul mercato di quote azionarie societarie già esistenti, ossia che non devono essere emesse per l'occasione. L**'**OPV è una modalità piuttosto diffusa come ingresso sui mercati regolamentati dal momento che i ricavati dalla vendita non vengono trasferiti nelle casse della società ma sono destinati agli azionisti venditori. Questa soluzione trova applicazione soprattutto nella privatizzazione delle aziende pubbliche, con le risorse raccolte in fase di quotazione della società che vengono destinate alle casse statali.

149 OPS, acronimo di Offerta Pubblica di Sottoscrizione**,** con questa modalità di quotazione in Borsa il Consiglio di Amministrazione sceglie di collocare sul mercato azioni di nuova emissione. In questo modo a trarre

La durata dell'offerta al pubblico è, generalmente, compresa tra un minimo di due e un massimo di quattro giorni, alla chiusura della stessa si effettua il pagamento e la consegna dei titoli, tramite il deposito presso Monte Titoli[150].

L'offerta al pubblico, in quanto sollecitazione all'investimento, deve essere condotta nel rispetto delle norme previste dal TUF, al capo I del titolo II della parte IV (Offerta al pubblico di sottoscrizione e vendita), e titolo I (Offerta al pubblico di sottoscrizione e vendita di prodotti finanziari) del Regolamento Emittenti, che prevedono la consegna al pubblico del prospetto informativo il cui contenuto sia stato preventivamente approvato da Consob; pertanto il prospetto di quotazione dovrà contenere anche gli elementi richiesti da Consob ai fini della sollecitazione, in particolare i dati relativi al prezzo e alle modalità di determinazione dello stesso. Nei cinque giorni successivi alla conclusione del periodo di adesione, il responsabile del collocamento pubblica i risultati della stessa, con le stesse modalità utilizzate per il prospetto.

Copia del relativo avviso è trasmessa a Consob e Borsa Italiana.

Il consuntivo dei risultati dell'offerta viene comunicato dall'Emittente (o dallo sponsor) entro il giorno di borsa aperta successivo alla data fissata per la chiusura della stessa.

4.3.5 Inizio negoziazioni e Stabilizzazione

Il procedimento di quotazione si conclude con l'inizio delle "negoziazioni ufficiali"[151] nel comparto o segmento prescelto.

L'inizio delle negoziazioni rileva anche ai fini della determinazione del prezzo di mercato.

Nei trenta giorni successivi a quello di inizio delle negoziazioni ufficiali (periodo di stabilizzazione del titolo), il consorzio di collocamento può intervenire sul mercato a sostegno del titolo.

---

beneficio sono le casse societarie nelle quali arrivano nuovi capitali da usare per investimenti e/o esigenze patrimoniali senza la necessità di pagare interessi sul capitale raccolto. Su quanto raccolto sul mercato i soci non hanno nessun diritto di acquisizione prioritaria. Con l'OPS si vuole aumentare il capitale di rischio dell'impresa senza chiedere sacrifici economici ai soci già in essere. A differenza dell'OPV, l'OPS porta a un effettivo aumento del capitale sociale.

[150] Glossario Borsa Italiana, Monte Titoli è una società multifunzionale di post-trading che offre servizi di gestione accentrata, di liquidazione, di regolamento e accessori ed è uno dei principali sistemi europei di regolamento titoli. Lo svolgimento di tali funzioni è effettuato in forma di impresa, sotto la vigilanza della Banca d'Italia e della Consob. Costituita nel 1978, Monte Titoli S.p.A. è dal 1986 il depositario centrale nazionale per tutti gli strumenti finanziari di diritto italiano, oggi accentrati presso la Società in forma quasi esclusivamente dematerializzata. Ciò significa che qualsiasi tipo di strumento finanziario, italiano o estero, rappresentato da titoli può essere accentrato in Monte Titoli e regolato a mezzo di scritture contabili senza alcuna movimentazione fisica dei titoli stessi. A partire dal 1989, Monte Titoli ha anche assunto il ruolo di sistema di regolamento dei saldi finali in titoli e dal 2003 gestisce Express II, la piattaforma di clearing e settlement che ha integrato in un unico ambiente i processi di liquidazione su base netta e su base lorda.

[151] Quelle sul segmento di borsa prescelto.

L'attività di stabilizzazione può essere facilitata riconoscendo al Global Coordinator due opzioni:

- Over-allotment/greenshoe option[152], ossia la facoltà riconosciuta al global coordinator di assegnare un quantitativo di azioni superiore a quello oggetto di offerta;
- Share lending option, la facoltà di chiedere in prestito un quantitativo di titoli.

L'attività di stabilizzazione[153] è esentata dall'applicazione delle disposizioni in materia di abuso di informazioni privilegiate e manipolazione di mercato, a condizioni che sia data comunicazione al pubblico di talune informazioni sulla medesima, per esempio il possibile esercizio della greenshoe option.

---

[152] www.borsaitaliana.it/lagreenshoe, L'opzione, che ha normalmente una durata di trenta giorni, è normalmente concessa da parte degli azionisti della società, che si rendono disponibili ad incrementare il numero di azioni poste in vendita, riducendo così la propria quota di partecipazione. L'esercizio della greenshoe - se necessario - non è deciso dalla società emittente, ma dai responsabili del consorzio di collocamento. L'opzione viene esercitata quando la domanda di titoli sul mercato in tale periodo è superiore all'offerta e quindi il prezzo del titolo tende a crescere al di sopra del prezzo di sottoscrizione. Se quindi l'IPO ha successo ed i titoli sono apprezzati dagli investitori, i membri del consorzio di collocamento chiederanno l'esercizio dell'opzione, la società collocherà un maggior numero di azioni e la struttura azionaria dell'emittente verrà modificata di conseguenza, incrementando il numero di titoli sul mercato e, di conseguenza, il flottante del titolo. Da questo punto di vista, l'esercizio della greenshoe rappresenta un'ulteriore modalità di remunerazione dei collocatori, poiché i ricavi dell'operazione dipendono dal numero complessivo di titoli collocati sul mercato. Nel caso in cui invece il titolo scendesse di prezzo rispetto al collocamento, i titoli necessari per "coprire" l'over allotment verranno acquistati dai componenti del consorzio di collocamento sul mercato (realizzando così un guadagno da trading, visto che i titoli dell'overallotment sono stati ceduti in collocamento al prezzo di offerta e sono stati riacquistati sul mercato a un prezzo inferiore). In queste condizioni il meccanismo della greenshoe e dell'over allotment hanno quindi lo scopo di stabilizzare il prezzo di titoli nei primi giorni di quotazione. In caso di scarsa domanda i collocatori acquisteranno titoli per coprire l'over allotment, e tali acquisti possono contribuire ad evitare eccessivi deprezzamenti. Solitamente la quantità di azioni riservata alla green shoe non supera il 15% dell'offerta globale. Questa soglia non è stabilita a livello normativo, ma si tratta di una pratica diffusa. Malgrado i collocatori dovrebbero desiderare la "fetta" più grande possibile in modo da intascare lauti guadagni in conto capitale in caso di apprezzamento dei titoli, una percentuale maggiore del 15% potrebbe non essere positivamente accolta sul mercato poiché potrebbe implicare il collocamento sul mercato di un quantitativo eccessivo di titoli rispetto alla domanda effettiva, penalizzando il risultato complessivo dell'operazione.

[153] Attività finalizzata a limitare le fluttuazioni di prezzo dei titoli sul mercato secondario nel periodo successivo la chiusura di un'offerta di vendita e/o sottoscrizione avente ad oggetto tali titoli. La Consob ha stabilito che la società oppure i membri dei consorzi di collocamento oppure il Global Coordinator possono procedere alla stabilizzazione qualora, nel periodo immediatamente successivo un'offerta di vendita o di sottoscrizione, il titolo oggetto dell'offerta subisca elevate oscillazioni di prezzo. Nel periodo fra i quindici giorni antecedenti l'inizio dell'offerta e i trenta successivi alla chiusura la stabilizzazione è soggetta a restrizioni; infatti essa può essere effettuata solo sui mercati regolamentati a condizione che non influenzi sensibilmente la quotazione del titolo e che sia data opportuna conoscenza al mercato con apposito comunicato stampa.

5
Fase post - IPO

5.1 Obblighi società quotata

Una volta concluso il processo di quotazione, l'Emittente deve conformarsi ad un insieme di regole e comportamenti che mirano a garantire la correttezza dell'andamento del titolo.

Il rispetto di queste regole e comportamenti accresce infatti la trasparenza e il controllo sulle attività della società da parte degli azionisti di minoranza e del pubblico in generale.

A questo riguardo, l'Emittente sarà tenuta ad adottare modelli di gestione e comportamento (cosiddetto *corporate governance*) e a rispettare taluni obblighi di informativa nei confronti del pubblico.

5.1.1 Corporate governance

"La corporate governance è l'insieme dei processi istituiti dalla società per un'efficiente e corretta direzione dell'azienda e controllo della stessa, conformemente a principi di etica, responsabilità e impegno, con lo scopo di garantire un trattamento equo a tutti gli azionisti, chiarezza e trasparenza dei ruoli e delle responsabilità del management"[154].

Borsa Italiana ha promosso tra le società quotate e i soggetti interessati (inclusi gli investitori istituzionali) la costituzione di un comitato per la corporate governance che ha redatto un Codice di Autodisciplina[155], che rappresenta "un modello di organizzazione societaria adeguato a gestire il corretto controllo dei rischi d'impresa e i potenziali conflitti di interesse. I codici di disciplina "hanno il pregio di indurre comportamenti virtuosi attraverso l'adozione spontanea, anziché con la rigidità dell'imposizione normativa"[156].

L'adesione al Codice, che negli anni è stato aggiornato in base a nuove esigenze, derivanti da una accresciuta consapevolezza e maturità degli interessati, dall'evoluzione della cosiddetta best-practice e dalle modifiche normative e regolamentari, resta volontaria da parte di ciascun Emittente, anche se è divenuto obbligatorio informare annualmente il mercato, con una apposita relazione, sulla propria adesione al Codice, descrivendo quali raccomandazioni dello stesso siano applicate e quali no, e in tal caso quali ne siano i motivi. L'inosservanza è punita

---

154 www.economiauniparthenope.it/icostidellaquotazione.

155 Vedasi nota 103.

156 Paolo Montalenti, *Trattato di Diritto Commerciale*, La Società Quotata, IV volume, Padova, CEDAM, 2004, pag. 19.

con sanzione amministrativa pecuniaria. Per ciascuno degli Articoli, il Codice evidenzia i principi ispiratori e taluni criteri applicativi, oltre ad un commento, che contiene una serie di indicazioni di cui le società dovrebbero comunque tener conto.

Il Codice contiene articoli destinati principalmente:

- al ruolo (art. 1[157]) e alla composizione del Consiglio di Amministrazione (art. 2[158]) , che è

[157] Art. 1: Ruolo del consiglio di amministrazione, Principi: 1.P.1. L'emittente è guidato da un consiglio di amministrazione che si riunisce con regolare cadenza e che si organizza e opera in modo da garantire un efficace svolgimento delle proprie funzioni. 1.P.2. Gli amministratori agiscono e deliberano con cognizione di causa e in autonomia, perseguendo l'obiettivo prioritario della creazione di valore per gli azionisti in un orizzonte di medio-lungo periodo.
Criteri applicativi: 1.C.1. Il consiglio di amministrazione:

a) esamina e approva i piani strategici, industriali e finanziari dell'emittente e del gruppo di cui esso sia a capo, monitorandone periodicamente l'attuazione; definisce il sistema di governo societario dell'emittente e la struttura del gruppo;
b) definisce la natura e il livello di rischio compatibile con gli obiettivi strategici dell'emittente, includendo nelle proprie valutazioni tutti i rischi che possono assumere rilievo nell'ottica della sostenibilità nel medio-lungo periodo dell'attività dell'emittente;
c) valuta l'adeguatezza dell'assetto organizzativo, amministrativo e contabile dell'emittente nonché quello delle controllate aventi rilevanza strategica, con particolare riferimento al sistema di controllo interno e di gestione dei rischi;
d) stabilisce la periodicità, comunque non superiore al trimestre, con la quale gli organi delegati devono riferire al consiglio circa l'attività svolta nell'esercizio delle deleghe loro conferite;
e) valuta il generale andamento della gestione, tenendo in considerazione, in particolare, le informazioni ricevute dagli organi delegati, nonché confrontando, periodicamente, i risultati conseguiti con quelli programmati;
f) delibera in merito alle operazioni dell'emittente e delle sue controllate, quando tali operazioni abbiano un significativo rilievo strategico, economico, patrimoniale o finanziario per l'emittente stesso; a tal fine stabilisce criteri generali per individuare le operazioni di significativo rilievo;
g) effettua, almeno una volta all'anno, una valutazione sul funzionamento del consiglio stesso e dei suoi comitati nonché sulla loro dimensione e composizione, tenendo anche conto di elementi quali le caratteristiche professionali, di esperienza, anche manageriale, e di genere dei suoi componenti, nonché della loro anzianità di carica. Nel caso in cui il consiglio di amministrazione si avvalga dell'opera di consulenti esterni ai fini dell'autovalutazione, la relazione sul governo societario fornisce informazioni sull'identità di tali consulenti e sugli eventuali ulteriori servizi 7 da essi forniti all'emittente o a società in rapporto di controllo con lo stesso;
h) tenuto conto degli esiti della valutazione di cui alla lettera g), esprime agli azionisti, prima della nomina del nuovo consiglio, orientamenti sulle figure manageriali e professionali, la cui presenza in consiglio sia ritenuta opportuna;
i) fornisce informativa nella relazione sul governo societario: (1) sulla propria composizione, indicando per ciascun componente la qualifica (esecutivo, non esecutivo, indipendente), il ruolo ricoperto all'interno del consiglio (ad esempio presidente o chief executive officer, come definito nell'articolo 2), le principali caratteristiche professionali nonché l'anzianità di carica dalla prima nomina; (2) sulle modalità di applicazione del presente articolo 1 e, in particolare, sul numero e sulla durata media delle riunioni del consiglio e del comitato esecutivo, ove presente, tenutesi nel corso dell'esercizio nonché sulla relativa percentuale di partecipazione di ciascun amministratore; (3) sulle modalità di svolgimento del processo di valutazione di cui alla precedente lettera g);
j) al fine di assicurare la corretta gestione delle informazioni societarie, adotta, su proposta dell'amministratore delegato o del presidente del consiglio di amministrazione, una procedura per la gestione interna e la comunicazione all'esterno di documenti e informazioni riguardanti l'emittente, con particolare riferimento alle informazioni privilegiate. 1.C.2. Gli amministratori accettano la carica quando ritengono di poter dedicare allo svolgimento diligente dei loro compiti il tempo necessario, anche tenendo conto dell'impegno connesso alle proprie attività lavorative e professionali, del numero di cariche di amministratore o sindaco da essi ricoperte in altre società quotate in mercati regolamentati (anche esteri),

in società finanziarie, bancarie, assicurative o di rilevanti dimensioni. Il consiglio, sulla base delle informazioni ricevute dagli amministratori, rileva annualmente e rende note nella relazione sul governo societario le cariche di amministratore o sindaco ricoperte dai consiglieri nelle predette società. 1.C.3. Il consiglio esprime il proprio orientamento in merito al numero massimo di incarichi di amministratore o sindaco nelle società di cui al paragrafo precedente che possa essere considerato compatibile con un efficace svolgimento dell'incarico di amministratore dell'emittente, tenendo conto della partecipazione dei consiglieri ai comitati costituiti all'interno del consiglio. A tal fine individua criteri generali differenziati in ragione dell'impegno connesso a ciascun ruolo (di consigliere esecutivo, non esecutivo o indipendente), anche in relazione alla natura e alle dimensioni delle società in cui gli incarichi sono ricoperti nonché alla loro eventuale appartenenza al gruppo dell'emittente. 1.C.4. Qualora l'assemblea, per far fronte ad esigenze di carattere organizzativo, autorizzi in via generale e preventiva deroghe al divieto di concorrenza previsto dall'art. 2390 cod. civ., il consiglio di amministrazione valuta nel merito ciascuna fattispecie problematica e segnala alla prima assemblea utile eventuali criticità. A tal fine, ciascun amministratore informa il consiglio, all'atto dell'accettazione della nomina, di eventuali attività 8 esercitate in concorrenza con l'emittente e, successivamente, di ogni modifica rilevante. 1.C.5. Il presidente del consiglio di amministrazione si adopera affinché la documentazione relativa agli argomenti all'ordine del giorno sia portata a conoscenza degli amministratori e dei sindaci con congruo anticipo rispetto alla data della riunione consiliare. Il consiglio fornisce nella relazione sul governo societario informazioni sulla tempestività e completezza dell'informativa pre-consiliare, fornendo indicazioni, tra l'altro, in merito al preavviso ritenuto generalmente congruo per l'invio della documentazione e indicando se tale termine sia stato normalmente rispettato. 1.C.6. Il presidente del consiglio di amministrazione, anche su richiesta di uno o più amministratori, può chiedere agli amministratori delegati che i dirigenti dell'emittente e quelli delle società del gruppo che ad esso fa capo, responsabili delle funzioni aziendali competenti secondo la materia, intervengano alle riunioni consiliari per fornire gli opportuni approfondimenti sugli argomenti posti all'ordine del giorno. La relazione sul governo societario fornisce informazioni sulla loro effettiva partecipazione.

[158] Art. 2: Composizione del consiglio di amministrazione, Principi 2.P.1. Il consiglio di amministrazione è composto da amministratori esecutivi e non esecutivi, dotati di adeguata competenza e professionalità. 2.P.2. Gli amministratori non esecutivi apportano le loro specifiche competenze alle discussioni consiliari, contribuendo all'assunzione di decisioni consapevoli e prestando particolare cura alle aree in cui possono manifestarsi conflitti di interesse. 2.P.3. Il numero, la competenza, l'autorevolezza e la disponibilità di tempo degli amministratori non esecutivi sono tali da garantire che il loro giudizio possa avere un peso significativo nell'assunzione delle decisioni consiliari. 2.P.4. È opportuno evitare la concentrazione di cariche sociali in una sola persona. 2.P.5. Il consiglio di amministrazione, allorché abbia conferito deleghe gestionali al presidente, fornisce adeguata informativa nella relazione sul governo societario in merito alle ragioni di tale scelta organizzativa.

Criteri applicativi, 2.C.1. Sono qualificati amministratori esecutivi dell'emittente: - gli amministratori delegati dell'emittente o di una società controllata avente rilevanza strategica, ivi compresi i relativi presidenti quando ad essi vengano attribuite deleghe individuali di gestione o quando essi abbiano uno specifico ruolo nell'elaborazione delle strategie aziendali; - gli amministratori che ricoprono incarichi direttivi nell'emittente o in una società controllata avente rilevanza strategica, ovvero nella società controllante quando l'incarico riguardi anche l'emittente; - gli amministratori che fanno parte del comitato esecutivo dell'emittente, quando manchi l'identificazione di un amministratore delegato o quando la partecipazione al comitato esecutivo, tenuto conto della frequenza delle riunioni e dell'oggetto delle relative delibere, comporti, di fatto, il coinvolgimento sistematico dei suoi componenti nella gestione corrente dell'emittente. L'attribuzione di poteri vicari o per i soli casi di urgenza ad amministratori non muniti di deleghe gestionali non vale, di per sé, a configurarli come amministratori esecutivi, salvo che tali poteri siano, di fatto, utilizzati con notevole frequenza. 2.C.2. Gli amministratori sono tenuti a conoscere i compiti e le responsabilità inerenti alla carica. Il presidente del consiglio di amministrazione cura che gli amministratori e i sindaci possano partecipare, successivamente alla nomina e durante il mandato, nelle forme più opportune, a iniziative finalizzate a fornire loro un'adeguata conoscenza del settore di attività in cui opera l'emittente, delle 12 dinamiche aziendali e della loro evoluzione, dei principi di corretta gestione dei rischi nonché del quadro normativo e autoregolamentare di riferimento. L'emittente riporta nella relazione sul governo societario la tipologia e le modalità organizzative delle iniziative che hanno avuto luogo durante l'esercizio di riferimento. 2.C.3. Il consiglio di amministrazione designa un amministratore indipendente quale lead independent director, nei seguenti casi: (i) se il presidente del consiglio di amministrazione è il principale responsabile della gestione dell'impresa (chief executive officer); (ii) se la carica di presidente è ricoperta dalla persona che controlla l'emittente. Il

l'organo responsabile della scelta e del perseguimento degli obiettivi della società, e dei cui membri va garantita l'indipendenza di giudizio, evitando concentrazioni di cariche e attribuendo sempre maggiore attenzione al ruolo degli amministratori indipendenti (art. 3[159]);

- al trattamento delle informazioni societarie, per le quali deve essere garantita la riservatezza, una gestione corretta e modalità di divulgazione all'esterno in conformità alle norme;
- all'istituzione di comitati interni al Consiglio di Amministrazione (art. 4[160]), al fine di

---

consiglio di amministrazione degli emittenti appartenenti all'indice FTSEMib designa un lead independent director se ciò è richiesto dalla maggioranza degli amministratori indipendenti, salvo diversa e motivata valutazione da parte del consiglio da rendere nota nell'ambito della relazione sul governo societario. 2.C.4. Il lead independent director: a) rappresenta un punto di riferimento e di coordinamento delle istanze e dei contributi degli amministratori non esecutivi e, in particolare, di quelli che sono indipendenti ai sensi del successivo articolo 3; b) collabora con il presidente del consiglio di amministrazione al fine di garantire che gli amministratori siano destinatari di flussi informativi completi e tempestivi. 2.C.5. Il chief executive officer di un emittente (A) non assume l'incarico di amministratore di un altro emittente (B) non appartenente allo stesso gruppo, di cui sia chief executive officer un amministratore dell'emittente (A).

159 Art. 3: Amministratori indipendenti, Principi 3.P.1. Un numero adeguato di amministratori non esecutivi sono indipendenti, nel senso che non intrattengono, né hanno di recente intrattenuto, neppure indirettamente, con l'emittente o con soggetti legati all'emittente, relazioni tali da condizionarne attualmente l'autonomia di giudizio. 3.P.2. L'indipendenza degli amministratori è valutata dal consiglio di amministrazione dopo la nomina e, successivamente, con cadenza annuale. L'esito delle valutazioni del consiglio è comunicato al mercato.

160 Art. 4: Istituzione e funzionamento dei comitati interni al consiglio di amministrazione, Principi 4.P.1. Il consiglio di amministrazione istituisce al proprio interno uno o più comitati con funzioni propositive e consultive secondo quanto indicato nei successivi articoli.
Criteri applicativi, 4.C.1. L'istituzione e il funzionamento dei comitati previsti dal Codice rispondono ai seguenti criteri: a) i comitati sono composti da non meno di tre membri. Tuttavia, negli emittenti il cui consiglio di amministrazione è composto da non più di otto membri, i comitati possono essere composti da due soli consiglieri, purché indipendenti. I lavori dei comitati sono coordinati da un presidente; b) i compiti dei singoli comitati sono stabiliti con la deliberazione con cui sono costituiti e possono essere integrati o modificati con successiva deliberazione del consiglio di amministrazione; c) le funzioni che il Codice attribuisce a diversi comitati possono essere distribuite in modo differente o demandate ad un numero di comitati inferiore a quello previsto, purché si rispettino le regole per la composizione di volta in volta indicate dal Codice e si garantisca il raggiungimento degli obiettivi sottostanti; d) le riunioni di ciascun comitato sono verbalizzate e il presidente del comitato ne dà informazione al primo consiglio di amministrazione utile; e) nello svolgimento delle proprie funzioni, i comitati hanno la facoltà di accedere alle informazioni e alle funzioni aziendali necessarie per lo svolgimento dei loro compiti nonché di avvalersi di consulenti esterni, nei termini stabiliti dal consiglio di amministrazione. L'emittente mette a disposizione dei comitati risorse finanziarie adeguate per l'adempimento dei propri compiti, nei limiti del budget approvato dal consiglio; f) alle riunioni di ciascun comitato possono partecipare soggetti che non ne sono membri, inclusi altri componenti del consiglio o della struttura dell'emittente, su invito del comitato stesso, con riferimento a singoli punti all'ordine del giorno; g) l'emittente fornisce adeguata informativa, nell'ambito della relazione sul governo societario, sull'istituzione e sulla composizione dei comitati, sul contenuto dell'incarico ad essi conferito nonché, in base alle indicazioni fornite da ogni comitato, sull'attività effettivamente svolta nel corso dell'esercizio, sul numero e sulla durata media delle riunioni tenutesi e sulla relativa percentuale di partecipazione di ciascun membro. 4.C.2. L'istituzione di uno o più comitati può essere evitata riservando le relative funzioni all'intero consiglio, sotto il coordinamento del presidente e alle seguenti condizioni: (i) gli amministratori indipendenti rappresentino almeno 20 la metà del consiglio di amministrazione, con arrotondamento all'unità inferiore qualora il consiglio sia formato da un numero dispari di persone; (ii) all'espletamento delle funzioni che il Codice attribuisce ai comitati medesimi siano dedicati, all'interno delle sedute consiliari, adeguati spazi, dei quali venga dato conto nella relazione sul governo societario; (iii) limitatamente al comitato controllo e rischi, l'emittente non sia controllato da un'altra società quotata, o sottoposto a direzione e coordinamento. Il consiglio di amministrazione illustra analiticamente nella relazione sul governo societario i motivi sottesi alla scelta di non istituire uno o più comitati; in particolare, motiva

garantire maggiore efficienza all'attività del Consiglio; si raccomanda l'istituzione di un comitato per la remunerazione, di un comitato per il controllo interno e per le nomine;

- alla nomina degli amministratori (art. 5[161]), che deve avvenire con le procedure più trasparenti possibili anche grazie alla costituzione di un comitato per le nomine, costituito per lo più da amministratori indipendenti;
- alla remunerazione dei consiglieri (art. 6[162]), che deve essere sufficiente a motivare

---

adeguatamente la scelta di non istituire il comitato controllo e rischi in relazione al grado di complessità dell'emittente e al settore in cui esso opera. Inoltre il consiglio procede periodicamente a rivalutare la scelta effettuata.

[161] Art. 5: Nomina degli amministratori, Principi 5.P.1. Il consiglio di amministrazione costituisce al proprio interno un comitato per le nomine, composto, in maggioranza, da amministratori indipendenti.
Criteri applicativi, 5.C.1. Il comitato per le nomine è investito delle seguenti funzioni: a) formulare pareri al consiglio di amministrazione in merito alla dimensione e alla composizione dello stesso ed esprimere raccomandazioni in merito alle figure professionali la cui presenza all'interno del consiglio sia ritenuta opportuna nonché sugli argomenti di cui agli artt. 1.C.3 e 1.C.4; b) proporre al consiglio di amministrazione candidati alla carica di amministratore nei casi di cooptazione, ove occorra sostituire amministratori indipendenti. 5.C.2. Il consiglio di amministrazione valuta se adottare un piano per la successione degli amministratori esecutivi. Nel caso in cui abbia adottato tale piano, l'emittente ne dà informativa nella relazione sul governo societario. L'istruttoria sulla predisposizione del piano è effettuata dal comitato per le nomine o da altro comitato interno al consiglio a ciò preposto.

[162] Art. 6: Remunerazione degli amministratori, Principi 6.P.1. La remunerazione degli amministratori e dei dirigenti con responsabilità strategiche è stabilita in misura sufficiente ad attrarre, trattenere e motivare persone dotate delle qualità professionali richieste per gestire con successo l'emittente. 6.P.2. La remunerazione degli amministratori esecutivi e dei dirigenti con responsabilità strategiche è definita in modo tale da allineare i loro interessi con il perseguimento dell'obiettivo prioritario della creazione di valore per gli azionisti in un orizzonte di medio-lungo periodo. Per gli amministratori che sono destinatari di deleghe gestionali o che svolgono, anche solo di fatto, funzioni attinenti alla gestione dell'impresa nonché per i dirigenti con responsabilità strategiche, una parte significativa della remunerazione è legata al raggiungimento di specifici obiettivi di performance, anche di natura non economica, preventivamente indicati e determinati in coerenza con le linee guida contenute nella politica di cui al successivo principio 6.P.4. La remunerazione degli amministratori non esecutivi è commisurata all'impegno richiesto a ciascuno di essi, tenuto anche conto dell'eventuale partecipazione ad uno o più comitati. 6.P.3. Il consiglio di amministrazione costituisce al proprio interno un comitato per la remunerazione, composto da amministratori indipendenti. In alternativa, il comitato può essere composto da amministratori non esecutivi, in maggioranza indipendenti; in tal caso, il presidente del comitato è scelto tra gli amministratori indipendenti. Almeno un componente del comitato possiede una adeguata conoscenza ed esperienza in materia finanziaria o di politiche retributive, da valutarsi dal consiglio di amministrazione al momento della nomina. 6.P.4. Il consiglio di amministrazione, su proposta del comitato per la remunerazione, definisce una politica per la remunerazione degli amministratori e dei dirigenti con responsabilità strategiche. 6.P.5. L'emittente, in occasione della cessazione dalla carica e/o dello scioglimento del rapporto con un amministratore esecutivo o un direttore generale, rende note, ad esito dei processi interni che conducono all'attribuzione o al riconoscimento di indennità e/o altri benefici, informazioni dettagliate in merito, mediante un comunicato diffuso al mercato.
Criteri applicativi, 6.C.1. La politica per la remunerazione degli amministratori esecutivi o investiti di particolari cariche definisce linee guida con riferimento alle tematiche e in coerenza con i criteri di seguito indicati: a) la componente fissa e la componente variabile sono adeguatamente bilanciate in funzione degli obiettivi strategici e della politica di gestione dei rischi dell'emittente, tenuto anche conto del settore di attività in cui 25 esso opera e delle caratteristiche dell'attività d'impresa concretamente svolta; b) sono previsti limiti massimi per le componenti variabili; c) la componente fissa è sufficiente a remunerare la prestazione dell'amministratore nel caso in cui la componente variabile non fosse erogata a causa del mancato raggiungimento degli obiettivi di performance indicati dal consiglio di amministrazione; d) gli obiettivi di performance - ovvero i risultati economici e gli eventuali altri obiettivi specifici cui è collegata l'erogazione delle componenti variabili (ivi compresi gli obiettivi definiti per i piani di remunerazione basati su azioni) -

l'attività dei consiglieri a favore dell'Emittente, e, per quelli esecutivi, va anche ancorata

---

sono predeterminati, misurabili e collegati alla creazione di valore per gli azionisti in un orizzonte di medio-lungo periodo; e) la corresponsione di una porzione rilevante della componente variabile della remunerazione è differita di un adeguato lasso temporale rispetto al momento della maturazione; la misura di tale porzione e la durata del differimento sono coerenti con le caratteristiche dell'attività d'impresa svolta e con i connessi profili di rischio; f) sono previste intese contrattuali che consentono alla società di chiedere la restituzione, in tutto o in parte, di componenti variabili della remunerazione versate (o di trattenere somme oggetto di differimento), determinate sulla base di dati che si siano rivelati in seguito manifestamente errati; g) l'indennità eventualmente prevista per la cessazione del rapporto di amministrazione è definita in modo tale che il suo ammontare complessivo non superi un determinato importo o un determinato numero di anni di remunerazione. Tale indennità non è corrisposta se la cessazione del rapporto è dovuta al raggiungimento di risultati obiettivamente inadeguati. 6.C.2. Nel predisporre piani di remunerazione basati su azioni, il consiglio di amministrazione assicura che: a) le azioni, le opzioni e ogni altro diritto assegnato agli amministratori di acquistare azioni o di essere remunerati sulla base dell'andamento del prezzo delle azioni abbiano un periodo medio di vesting pari ad almeno tre anni; b) il vesting di cui al punto a) sia soggetto a obiettivi di performance predeterminati e misurabili; c) gli amministratori mantengano sino al termine del mandato una quota delle azioni assegnate o acquistate attraverso l'esercizio dei diritti di cui al punto a). 6.C.3. I criteri 6.C.1 e 6.C.2 si applicano, in quanto compatibili, anche alla determinazione - da parte degli organi a ciò delegati - della remunerazione dei dirigenti con responsabilità strategiche. I meccanismi di incentivazione del responsabile della funzione di internal audit e del dirigente preposto alla redazione dei documenti contabili societari sono coerenti con i compiti ad essi assegnati. 6.C.4. La remunerazione degli amministratori non esecutivi non è - se non per una parte non significativa - legata ai risultati economici conseguiti dall'emittente. Gli amministratori non esecutivi non sono destinatari di piani di remunerazione basati su azioni, salvo motivata decisione dell'assemblea dei soci. 6.C.5. Il comitato per la remunerazione: - valuta periodicamente l'adeguatezza, la coerenza complessiva e la concreta applicazione della politica per la remunerazione degli amministratori e dei dirigenti con responsabilità strategiche, avvalendosi a tale ultimo riguardo delle informazioni fornite dagli amministratori delegati; formula al consiglio di amministrazione proposte in materia; - presenta proposte o esprime pareri al consiglio di amministrazione sulla remunerazione degli amministratori esecutivi e degli altri amministratori che ricoprono particolari cariche nonché sulla fissazione degli obiettivi di performance correlati alla componente variabile di tale remunerazione; monitora l'applicazione delle decisioni adottate dal consiglio stesso verificando, in particolare, l'effettivo raggiungimento degli obiettivi di performance. 6.C.6. Nessun amministratore prende parte alle riunioni del comitato per la remunerazione in cui vengono formulate le proposte al consiglio di amministrazione relative alla propria remunerazione. 6.C.7. Qualora intenda avvalersi dei servizi di un consulente al fine di ottenere informazioni sulle pratiche di mercato in materia di politiche retributive, il comitato per le remunerazioni verifica preventivamente che esso non si trovi in situazioni che ne compromettano l'indipendenza di giudizio. 6.C.8. La comunicazione al mercato di cui al principio 6.P.5 comprende: a) adeguate informazioni sull'indennità e/o altri benefici, incluso il relativo ammontare, la tempistica di erogazione - distinguendo la parte corrisposta immediatamente da quella eventualmente soggetta a meccanismi di differimento e distinguendo altresì le componenti attribuite in forza della carica di amministratore da quelle relative a eventuali rapporti di lavoro dipendente - ed eventuali clausole di restituzione, con particolare riferimento a: - indennità di fine carica o di cessazione del rapporto di lavoro, specificando la fattispecie che ne giustifica la maturazione (ad esempio, per scadenza dalla carica, revoca dalla medesima o accordo transattivo); - mantenimento dei diritti connessi ad eventuali piani di incentivazione monetaria o basati su strumenti finanziari; - benefici (monetari o non monetari) successivi alla cessazione dalla carica; - impegni di non concorrenza, descrivendone i principali contenuti; - ogni altro compenso attribuito a qualsiasi titolo e in qualsiasi forma; 27 b) informazioni circa la conformità o meno dell'indennità e/o degli altri benefici alle indicazioni contenute nella politica per la remunerazione, nel caso di difformità anche parziale rispetto alle indicazioni della politica medesima, informazioni sulle procedure deliberative seguite in applicazione della disciplina Consob in materia di operazioni con parti correlate; c) indicazioni circa l'applicazione, o meno, di eventuali meccanismi che pongono vincoli o correttivi alla corresponsione dell'indennità nel caso in cui la cessazione del rapporto sia dovuta al raggiungimento di risultati obiettivamente inadeguati, nonché circa l'eventuale formulazione di richieste di restituzione di compensi già corrisposti; d) informazione circa il fatto che la sostituzione dell'amministratore esecutivo o del direttore generale cessato è regolata da un piano per la successione eventualmente adottato dalla società e, in ogni caso, indicazioni in merito alle procedure che sono state o saranno seguite nella sostituzione dell'amministratore o del direttore.

all'obiettivo della creazione di valore per l'azienda in un orizzonte temporale di medio periodo, fissandone obiettivi e criteri di valutazione;

- al sistema di controllo interno (art. 7[163]), che consente di meglio misurare, gestire e

[163] Art. 7: Sistema di controllo interno e di gestione dei rischi, Principi 7.P.1. Ogni emittente si dota di un sistema di controllo interno e di gestione dei rischi costituito dall'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi. Tale sistema è integrato nei più generali assetti organizzativi e di governo societario adottati dall'emittente e tiene in adeguata considerazione i modelli di riferimento e le best practices esistenti in ambito nazionale e internazionale. 7.P.2. Un efficace sistema di controllo interno e di gestione dei rischi contribuisce a una conduzione dell'impresa coerente con gli obiettivi aziendali definiti dal consiglio di amministrazione, favorendo l'assunzione di decisioni consapevoli. Esso concorre ad assicurare la salvaguardia del patrimonio sociale, l'efficienza e l'efficacia dei processi aziendali, l'affidabilità delle informazioni fornite agli organi sociali ed al mercato, il rispetto di leggi e regolamenti nonché dello statuto sociale e delle procedure interne. 7.P.3. Il sistema di controllo interno e di gestione dei rischi coinvolge, ciascuno per le proprie competenze: a) il consiglio di amministrazione, che svolge un ruolo di indirizzo e di valutazione dell'adeguatezza del sistema e individua al suo interno: (i) uno o più amministratori, incaricati dell'istituzione e del mantenimento di un efficace sistema di controllo interno e di gestione dei rischi (nel seguito dell'articolo 7, l'"amministratore incaricato del sistema di controllo interno e di gestione dei rischi"), nonché (ii) un comitato controllo e rischi, avente le caratteristiche indicate nel principio 7.P.4, con il compito di supportare, con un'adeguata attività istruttoria, le valutazioni e le decisioni del consiglio di amministrazione relative al sistema di controllo interno e di gestione dei rischi, nonché quelle relative all'approvazione delle relazioni finanziarie periodiche; b) il responsabile della funzione di internal audit, incaricato di verificare che il sistema di controllo interno e di gestione dei rischi sia funzionante e adeguato; c) gli altri ruoli e funzioni aziendali con specifici compiti in tema di controllo interno e gestione dei rischi, articolati in relazione a dimensioni, complessità e profilo di rischio dell'impresa; d) il collegio sindacale, anche in quanto comitato per il controllo interno e la revisione contabile, che vigila sull'efficacia del sistema di controllo interno e di gestione dei rischi. L'emittente prevede modalità di coordinamento tra i soggetti sopra elencati al fine di massimizzare l'efficienza del sistema di controllo interno e di gestione dei rischi e di ridurre le duplicazioni di attività. 7.P.4. Il comitato controllo e rischi è composto da amministratori indipendenti. In alternativa, il comitato può essere composto da 31 amministratori non esecutivi, in maggioranza indipendenti; in tal caso, il presidente del comitato è scelto tra gli amministratori indipendenti. Se l'emittente è controllato da altra società quotata o è soggetto all'attività di direzione e coordinamento di un'altra società, il comitato è comunque composto esclusivamente da amministratori indipendenti. Almeno un componente del comitato possiede un'adeguata esperienza in materia contabile e finanziaria o di gestione dei rischi, da valutarsi da parte del consiglio di amministrazione al momento della nomina.
Criteri applicativi, 7.C.1. Il consiglio di amministrazione, previo parere del comitato controllo e rischi: a) definisce le linee di indirizzo del sistema di controllo interno e di gestione dei rischi, in modo che i principali rischi afferenti all'emittente e alle sue controllate risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati, determinando inoltre il grado di compatibilità di tali rischi con una gestione dell'impresa coerente con gli obiettivi strategici individuati; b) valuta, con cadenza almeno annuale, l'adeguatezza del sistema di controllo interno e di gestione dei rischi rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto, nonché la sua efficacia; c) approva, con cadenza almeno annuale, il piano di lavoro predisposto dal responsabile della funzione di internal audit, sentiti il collegio sindacale e l'amministratore incaricato del sistema di controllo interno e di gestione dei rischi; d) descrive, nella relazione sul governo societario, le principali caratteristiche del sistema di controllo interno e di gestione dei rischi e le modalità di coordinamento tra i soggetti in esso coinvolti, esprimendo la propria valutazione sull'adeguatezza dello stesso; e) valuta, sentito il collegio sindacale, i risultati esposti dal revisore legale nella eventuale lettera di suggerimenti e nella relazione sulle questioni fondamentali emerse in sede di revisione legale. Il consiglio di amministrazione, su proposta dell'amministratore incaricato del sistema di controllo interno e di gestione dei rischi e previo parere favorevole del comitato controllo e rischi, nonché sentito il collegio sindacale: - nomina e revoca il responsabile della funzione di internal audit; - assicura che lo stesso sia dotato delle risorse adeguate all'espletamento delle proprie responsabilità; - ne definisce la remunerazione coerentemente con le politiche aziendali. 7.C.2. Il comitato controllo e rischi, nell'assistere il consiglio di amministrazione: a) valuta, unitamente al dirigente preposto alla redazione dei documenti contabili societari e sentiti il revisore legale e il collegio sindacale, il corretto utilizzo dei principi contabili e, nel caso di gruppi, la loro 32 omogeneità ai fini della redazione del bilancio consolidato; b) esprime pareri su specifici aspetti inerenti alla identificazione dei

monitorare i rischi e garantisce la salvaguardia del patrimonio sociale;

- ai sindaci (art. 8[164]), al fine di garantirne l'effettiva autonomia;

---

principali rischi aziendali; c) esamina le relazioni periodiche, aventi per oggetto la valutazione del sistema di controllo interno e di gestione dei rischi, e quelle di particolare rilevanza predisposte dalla funzione internal audit; d) monitora l'autonomia, l'adeguatezza, l'efficacia e l'efficienza della funzione di internal audit; e) può chiedere alla funzione di internal audit lo svolgimento di verifiche su specifiche aree operative, dandone contestuale comunicazione al presidente del collegio sindacale; f) riferisce al consiglio, almeno semestralmente, in occasione dell'approvazione della relazione finanziaria annuale e semestrale, sull'attività svolta nonché sull'adeguatezza del sistema di controllo interno e di gestione dei rischi; g) supporta, con un'adeguata attività istruttoria, le valutazioni e le decisioni del consiglio di amministrazione relative alla gestione di rischi derivanti da fatti pregiudizievoli di cui il consiglio di amministrazione sia venuto a conoscenza. 7.C.3. Ai lavori del comitato controllo e rischi partecipa il presidente del collegio sindacale o altro sindaco da lui designato; possono comunque partecipare anche gli altri sindaci. 7.C.4. L'amministratore incaricato del sistema di controllo interno e di gestione dei rischi: a) cura l'identificazione dei principali rischi aziendali, tenendo conto delle caratteristiche delle attività svolte dall'emittente e dalle sue controllate, e li sottopone periodicamente all'esame del consiglio di amministrazione; b) dà esecuzione alle linee di indirizzo definite dal consiglio di amministrazione, curando la progettazione, realizzazione e gestione del sistema di controllo interno e di gestione dei rischi e verificandone costantemente l'adeguatezza e l'efficacia; c) si occupa dell'adattamento di tale sistema alla dinamica delle condizioni operative e del panorama legislativo e regolamentare; d) può chiedere alla funzione di internal audit lo svolgimento di verifiche su specifiche aree operative e sul rispetto delle regole e procedure interne nell'esecuzione di operazioni aziendali, dandone contestuale comunicazione al presidente del consiglio di amministrazione, al presidente del comitato controllo e rischi e al presidente del collegio sindacale; e) riferisce tempestivamente al comitato controllo e rischi (o al consiglio di amministrazione) in merito a problematiche e criticità emerse nello svolgimento della propria attività o di cui abbia avuto comunque notizia, affinché il comitato (o il consiglio) possa prendere le opportune iniziative. 7.C.5. Il responsabile della funzione di internal audit: 33 a) verifica, sia in via continuativa sia in relazione a specifiche necessità e nel rispetto degli standard internazionali, l'operatività e l'idoneità del sistema di controllo interno e di gestione dei rischi, attraverso un piano di audit, approvato dal consiglio di amministrazione, basato su un processo strutturato di analisi e prioritizzazione dei principali rischi; b) non è responsabile di alcuna area operativa e dipende gerarchicamente dal consiglio di amministrazione; c) ha accesso diretto a tutte le informazioni utili per lo svolgimento dell'incarico; d) predispone relazioni periodiche contenenti adeguate informazioni sulla propria attività, sulle modalità con cui viene condotta la gestione dei rischi nonché sul rispetto dei piani definiti per il loro contenimento. Le relazioni periodiche contengono una valutazione sull'idoneità del sistema di controllo interno e di gestione dei rischi; e) predispone tempestivamente relazioni su eventi di particolare rilevanza; f) trasmette le relazioni di cui ai punti d) ed e) ai presidenti del collegio sindacale, del comitato controllo e rischi e del consiglio di amministrazione nonché all'amministratore incaricato del sistema di controllo interno e di gestione dei rischi; g) verifica, nell'ambito del piano di audit, l'affidabilità dei sistemi informativi inclusi i sistemi di rilevazione contabile. 7.C.6. La funzione di internal audit, nel suo complesso o per segmenti di operatività, può essere affidata a un soggetto esterno all'emittente, purché dotato di adeguati requisiti di professionalità, indipendenza e organizzazione. L'adozione di tali scelte organizzative, adeguatamente motivata, è comunicata agli azionisti e al mercato nell'ambito della relazione sul governo societario.

164 Art. 8: Sindaci, Principi 8.P.1. I sindaci agiscono con autonomia e indipendenza anche nei confronti degli azionisti che li hanno eletti. 8.P.2. L'emittente predispone le misure atte a garantire un efficace svolgimento dei compiti propri del collegio sindacale. Criteri applicativi 8.C.1. I sindaci sono scelti tra persone che possono essere qualificate come indipendenti anche in base ai criteri previsti dal presente Codice con riferimento agli amministratori. Il collegio verifica il rispetto di detti criteri dopo la nomina e successivamente con cadenza annuale, trasmettendo l'esito di tali verifiche al consiglio di amministrazione che le espone, dopo la nomina, mediante un comunicato diffuso al mercato, e, successivamente, nell'ambito della relazione sul governo societario, con modalità conformi a quelle previste per gli amministratori. 8.C.2. I sindaci accettano la carica quando ritengono di poter dedicare allo svolgimento diligente dei loro compiti il tempo necessario. 8.C.3. La remunerazione dei sindaci è commisurata all'impegno richiesto, alla rilevanza del ruolo ricoperto nonché alle caratteristiche dimensionali e settoriali dell'impresa. 8.C.4. Il sindaco che, per conto proprio o di terzi, abbia un interesse in una determinata operazione dell'emittente informa tempestivamente e in modo esauriente gli altri sindaci e il presidente del consiglio di amministrazione circa natura, termini, origine e

- ai rapporti con gli azionisti (art. 9[165]), ai quali devono essere fornite con tempestività le informazioni che possano essere rilevanti ai fini di un corretto esercizio dei propri diritti di socio;
- ai sistemi di amministrazione e controllo nei sistemi dualistico e monistico (art. 10[166]), fornendo criteri di adattamento dei principi sopra esaminati.

---

portata del proprio interesse. 8.C.5. Nell'ambito delle proprie attività, i sindaci possono chiedere alla funzione di internal audit lo svolgimento di verifiche su specifiche aree operative o operazioni aziendali. 8.C.6. Il collegio sindacale e il comitato controllo e rischi si scambiano tempestivamente le informazioni rilevanti per l'espletamento dei rispettivi compiti.

165 Art. 9: Rapporti con gli azionisti, Principi 9.P.1. Il consiglio di amministrazione promuove iniziative volte a favorire la partecipazione più ampia possibile degli azionisti alle assemblee e a rendere agevole l'esercizio dei diritti dei soci. 9.P.2. Il consiglio di amministrazione si adopera per instaurare un dialogo continuativo con gli azionisti fondato sulla comprensione dei reciproci ruoli. Criteri applicativi 9.C.1. Il consiglio di amministrazione assicura che venga identificato un responsabile incaricato della gestione dei rapporti con gli azionisti e valuta periodicamente l'opportunità di procedere alla costituzione di una struttura aziendale incaricata di tale funzione. 9.C.2. Alle assemblee, di norma, partecipano tutti gli amministratori. Le assemblee sono occasione anche per la comunicazione agli azionisti di informazioni sull'emittente, nel rispetto della disciplina sulle informazioni privilegiate. In particolare, il consiglio di amministrazione riferisce in assemblea sull'attività svolta e programmata e si adopera per assicurare agli azionisti un'adeguata informativa circa gli elementi necessari perché essi possano assumere, con cognizione di causa, le decisioni di competenza assembleare. 9.C.3. Il consiglio di amministrazione propone all'approvazione dell'assemblea un regolamento che indichi le procedure da seguire al fine di consentire l'ordinato e funzionale svolgimento delle riunioni assembleari, garantendo, al contempo, il diritto di ciascun socio di prendere la parola sugli argomenti posti in discussione. 9.C.4. Il consiglio di amministrazione, in caso di variazioni significative nella capitalizzazione di mercato delle azioni dell'emittente o nella composizione della sua compagine sociale, valuta l'opportunità di proporre all'assemblea modifiche dello statuto in merito alle percentuali stabilite per l'esercizio delle azioni e delle prerogative poste a tutela delle minoranze.

166 Art. 10: Sistemi di amministrazione e controllo dualistico e monistico, Principi 10.P.1 In caso di adozione di un sistema di amministrazione e controllo dualistico o monistico, gli articoli precedenti si applicano in quanto compatibili, adattando le singole previsioni al particolare sistema adottato, in coerenza con gli obiettivi di buon governo societario, trasparenza informativa e tutela degli investitori e del mercato perseguiti dal Codice e alla luce dei criteri applicativi previsti dal presente articolo. 10.P.2. Nel caso in cui sia proposta l'adozione di un nuovo sistema di amministrazione e controllo, gli amministratori informano i soci e il mercato in merito alle ragioni di tale proposta, nonché al modo nel quale si prevede che il Codice sarà applicato al nuovo sistema di amministrazione e controllo. 10.P.3. Nella prima relazione sul governo societario pubblicata successivamente alla modifica del sistema di amministrazione e controllo, l'emittente illustra in dettaglio le modalità con cui il Codice è stato applicato a tale sistema. Tali informazioni sono pubblicate anche nelle relazioni successive, indicando eventuali modifiche relative alle modalità di recepimento del Codice nell'ambito del sistema di amministrazione e controllo prescelto. Criteri applicativi 10.C.1. Nel caso di adozione del sistema di amministrazione e controllo dualistico, l'applicazione del Codice si informa ai seguenti criteri: a) salvo quanto previsto dal successivo punto b), gli articoli del Codice che fanno riferimento al consiglio di amministrazione e al collegio sindacale, o ai loro componenti, trovano applicazione, in linea di principio, rispettivamente al consiglio di gestione e al consiglio di sorveglianza o ai loro componenti; b) l'emittente, in ragione delle specifiche opzioni statutarie adottate, della configurazione degli organi di amministrazione e controllo - anche in relazione al numero dei loro componenti e delle competenze ad essi attribuite - nonché delle specifiche circostanze di fatto, può applicare le previsioni riguardanti il consiglio di amministrazione o gli amministratori al consiglio di sorveglianza o ai suoi componenti; c) le disposizioni in materia di nomina degli amministratori previste dall'art. 5 del presente Codice si applicano, in quanto compatibili, alla nomina dei membri del consiglio di sorveglianza e/o dei membri del consiglio di gestione. 10.C.2. Nel caso di adozione del sistema di amministrazione e controllo monistico, l'applicazione del Codice si informa ai seguenti criteri: a) gli articoli del Codice che fanno riferimento al consiglio di amministrazione e al collegio sindacale, o ai loro componenti, trovano applicazione, in linea di principio, rispettivamente al consiglio di amministrazione e al comitato per il controllo sulla gestione o ai loro componenti; 42 b) le funzioni attribuite al comitato controllo e rischi dall'art. 7 del presente Codice possono essere riferite al comitato per il controllo sulla gestione previsto dall'art. 2409-octiesdecies cod. civ., ove rispetti i criteri di composizione indicati nello stesso art. 7.

5.1.2 Obblighi informativi

La società quotata deve mettere a disposizione del pubblico una serie di informazioni relative alla vita della società, che sarà tanto più efficace quanto più sia resa con correttezza e trasparenza. In relazione ai contenuti dell'informazione, occorre distinguere tra:

- comunicazioni di informazioni privilegiate;
- comunicazioni periodiche (di dati contabili);
- comunicazioni a carattere episodico legate ad operazioni di carattere straordinario;
- comunicazioni relative all'acquisto di strumenti finanziari dell'Emittente da parte di amministratori e managers della stessa (internal dealing).

Occorre inoltre tener conto che in relazione alle società quotate sussistono, da parte degli azionisti, obblighi di comunicazione di partecipazioni rilevanti nonché di pubblicazione di patti parasociali relativi all'Emittente.

Di seguito vengono esaminati, in maniera sintetica, gli obblighi di informazione maggiormente rilevanti.

Comunicazione di informazioni privilegiate

Si parla di "informazione privilegiata" ai sensi dell'art. 7 co. 1 l. a) del Regolamento UE n. 596/2014[167] e dell'art. 181[168] TUF, quando si ha "un'informazione che ha un carattere preciso,

[167] Il Regolamento UE n. 596/2014 ha abrogato la Direttiva 2003/6/CE che per prima ha disciplinato gli abusi di mercato. Con riferimento alla nozione di informazione privilegiata il Regolamento ha mantenuto quella contenuta nella Direttiva.

[168] Art. 181: "1. Ai fini del presente titolo per informazione privilegiata si intende un'informazione di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari.

2. In relazione ai derivati su merci, per informazione privilegiata si intende un'informazione di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più derivati su merci, che i partecipanti ai mercati su cui tali derivati sono negoziati si aspettano di ricevere secondo prassi di mercato ammesse in tali mercati.
3. Un'informazione si ritiene di carattere preciso se:
   a) si riferisce ad un complesso di circostanze esistente o che si possa ragionevolmente prevedere che verrà ad esistenza o ad un evento verificatosi o che si possa ragionevolmente prevedere che si verificherà;
   b) è sufficientemente specifica da consentire di trarre conclusioni sul possibile effetto del complesso di circostanze o dell'evento di cui alla lettera a) sui prezzi degli strumenti finanziari.
4. Per informazione che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di strumenti finanziari si intende un'informazione che presumibilmente un investitore ragionevole utilizzerebbe come uno degli elementi su cui fondare le proprie decisioni di investimento.
5. Nel caso delle persone incaricate dell'esecuzione di ordini relativi a strumenti finanziari, per informazione privilegiata si intende anche l'informazione trasmessa da un cliente e concernente gli ordini del cliente in attesa di esecuzione, che ha un carattere preciso e che concerne, direttamente o indirettamente, uno o più emittenti di strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari".

che non è stata resa pubblica e che concerne, direttamente o indirettamente, uno o più emittenti di strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari ovvero sui prezzi di strumenti finanziari derivati connessi". Si ritiene che la notizia sia precisa quando riguarda circostanze esistenti, o che potrebbero venire ad esistenza, o fatti che si siano verificati o possano verificarsi (co. 3 l. a) art. 181 TUF), e quando è sufficientemente dettagliata da permettere di trarre conclusioni sull'effetto che tali circostanze o eventi potrebbero avere sugli strumenti finanziari (co. 3 l. b) art. 181 TUF). La nozione di "informazione privilegiata" è pertanto assai ampia e, non riferendosi a circostanze o eventi specifici, rimette agli emittenti la valutazione sugli effetti che la stessa potrebbe produrre sul prezzo, che vanno valutati alla luce di un criterio di ragionevolezza.

L'art. 114[169] del TUF stabilisce che le "informazioni privilegiate" devono essere comunicate al pubblico, senza indugio, dagli emittenti e dai soggetti che li controllano.

L'art. 66 del Regolamento Emittenti stabilisce le caratteristiche e le modalità di invio del comunicato, che va trasmesso alla società di gestione del mercato che lo mette immediatamente a disposizione del pubblico e ad almeno due agenzie di stampa, inoltre il comunicato è contestualmente trasmesso alla Consob.

Il comunicato deve descrivere gli elementi essenziali del fatto in modo da consentire una valutazione completa e corretta di quanto in esso descritto, e deve inoltre contenere collegamenti e raffronti con il contenuto dei comunicati precedenti (co. 2 l. a).

È prevista l'emissione di un comunicato con riferimento alle situazioni contabili dell'Emittente destinate ad essere riportate nel bilancio di esercizio, nel bilancio consolidato, nella relazione semestrale e nella relazione trimestrale, quando tali situazioni vengano comunicate a soggetti esterni che non siano tenuti ad obblighi di riservatezza e comunque non appena abbiano acquistato un sufficiente grado di certezza (co. 3 l. a) e alle deliberazioni con le quali l'organo competente approva il progetto di bilancio, la proposta di distribuzione del dividendo, il bilancio consolidato, la relazione semestrale e quella trimestrale (co. 3 l. b).

È consentito, a certe condizioni, ritardare la comunicazione (art. 66 bis) di informazioni privilegiate quando la comunicazione possa pregiudicare i legittimi interessi (co. 1) dell'Emittente e dei soggetti che li controllano, purché sia garantita la segretezza dell'informazione (co. 3) e la mancata diffusione non induca in errore il pubblico su circostanze essenziali (co. 2).

[169] Vedasi nota 95.

Comunicazione periodiche di dati contabili

L'informazione periodica riguarda la "messa a disposizione del pubblico dei documenti contabili che la società predispone a cadenze prestabilite"[170].

In particolare, entro quattro mesi dalla chiusura dell'esercizio, gli emittenti quotati aventi l'Italia come Stato membro d'origine mettono a disposizione del pubblico presso la sede sociale, sul sito Internet e con le altre modalità previste dalla Consob con regolamento, la relazione finanziaria annuale, comprendente il progetto di bilancio di esercizio o, per le società che abbiano adottato il sistema di amministrazione e controllo dualistico, il bilancio di esercizio, nonché il bilancio consolidato, ove redatto, la relazione sulla gestione e l'attestazione prevista all'articolo 154-bis co. 5[171] (art. 154 ter co. 1 TUF).

Il co. 2 stabilisce che gli emittenti quotati aventi l'Italia come Stato membro d' origine pubblicano, quanto prima possibile e comunque entro tre mesi dalla chiusura del primo semestre dell'esercizio, una relazione finanziaria semestrale comprendente il bilancio semestrale abbreviato, la relazione intermedia sulla gestione e l'attestazione prevista dall'articolo 154-bis, comma 5.

Per la relazione intermedia sulla gestione il co. 4 stabilisce che deve contenere almeno riferimenti agli eventi importanti che si sono verificati nei primi sei mesi dell'esercizio e alla loro incidenza sul bilancio semestrale abbreviato, unitamente a una descrizione dei principali rischi e incertezze per i sei mesi restanti dell'esercizio.

Per gli emittenti azioni quotate aventi l'Italia come Stato membro d'origine, la relazione intermedia sulla gestione contiene, altresì, informazioni sulle operazioni rilevanti con parti correlate.

---

[170] Renzo Costi-Luca Enriques, *Trattato di Diritto Commerciale*, Il Mercato Mobiliare, VIII volume, Padova, CEDAM, 2004, pag. 211.

[171] 5. Gli organi amministrativi delegati e il dirigente preposto alla redazione dei documenti contabili societari attestano con apposita relazione sul bilancio di esercizio, sul bilancio semestrale abbreviato e, ove redatto, sul bilancio consolidato:
a) l'adeguatezza e l'effettiva applicazione delle procedure di cui al comma 3 nel corso del periodo cui si riferiscono i documenti;
b) che i documenti sono redatti in conformità ai principi contabili internazionali applicabili riconosciuti nella Comunità europea ai sensi del regolamento (CE) n. 1606/2002 del Parlamento europeo e del Consiglio, del 19 luglio 2002;
c) la corrispondenza dei documenti alle risultanze dei libri e delle scritture contabili;
d) l'idoneità dei documenti a fornire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria dell'emittente e dell'insieme delle imprese incluse nel consolidamento;
e) per il bilancio d'esercizio e per quello consolidato, che la relazione sulla gestione comprende un'analisi attendibile dell'andamento e del risultato della gestione, nonché della situazione dell'emittente e dell'insieme delle imprese incluse nel consolidamento, unitamente alla descrizione dei principali rischi e incertezze cui sono esposti;
f) per il bilancio semestrale abbreviato, che la relazione intermedia sulla gestione contiene un'analisi attendibile delle informazioni di cui al comma 4 dell'articolo 154-ter.

Comunicazione episodica di operazioni straordinarie

In caso di operazioni straordinarie[172], che sono idonee ad influire sulla società e sulla valutazione della stessa da parte degli investitori, seguendo il dettato dell'art. 70[173] Reg.

[172] Operazioni realizzate al di fuori della gestione ordinaria delle società per diverse ragioni, come la modifica della struttura o della forma giuridica dell'impresa, il trasferimento della titolarità dell'azienda o del controllo dell'impresa, ovvero la liquidazione dell'azienda per procedere alla chiusura. Le operazioni straordinarie sono variegate. Alcune possono riguardare la generalità delle imprese (cessione e conferimento d'azienda; liquidazione ordinaria o coatta), altre solo le s. (trasformazioni, fusioni, scissioni, scambio di partecipazioni). La maggior parte di queste operazioni è volontaria, mentre alcune (come il fallimento o la liquidazione coatta amministrativa) sono obbligatorie. Altre tipologie includono le operazioni 'dirette', come per es. la cessione d'azienda, oppure 'mediate' (nel senso che si realizzano attraverso la cessione delle partecipazioni). Le operazioni principali sono la trasformazione, la fusione, la scissione, il conferimento, la cessione e la liquidazione. Per es., si realizza la trasformazione del modello organizzativo della s., attraverso la fusione, quando si concentrano in un'unica struttura societaria il patrimonio e le risorse allocate in altre società. Invece, la scissione aziendale o di rami d'azienda può essere necessaria per alleggerire la struttura sociale esistente. Con la scissione, possono mutare i rapporti di forza tra i soci, ovvero restare invariati rispetto alle condizioni originarie (scissione non proporzionale/proporzionale), ma soggettivamente non muta la proprietà che rimane in capo agli stessi soci originari. Nel caso di conferimento, la società ha proceduto allo scorporo o al conferimento a partecipare nella s. beneficiaria, mentre i soci rimangono proprietari della s. scorporante o conferente.

[173] Art. 70: "1. Gli emittenti azioni, almeno trenta giorni prima dell'assemblea convocata per deliberare sulla fusione o sulla scissione, mettono a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, la documentazione prevista dall'articolo 2501-septies, numeri 1) e 3) e dagli articoli 2506-bis e 2506-ter del codice civile.

2. La relazione illustrativa dell'organo amministrativo prevista dagli articoli 2501-quinquies e 2506-ter del codice civile è redatta secondo i criteri generali indicati nell'Allegato 3A e resa pubblica con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies.
3. Gli emittenti azioni trasmettono alla Consob:
   a) copia dell'atto di fusione o di scissione con l'indicazione della data di iscrizione nel registro delle imprese, entro dieci giorni dall'avvenuto deposito previsto dagli articoli 2504 e 2506-ter del codice civile attraverso il sistema di Teleraccolta, secondo le specifiche modalità indicate dalla Consob con propria comunicazione;
   b) lo statuto modificato, entro trenta giorni dal deposito nel registro delle imprese attraverso il sistema di Teleraccolta, secondo le specifiche modalità indicate dalla Consob con propria comunicazione.
4. Per gli aumenti di capitale mediante conferimento di beni in natura, gli emittenti azioni:
   a) almeno trenta giorni prima di quello dell'assemblea trasmettono alla Consob, attraverso il sistema di Teleraccolta, secondo le specifiche modalità indicate dalla Consob con propria comunicazione, la relazione illustrativa dell'organo amministrativo prevista dall'articolo 2441, comma 6, del codice civile, redatta secondo i criteri generali indicati nell'Allegato 3A;
   b) almeno ventun giorni prima di quello dell'assemblea mettono a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, la relazione illustrativa prevista dalla precedente lettera a);
   c) almeno ventun giorni prima di quello dell'assemblea mettono a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, il parere sulla congruità del prezzo di emissione delle azioni rilasciato da un revisore legale o da una società di revisione legale. La relazione giurata dell'esperto designato dal tribunale ai sensi dell'articolo 2343 del codice civile ovvero la documentazione indicata dall'articolo 2343-ter, comma 2, del codice civile, è messa a disposizione del pubblico, con le medesime modalità, almeno quindici giorni prima di quello fissato per l'assemblea.
6. Gli emittenti azioni, in ipotesi di operazioni significative di fusione, scissione o di aumento di capitale mediante conferimento di beni in natura, individuate secondo i criteri generali indicati nell'Allegato 3B, o su richiesta della Consob, in relazione alle caratteristiche dell'operazione salvo quanto previsto al comma 8, mettono a disposizione del pubblico presso la sede sociale, e con modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, almeno quindici giorni prima di quello fissato per l'assemblea, un documento informativo redatto in conformità all'Allegato 3B.

Emittenti, la società è tenuta a predisporre, un documento informativo che dia contezza delle caratteristiche dell'operazione da effettuare e inoltre mettere a disposizione del pubblico alcuni dei documenti relativi all'operazione (delibere degli organi competenti, relazione dell'organo amministrativo, eventuali relazioni dell'organo di controllo o della società di revisione).

La normativa cita, tra le operazioni straordinarie, i casi "tipici" delle fusioni, scissioni, aumenti di capitale con conferimento di beni in natura, ma vi rientrano naturalmente la costituzione di patrimoni destinati ad uno specifico affare (art. 70 bis[174] Reg. Emittenti), ai sensi dell'art. 2447[175] bis c.c., le acquisizioni e le cessioni (art. 71[176]), le altre modifiche dell'atto

---

7. Nei casi in cui le operazioni indicate nei commi precedenti siano deliberate da organi diversi dall'assemblea ai sensi degli articoli 2365, comma 2, 2505, comma 2, 2505-bis, comma 2, 2506-ter nonché dell'articolo 2443, commi 2 e 3, del codice civile:
   a) i documenti indicati nei commi 1 e 4 per i quali il codice civile prevede la messa a disposizione dei soci prima della delibera dell'organo competente, sono messi a disposizione del pubblico nei termini previsti dal codice civile presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies;
   b) il documento informativo indicato nel comma 6 è messo a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, entro quindici giorni dalla delibera dell'organo competente;
   c) il verbale delle deliberazioni adottate è messo a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, entro trenta giorni dalla data delle deliberazioni.

7-bis. Alla diffusione delle informazioni previste nel presente articolo si applica l'articolo 65-bis, comma 2.

8. Fermi restando gli obblighi informativi previsti dalla legge e salvo che il regolamento adottato dalla società di gestione del mercato disponga diversamente, gli emittenti possono derogare all'adempimento previsto dal comma 6, dandone comunicazione alla Consob, alla società di gestione del mercato e al pubblico all'atto della presentazione della domanda finalizzata all' ammissione alle negoziazioni delle proprie azioni. L'informazione relativa a tale scelta viene fornita dagli emittenti azioni anche all'interno delle relazioni finanziarie pubblicate ai sensi dell'articolo 154-ter del Testo unico".

[174] Art. 70-bis: "1. Gli emittenti azioni mettono a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, il verbale della deliberazione costitutiva di patrimoni destinati a uno specifico affare contestualmente alla richiesta di iscrizione nel registro delle imprese previsto dall'articolo 2436, comma 1, del codice civile.

2. Nei casi in cui l'operazione indicata nel comma 1 sia deliberata dall'assemblea, gli emittenti azioni:
   a) almeno trenta giorni prima di quello fissato per l'assemblea trasmettono alla Consob attraverso il sistema di Teleraccolta, secondo le specifiche modalità indicate dalla Consob con propria comunicazione, la relazione illustrativa dell'organo amministrativo recante le informazioni previste dagli articoli 2447-ter, comma 1 e 2447-novies, comma 4, del codice civile;
   b) almeno ventun giorni prima di quello fissato per la relativa convocazione, mettono a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, la relazione illustrativa dell'organo amministrativo.

4. Gli stessi emittenti mettono a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, la documentazione prevista dall'articolo 2447-novies, comma 1, del codice civile, contestualmente al deposito presso l'ufficio del registro delle imprese.

5. Gli stessi emittenti mettono a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, il contratto previsto dall'articolo 2447-bis, comma 1, lettera b), del codice civile, contestualmente alla richiesta di iscrizione nel registro delle imprese prevista dall'articolo 2447-decies, comma 3, lettera a).

6. Alla diffusione al pubblico delle informazioni previste nel presente articolo si applica l'articolo 65-bis, comma 2".

[175] Vedasi nota 101.

costitutivo e le emissioni di obbligazioni (art. 72[177]), l'acquisto e alienazione di azioni proprie (art. 73[178]).

---

[176] Art. 71: "1. Gli emittenti azioni, in ipotesi di operazioni di acquisizione o di cessione significative, individuate secondo i criteri generali indicati nell'Allegato 3B, o su richiesta della Consob, in relazione alle caratteristiche dell'operazione, salvo quanto previsto al comma 1-bis, mettono a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, entro quindici giorni dalla conclusione dell'operazione, un documento informativo redatto in conformità all'Allegato 3B. Si applica l'articolo 65-bis, co. 2.

1-bis. Fermi restando gli obblighi informativi previsti dalla legge e salvo che il regolamento adottato dalla società di gestione del mercato disponga diversamente, gli emittenti possono derogare all'adempimento previsto dal comma 1, dandone comunicazione alla Consob, alla società di gestione del mercato e al pubblico all'atto della presentazione della domanda finalizzata all'ammissione alle negoziazioni delle proprie azioni. L'informazione relativa a tale scelta viene fornita dagli emittenti azioni anche all'interno delle relazioni finanziarie pubblicate ai sensi dell'articolo 154-ter del Testo unico".

[177] Art. 72: "1. Gli emittenti azioni, trasmettono alla Consob attraverso il sistema di Teleraccolta, secondo le specifiche modalità indicate dalla Consob con propria comunicazione, almeno trenta giorni prima di quello fissato per l'assemblea convocata per deliberare le modifiche dello statuto diverse da quelle previste da altre disposizioni della presente Sezione o l'emissione di obbligazioni, la relazione illustrativa dell'organo amministrativo redatta in conformità all'Allegato 3A. La medesima relazione è altresì messa a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, almeno ventun giorni prima di quello fissato per l'assemblea. Lo statuto modificato, entro trenta giorni dal deposito nel registro delle imprese, è trasmesso alla Consob attraverso il sistema di Teleraccolta, secondo le specifiche modalità indicate dalla Consob con propria comunicazione.

3. Gli stessi emittenti, in occasione di operazioni di aumento del capitale sociale con esclusione o limitazione del diritto di opzione, ai sensi dell'articolo 2441, comma 4, secondo periodo, e comma 5, del codice civile, nel termine e con le modalità previste dal comma 1, mettono a disposizione del pubblico anche la relazione della società di revisione sulla corrispondenza tra il prezzo di emissione e il valore di mercato delle azioni o il parere della società di revisione sulla congruità del prezzo di emissione delle azioni.
4. Gli stessi emittenti, in occasione di operazioni di conversione facoltativa di azioni di una categoria in azioni di categoria diversa, mettono a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, nonché presso i depositari, per il tramite della società di gestione accentrata e con le modalità da questa stabilite, almeno il giorno di borsa aperta antecedente l'inizio del periodo di conversione, la relazione illustrativa dell'organo amministrativo già pubblicata ai sensi dei commi 1 e 2 integrata con le informazioni necessarie per la conversione. I depositari, tramite la società di gestione accentrata, comunicano giornalmente i dati sulle richieste di conversione alla società di gestione del mercato che li pubblica nel proprio sito internet entro il giorno di borsa aperta successivo. L' emittente, entro dieci giorni dalla conclusione del periodo di conversione, rende noti i risultati della conversione con un avviso diffuso con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies.
5. In occasione di operazioni di conversione obbligatoria di azioni di una categoria in azioni di una categoria diversa, gli emittenti danno notizia della data in cui avrà luogo la conversione entro il giorno di borsa aperta antecedente tale data con un avviso diffuso con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies.
6. Nei casi in cui le operazioni indicate nei commi 1 e 3 siano deliberate da organi diversi dall' assemblea ai sensi degli articoli 2365, comma 2, 2410, comma 1, 2420-ter e 2443 del codice civile:
   a) i documenti indicati nei commi 1 e 3, per i quali il codice civile prevede la messa a disposizione dei soci prima della delibera dell'organo competente sono messi a disposizione del pubblico, nei termini previsti dal codice civile, presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies;
   b) il verbale delle deliberazioni adottate è messo a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, entro trenta giorni dalla data delle deliberazioni.
7. Alla diffusione al pubblico delle informazioni previste nei commi 1, 3, 4, primo periodo, e 6 si applica l'articolo 65-bis, comma 2.

Internal dealing

La normativa che disciplina l'"internal dealing", composta dall'art. 114 co. 7[179] TUF e dagli artt. 152 sexies e ss. Reg. Emittenti, esige che venga data adeguata comunicazione all'esterno di operazioni di acquisto, vendita, sottoscrizione o scambio di azioni o strumenti finanziari quotati (le cosiddette *operazioni rilevanti*) svolte da soggetti che ricoprano incarichi rilevanti all'interno della società e le persone ad essi strettamente collegate (cosiddetti *soggetti rilevanti*).

Risultano "soggetti rilevanti", sia all'interno dell'Emittente stessa che di eventuali società controllate:

- i componenti dell'organo amministrativo e di controllo della società (art. 152 sexies co. 1 l. c.1);
- i soggetti che svolgono funzioni di direzione (co. 1 l. c.2);
- i dirigenti che hanno accesso ad informazioni privilegiate e possono prendere decisioni che sono in grado di condizionare le prospettive della società (co. 1 l. c.3);
- chiunque detenga una partecipazione di almeno il dieci per cento, rappresentata da diritti di voto, nonché chiunque altro controlli l'Emittente quotato (co. 1 l. c.4).

Le persone strettamente collegate ai soggetti rilevanti sono: il coniuge non legalmente separato, i figli a carico e, se conviventi da almeno un anno, i genitori, i parenti e gli affini dei soggetti rilevanti (co. 1 l. d.1); le persone giuridiche, le società di persone e i trust di cui il soggetto rilevante (o le persone sub d. 1) sia titolare (co. 1 l. d.2); le persone giuridiche controllate dal soggetto rilevante o dai soggetti sub d.1 (co. 1 l. d.3); le società di persone i cui interessi economici siano equivalenti a quelli di un soggetto rilevante o delle persone sub d.1 (co. 1 l. d.4), i trust costituiti a beneficio di un soggetto rilevante o delle persone sub d.1 (co 1 l. d.5).

Le "operazioni rilevanti" nel senso sopra visto, svolte sui titoli dell'Emittente dai soggetti sopra indicati che siano di importo, anche complessivo di varie operazioni svolte nell'anno, superiore a cinquemila euro (combinato disposto co. 3 l. a) e co. 4 art. 152 septies), devono

---

8. Le deliberazioni di distribuzione di acconti sui dividendi sono trasmesse alla Consob entro trenta giorni dalla riunione consiliare attraverso il sistema di Teleraccolta, secondo le specifiche modalità indicate dalla Consob con propria comunicazione".

[178] Art. 73: "1. Gli emittenti azioni, almeno ventun giorni prima di quello fissato per l'assemblea convocata per deliberare in merito all'acquisto e all'alienazione di azioni proprie, mettono a disposizione del pubblico presso la sede sociale e con le modalità indicate dagli articoli 65-quinquies, 65-sexies e 65-septies, la relazione illustrativa dell'organo amministrativo redatta in conformità all'Allegato 3A. Alla diffusione al pubblico delle informazioni previste nel presente comma si applica l'articolo 65-bis, comma 2".

[179] Vedasi nota 95.

essere comunicate sia a Consob che al pubblico con modalità e tempi previsti nel Regolamento Emittenti (art. 152 octies[180]).

Comunicazioni di partecipazioni rilevanti

Ancora a motivi di trasparenza e di chiarezza sono dovute "le regole che impongono di rendere conoscibili le partecipazioni rilevanti in società quotate e in società di capitali non quotate o in società a responsabilità limitata, anche estere e la pubblicazione dei patti parasociali che regolano l'esercizio di voto nelle società quotate"[181].

Con riferimento alle partecipazioni rilevanti, l'art. 120 TUF stabilisce l'obbligo di comunicazione alla società partecipata ed a Consob, nonché obblighi di informazione al pubblico, da parte di coloro che partecipano in una società con azioni quotate in misura superiore al tre[182] per cento del capitale o cinque per cento per le PMI (co. 2).

---

[180] Art. 152-octies: "1. I soggetti rilevanti indicati nell'articolo 152-sexies, comma 1, lettere c.1), c.2) e c.3) comunicano alla Consob le operazioni sulle azioni e sugli strumenti finanziari collegati, compiute da loro stessi e dalle persone strettamente legate entro cinque giorni di mercato aperto a partire dalla data della loro effettuazione.

2. I soggetti rilevanti indicati nell'articolo 152-sexies, comma 1, lettere c.1), c.2) e c.3) comunicano all'emittente quotato le operazioni indicate al comma 1 entro i termini ivi stabiliti.
3. L'emittente quotato pubblica le informazioni ricevute ai sensi del comma 2, entro la fine del giorno di mercato aperto successivo a quello del loro ricevimento e le trasmette contestualmente al meccanismo di stoccaggio autorizzato.
4. I soggetti rilevanti indicati nell'articolo 152-sexies, comma 1, lettera c.4) comunicano alla Consob e pubblicano le informazioni indicate al comma 1, entro la fine del quindicesimo giorno del mese successivo a quello in cui è stata effettuata l'operazione.
5. La comunicazione al pubblico prevista dal comma 4 può essere effettuata, per conto dei soggetti rilevanti ivi indicati, dall'emittente quotato, a condizione che, previo accordo, tali soggetti rilevanti inviino le informazioni indicate al comma 1 all'emittente quotato, nei termini indicati al comma 4. In tal caso l'emittente quotato pubblica le informazioni entro la fine del giorno di mercato aperto successivo a quello in cui ha ricevuto le informazioni dai predetti soggetti rilevanti.
6. La comunicazione alla Consob prevista dai commi 1 e 4 può essere effettuata, per conto di tutti i soggetti rilevanti, dall'emittente quotato entro i termini, rispettivamente, indicati nei predetti commi.
7. Le comunicazioni previste dai precedenti commi sono effettuate secondo le modalità indicate nell'Allegato 6.
8. Gli emittenti quotati e le società da questi controllate, indicate nell'articolo 152-sexies, comma 1, lettera c.3), devono:
   a) istituire una procedura diretta a identificare tra i propri dirigenti i soggetti obbligati a effettuare le comunicazioni previste dall'articolo 114, comma 7, del Testo unico, come individuati nello stesso articolo e nel presente Titolo;
   b) dare informazione ai soggetti identificati ai sensi della lettera precedente dell'avvenuta identificazione e degli obblighi connessi.
9. Gli emittenti quotati devono individuare il soggetto preposto al ricevimento, alla gestione e alla diffusione al mercato delle informazioni previste dal presente Titolo.
10. I soggetti rilevanti rendono nota alle persone strettamente legate la sussistenza delle condizioni in base alle quali tali ultime persone sono tenute agli obblighi di comunicazione previsti dall'articolo 114, comma 7, del Testo unico".

[181] Francesco Galgano, *Diritto Commerciale*, *Le società*, Bologna, Zanichelli, 2012, XVIII Edizione, pag. 435.

[182] L'art. 1 d.lgs. 25/2016 ha sostituito la parola "due" con la parola "tre".

Il TUF stabilisce che sia la Consob (Reg. Emittenti, art. 118), a determinare i criteri di calcolo delle partecipazioni (co. 4 l. b).

In relazione alla partecipazione in società quotate, l'obbligo "grava su chiunque venga a disporre della partecipazione, e dunque sia persone fisiche che persone giuridiche"[183], indipendentemente dalla cittadinanza degli individui o nazionalità delle persone giuridiche.

La comunicazione deve inoltre essere resa in caso di superamento delle soglie percentuali del 2, 5, 7.5, 10 e successivi multipli di 5 o di riduzione della partecipazione entro le soglie sopra indicate (art. 117 co. 1 l. b) e c)).

Ai fini della comunicazione, sono considerate partecipazioni:

- art. 118 co. 1, le azioni delle quali un soggetto è titolare, anche se il diritto di voto spetta o è attribuito a terzi e le azioni in relazione alle quali spetta o è attribuito il diritto di voto (l. a) creditore pignoratizio/usufruttuario, l. b) depositario, l. c) delega, l. d) trasferimento);
- art. 118 co. 3, le azioni delle quali sono titolari interposte persone, fiduciari, società controllate e le azioni in relazione alle quali il diritto di voto spetta o è attribuito ad alcuno di questi soggetti.

L'art. 119 Reg. Emittenti tiene anche conto delle così dette "partecipazioni potenziali[184]", rappresentate dalle azioni emesse e sottoscritte che un soggetto può acquistare o vendere di propria iniziativa, direttamente o per il tramite di interposte persone, fiduciari, società controllate, stabilendo obblighi di comunicazione relativi alle soglie del 5%, 10%, 15%, 20%, 25%, 30%, 50% e 75% (co. 1 l. a) e la riduzione al di sotto delle soglie sopra indicate (co. 1 l. b).

Il co. 2 stabilisce l'obbligo di comunicazione per la "posizione lunga complessiva[185]"in relazione al superamento delle soglie del 5%, 10%, 20% 30% e 50% (l. a) e la relativa riduzione (l. b).

---

183 www.economiauniparthenope.it/icostidellaquotazione.

184 Glossario Borsa Italiana.

185 www.bankpedia.org/posizionelunga, "È la posizione dell'operatore di una borsa valori o di una borsa merci che si trova ad avere, in un dato momento, una quantità di titoli o di merci superiore a quella che deve consegnare in base ai contratti stipulati. Per estensione si dice che nei contratti a termine assume una posizione lunga il compratore che ha titolo a ricevere titoli o merci. Dall'altra parte viene invece denominata posizione corta quella del venditore. Le Istruzioni di vigilanza della Banca d'Italia definiscono posizione lunga (o creditoria) lorda l'insieme dei titoli in portafoglio, i titoli da ricevere per operazioni da regolare (a pronti o a termine) e le altre operazioni "fuori bilancio" che comportano l'obbligo o il diritto di acquistare titoli, valute, merci, indici, tassi di interesse o di cambio prefissati; posizione lunga (o creditoria) lorda in valute le attività in valuta, le valute da ricevere per operazioni da regolare(a pronti o a termine) e le altre operazioni "fuori bilancio" che comportino l'obbligo o il diritto di acquistare attività in valuta; posizione netta lunga su un titolo, la posizione che risulta dalla differenza tra le posizioni creditorie lorde e quelle debitorie lorde, in bilancio e fuori bilancio, relative alla medesima emissione per i titoli di

Il termine entro cui effettuare la comunicazione è di cinque giorni di mercato aperto dall'operazione che fa sorgere l'obbligo, indipendentemente dalla data di esecuzione (art. 121 co. 1).

L'omissione delle comunicazioni o l'attestazione di dichiarazione false è punita con sanzioni amministrative, penali e civili.

Nel caso di comunicazioni di partecipazioni rilevanti da chiunque detenute, è prevista la sospensione del diritto di voto per le azioni per le quali non è stata effettuata la comunicazione.

Comunicazioni di patti parasociali

L'art. 122 co. 1 TUF prevede che i patti parasociali che abbiano ad oggetto l'esercizio del diritto di voto nelle società con azioni quotate e loro controllanti, devono essere, entro cinque giorni dalla loro stipula:

- comunicati a Consob (l. a);
- pubblicati per estratto sulla stampa quotidiana (l. b);
- depositati presso il registro delle imprese ove ha sede la società (l. c);
- comunicati alle società con azioni quotate (l. d).

In caso di inosservanza degli obblighi prescritti al primo comma i patti sono nulli (co. 3)

In caso di mancata comunicazione, non può essere esercitato il diritto di voto per le azioni per le quali non sono stati adempiuti gli obblighi (co. 4).

Per quanto riguarda la durata l'art. 123 co. 1 stabilisce che i patti a tempo determinato, non possano avere durata superiore a tre anni, ma possono essere rinnovati alla scadenza, mentre, nel caso siano stipulati a tempo indeterminato, ciascun contraente ha facoltà di recedere con preavviso di sei mesi (co. 2).

Il Regolamento Emittenti ha "disciplinato in modo analitico (agli artt. 127 e ss.) le modalità di comunicazione, il contenuto e la pubblicazione dell'estratto"[186].

Il co. 1 del sopracitato articolo prevede che l'obbligo di comunicazione a Consob grava in solido su tutti gli aderenti al patto, il co. 2 richiede la trasmissione, entro cinque giorni dalla stipulazione, della copia integrale del patto conforme all'originale (l. a), copia dell'estratto (l. b), informazioni identificative degli aderenti al patto (l. c).

---

debito; posizione netta in valuta la differenza tra la posizione lunga lorda e la posizione corta lorda in ciascuna valuta".

[186] Paolo Montalenti, *Trattato di Diritto Commerciale*, *La Società Quotata*, IV volume, Padova, CEDAM, 2004, pag. 143.

Ulteriori comunicazioni sono richieste dall'art. 128 per i casi di: modifiche al patto (co. 1 l. a), variazioni dei diritti di voto (l. b) e rinnovo/scioglimento del patto (l. c).

L'art. 129 stabilisce che L'estratto nel suo contenuto minimo deve dare almeno l'indicazione del tipo di patto, la percentuale complessiva del capitale sociale, avente diritto di voto, ovvero il numero complessivo dei diritti di voto conferiti nel patto, la denominazione dell'emittente e degli aderenti nonché l'indirizzo del sito internet dove sono pubblicate le informazioni essenziali indicate nell'articolo 130[187].

[187] Art. 130: "1. Nel sito internet indicato ai sensi dell'articolo 129 sono riportate le informazioni necessarie per una compiuta valutazione del patto e almeno le seguenti indicazioni: a) la società i cui strumenti finanziari sono oggetto del patto; b) il numero dei diritti di voto riferiti alle azioni e degli strumenti finanziari che attribuiscono diritti di acquisto o di sottoscrizione di azioni o diritti di voto ai sensi dell'articolo 2351, ultimo comma, del codice civile, complessivamente conferiti, la loro percentuale rispetto al numero totale dei diritti di voto rappresentativi del capitale sociale e degli strumenti finanziari emessi della medesima categoria e, nel caso di strumenti finanziari che attribuiscono diritti di acquisto o sottoscrizione, il numero complessivo dei diritti di voto riferibili alle azioni che possono essere acquistate o sottoscritte; c) i soggetti aderenti al patto, esplicitando:

- il numero dei diritti di voto riferiti alle azioni o degli strumenti finanziari che attribuiscono diritti di acquisto o di sottoscrizione di azioni o diritti di voto ai sensi dell'articolo 2351, ultimo comma, del codice civile, da ciascuno conferiti;
- le percentuali dei diritti di voto riferiti alle azioni da ciascuno conferiti rispetto al numero totale dei diritti di voto conferiti e al numero totale delle azioni della medesima categoria rappresentative del capitale sociale; se il patto ha ad oggetto strumenti finanziari che attribuiscono diritti di acquisto o di sottoscrizione di azioni o diritti di voto ai sensi dell'articolo 2351, ultimo comma, del codice civile, le percentuali di strumenti da ciascuno conferiti rispetto al numero totale degli strumenti conferiti e al numero totale degli strumenti emessi della medesima categoria nonché il numero delle azioni che possono essere acquistate o sottoscritte;
- il soggetto che in virtù del patto esercita il controllo della società o che è in grado di determinare la nomina di un componente dell'organo di amministrazione o controllo riservata a strumenti finanziari.

Nei patti conclusi in forma associativa e in quelli conclusi fra più di cinquanta soggetti, le informazioni relative agli aderenti aventi una partecipazione non superiore all'un per cento possono essere sostituite dall'indicazione del numero complessivo di tali soggetti, del numero dei diritti di voto riferiti alle azioni complessivamente conferiti e delle percentuali da queste rappresentate rispetto ai parametri sopra indicati. Entro sette giorni dalla pubblicazione dell'avviso di convocazione dell'assemblea di bilancio della società, ovvero dell'assemblea convocata ai sensi dell'articolo 2364-bis del codice civile, è trasmesso alla società stessa un elenco contenente l'indicazione aggiornata delle generalità di tutti gli aderenti e del numero dei diritti di voto riferiti alle azioni da ciascuno conferiti. L'elenco è reso disponibile dalla società per la consultazione da parte del pubblico; d) il contenuto e la durata del patto, precisandone la data di stipula e la relativa efficacia; e) l'ufficio del registro delle imprese presso cui il patto è depositato e la data del deposito.

2. Le informazioni previste dal comma 1, lettera c) sono integrate, se oggetto di previsione nell'accordo, dall'indicazione: a) del tipo di patto tra quelli previsti dall'articolo 122, commi 1 e 5, del Testo unico; b) degli organi del patto, dei compiti ad essi attribuiti e delle modalità di composizione e di funzionamento; c) della disciplina del rinnovo del patto e del recesso dallo stesso; d) delle clausole penali; e) del soggetto presso il quale gli strumenti finanziari sono depositati.
3. Qualora con la pubblicazione dell'estratto e delle informazioni essenziali nel sito internet si intenda assolvere anche agli obblighi di cui all'articolo 120, dovranno altresì essere pubblicati:
   a) l'indicazione dei soggetti che controllano gli aderenti al patto;
   b) il numero dei diritti di voto riferiti alle azioni degli aderenti e non conferiti al patto".

5.2 Revoca dalla quotazione

La permanenza del titolo sul mercato quotato può essere interrotta, è infatti possibile il verificarsi della necessità di sottrarre i titoli dalla quotazione, questa operazione è chiamata delisting.

Con il termine delisting si indica la "rimozione di un titolo azionario dal mercato su cui è quotato, il titolo in oggetto cesserà quindi di essere negoziato sul mercato regolamentato"[188], il ritiro dalle negoziazioni dei titoli della società può avvenire per volontà dell'azionista di maggioranza della società o per decisione di Borsa Italiana.

Questa seconda ipotesi, che è la più frequente, nel Regolamento di Borsa trova collocazione al titolo 2.5, e prevede due possibili azioni: la sospensione e la revoca.

Ai sensi dell'art. 2.5.1 co.1. Borsa Italiana può disporre:

a) la sospensione dalla quotazione di uno strumento finanziario, se la regolarità del mercato dello strumento stesso non è temporaneamente garantita o rischia di non esserlo ovvero se lo richieda la tutela degli investitori;
b) la revoca dalla quotazione di uno strumento finanziario, in caso di prolungata carenza di negoziazione ovvero se reputa che, a causa di circostanze particolari, non sia possibile mantenere un mercato normale e regolare per tale strumento.

Il co. 2 con riferimento alla sospensione stabilisce che Borsa Italiana fa prevalente riferimento ai seguenti elementi:

a) diffusione o mancata diffusione di notizie che possono incidere sul regolare andamento del mercato;
b) delibera di azzeramento del capitale sociale e di contemporaneo aumento al di sopra del limite legale;
c) ammissione dell'emittente a procedure concorsuali;
d) scioglimento dell'emittente;
e) giudizio negativo della società di revisione, ovvero impossibilità per la società di revisione di esprimere un giudizio, per due esercizi consecutivi.

Per quanto attiene la revoca, il co. 7 richiede che Borsa Italiana faccia riferimento ai seguenti elementi:

a) controvalore medio giornaliero delle negoziazioni eseguite nel mercato e numero medio di titoli scambiati, rilevati in un periodo di almeno diciotto mesi;

[188] Glossario Borsa Italiana.

b) frequenza degli scambi registrati nel medesimo periodo;
c) grado di diffusione tra il pubblico degli strumenti finanziari in termini di controvalore e di numero dei soggetti detentori;
d) ammissione dell'emittente a procedure concorsuali;
e) giudizio negativo della società di revisione, ovvero impossibilità per la società di revisione di esprimere un giudizio, per due esercizi consecutivi;
f) scioglimento dell'emittente;
g) sospensione dalla quotazione per una durata superiore a diciotto mesi.

6
Spunti da esperienze recenti

6.1 Banca Popolare di Vicenza

La banca nasce nel 1866 come prima banca vicentina e per circa un secolo rimane radicata esclusivamente nel territorio cittadino[189].

Negli anni Novanta inizia l'acquisizione di alcuni istituti di credito locali, dando attuazione a un piano di sviluppo che si conclude nel 1998 con la nascita del Gruppo Banca Popolare di Vicenza.

Nel settembre 2015 viene condotta un'indagine sul periodo antecedente il 2014, necessaria dopo l'intervento della BCE sui conti dell'istituto che ha comportato una svalutazione notevole, con ripercussioni sulla stabilità e sull'immagine.

L'inchiesta ruota attorno al presidente e all'ex direttore generale, indagati per aggiotaggio[190] e ostacolo alla vigilanza.

La nuova dirigenza decide per un piano industriale[191] che si basa su:

- Eliminazione partecipazioni improduttive (ad eccezione di quelle strategiche);
- Chiusura filiali improduttive;
- Trasformazione in S.p.A.;
- Aumento di capitale;
- Quotazione in borsa.

Nel marzo 2016 l'assemblea dei soci delibera la trasformazione in S.p.A., l'aumento di capitale e la quotazione.

---

189 www.bancapopolaredivicenza/storia.

190 Art. 501 c.p.: "Chiunque, al fine di turbare il mercato interno dei valori o delle merci, pubblica o altrimenti divulga notizie false, esagerate o tendenziose o adopera altri artifici atti a cagionare un aumento o una diminuzione del prezzo delle merci, ovvero dei valori ammessi nelle liste di borsa o negoziabili nel pubblico mercato, è punito con la reclusione fino a tre anni e con la multa da cinquecentosedici euro a venticinquemilaottocentoventidue euro.
Se l'aumento o la diminuzione del prezzo delle merci o dei valori si verifica, le pene sono aumentate. Le pene sono raddoppiate:
1) se il fatto è commesso dal cittadino per favorire interessi stranieri;
2) se dal fatto deriva un deprezzamento della valuta nazionale o dei titoli dello Stato, ovvero il rincaro di merci di comune o largo consumo.
Le pene stabilite nelle disposizioni precedenti si applicano anche se il fatto è commesso all'estero, in danno della valuta nazionale o di titoli pubblici italiani. La condanna importa l'interdizione dai pubblici uffici".

191 Amministratore Delegato Francesco Iorio.

Il 2 maggio 2016 Borsa S.p.A. decide di non disporre l'inizio delle quotazioni per Banca Popolare di Vicenza, facendo decadere il provvedimento di ammissione.

La decisione di non ammettere alla quotazione è stata presa dopo che l'offerta globale aveva collocato solo una piccola quota dell'aumento da un miliardo e mezzo lanciata dall'istituto.

Secondo i risultati infatti il 91,72% sarebbe stato destinato al fondo al Fondo Atlante[192], il 4,97% a Mediobanca, comunque indicato come non computabile ai fini del flottante, e solo lo 0,1% ad altri investitori istituzionali.

In questo modo il pubblico avrebbe detenuto solamente lo 0,36% del capitale, a fronte del 25% richiesto dal Regolamento di Borsa[193] come flottante minimo per essere ammessi, di conseguenza la società di gestione della borsa ha motivato l'esclusione scrivendo che "non sussistono i presupposti per garantire il regolare funzionamento del mercato, a causa dei risultati dell'offerta di sottoscrizione delle azioni"[194].

Infatti l'avvio delle negoziazioni era subordinato alla "verifica della sufficiente diffusione degli strumenti finanziari".

Il fallimento della procedura di quotazione ha comportato una serie di ripercussioni[195]:

- I 120mila soci che hanno le azioni della Popolare di Vicenza ancora una volta non avranno un vero mercato per rivenderle;
- I seimila risparmiatori che avevano deciso di esercitare il loro diritto di prelazione e di acquistare nuove azioni in questo aumento di capitale, non possono più farlo: dato che la quotazione è decaduta, è venuta meno l'intera offerta di azioni. Così questi risparmiatori, che speravano con le nuove azioni di abbassare il valore di carico e di recuperare in prospettiva qualcosa, vengono privati anche di questo diritto;
- Dato che la Popolare di Vicenza resta fuori dalla Borsa, non è sottoposta alla normativa dell'Opa;

---

[192] Il fondo Atlante (tecnicamente un "Fondo di investimento alternativo chiuso riservato") è uno strumento gestito da una società privata, la Quaestio SGR, ma la sua creazione è stata coordinata con il governo italiano e i principali gruppi finanziari del paese. Al momento la dotazione del fondo, cioè i capitali che potrà investire nei suoi due scopi: sostenere gli aumenti di capitale di alcune banche italiane e acquistare crediti deteriorati, arriva in gran parte dalle due principali banche italiane, Unicredit e Banca Intesa, che hanno assegnato al fondo ognuna circa un miliardo di euro. Fondazioni bancarie e altri istituti hanno investito circa cinquecento milioni, mentre altri cinquecento arrivano da Cassa Depositi e Prestiti. Una struttura formalmente privata ma di fatto completamente controllata dal ministero dell'Economia.

[193] Vedasi nota 90.

[194] Nota di Borsa Italiana S.p.A. datata 2 maggio 2016.

[195] www.ilsole24ore.it.

- Per i grandi soci che già avevano azioni della Popolare di Vicenza, il discorso è analogo: anche loro vengono privati dei diritti degli azionisti di minoranza delle società quotate. Per i grandi (primo fra tutti Mediobanca) che invece si erano candidati a comprare azioni della banca questa volta, la mancata quotazione è forse una liberazione: dato che la banca non va più in Borsa, loro non possono più rilevare le azioni;
- Per il fondo Atlante, che ora diventa azionista con il 99,33% della banca vicentina, la mancata quotazione significa, nell'immediato, spendere centoventi milioni di euro in più per rilevare le azioni che avrebbero comprato gli altri investitori: questo significa che il già esiguo patrimonio di Atlante (4,2 miliardi), che in prospettiva servirà anche per rilevare crediti in sofferenza dalle banche, si assottiglia leggermente. Ma per il fondo di sistema la mancata quotazione, a parte questo minimo inconveniente, potrebbe essere in realtà qualcosa di positivo. Atlante avrà infatti tutto il tempo per risanare la banca, senza la pressione della Borsa.

6.2 *Technogym*

Fondata nel 1983, Technogym è un'azienda leader mondiale nella fornitura di tecnologie, servizi e prodotti di design per il settore Fitness e Wellness. Technogym offre una gamma completa di attrezzi per l'allenamento cardio, forza e funzionale, oltre ad una piattaforma digitale cloud che consente agli utenti di connettersi alla loro personale esperienza wellness in qualunque luogo sia tramite i prodotti Technogym stessi sia con dispositivi mobile.

"L'azienda oggi conta circa duemila dipendenti presso le quattordici filiali in Europa, Stati Uniti, Asia, Medio Oriente, Australia e Sud America ed esporta il 90% della propria produzione in oltre cento paesi"[196].

Technogym ha attrezzato 65mila centri Wellness e oltre duecentomila abitazioni nel mondo. Technogym è stata fornitore ufficiale delle ultime cinque edizioni dei Giochi Olimpici: Sydney 2000, Atene 2004, Torino 2006, Pechino 2008, Londra 2012, ed è stata scelta come fornitore ufficiale anche per Rio 2016.

La società aveva avviato l'offerta al mercato con molte richieste e chiuso il collocamento di azioni con una domanda pari a quattro volte l'offerta, mentre il prezzo delle azioni è stato

[196] www.borsaitaliana.it/technogym.

fissato in 3,25 euro dando alla società una capitalizzazione iniziale pari a circa 650 milioni di euro. La quotazione è stata resa possibile dal fondo inglese di private equity, Arle Capital Partners, che dopo otto anni ha deciso di vendere il 25% (28,75% post greenshoe) del 40% in mano alla controllata Salhaouse.

Mediobanca ha agito come sponsor e come responsabile del collocamento per l'Offerta pubblica, mentre i Coordinatori dell'Offerta globale di vendita e Joint Bookrunners e sottoscrizione sono stati Mediobanca, Goldman Sachs e J. P. Morgan, inoltre Nextam ha agito come Co-lead manager.

L'operazione è stata strutturata come offerta pubblica di vendita (Opv), in modo da consentire l'uscita del fondo, mentre la quota restante di maggioranza (ossia il 60%) è rimasta in mano ai fratelli Nerio e Pierluigi Alessandri.

Conclusioni

La quotazione in borsa rappresenta una scelta di notevole rilievo per il management di una società, le cui implicazioni sono non solo economiche, ma anche organizzative.

Si tratta di una decisione che comporta un impegno protratto nel tempo, infatti non si limita alla fase di ammissione, ma richiede la permanenza continua di requisiti e una protratta attività dell'azienda finalizzata a mantenere trasparente il rapporto con gli azionisti e le autorità di vigilanza.

L'analisi e la ricostruzione della procedura di ammissione, obiettivo di questo elaborato, non poteva prescindere da un primario sguardo al consolidamento della definizione di borsa valori, definizione che si è presentata a partire dalla metà del 1500 con la nascita delle prime borse nell'Europa del Nord, e che ora definisce gli odierni sistemi di vendita e acquisto di titoli azionari.

Altro elemento di studio sono state le motivazioni alla base della decisione di accedere alla quotazione, dove si è evidenziata non solo la necessità di accedere ad un canale di finanziamento diverso dal solito credito bancario, ma si è dimostrata anche la possibilità di utilizzare la procedura di quotazione per una riorganizzazione dell'assetto societario e del management, nonché per scopi di pubblicizzazione dell'immagine aziendale.

Sono inoltre stati definiti all'interno di questo studio le figure essenziali e potenziali, previste a livello normativo, con cui la società quotanda entra in relazione nel procedimento di ammissione alla quotazione.

L'analisi della procedura ha portato alla divisione delle fasi di ammissione in tre momenti:

- un momento preliminare dove la società si predispone per la procedura, garantendo la presenza dei requisiti tramite documentazione e scegliendo il segmento di mercato più idoneo a soddisfare le esigenze;
- il secondo momento si contraddistingue per importanza e complessità, la società infatti presenta la domanda di ammissione che deve essere analizzata dalla società di gestione del mercato (Borsa S.p.A.), la quale verifica la sussistenza dei requisiti e può rigettare la richiesta, si passa poi all'istruttoria di Consob sul prospetto e la pubblicazione dello stesso in caso di approvazione. Chiusa la parte degli enti di vigilanza la società affronta il collocamento di titoli sul mercato, fase di notevole importanza, connotata dalla necessità di una immagine solida dell'azienda, tale da convincere gli investitori

(istituzionali e non) della positiva riuscita dell'operazione. Questa parte si conclude con la fissazione del prezzo e l'inizio della negoziazione.

- Il terzo momento si riferisce agli obblighi che derivano dalla quotazione, in particolare si è analizzato sia l'aspetto interno (corporate governance) finalizzato all'equo trattamento degli azionisti e alla trasparente responsabilità del management, sia l'aspetto esterno (obblighi informativi) che sono garanzia di aggiornamento per il pubblico in relazione ad avvenimenti particolari o a scadenze periodiche, garantendo un continuo flusso informativo essenziale per la correttezza del rapporto azionista-società.

L'attualità e l'importanza dell'argomento oggetto di trattazione si evince inoltre dall'analisi di due situazioni reali che si sono concluse in modo diverso, portando con sé conseguenze di notevole rilievo non solo per le aziende coinvolte, ma anche per il mercato nel suo complesso.

La ricostruzione della procedura di ammissione alla quotazione in Borsa, con una analisi specifica di ogni momento, consente di mettere in luce la complessità dell'operazione, che deriva dal rispetto di norme primarie e secondarie stringenti e dalla presenza di una molteplicità di soggetti con compiti e ruoli diversi.

L'articolazione e la complessità della procedura potrebbero essere intesi come elementi di ostruzione all'accesso a un mercato di capitali che può avere notevole valenza strategica per una società in espansione, limitando di fatto le possibilità di guadagno e incremento di produzione.

La necessità di un procedimento articolato, che sottopone la società ad un notevole stress e a controlli serrati da parte di soggetti esterni diviene essenziale per salvaguardare prima di tutto l'integrità del mercato, poi l'integrità della società stessa.

L'ammissione di una società che non è in grado di garantire ab origine la stabilità e la sicurezza necessari per il corretto svolgimento delle contrattazioni comporta ripercussioni sul buon andamento del mercato, in particolare espone il settore di quotazione ad una instabilità capace di causare gravi perdite per tutto il comparto, senza contare che in un mercato altamente globalizzato e multinazionale gli eventi che coinvolgono una Borsa si ripercuotono su scala mondiale.

La mancata ammissione per mancanza di requisiti è però anche uno strumento di tutela verso la società stessa e la sua immagine, impedendo l'ammissione al mercato quotato a chi non ha le capacità si evita che la società si trovi in difficoltà, non riuscendo a raggiungere gli obiettivi stabiliti e richiesti, non fornendo le garanzie dovute agli azionisti, associando il nome dell'azienda a poca se non nulla affidabilità.

Si può quindi concludere che la procedura di ammissione alla quotazione, disciplinata nelle fonti di riferimento, rappresenta uno strumento vitale per il corretto svolgimento delle contrattazioni, la complessità del procedimento risulta infatti necessaria per la determinazione di ammissione, inoltre i continui interventi di soggetti controllori, non solo nella fase di ammissione, ma anche in quella successiva, è un indice di garanzia del rispetto delle prescrizioni, essenziale in un settore che influenza notevolmente l'economia globale.

Bibliografia e sitografia

- S. Alvaro, P. Ciccaglioni, G. Siciliano*, L'autodisciplina in materia di corporate governance Un'analisi dell'esperienza italiana*, QUADERNI GIURIDICI 2, Consob, 2013;
- Banca d'Italia, *Il sistema dei controlli interni, il sistema informativo e la continuità operativa*, note alla Circolare n. 285 del 19 dicembre 2013, Parte Prima, Titolo IV, Capitoli 3, 4 e 5;
- M. C. Cardarelli, sub art.14 (m), a cura di Nigro e Santoro, Torino, 2007;
- G. Chesini, *La regolamentazione e l'organizzazione dei mercati degli strumenti finanziari*, Padova, 1999;
- Renzo Costi-Luca Enriques, *Trattato di Diritto Commerciale*, Il Mercato Mobiliare, VIII volume, Padova, CEDAM, 2004;
- M. De Ambroggi, *La quotazione in borsa*, Parma, Facoltà di economia, 2012;
- S. Dell'Atti, S. Sylos Labini, *Trasparenza informativa: L'impatto delle nuove regole su banche*, Egea, Milano, Maggio 2014;
- Michele de Mari, *La quotazione di azioni nei mercati regolamentati: profili negoziali e rilievo organizzativo*, Torino, Giappichelli Editore, 2004;
- F. Ferrara, F. Corsi, *Gli imprenditori e le società*, Giuffrè, Milano, 2009;
- John Kenneth Galbraith, *Storia dell'Economia*, Milano, Rizzoli, 1988;
- Francesco Galgano, *Diritto Commerciale, Le società*, Bologna, Zanichelli, 2012, XVIII Edizione;
- Francesco Galgano, *Diritto Commerciale, L'imprenditore*, Bologna, Zanichelli, 2012, XVIII Edizione;
- G. Gasbarri, *I controlli interni nelle società quotate- Gli assetti della disciplina italiana e i problemi aperti in Consob*, in QUADERNI GIURIDICI CONSOB 4, Settembre 2013;
- Paolo Montalenti*, Trattato di Diritto Commerciale, La Società Quotata*, IV volume, Padova, CEDAM, 2004;
- L. Nazzicone, S. Providenti, *Amministrazione e controlli nella società per azioni*, Giuffrè, Milano, 2010;
- Donato Ivano Pace, *Ammissione sospensione esclusione dai mercati regolamentati*, Milano, Giuffrè Editore, 2012;
- G. Siciliano, *Cento anni di Borsa Italiana*, Bologna, 2001;
- *La scelta di quotarsi in borsa e l'impatto sull'azienda*, corso di Gestione finanziaria delle imprese, Facoltà di Economia, LIUC;
- *Comitato per la corporate governance,* Codice di autodisciplina della borsa italiana, Luglio 2014;

- Regolamento n. 11971 del 14 maggio 1999, come successivamente modificato, con delibera Consob n. 15232 del 29 novembre 2005 (Regolamento Emittenti);
- Regolamento dei mercati organizzati e gestiti da Borsa Italiana;
- Testo Unico delle disposizioni in materia di intermediazione finanziaria d. lgs. 58 del 1998 (TUF);
- Testo unico delle leggi in materia bancaria e creditizia d.lgs. 385 del 1993 (TUB);
- Testo unico delle imposte sui redditi d.p.r. 917 del 1986 (TUIR);
- www.bankpedia.org
- www.borsaitaliana.it
- www.consob.it
- www.economiauniparthenope.it
- www.italianieuropei.it
- www.misterfisco.it
- www.wikipedia.org

CYBERCRIME
ASPETTI GIURIDICI E STRUMENTI DI CONTRASTO AI REATI CONNESSI AL *CYBERSPACE*

Ten. Giovanni De Liso

"Che io possa avere la forza di cambiare le cose che posso cambiare,
che io possa avere la pazienza di accettare le cose che non posso cambiare,
che io possa avere soprattutto l'intelligenza di saperle distinguerle"

San Tommaso Moro

INDICE

Introduzione

Mentre i *leader* mondiali accelerano gli sforzi per mettere a punto un nuovo catalogo di sviluppo per la lotta ai reati consumati nel mondo digitale, l'utilizzo globale di *internet* continua ad espandersi: quasi tre miliardi della popolazione mondiale utilizza piattaforme *online* per comunicare, lavorare, imparare o accedere a servizi pubblici[1].

Non c'è da sorprendersi, quindi, che la crescita della comunità internazionale stia valutando come sfruttare al meglio i vantaggi derivanti dall'utilizzo delle nuove Tecnologie della Comunicazione (ICT)[2]. Tale sviluppo, tuttavia, potrebbe essere pericoloso se non accompagnato da una discussione seria sulla necessità di affrontare i rischi posti dalla proliferazione di applicazioni infrastrutturali ICT e di un progresso sostenibile di *internet.*

Infatti, contestualmente all'evoluzione dei dispositivi digitali, si è avuta la nascita di molte e nuove forme di reato e di aggressione criminosa talvolta commesse per mezzo di sistemi informatici e/o telematici. Proprio per tali ragioni, si è ritenuto necessario con il presente studio approfondire questo tema, essendo il crimine informatico, seppur in continua mutazione, la nuova frontiera alla quale dover volgere lo sguardo.

Le Forze di Polizia, infatti, non possono non essere al passo con i tempi, per continuare a garantire il complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale, sia sul piano preventivo che su quello repressivo.

A tal fine è necessario conoscere e studiare ciò che si contrasta, impegnandosi a comprendere gli aspetti principali di ciò che si affronta, e padroneggiare con sapienza e consapevolezza gli strumenti offerti dalla procedura penale e dal diritto internazionale.

Alla luce di tali obiettivi, il primo capitolo del presente lavoro si concentrerà sugli aspetti fenomenologici e sulle questioni processuali legate al *Cybercrime,* cercando di spiegare in modo semplice e chiaro gli elementi teorici e tecnici utili a comprendere il mondo affascinante e complesso del *Cyberspace*, partendo dal concetto di "domicilio informatico", spiegando chi è un *hacker,* fino a trattare della differenza tra programmi dannosi e sabotaggi informatici.

Una volta analizzato il substrato teorico, si procederà a trattare i principali profili di diritto processuale penale implicati e le tecniche specifiche di indagini sui reati informatici: la

---

1 Pawlak P., *Riding the digital wave, The impact of cyber capacity building on human development,* Report n. 21, dicembre 2014.

2 Le Tecnologie dell'Informazione e della Comunicazione (*TIC,* in inglese *Information and Communications Technology* - ICT), sono l'insieme dei metodi e delle tecnologie che realizzano i sistemi di trasmissione, ricezione ed elaborazione di informazioni (tecnologie digitali comprese).

procedura penale, invero, trovandosi ad affrontare nuove affascinanti sfide giorno dopo giorno, data la straordinaria e spaventosa mutevolezza del mondo informatico, necessita di essere protagonista dell'analisi, specie alla luce delle continue modifiche dovute alle direttive comunitarie.

Il terzo capitolo tratterà delle "prove informatiche" per soffermarsi più specificamente sulla loro natura e sulle loro specifiche modalità di acquisizione e conservazione, senza dimenticare il concetto di autenticità, di duplicazione e di integrità, per poi concludere sottolineando l'importanza del fattore del tempo per le "prove digitali".

Il quarto ed ultimo capitolo, sarà infine incentrato sul contrasto internazionale alla criminalità informatica e all'analisi della strategia dell'Unione Europea per la *Cyber* sicurezza. Si procederà all'analisi degli gli strumenti internazionali volti alla lotta al *cybercrime,,* alla *cyberdefence policy* e all'*Interantional cyberspace policy*. In conclusione, ci si soffermerà sugli organi principali che si occupano maggiormente di questo tema.

CAPITOLO PRIMO

I reati informatici: aspetti fenomenologici e questioni processuali

1. Il *Cyberspace* e il cosiddetto *domicilio informatico*

La globalizzazione ha creato un orizzonte comune a livello planetario per gran parte dell'umanità, che si caratterizza per il fatto di essere costituito, per una parte non marginale, da quello che viene chiamato ormai comunemente *"Cyberspace"*.

Ufficialmente, l'ISO[3] / IEC[4] 27032 definisce il *Cyberspace* come «l'ambiente complesso risultante dall'interazione di persone, *software* e servizi su *Internet* per mezzo di dispositivi e reti ad esso collegati tecnologia, che non esiste in nessun fisico modulo»[5].

Si tratta perciò di una realtà virtuale, non per questo meno incisiva sulla vita reale, un "meta-territorio", ossia una dimensione che non si caratterizza per le normali coordinate spazio-temporali, ma vi si sovrappone, simulandole.

Sembra dunque alludersi a un ambiente virtuale *online* complesso, molto variabile o fluido, e quindi di difficile quantificazione, specie nello stabilire i rischi per la sicurezza associati ad esempio alle informazioni. Proprio per comprendere e saper scegliere quali strumenti giuridici utilizzare al fine di contrastare tutte le violazioni e i crimini legati al *cyberspace,* è importante sapere quanto di questo spazio rientri nel concetto del cosiddetto *domicilio informatico.*

---

[3] L'Organizzazione Internazionale per la Normazione (in inglese *International Organization for Standardization*) - abbreviazione ISO - è la più importante organizzazione a livello mondiale per la definizione di norme tecniche. Il termine "ISO" non è un acronimo, bensì deriva dal greco ἴσος, che significa "uguale". La scelta di un termine di origine greca, anziché di un acronimo, è stata determinata dall'intento di ricerca di un'abbreviazione che avesse carattere di universalità (l'acronimo è invece solitamente legato alla lingua rispetto alla quale viene usato).

[4] La Commissione Elettrotecnica Internazionale (*International Electrotechnical Commission* in inglese, *Commission Electrotechnique Internationale* in francese), acronimo *IEC* (dal nome inglese), è un'organizzazione internazionale per la definizione di *standard* in materia di elettricità, elettronica e tecnologie correlate. La maggior parte di essi sono definiti in collaborazione con l'*ISO* (Organizzazione Internazionale per la Normazione). Questa commissione è formata da rappresentanti di enti di standardizzazione nazionali riconosciuti. La *IEC* ha il compito di sviluppare e distribuire gli *standard* per le unità di misura, in particolare il *gauss*, l'*hertz* e il *webe*r. Essa, inoltre, è stata la prima a proporre un sistema, il Sistema Giorgi, che intorno al 1960 si è modificato nel sistema delle unità SI. Sono identificati da numeri interi progressivi e il loro titolo ricalca la forma seguente: *IEC 60411 Graphical Symbols*. Gli *standard*s sviluppati congiuntamente con l'*ISO* utilizzano gli identificatori numerici di questo ed hanno titoli di una forma come la seguente: *ISO/IEC 7498-1:1994 Open Systems Interconnection: Basic Reference Model.* Il comitato *ISO/IEC Joint Technical Committee 1 (ISO/IEC JTC1)* è descritto più dettagliatamente nella voce dedicata all'*ISO*.

[5] *«The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form».*

Secondo la Corte di Cassazione[6] «… deve ritenersi *domicilio informatico*, quello spazio ideale - ma anche fisico in cui sono contenuti i dati informatici - di pertinenza della persona, cui si estende la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto».[7]

Pertanto, un domicilio informatico è un'area di pertinenza virtuale a geometria variabile nella disponibilità diretta della parte, la quale non necessariamente coincide con il contenuto informativo del dispositivo fisico in esame, ma può essere distribuito anche in aree diverse dal territorio nazionale, come ad esempio il *Cloud* [8].

2. Il Dato Informatico

Premettendo che per "dato" si intende la rappresentazione oggettiva di un fatto o evento che consenta la sua trasmissione oppure interpretazione da parte di un soggetto umano o di uno strumento informatico e per informazione, l'interpretazione e il significato assegnato a uno o più dati, la definizione di *domicilio informatico* appena indicata richiama il paradigma *RID* (Riservatezza, Integrità e Disponibilità) fondamento della Sicurezza Informatica:

- Con il termine *Riservatezza* si intende che le informazioni devono essere accessibili direttamente o indirettamente solo alle persone che ne hanno diritto e che sono espressamente autorizzate a conoscerle.
- Con il termine *Integrità* si comprende che i dati e le rispettive informazioni devono essere protette da alterazioni, quali modifiche, danneggiamenti o cancellazioni improprie, anche accidentali.
- Con il termine *Disponibilità* si vuole indicare che i dati e le rispettive informazioni devono essere sempre accessibili agli utilizzatori che ne hanno diritto nei tempi e nei

---

6 Cass., sez. VI, 14 dicembre 1999, n. 3067, in Cass. pen., 2000; Cass., sez. V , 6 luglio 2007, n. 31135, in *Dirittoitalia.it*.

7 Art. 15 Cost.

8 In informatica con il termine inglese *cloud* (in italiano "nuvola") si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità *on demand* attraverso *internet* a partire da un insieme strumenti preesistenti e configurabili. Esse non vengono pienamente configurate e messe in opera dal fornitore apposta per l'utente, ma gli sono assegnate, rapidamente e convenientemente, grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti lasciando all'utente parte dell'onere della configurazione. Quando l'utente la rilascia, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel *pool* condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.

modi previsti. La disponibilità delle informazioni va assicurata in base ad un livello di servizio concordato.

Fino all'introduzione della Legge 18 marzo 2008, n. 48, che ha ratificato la Convenzione di Budapest sul *Cybercrime* del 23 novembre 2001, il «*dato informatico*» era considerato di fatto una cosiddetta "prova atipica".[9]

L'art.1, comma 1 del trattato n. 185 del Consiglio d'Europa definisce, infatti, il dato informatico come «qualsiasi rappresentazione di fatti, informazioni o concetti in una forma adatta per l'elaborazione di un sistema informatico, compreso un programma atto in grado si far funzionare un sistema informatico»,[10] il quale non è altro che un dispositivo o un gruppo di dispositivi interconnessi o collegati, uno o più dei quali, secondo un programma, esegue l'elaborazione automatica dei dati.[11]

Nel nostro Paese il concetto di *sistema informatico* è solo parzialmente corrispondente a quello europeo: infatti, secondo la Corte di Cassazione «deve ritenersi *sistema informatico* un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (*bit*), in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente».[12] La parte mancante è tradotta in Italia con il concetto di *sistema telematico* che «è l'insieme di più sistemi informatici collegati tra loro per lo scambio di informazioni, purché siano connessi in modo permanente, e purché lo scambio di informazioni sia il mezzo necessario per conseguire i fini operativi del sistema».[13]

---

9 Tale argomento è trattato nel cap.2, par 5.

10 «*"Computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*».

11 «*"Computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*».

12 Cass., sez. VI, 14 dicembre1999, n. 3067, in Cass. pen., 2000. Cass., sez. V , 6 luglio 2007, n. 31135, in *Dirittoitalia.it*.

13 Cass., sez. VI, 14 dicembre1999, n. 3067, in Cass. pen., 2000. Cass., sez. V , 6 luglio 2007, n. 31135, in *Dirittoitalia.it*.

3. Metodi di intrusione nei sistemi e nelle reti

A prima vista, i comportamenti illeciti aventi ad oggetto un dispositivo informatico sembrano essere caratterizzati da un alto grado di abilità tecnica da parte dell'autore; questa impressione iniziale, però, deve essere assolutamente smentita. Va infatti premesso che anche le violazioni più complesse possono essere compiute da soggetti privi di competenze specifiche, grazie a particolari programmi scaricati da *internet* e poi semplicemente avviati dal proprio *computer* (si pensi alla diffusione di *virus* oppure all'intercettazione di comunicazioni *online*, oggi consentite da applicazioni pronte all'uso e condivise gratuitamente sul *web*).

Partiamo, dunque, introducendo il concetto di *hacking*: esso è un comportamento volto a violare la sicurezza dei sistemi informatici e delle reti telematiche.

In linea di principio, l'accesso abusivo a un dispositivo elettronico non è animato da un fine di lucro, bensì da un mero scopo ludico. Non è infrequente, tuttavia, che il soggetto, una volta superate le barriere di protezione, decida di copiare le informazioni contenute nel sistema violato, oppure di inserirvi un programma dannoso.[14]

Negli Stati Uniti questa nuova forma di estorsione si riscontra soprattutto presso le grandi aziende, le quali, pur di non diffondere nel pubblico la notizia negativa di una falla nella sicurezza informatica, sono disposte a pagare immediatamente gli *hacker* che le minacciano. In Italia non si conoscono ancora casi del genere, dato che nei resoconti sulla sicurezza informatica delle imprese vengono riportate in generale le violazioni delle misure di protezione senza specificare se contestualmente vi siano stati o meno comportamenti di minaccia o estorsione[15].

I metodi con cui sono attuate le intrusioni nei sistemi informatici sono molto vari, da quelli rudimentali ai più sofisticati; sebbene gli accessi abusivi più insidiosi a sistemi informatici siano compiuti a distanza, per esempio da *hackers* entrati illegalmente nella medesima connessione *internet* del *computer* bersaglio, sono decisamente più frequenti le violazioni

---

[14] Solo per citare i principali testi di riferimento di una letteratura vastissima: Casey E., *Digital evidence and computer crime. Forensic Science, computer and thè internet,* Elsevier Academic Press, Second Edition, 2004; Clifford R. D., *Cybercrime: thè investigation, prosecution and defense of a computer-related crime,* cit.; Leman-Langlois S. (editing), *Technocrime,* cit.; Moore R., *Cybercrime: investigating high-technology computer crime,* cit.; Smith R. G., Grabosky P., Urbas G., *Cyber criminals on trial,* Cambridge, 2004. Come si può notare dalla semplice lettura dei titoli, questi lavori hanno in comune un taglio poco dottrinale e molto pratico, essendo focalizzati sulle modalità di investigazione e sulle regole processuali riguardanti i reati informatici.

[15] Per una prospettiva più dogmatica e normativa occorre rifarsi al primo "manuale" di diritto penale dell'informatica, ormai divenuto un classico della materia, scritto da un illustre Autore tedesco: Sfeber U., *The intemational handbook for computer crime. Computer-Related Economie Crime and the Infringements of Privacy*, New York, 1986.

commesse *in loco* sulle macchine aziendali da parte di dipendenti insoddisfatti o da poco licenziati.

Occorre precisare che il fenomeno del *phishing* si distacca totalmente da quello *dell'hacking,* per il motivo che l'*hacker* mira semplicemente ad accedere nel sistema informatico della vittima, mente il *phisher* intende sfruttarne il profilo finanziario, per cui anche le disposizioni penali applicabili sono assai diverse: da un lato, l'*hacking* è sanzionato dall'art. 615 *ter* c.p., dall'altro, il *phishing,* qualora sia seguito dall'effettivo conseguimento in capo al *phisher* di un'utilità patrimoniale, è in genere ricondotto dalla giurisprudenza alla fattispecie della truffa (art. 640 c.p.). Resta comunque il fatto che per la commissione di entrambi i reati è possibile servirsi dei medesimi comportamenti di *social engineering.*

Passando ora alle tecniche di intrusione più sofisticate, in quanto richiedenti competenze informatiche di buon livello, dobbiamo considerare prima di tutto l'installazione di programmi di *key-logging*[16] che registrano ogni tasto premuto sulla tastiera del dispositivo e trasmettono in tempo reale queste informazioni alla cosiddetta "casa madre", ossia il *computer* dell'*hacker*. Basta che l'utente abbia digitato una sola volta sulla tastiera sorvegliata il codice di accesso perché l'*hacker* entri in possesso immediato della *password*. Questo particolare tipo di programma penetra nel sistema informatico in vari modi: innanzitutto, può essere installato inavvertitamente dall'utente durante il *download* di diversi *software* o visitando siti *internet* poco sicuri; inoltre, non mancano casi in cui sono i supporti esterni, quali *cd-rom*, penne *usb* e periferiche auto-installanti *(plugandplay),* a contenere il *key-logger*.

Oltre ai programmi di *key-logging,* gli *hackers* possono attaccare il sistema bersaglio tramite *software* di decifrazione delle *passwords*, noti come *decryptor*. In realtà questi metodi sono estremamente costosi in termini di tempo e di denaro, poiché in caso di diversi livelli di protezione si ottiene l'accesso anche dopo settimane o mesi.

Ciò comporta che la tecnica di decifrare le *passwords* sia adottata solo in presenza di notevoli interessi economici o strategici, come è accaduto in alcuni casi di spionaggio industriale o militare. Difficilmente, quindi, l'archivio elettronico di un *personal computer* verrà violato con metodi di decifrazione delle *passwords*; assai più frequente, invece, è l'abuso del meccanismo di cifratura, soprattutto a seguito dell'accesso abusivo a un dispositivo informatico. Per coprire le proprie azioni illegali, infatti, gli "intrusi" nelle reti telematiche nascondono l'origine dell'attacco criptandone ogni passaggio e rendendo così quasi impossibili le indagini penali.

In aggiunta, i codici d'accesso sono acquisiti facendo uso della tecnica nota come *"XXS* -

16 Su *key-loggers, decryptors* e sull'utilizzo investigativo da parte delle forze di polizia statunitensi.

cross site scripting"[17] grazie alla quale in un sito *internet* lecito vengono inseriti dei comandi dannosi, capaci di leggere negli archivi dei singoli *computers* che si connettono alla pagina *web* modificata. I siti oggetto di simili violazioni sono soprattutto quelli di istituzioni bancarie, previdenziali e commerciali, le quali offrono servizi *online* dietro registrazione e inserimento di dati sensibili come il numero di carta d'identità, di conto corrente bancario o di carta di credito. In questo modo assistiamo ad attacchi combinati: da un lato, l'*hacker* può leggere direttamente le informazioni registrate sul sito violato; dall'altro, il *software* di *scripting* risale alla fonte di queste informazioni, ossia prende visione dei *files* memorizzati nei *computers* connessi al sito.

Altre modalità di intrusione nei sistemi informatici sono caratterizzate dall'induzione in errore del titolare del codice d'accesso, grazie al "dirottamento" vero e proprio dei comandi impartiti dall'utente legittimo.

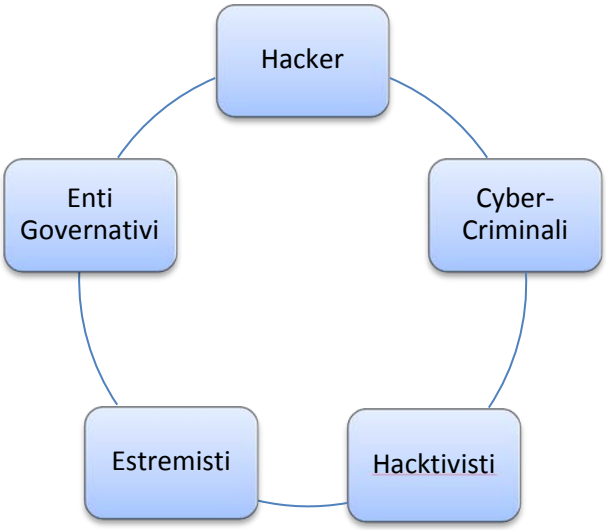
Queste condotte sono piuttosto difficili da qualificare sotto un'unica fattispecie incriminatrice, constando al contempo in un accesso abusivo e in un'intercettazione telematica illecita. Per quanto riguarda il "dirottamento" dei comandi (cosiddetto *spoofmg*), esso altera i meccanismi che associano le istruzioni digitate sulla tastiera alle operazioni compiute dal *computer*: ad esempio, un determinato indirizzo *web* conduce, invece che al sito *internet* desiderato, a uno falso, creato per richiedere informazioni personali alla vittima *(web spoofing*). Ancora più sofisticati sono i metodi di *IP spoofmg*, *DNS spoofmg* e *HTTP spoofing,* i quali si basano sulla clonazione delle credenziali d'accesso di un *computer* a una rete aperta (come *internet)* o chiusa, qualora metta in condivisione un numero determinato di dispositivi.

Volendo schematizzare il funzionamento di questi accessi abusivi assai complessi sotto il profilo tecnico, *l'hacker* si intromette nella connessione tra il singolo *computer* e il *computer server*, che, una volta riconosciuto l'utente, lo collegherà alla rete: grazie a questa intrusione il soggetto estraneo riesce a farsi autorizzare dal *server* ad accedere a tutti gli archivi condivisi in via telematica, senza nemmeno dover violare le misure di protezione del *computer* "dirottato", bensì sostituendosi ad esso nella navigazione.

---

[17] Sui dettagli tecnici del metodo XXS e dei vari tipi di spoofmg si soferma Sieber U., *Organised crime in Europe: thè threat of cyber crime*, Situation Repori 2004, Council of Europe Publishing, 2005, p. 89-91.

4. Chi "*HACKERA*"?



Oltre ai cosiddetti *hackers* di cui si è già trattato, esistono altre tipologie di soggetti, sintetizzati e rappresentati nello schema sopra riportato, i quali interagiscono in maniera diversa e in modo più o meno lecito all'interno del *cyberspace*:

- il cosiddetto *Cyber-Criminale* è un soggetto il cui unico interesse è l'«ingiusto profitto con l'altrui danno», perseguito attraverso strumenti come *botnet*[18], *skimming*[19], *blackmail*[20] e realizzato mediante mezzi di pagamento virtuale (es. *BitCoin*).[21] Rispetto al criminale comune, egli approfitta della Rete per realizzare le attività criminose su un territorio potenzialmente vasto quanto l'intero globo terrestre, nonché la quantità di vittime fa sì

[18] Una *botnet* è una rete formata da dispositivi informatici collegati ad *internet* e infettati da *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 distribuiti 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*.

[19] La lettura orientativa (talvolta chiamata anche col termine inglese *skimming*), è un processo che consiste nel cercare visivamente all'interno di una pagina degli indizi che aiutino a farsi un'idea sommaria dei contenuti della stessa. Ciò avviene solitamente a una velocità molto superiore (intorno alle settecento parole al minuto), rispetto a una normale lettura fatta per comprendere completamente un testo (circa 200-230 parole al minuto), e infatti porta a livelli di comprensione molto scarsi, soprattutto se si sta leggendo un testo ricco di contenuto informativo. Gli esperti considerano questa pratica rischiosa, e pertanto consigliano di usarla solo quando la comprensione non è necessaria.

[20] Estorsione.

[21] Il cosiddetto *Bitcoin* è una moneta elettronica creata nel 2009 da Satoshi Nakamoto. È anche il nome del progetto *software open source* sviluppato per il suo uso. Il *Bitcoin* è una delle prime implementazioni del concetto chiamato *cryptomoneta*, che fu per la prima volta descritto nel 1998 da Wei Dai nella *mailing list cypherpunks*. È considerata moneta digitale ogni sorta di dato, che sia accettato come pagamento per beni e servizi e pagamenti per i debiti in un dato Paese o contesto socio-economico. Il *Bitcoin* è sviluppato attorno all'idea dell'uso della crittografia per controllare la creazione e il trasferimento di moneta, invece di appoggiarsi ad autorità centrali.

che si configuri una mancata percezione del disegno criminoso, il quale il più delle volte sfocia in vere e proprie associazioni per delinquere[22]

- i cosiddetti *Hacktivisti* sono definiti dalla Corte di Cassazione [23] come « una organizzazione non statica, operante in una dimensione di per sé aperta e non individuabile su una base meramente territoriale». Un esempio su tutti è *Anonymous*[24], di fatto un'associazione per delinquere di carattere transnazionale (art. 416 c.p.), in quanto è caratterizzata da un progetto di comune attacco infrastrutturale, con una ripartizioni dei ruoli;
- i cosiddetti *Estremisti* sono complessi da descrivere, poiché sono varie le forme di *cyber-estremismo* esistenti: un esempio è il terrorismo, il cui principale interesse è quello di creare panico ed insicurezza nell'opinione pubblica (es. *Defacement*[25]); ma vi rientra anche la propaganda e il proselitismo al fine di reclutare nuovi seguaci (es. *Socialnetworking*), ovvero pure il cosiddetto *Cyber-Bullismo*, ossia qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, nonché qualunque forma di furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica;
- i cosiddetti *Enti Governativi* sviluppano e/o impiegano *malware* per diversi fini: investigativi, di giustizia (es. uso di agenti nelle intercettazioni attive), informativi, di sicurezza nazionale (es. *The Dukes*[26], *Turla*[27]). Si tratta di militari o comunque di appartenenti alle forze dell'ordine che usano vere e proprie *cyber-weapons* (es. *Stuxnet*, attacco informatico subito dall'Estonia nel 2007[28]).

---

22 Art. 416 c.p.

23 Cass., sez. fer., 16 dicembre 2013, n. 50620, c.c. 12 dicembre 2013, Preite.

24 *Anonymous* è una forma di attivismo e un fenomeno *internet* che identifica singoli utenti o intere comunità *online* che agiscono anonimamente - in modo coordinato o anche individualmente - per perseguire un obiettivo concordato anche approssimativamente.

25 *Defacing* (termine inglese che, come il suo sinonimo *defacement*, ha il significato letterale di «sfregiare, deturpare, sfigurare», in italiano reso raramente con "defacciare") nell'ambito della sicurezza informatica ha solitamente il significato di cambiare illecitamente la *home page* di un sito *web* (la sua "faccia") o modificarne, sostituendole, una o più pagine interne. Pratica che, condotta da parte di persone non autorizzate e all'insaputa di chi gestisce il sito, è illegale in tutti i Paesi del mondo.

26 *Dukes* - un gruppo *APT* che conduce campagne di *cyber spionaggio* e lo *spear-phishing* per manipolare i propri bersagli e portarli ad esporsi agli attacchi da loro condotti.

27 *Turla* è un'operazione di presunta matrice russa che in otto anni ha preso di mira organizzazioni militari e di *intelligence*, istituzioni governative, ambasciate, istituti di ricerca e altri obiettivi di primo piano, spiega Kaspersky (nota azienda per prodotti utili alla difesa del proprio cyberspace), infettando centinaia di *computers* (*Windows* e non solo) in più di quarantacinque Paesi prevalentemente localizzati in Asia.

28 *Stuxnet* è un virus informatico creato e appositamente e diffuso dal governo USA (nell'ambito dell'operazione "Giochi Olimpici" iniziata da Bush nel 2006 e che consisteva in un "ondata" di "attacchi digitali" contro l'Iran) in collaborazione col governo israeliano. Lo scopo del *software* era di sabotare la centrale nucleare iraniana di Natanz, in particolare disabilitare le centrifughe della centrale, impedendo la rilevazione dei malfunzionamenti e del virus stesso.

5. Programmi dannosi e sabotaggi informatici

Gli accessi non autorizzati nelle memorie elettroniche sono senza dubbio molto frequenti, ma non rappresentano la minaccia più grave alla sicurezza dei sistemi informatici; la maggior preoccupazione degli utenti di *computers*, invero, è di evitare i virus e gli altri programmi dannosi. La diffusione di *software* pericolosi assume rilevanza penale autonoma, a prescindere dal verificarsi di un danno al sistema informatico, in forza dell'art. 615 *quinquies* c.p., introdotto dalla Legge n. 547 del 1993.

Pertanto, non si può comprendere l'oggetto materiale delle condotte incriminate senza prima fare chiarezza sui concetti di programma dannoso e di virus. I programmi dannosi sono meglio noti sotto il nome di *malware*, una contrazione di *malicious software*, che si può tradurre letteralmente come *software* "maligni". I *malware* rappresentano una categoria ampia, che racchiude una molteplicità di programmi aventi effetti negativi sul normale funzionamento di un sistema informatico. II tipo di *malware* più noto è senza dubbio il *virus*, al punto che impropriamente per virus si indicano tutti i programmi dannosi in generale. La caratteristica specifica dei virus è quella di essere ospitati da un altro programma, all'interno del quale si annidano e si diffondono. In altre parole, un virus non è un programma a sé stante, bensì consiste in una serie di comandi aggiunta ad un'applicazione preesistente.

Il meccanismo con cui opera un virus è abbastanza semplice: quando il *software* contenitore si attiva, immediatamente entra in funzione anche il virus, oppure attende il verificarsi di una condizione prefissata dal suo programmatore (in quest'ultimo caso il virus funziona come una bomba a orologeria e perciò è chiamato *logic bomb* - bomba logica).

I primi virus erano ospitati soltanto da alcuni programmi particolari, detti eseguibili, i quali eseguivano operazioni indipendenti dall'intervento umano.

Oggi, invece, pressoché tutti i *files* e le applicazioni possono avere al loro interno un virus, in quanto anche una semplice pagina scritta con in formato w*ord* consente lo svolgimento di azioni automatiche (in gergo macro).

Nella comunità degli *hackers* chi crea virus in questo modo riceve il soprannome alquanto spregiativo di "*script kid*", ossia di "ragazzino nella programmazione".

Gli *script kiddies* rappresentano una seria minaccia alla sicurezza dei sistemi informatici, soprattutto per il fatto che, essendo degli *hackers* alle prime armi, spesso ignorano gli effetti reali delle proprie azioni e possono dare luogo a danneggiamenti molto più devastanti del previsto.

Un caso clamoroso avvenne nel 2000, quando uno *script kid* quindicenne (conosciuto con il nome di MafiaBoy) causò seri danni economici (quasi due miliardi di dollari) ai più importanti siti di commercio elettronico negli Stati Uniti e in Canada, semplicemente utilizzando programmi *malware* scaricati da *internet*.

Tornando ai diversi tipi di *malware,* bisogna precisare che i virus sono comunque del tutto inoffensivi una volta isolati dal *software* contenitore. Questo permette di distinguere i virus dai cosiddetti *worm* ("vermi" in inglese), che al contrario sono dei programmi autosufficienti, in grado di replicarsi e di danneggiare il *computer* da soli. I *worm* sono meno famosi dei virus, tuttavia dopo l'avvento di *internet* sono divenuti il tipo di *malware* più diffuso e più insidioso in assoluto. A differenza dei virus, che possono essere bloccati evitando di aprire il *file* infetto, essi entrano nei dispositivi informatici in modo invisibile, sfruttando le falle (cosiddetti *bugs)* nei sistemi operativi o nei programmi anti-virus, e si riproducono spontaneamente negli archivi elettronici del sistema attaccato.

Dopo l'auto-replicazione, le nuove copie di *worms* vanno ad attaccare tutti i *computers* connessi al dispositivo infetto, secondo due modalità alternative: o inviando loro messaggi automatici di posta elettronica con il virus in allegato*,* oppure sfruttando falle simili a quelle del sistema informatico infetto.

Gli effetti di questo programma differiscono in parte da quelli di un virus: se quest'ultimo ha come scopo necessario la cancellazione della memoria elettronica o il malfunzionamento delle applicazioni, per un worm questo effetto è soltanto eventuale. Il primo obiettivo è infatti quello di "bucare" le barriere di sicurezza di un dispositivo, per consentire in un secondo momento l'installazione di altri programmi dannosi. Questo non deve portare a ritenere che i *worms* di per sé siano software innocui o, al massimo, fastidiosi: il loro processo di auto-riproduzione impiega le risorse del *computer* attaccato, fino a impedire il normale funzionamento dei programmi di prevenzione e diagnostica contro il *malware*. Peraltro, la fase successiva di diffusione produce sovente una mole gigantesca di *e-mail* indesiderate, in grado di saturare le caselle di posta elettronica dei destinatari o, nei casi più gravi, di sovraccaricare il computer server. Non mancano, infine, *worms* a scopo esclusivamente distruttivo, che causano danni irreversibili all'archivio elettronico o al sistema operativo, analogamente ai virus informatici.

Devono essere tenuti distinti dai *worms* altri due tipi di programmi dannosi, i *trojan* e le *backdoors*, che non di rado aggrediscono congiuntamente il dispositivo bersaglio, tramite un meccanismo a scatole cinesi: il programma interviene per primo, poiché è in grado di superare

le misure di protezione e di installarsi autonomamente nella memoria elettronica del *computer*; all'interno del *worm* può trovarsi un *trojan*, che a sua volta include delle cosiddette *backdoor*.

Andando per ordine, i *trojan* prendono il loro nome dal Cavallo di Troia, in quanto essi sono sempre contenuti in un programma apparentemente inoffensivo.

Mentre i *worm* si diffondono automaticamente, i *trojan* hanno bisogno di un'azione diretta da parte della vittima e per questo motivo sono spesso nascosti all'interno di programmi condivisi tra gli utenti, primi fra tutti i videogiochi su *internet*. In alternativa, i *trojan* vengono trasmessi inconsapevolmente, essendo veicolati da un *worm*.

Gli effetti dannosi di un *trojan* sono diversi da quelli distruttivi o impeditivi propri di un virus informatico: di solito, il primo sottrae in tutto o in parte il dominio della macchina al legittimo utilizzatore, per consentire all' *hacker* di intervenire sul sistema e sottrarre le informazioni in esso contenute senza che il titolare se ne accorga.

Negli ultimi dieci anni, peraltro, si è affermato un nuovo uso criminoso dei *trojan*: essi non sono più finalizzati al furto di dati digitali, bensì al controllo remoto dei dispositivi infetti, che in tal modo diventano strumenti per la commissione di attacchi informatici. Il *trojan* è immesso in una molteplicità di *computer*s e lasciato inattivo per un certo periodo di tempo; quando scade il termine fissato dall'*hacker* il programma dannoso si risveglia e comincia a impartire comandi a tutti i sistemi violati, formando così una vera e propria rete di automi (detti *zombie*). Questo è il fenomeno conosciuto sotto il nome di *botnet*, del quale si tratterà *infra,* a proposito dei cosiddetti attacchi *DDoS*. Ai fini del presente paragrafo evidenziamo solo la tecnica informatica impiegata, che consiste per l'appunto nella diffusione massiccia di programmi *trojans*.

Per quanto concerne le *backdoor*, sono quasi sempre contenute in un "cavallo di Troia" informatico; il significato in italiano di *backdoor* è "porta sul retro", ciò che indica un programma che crea delle aperture nascoste nelle misure di sicurezza di un dispositivo informatico. Una volta aperta questa "porta di servizio", qualunque *hacker* che ne conosca l'esistenza può entrare nella memoria e nel sistema operativo del *computer*, in modo da utilizzarlo in qualità di amministratore e a totale insaputa del legittimo titolare.

Di conseguenza, la *backdoor* semplifica sensibilmente l'azione degli *hackers,* poiché attraverso questa "porta lasciata aperta" chiunque può prendere il controllo di un sistema quando vuole, fino al momento in cui viene scoperto e risolto il difetto di protezione.

Gli effetti negativi delle *backdoor* sono molto preoccupanti: invero, esse espongono il *computer* a un numero illimitato di attacchi da remoto, dal furto di dati sensibili fino alla commissione di sabotaggi informatici.

In sintesi, i programmi a scopo esclusivamente dannoso, denominati *malware* dalle discipline informatiche, si distinguono in quattro categorie principali: i virus, i *worms*, i *trojan horses* e le *backdoor*. I loro effetti potenziali sono la distruzione della memoria elettronica, l'alterazione del funzionamento del sistema oppure la perdita del controllo su di esso da parte del titolare.

Per concludere questa rapida introduzione alle varie tecniche di danneggiamento informatico, è utile accennare ai sabotaggi virtuali realizzati su internet.

Queste forme di abuso delle reti telematiche sono note con l'acronimo di "*DoS*", che sta per *Denial of Service*, in italiano "blocco del servizio". Essi prendono di mira siti *web* popolari (come quelli di commercio elettronico), di pubblica utilità o di enti istituzionali, sovraccaricandoli di richieste di informazioni fino alla completa paralisi (*crash*) degli stessi.

Talvolta gli attacchi sono giustificati dagli autori sulla base di ideologie estremiste o di mobilitazioni contro determinati governi o imprese multinazionali: l'episodio più noto negli ultimi mesi è stato il sabotaggio di alcuni siti ritenuti "collaborazionisti" con le forze di polizia, ad opera dei sostenitori di Julien Assange, portavoce di *Wikileaks* .

Una variante più recente è il cosiddetto attacco "*DDoS*", sigla di *Distributed Denial of Service*, ossia "blocco diffuso del servizio". A differenza del primo tipo di sabotaggio telematico, commesso da uno o più *hackers* in modo simultaneo, l'attacco DDoS si serve dei *computer*s altrui, precedentemente infettati da un *trojan* e coordinati così in una *botnet* (rete di *robot).*

Quando si verificano le condizioni prestabilite nel programma *malware*, i *computers* si trasformano in *robot* e rispondono ai comandi impartiti da un soggetto esterno, il quale può eseguire un attacco *Denial of Service* avendo a disposizione un numero elevatissimo di macchine. È intuibile quanto siano dannosi sabotaggi telematici a così ampio raggio, senza considerare il problema dell'individuazione degli autori effettivi, dato che la maggior parte dei dispositivi viene sfruttata all'insaputa del titolare.

Emblematici in tal senso sono i due episodi principali di attacchi *DDoS,* il primo avvenuto ai danni dei siti della pubblica amministrazione estone nel 2007, il secondo tramite la diffusione a livello globale del *worm* di nome *Stuxnet* nel 2010: in entrambi i casi sono state causate gravissime perdite economiche in tutto il mondo, ma gli ideatori e gli esecutori dei danneggiamenti sono rimasti ignoti. Esistono tuttavia forme di sabotaggio virtuale meno distruttive, primo fra tutti il *defacing*, una pratica impiegata soprattutto in segno di protesta, la quale come detto consiste nell'alterazione dell'aspetto di una pagina web, inserendovi messaggi offensivi, dure contestazioni politiche o addirittura una schermata nera.

6. Alcuni reati informatici "impropri"

Nei paragrafi che precedono abbiamo descritto la fenomenologia dei reati informatici in senso proprio; le fattispecie di accesso abusivo a un sistema e di danneggiamento informatico, difatti, sono nate insieme alla diffusione dei dispositivi elettronici e della rete *internet* e sono perciò difficilmente assimilabili a reati tradizionali come la violazione di domicilio, il furto o il danneggiamento comune, mancandone l'oggetto materiale.

Si può quindi sostenere che i *cybercrimes* si caratterizzino per la peculiarità dell'*oggetto* dell'azione criminosa, il quale consiste, chiaramente, nel *software* di un sistema informatico o di una rete di *computers*[29]. Facendo l'esempio del sabotaggio virtuale sopra descritto, esso non può ritenersi integrato qualora un soggetto distrugga fisicamente un *computer*, poiché in tal caso egli commette il reato di danneggiamento comune; risponde al contrario di un reato informatico il soggetto che renda inservibile tale dispositivo sovraccaricandolo di operazioni o inserendovi un *malware,* in quanto l'azione è diretta contro la componente logica e immateriale del *computer* e non sulla sua struttura fisica[30].

Altri reati sono invece definiti comunemente *"cybercrimes"* in maniera impropria, poiché è diverso il ruolo del dispositivo elettronico nella condotta illecita: se per i reati informatici in senso stretto il *software* è *l'oggetto necessario* dell'azione, per quelli in senso lato esso è soltanto uno *strumento eventuale* per la realizzazione del fatto.

Più esplicitamente: mentre le condotte di *hacking* sono illeciti assolutamente nuovi per il diritto penale, fenomeni criminosi quali le frodi informatiche oppure le intercettazioni *online* rappresentano solo modalità innovative di reati tradizionali come la truffa e l'intercettazione di comunicazioni. Il criterio della strumentalità non può fondare la definizione dei reati informatici, poiché, al limite, quasi tutti i reati potrebbero essere commessi con l'ausilio delle tecnologie elettroniche e quindi avremmo un'infinità di *cybercrimes,* mere "copie tecnologiche" di fattispecie previgenti.

---

[29] La notizia dell'attacco all'Estonia causò un vero e proprio *shock* all'Unione Europea e agli esperti di sicurezza, poiché l'Estonia è un Paese modello sul piano delle tecnologie informatiche (per darne un'idea, l'intera gestione della pubblica amministrazione è digitale). Un rapporto molto completo al riguardo è stato pubblicato sul sito *http://www.wired.eom/politics/securitv/magazine/l 5-09/f estonia.* Sul caso *Stuxnet,* sono state fatte molte ipotesi, la più diffusa delle quali sostiene che dietro questo potentissimo *worm* vi sia una "guerra cibernetica" in atto tra Stati Uniti e Israele, da un lato**,** e l'Iran, dall'altro. Tra i vari *computers* danneggiati figurano, infatti, anche quelli delle centrali nucleari iraniane. In proposito, si consulti *http://uk.reuters.eom/article/2010/09/24/us-securitv-cvber-iranfb.* La classificazione è illustrata da Clough J, *Principles of cybercrime*, Cambridge, 2010, p. 11-13.

[30] In senso conforme al testo Pica G., v. *Reati informatici e telematici,* in *Dige. Disc. pen. Eco.,* Aggiomam. I, 2000, p. 526; *contra* Pecorella C., *Diritto penale dell'informatica,* Padova, 2006, p. 115.

L'unico criterio per individuare i *cybercrimes* in modo selettivo e rigoroso è dunque esclusivamente quello dell'oggetto dell'aggressione.

La distinzione tra reati informatici propri e impropri appare lineare e schematica a livello teorico, poiché basta semplicemente individuare il ruolo del *computer* nella dinamica criminosa (oggetto dell'azione o suo strumento) e, di conseguenza, "etichettare" la condotta come *cybercrime* oppure come reato tradizionale commesso tramite mezzi elettronici.

Nella pratica, però, questa classificazione mostra segni di cedimento, perché spesso è controverso l'oggetto dell'azione (si pensi alla frode elettronica, dove parte della giurisprudenza individua l'oggetto materiale nel *computer* manipolato e altra parte, maggioritaria, nel patrimonio dell'utente). I concetti di oggetto dell'azione e di strumentalità subiscono, infatti, una torsione e una sovrapposizione in ambito di reati informatici, nel senso che non è sempre agevole scindere i casi in cui l'abuso del *computer* è l'oggetto della condotta da quelli in cui esso sia solo un mezzo per la lesione di interessi ulteriori[31]. Emblematico è il fenomeno del furto di identità digitale; circa il cosiddetto *identity thief* : si dibatte da tempo se sia qualificabile o meno come reato informatico: da un lato, infatti, oggetto dell'azione sono i dati informatici di un soggetto (*cybercrime* non previsto dalla nostra legislazione), dall'altro possiamo interpretare queste condotte non come accessi abusivi a un archivio elettronico, ma come violazioni della *privacy* per mezzo di dispositivi tecnologici (applicazione estensiva dei reati previsti dal Codice della *Privacy*).

Come si vede dall'esempio appena riportato, decidere in merito alla natura informatica di un reato non ha pura rilevanza teorica, bensì incide sulla tipicità delle condotte e in particolare sulla loro sussumibilità sotto fattispecie incriminatrici già esistenti. In definitiva, è opportuno impiegare le nozioni di reato informatico proprio e improprio soltanto a livello orientativo, senza accettarle acriticamente e rigidamente.

7. Principali problemi di diritto penale sostanziale e processuale[32]

L'abuso delle tecnologie informatiche pone numerosi interrogativi per l'ordinamento giuridico in generale e per il diritto penale in particolare; la natura immateriale e spesso transnazionale delle condotte entra in corto circuito con le categorie tradizionali del soggetto

[31] Alma M., Perroni C., *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici,* in *Dir. pen. proc.,* 1997, n. 4, p. 506-507.

[32] Liberamente tratto da Milanetti F., *Accesso abusivo e danneggiamento dei sistemi informatici aspetti criminologici e giuridici*, Università La Sapienza.

attivo del reato, del bene giuridico tutelato, dell'elemento psicologico e così via il punto di partenza è un dato fondamentale: i reati informatici non aggrediscono e non strumentalizzano cose mobili o tangibili, bensì dati e programmi elettronici, ossia la componente logica di un dispositivo. Questo è l'elemento comune a tutti i *cybercrimes,* sia in senso stretto sia in senso lato; anche le violazioni commesse su reti telematiche, infatti, possono essere scomposte in una serie di alterazioni o di interruzioni del funzionamento di singoli *software.*

Il contesto necessariamente virtuale entro il quale si inscrive questa categoria di illeciti non può che influenzare a monte le fattispecie incriminatrici e a valle le relative disposizioni processuali. È facile prevedere che non manchino i problemi, soprattutto a causa dell'insuperabile divario tra la rapida evoluzione tecnologica dei fenomeni criminosi e la rigidità propria della legislazione penale. Verranno affrontate in questa sede le questioni di maggior interesse per quanto riguarda i principi generali della materia penale-informatica, guardando prima ai profili sostanziali e poi a quelli processuali.

La descrizione della fenomenologia dei reati informatici dà un'idea della molteplicità dei comportamenti passibili di sanzione penale; il primo dubbio che sorge attiene all'identificazione dei beni giuridici da questi lesi. L'offensività dei *cybercrimes* è infatti difficile da cogliere in alcuni casi: mentre un atto vandalico nei confronti di un sistema elettronico produce immediate conseguenze negative sul piano patrimoniale, la mera detenzione nel proprio *computer* di programmi dannosi o di codici di accesso altrui, senza diffonderli né comunicarli a terzi, sembrerebbe un comportamento innocuo. Per fondare qualsiasi tipo di incriminazione non si può prescindere dall'osservanza dei principi di *extrema ratio,* determinatezza e tassatività; ancora più importante in questo ambito del diritto penale è riuscire a mantenere una proporzione tra la severità della risposta punitiva e il grado di intensità dell'offesa a beni giuridici rilevanti. La correlazione tra gravità della violazione e gravità della sanzione non è sempre rispettata dai reati informatici previsti nel nostro codice penale, dove anzi figurano esempi di fattispecie di pericolo presunto assai criticabili.

In ogni caso, resta sullo sfondo la domanda fondamentale: quali beni giuridici sono lesi dai reati informatici? La ricerca di un interesse protetto unitario sotteso a tutti i reati informatici, tuttavia, fornisce risultati alquanto deludenti, poiché volendo adattare il "bene giuridico informatico" alle diverse fattispecie non si fa altro che dilatarne il significato fino all'indistinto.

A ben vedere, la collocazione delle disposizioni sui delitti informatici in capi distinti del codice penale è una spia evidente dell'eterogeneità dei beni giuridici offesi dagli abusi dei dispositivi elettronici. Inoltre, la scelta del legislatore di inserire nel codice, e non in una legge

complementare, le fattispecie penali informatiche dimostra che, almeno tendenzialmente, gli interessi tutelati dovrebbero essere gli stessi dei corrispondenti reati tradizionali. Questa osservazione è agevolmente dimostrabile con riferimento ai reati informatici "impropri", tra i quali figurano il falso informatico (art. 491 *bis* c.p.), la violazione di corrispondenza telematica (art. 616 c.p.), l'intercettazione di comunicazioni informatiche (art. 617 *quater* c.p.) e la frode informatica (art. 640 *ter* c.p.). Tali previsioni possono essere ritenute degli "aggiornamenti tecnologici" di incriminazioni preesistenti, sotto il profilo specifico delle modalità della condotta, ma non muta l'interesse protetto. Il discorso opposto vale per i reati informatici in senso tecnico: qui sussiste effettivamente un problema di individuazione del bene giuridico e le interpretazioni a disposizione sono molte. In primo luogo, dobbiamo suddividere in due gruppi i *cybercrimes* "veri e propri": da una parte il reato di accesso abusivo, dall'altra le diverse forme di danneggiamento informatico.

Sul fondamento punitivo dell'accesso abusivo di cui all'art. 615 *ter* c.p.[33] sono state proposte varie teorie: la più diffusa tra gli studiosi, recepita dalla Corte di Cassazione[34], vi ravvede la difesa di un nuovo bene, il cosiddetto *domicilio informatico*. Come in precedenza affermato, i dati registrati su un *computer* e protetti da misure di sicurezza sono la proiezione "virtuale" del domicilio fisico; quindi, il domicilio fisico e quello informatico costituiscono entrambi spazi di esclusiva pertinenza della persona, cui estendere la tutela della riservatezza, bene di rango costituzionale *ex* art. 14 Cost.

Funzionale alla piena protezione della "riservatezza informatica" è allora la fattispecie di pericolo prevista dall'art. 615 *quater* c.p., che incrimina la detenzione e la diffusione abusiva di codici di accesso: il legislatore intende perseguire non solo le avvenute violazioni della sicurezza, ma anche le condotte univocamente dirette all'intrusione nel sistema, come il procurarsi illegittimamente *passwords* altrui. Altra dottrina critica la tesi del domicilio informatico, poiché porta a un arretramento eccessivo della soglia di rilevanza penale: assumendo tale posizione, infatti, saremmo portati a tipizzare le semplici violazioni delle misure di protezione, non accompagnate da un'effettiva cognizione dei dati riservati[35].

---

[33] L'art. 615 *ter* c.p. (Accesso abusivo a un sistema informatico o telematico) punisce la condotta di chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo; il reato è punito con la reclusione fino a tre anni.

[34] Cass., sez. VI, 4 ottobre 1999, n 3554, Piersanti, in *Cass. pen.*, *2000, p.* 2990 e disponibile anche sul sito *http://www.ictlex.net.*
In argomento, in dottrina, si v. Mantovani F., *Diritto Penale. Parie speciale. Delitti contro il patrimonio,* Padova, 2009, p. 136.

[35] Mantovani F., *Diritto Penale, delitti contro la persona*, I. ed. Cedam, 1995, p. 359.

Se il bene protetto è la riservatezza degli archivi elettronici, allora risulta contraddittorio punire il mero ingresso o mantenimento abusivo nella memoria del *computer*, senza appurare se ne sia stato letto il contenuto.

Rimanendo in tema di bene giuridico protetto, vi è stato chi ha assunto una prospettiva ulteriore, rifiutando le tesi del domicilio informatico e della riservatezza, nonché quella, del tutto isolata, dell'accesso abusivo come reato di pericolo astratto rispetto al danneggiamento. Secondo tale impostazione, la disposizione tutelerebbe piuttosto l'interesse all'"indisturbato godimento" di un dispositivo informatico; l'art. 615 *ter* c.p., cioè, dovrebbe incriminare le turbative nella fruizione di un *computer* ai danni del legittimo utilizzatore. Il requisito delle misure di protezione servirebbe a selezionare le condotte dotate di maggior disvalore, poiché altrimenti sarebbero incriminati tutti gli usi indebiti di un sistema, con l'effetto abnorme di una penalizzazione a tappeto. È infatti esplicita nella Relazione alla Legge 547/93 la volontà del legislatore di non punire i semplici "furti di tempo", ossia gli sfruttamenti parassitari dei servizi informatici altrui.

La tesi presta il fianco a molte critiche: prima fra tutte, la disposizione in esame non accenna neppure indirettamente ad un effetto di turbativa arrecato dall'ingresso abusivo nel sistema; inoltre, non si comprende a quale posizione giuridica debba riferirsi il "godimento indisturbato", potendo insistere sullo stesso *computer* diritti e facoltà di fonte e contenuto differente. Infine, il difetto principale di questa ipotesi esegetica è lo scarso attaccamento alla realtà delle intrusioni negli archivi informatici: nella maggior parte dei casi questi accessi abusivi avvengono senza disturbare l'utente legittimo del *computer,* anzi spesso non sono neppure scoperti. Ricordiamo solo l'esempio dei programmi *backdoors*, che creano falle nascoste nelle misure di protezione del dispositivo, senza che la vittima possa accorgersene. La teoria del "godimento indisturbato" ha però il pregio di sottolineare un aspetto sottovalutato dai sostenitori del "domicilio informatico": i dati contenuti in un dispositivo elettronico non possono essere *de plano* assimilati ai dati riservati né ai dati sensibili, anzi i *files* protetti non hanno tipicamente un contenuto personalistico, bensì un valore economico.

Inoltre, a difesa della riservatezza dell'individuo esistono già le sanzioni penali del Codice della *Privacy* (artt. 167 e ss. del d.lgs. 196/2003), che predispongono una tutela ampia ed esaustiva dei dati personali contro qualsiasi intervento o trattamento abusivo, a prescindere dalla loro archiviazione in un sistema informatico protetto.

Non si può negare che la collocazione codicistica dell'art. 615 *ter* c.p. e la terminologia impiegata dal legislatore del 1993 per la descrizione del fatto tipico siano poco felici, in quanto

suggeriscono un'analogia tra domicilio fisico e sistema informatico giuridicamente debole e inesistente nella realtà[36]. Bisogna, peraltro, evidenziare il fatto che l'art. 615 *ter* c.p. contempla espressamente l'accesso a sistemi e non a dati, quindi il baricentro dell'incriminazione non poggia sul contenuto personale del dispositivo informatico, ma sulla protezione con mezzi logici dello stesso; a conferma ulteriore possiamo citare la circostanza aggravante prevista dal terzo comma della disposizione, in cui figurano i *computers* di pubblica utilità, per i quali non si può assolutamente parlare di archivio elettronico come proiezione della sfera personale. Trattare quindi del bene della riservatezza informatica disorienta, poiché il reato di accesso abusivo tutela sì un bene giuridico autonomo, ma questo a ben vedere è la stessa *sicurezza informatica.*

Cosa significa sicurezza informatica? Vuol dire che il legislatore predispone una difesa aggiuntiva, mai esclusiva, dei dispositivi informatici: l'utente deve prima organizzare delle misure di protezione di tipo tecnico, anche molto semplici[37], poi se queste non hanno funzionato ed è avvenuta un'intrusione abusiva interviene il diritto.

Questa interpretazione rende la fattispecie pienamente conforme ai principi di proporzione e sussidiarietà dell'intervento punitivo: qualora il soggetto passivo dell'accesso non si sia precedentemente "cautelato", dimenticando di predisporre delle barriere minime agli ingressi non autorizzati nel proprio sistema informatico, non può esigere dall'ordinamento giuridico una reazione repressiva contro l'*hacker.*

In effetti, in assenza di limitazioni all'accesso o al mantenimento in un sistema informatico, non si può nemmeno parlare di abusività della condotta, né di violazione della sicurezza, poiché i sistemi e le reti possono essere solo di due modi: "protetti", cioè sono utilizzabili solo da un numero determinato di soggetti, oppure "aperti", ossia a disposizione di chiunque. Da tali considerazioni discende la soluzione per la qualificazione giuridica dei cosiddetti "furti di tempo": essi non sono puniti dall'art. 615 *ter* c.p., perché non violano la sicurezza informatica, causando solo uno spreco di risorse, penalmente irrilevante.[38] Nel 2004 la Corte di Cassazione ha stabilito che non è ravvisabile il reato di accesso abusivo se il sistema

---

[36] Mantovani F., *Diritto Penale, delitti contro la persona*, I. ed. Cedam, 1995.

[37] Per le incertezze sul concetto di riservatezza in generale si veda Mantovani F., *Diritto Penale. Parte speciale. Delitti contro la persona,* Padova, 2008, p. 533, nota n. 3.
Secondo la giurisprudenza prevalente l'art. 615 *ter* c.p. incrimina anche la violazione di misure insufficienti alla reale protezione del computer, dovendosi escludere un requisito di idoneità delle barriere tecniche, Cass. pen., sez. V, 7 novembre - 6 dicembre 2000, n. 1675, rie. Zara, pubblicata su *Cass. pen.,* 2002, p. 1018 in senso contrario GUP Roma, 4-21 aprile 2000, disponibile sul sito *www.penale.it.*

[38] Aterno S., *Le misure di sicurezza nel reato di accesso abusivo: l'agente deve averle neutralizzate, commento a sentenza della Cassazione sul reato di accesso abusivo*, in *Diritto dell'internet*, 1, 2008, Ipsoa.

informatico o telematico nel quale l'imputato si inserisce non risulta obiettivamente protetto da misure di sicurezza (per un uso specifico)[39].

Se tutto ciò è vero - si è osservato in dottrina - il concetto di domicilio informatico come bene giuridico tutelato deve essere rivisto. Il bene protetto nell'intrusione informatica non può essere (soltanto) ciò che intendiamo comunemente come "domicilio" definito inviolabile, protetto con l'art. 614 c.p. e poi tutelato costituzionalmente con l'art. 14 perché altrimenti non si spiegherebbe come mai la tutela è condizionata dalla presenza delle misure di sicurezza[40].

Il concetto di "domicilio" - si aggiunge - comunemente inteso, di cui al Titolo XII, Capo 11, sezione IV, del codice penale è qualcosa di diverso, tanto che la sua tutela non è limitata dal requisito delle protezioni o "misure di sicurezza". In caso di intrusione informatica ritenere che il solo bene giuridico tutelato sia il "domicilio informatico" può creare qualche problema interpretativo e applicativo, anche perché mal si concilia con le ipotesi aggravate del sistema informatico di interesse pubblico, di interesse militare o relativo all'ordine pubblico, alla sicurezza pubblica o alla sanità[41]. Dietro l'analisi della struttura del reato di accesso abusivo ad un sistema informatico vi è dunque, la riflessione[42] sul dilemma riguardo la sua collocazione come reato "di pericolo astratto" o reato "di danno".

È preferibile interpretare anche la fattispecie incriminatrice *ex* art. 615 *quater* c.p., in modo da descriverla come un reato di pericolo concreto. Infatti, la previsione del requisito dell'*idoneità* dei codici a violare le barriere poste all'accesso di un sistema dovrebbe essere accertata effettivamente e non presunta o dedotta dalle caratteristiche astratte della *password*.

Per esempio, procurarsi o diffondere una parola chiave (seppur esatta) di un *computer* con più livelli di protezione non integra il reato, poiché il codice d'accesso è inidoneo in concreto a ledere la sicurezza di quel particolare dispositivo informatico. Lo stesso ragionamento può essere applicato alle *passwords* errate, da ritenere escluse dalla fattispecie anche quando presentino delle qualità astrattamente idonee a violare le misure di protezione.

Passando al secondo gruppo di reati informatici *strictu sensu* intesi, l'individuazione del bene giuridico sottostante alle incriminazioni del danneggiamento virtuale si dimostra meno problematica.

---

[39] "*Non c'è reato di accesso abusivo se sul sistema informatico "attaccato" mancano le misure di sicurezza*" (art. 615 ter c.p.), commento alla sentenza della Corte di Cassazione sez. VI, 27 ottobre 2004 (dep. 30 novembre 2004), n. 46509, *http://www.penale.it/page.asp?mode=1&IDPag=174*.

[40] Mantovani F., *Diritto Penale, delitti contro la persona*, I. ed. Cedam, 1995, p. 359.

[41] Idem; si consenta il rinvio a Cass. 4 ottobre 1999, n. 3067, p. 2990, in *Cassazione penale*, 2000, con nota critica di S. Aterno a p. 2994.

[42] Atemo S., *Il reato di accesso abusivo a sistema informatico tra reato di danno e reato di pericolo*, in *www.penale.it*

In dottrina è opinione condivisa che l'interesse protetto sia *l'integrità informatica,* ossia la salvaguardia di dati, programmi e sistemi dalla loro alterazione o cancellazione abusiva[43]. Occorre però chiarire il concetto di "integrità": esso non si riduce a una conservazione statica delle impostazioni fissate nel *computer,* ma si rivolge alla *funzionalità* del dispositivo, in altri termini alla sua capacità di svolgere operazioni.

La precisazione ha importanti ricadute applicative: nel caso in cui un *malware* cancelli alcuni dati contenuti nella memoria elettronica di un *computer*, il sistema operativo non subisce danni, né tantomeno il programma che gestisce il salvataggio dei *files,* ma quello specifico archivio è reso inservibile per la funzione cui l'utente lo aveva destinato e quindi ricorre una lesione della integrità informatica.

Viceversa, il criterio della funzionalità consente di escludere la tipicità di alterazioni minime come la modifica temporanea dell'aspetto grafico di uno schermo (che invece sarebbe rilevante in una concezione rigida della integrità informatica).

Anche l'inserimento di dati falsi o estranei in *files* preesistenti è una condotta lecita di principio, fatta eccezione per l'intervento abusivo su un documento informatico avente efficacia probatoria, punibile ai sensi dell'art. 491 *bis* c.p., cioè a titolo di falso informatico. Dagli esempi fatti emerge chiaramente come le offese all'integrità informatica, per essere ritenute tali, debbano comportare l'inservibilità - quantomeno parziale - dei dati o dei sistemi alterati, ispirandosi così al modello del danneggiamento comune di cui all'art. 635 c.p.; la condotta del "rendere inservibili" era contemplata dall'art. 635 *ter* c.p. nella versione originaria del 1993 ed oggi dagli articoli 635 *quater* e 635 *quinquies* c.p., che sanzionano il danneggiamento di sistemi informatici e telematici.

L'interesse all'integrità dei dispositivi assume valenze diverse a seconda della funzione pubblica o privata dei *computers* danneggiati: le aggressioni a sistemi di uso privato sono perseguite in un'ottica patrimonialistica (procedibilità a querela della persona offesa, sulla falsariga della fattispecie non aggravata di danneggiamento), mentre le azioni rivolte contro impianti di pubblica utilità sono represse già allo stadio dell'attentato, poiché oltre all'integrità informatica esse minacciano l'ordine pubblico e l'incolumità pubblica.

Pure il reato di diffusione di programmi dannosi, previsto dall'art. 615 *quinquies* c.p., è finalizzato alla tutela dell'integrità informatica, anticipando la soglia di rilevanza penale a un momento anteriore rispetto all'evento lesivo. Sicuramente si tratta di una fattispecie di pericolo, per alcuni commentatori addirittura di reato ostacolo.

---

[43] Pecorella C., *Il diritto penale dell'informatica*, Padova, 2006, p. 59.

In ogni caso, la fattispecie è stata molto discussa in dottrina sin dalla sua introduzione con la Legge 547/1993; in seguito, la Legge 48/2008 di ratifica della Convenzione sul *Cybercrime* ha nuovamente riscritto il fatto tipico antigiuridico.

Sintetizzando, il testo originale dell'art. 615 *quinquies* c.p. puniva una serie di condotte relative a programmi «aventi per scopo o per effetto» il danneggiamento informatico.

Il legislatore aveva adottato un criterio obiettivo per selezionare i comportamenti illeciti, ossia guardava alle caratteristiche dei *malwares* in sé, senza considerare le reali intenzioni dell'agente: al limite, poteva essere punito anche l'esperto informatico che testasse un *virus* a scopo scientifico e che, inavvertitamente, cagionasse danni al sistema in uso. La deriva verso un'imputazione colposa e persino obiettiva era un rischio evidente; sotto il profilo dell'offesa dell'integrità informatica, inoltre, la fattispecie contemplava le condotte di diffusione, comunicazione e consegna del programma dannoso, che sono ancora ben lontane dal danneggiamento di un sistema, in quanto prescindono dalla successiva attivazione del *malware.* Per come era formulata, la fattispecie poteva pacificamente applicarsi alla diffusione di un *virus* mai entrato in funzione o innocuo per un difetto di programmazione[44], soltanto perché creato con l'obiettivo di danneggiare. La novella del 2008 ha introdotto un elemento soggettivo di tipicità, inserendo il dolo specifico di «danneggiare illecitamente un sistema ovvero di alterarne il funzionamento»; tuttavia, ha allo stesso tempo eliminato il parametro oggettivo della portata dannosa del programma. Considerato il fatto che l'elenco delle condotte è stato dilatato fino a comprendere la produzione e la detenzione di un *malware*, il risultato della modifica è un'ulteriore anticipazione della tutela, assai difficile da adeguare ai principi di offensività e proporzione.[45]

Se già si sospettava che l'art. 615 *quinquies* c.p. fosse nato come un reato di pericolo presunto, adesso, dopo le modifiche del 2008, questo sospetto è divenuto certezza. L'intenzione -non dichiarata- del legislatore è quella di incriminare il cosiddetto "rischio tecnologico" insito al settore dell'informatica; perde significato l'offensività della condotta, perché il disvalore è concentrato tutto sulla mera volontà di ledere l'integrità dei sistemi altrui.

---

[44] Il testo attuale dell'art. 615 *quinquies* c.p. (*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico),* così recita: *«Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due armi e con la multa sino a euro 10.329».* Mantovani F., *Diritto Penale. Parte speciale. Delitti contro la persona,* Padova, 2008, p. 526-527.

[45] Salvadori I., *Hacking, cracking e nuove forme di attacco ai sistemi d'informazione. Profili di diritto penale e prospettive de jure condendo*, in *Cyber. Dir.,* 2008, n. 9, p. 352-353.

Probabilmente la giurisprudenza compirà un'opera di ortopedia interpretativa, che eviti risvolti pratici abnormi: stando alla lettera della disposizione, per fare solo un esempio, è tipica la condotta di chi, animato da intenti vandalici, crei un programma assolutamente inoffensivo e lo salvi nel *computer,* senza neppure comunicarlo all'esterno.

Dov'è la messa in pericolo dell'integrità informatica? Forse sarebbe stato meglio tenere tutti e due i criteri selettivi: quello oggettivo, sulle qualità del programma, e soggettivo, il nuovo dolo specifico.

Inoltre, dovrebbero essere tipizzate esclusivamente le condotte diffusive, poiché la produzione e la detenzione di un programma dannoso non sono affatto pericolose per l'integrità dei *computer*s altrui. Così l'area di operatività della norma si restringerebbe e, forse, avremmo finalmente stabilito un collegamento tra l'inoculazione volontaria del *malware* nel dispositivo bersaglio e la probabilità dell'evento lesivo.

Bisogna sottolineare a questo punto che i due "beni informatici" della sicurezza e dell'integrità devono essere tenuti su piani distinti: essi hanno significati diversi, dato che la sicurezza riguarda lo "scudo esterno" dei dispositivi e l'integrità il loro funzionamento interno.

Alcuni indici normativi dimostrano che il fondamento punitivo dell'accesso abusivo è differente da quello del danneggiamento informatico[46]; il più importante fra questi è l'assenza del requisito delle misure di protezione nelle disposizioni sul sabotaggio virtuale. Sono pertanto penalmente rilevanti tutte le condotte distruttive, modificative e comunque lesive della funzionalità di un dispositivo informatico indipendentemente dall'esistenza di barriere di sicurezza.

L'integrità dei *softwares* è allora tutelata in maniera autonoma dalla sicurezza dei sistemi: se un soggetto commette un accesso abusivo e dopo ciò danneggia il *computer* violato, egli sarà punito ai sensi del reato aggravato dall'evento di cui all'art. 615 *ter,* comma 2, n. 3 c.p.; in breve, il reato di danneggiamento non assorbe quello di ingresso illecito, né accade l'inverso.[47]

Dopo queste riflessioni sugli interessi lesi dai reati informatici, possiamo concludere che i beni giuridici nuovi, nati dall'affermazione delle tecnologie informatiche nella società, sono soltanto due: la *sicurezza*, tutelata dalle norme sull'accesso abusivo e sulla detenzione illecita di *password*s altrui, e l'*integrità*, protetta a stadi differenziati dai reati di danneggiamento, di attentato a computer pubblici e di produzione e distribuzione di *malwares*.

Dal punto di vista del diritto penale sostanziale, gli interessi protetti da reati informatici

---

46 In senso contrario Piciotti L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* cit., p. 62.

47 Lusitano D., *In tema di accesso abusivo a sistemi informatici o telematici*, in *Giur. it.,* 1998*,* p. 1926.

costituiscono, senza ombra di dubbio, il tema più complesso; sussistono tuttavia altre incongruenze con gli istituti di parte generale, che verranno adesso affrontati in modo schematico, per completare le osservazioni sui problemi generali posti dai *cybercrimes*.

Sono questioni non ancora affrontate dal legislatore né dalla giurisprudenza, sebbene esigano una soluzione chiara sin dalla promulgazione della Legge 547/1993.

CAPITOLO SECONDO

Aspetti di procedura penale e tecniche specifiche nelle indagini sui reati informatici

1. Evoluzione normativa per la tutela dei "Sistemi informatici o telematici"

L'Italia, dopo aver recepito nel 2008 le indicazioni europee in materia di protezione delle Infrastrutture Critiche e aver ratificato, nello stesso anno, la Convenzione di Budapest sul *Cybercrime*, con il Decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013, ha delineato il proprio Quadro strategico nazionale (Qsn)[48] per la sicurezza dello spazio cibernetico, identificando enti, attori, ruoli, responsabilità e procedure, pervenendo così alla individuazione della struttura nazionale di contrasto alle minacce informatiche rivolte verso strutture pubbliche e private.

In precedenza, le competenze sul tema erano attribuite a differenti organi, in un contesto normativo complesso e articolato, come di seguito delineato:

- La Direttiva del Presidente del Consiglio dei Ministri del 16 gennaio 2002 (Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali) sanciva l'importanza della protezione del patrimonio informativo gestito dai sistemi pubblici, in quanto risorsa di valore strategico per il Paese, raccomandando l'immediato avvio di azioni tese a conseguire una "base minima di sicurezza".
- I D.p.c.m. dell'11 aprile 2002 e del 22 luglio 2011 demandavano all'attuale Ufficio Centrale per la Segretezza (Ucse)[49] le funzioni di certificazione per i sistemi che trattavano informazioni classificate e per la definizione delle misure di sicurezza cibernetica da adottare a protezione dei sistemi e delle infrastrutture informatiche che trattavano informazioni classificate o coperte dal segreto di Stato.

[48] Il Quadro Strategico Nazionale (QSN) è il documento strategico-programmatico che definisce gli interventi e le strategie di politica regionale da attuarsi in Italia nel periodo 2007-2013.

[49] L'Ufficio centrale per la segretezza (UCSe) svolge funzioni direttive, consultive, di coordinamento e controllo in materia di tutela amministrativa del segreto di Stato e delle classifiche di segretezza; cura gli adempimenti istruttori relativi all'esercizio delle funzioni del Presidente del Consiglio quale Autorità nazionale per la sicurezza, a tutela del segreto di Stato; predispone le misure volte a garantire la sicurezza di quanto è coperto dalle classifiche di segretezza; si occupa del rilascio e della revoca delle abilitazioni di sicurezza per le persone fisiche e giuridiche; conserva e aggiorna l'elenco di tutti i soggetti muniti di NOS; cura l'attività di negoziazione e predisposizione degli accordi di sicurezza con organizzazioni internazionali e Paesi esteri.

- Il Decreto interministeriale 14 gennaio 2003, modificato dal Dpcm del 5 settembre 2011, istituiva l'Osservatorio permanente per la sicurezza e la tutela delle reti e delle comunicazioni presso l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (*Iscti*: noto anche come "*Iscom*" in quanto riferito alla precedente denominazione dell'Ente: Istituto Superiore delle Comunicazioni) del Ministero dello Sviluppo economico (Mise).
- Il D.lgs. del 1° agosto 2003, n. 259, recante il Codice delle comunicazioni elettroniche, affidava all'allora Ministero delle Comunicazioni (confluito nell'attuale Mise) competenze in materia di sicurezza e integrità delle reti pubbliche di comunicazione elettronica accessibili al pubblico.
- Il D.p.c.m. del 30 ottobre 2003 identificava nell'*Iscom* (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione) l'organismo di certificazione della sicurezza nel settore della tecnologia dell'informazione, attribuendogli il compito di sovrintendere alle attività di valutazione e certificazione dei sistemi/prodotti IT commerciali (non classificati) e di emettere i relativi certificati.
- Il D.lgs. n. 82 del 7 marzo 2005, recante il Codice dell'Amministrazione digitale, in particolare riportava le disposizioni in materia di sicurezza informatica.
- Il D.l. n. 144 del 27 luglio 2005 (Misure urgenti per il contrasto del terrorismo internazionale) convertito con modificazioni nella Legge n.155 del 31 luglio 2005, all'art. 7 *bis*, stabiliva che «*Ferme restando le competenze dei Servizi informativi e di sicurezza[…] l'organo del ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione assicura i servizi di protezione delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del ministero dell'Interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate*».
- Con la Legge n. 124 del 3 agosto 2007 (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto) veniva affidato «*All'Aise e all'Aisi il compito di ricercare ed elaborare informazioni utili alla difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica da minacce provenienti, rispettivamente, dall'esterno e dall'interno, incluse quelle attuate con ricorso alle tecnologie informatiche*».
- Con il Decreto del Ministero dell'Interno del 9 gennaio 2008:
    - venivano individuate le infrastrutture critiche informatizzate di interesse nazionale;
    - veniva disposta l'istituzione del Centro Nazionale Anticrimine Informatico per la protezione delle infrastrutture critiche, quale unità organizzativa incardinata nel

Servizio di Polizia postale e delle comunicazioni, con compiti di prevenzione e repressione dei crimini informatici, di matrice comune, organizzata o terroristica aventi per obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale.

- Il D.p.c.m. del 1° aprile 2008, recante Regole tecniche e di sicurezza per il funzionamento del sistema pubblico di connettività, prescriveva la costituzione, presso ogni Pubblica amministrazione, di un'unità locale di sicurezza, cui veniva affidata la responsabilità di porre in atto tutte le fasi di prevenzione degli incidenti informatici e la gestione operativa degli stessi.
- Il D.lgs. n. 66 del 15 marzo 2010 (Codice dell'ordinamento militare), all'art. 89, stabiliva le attribuzioni delle Forze Armate e le direttive disciplinanti i compiti attinenti alla difesa cibernetica.
- Il D.p.c.m. del 5 maggio 2010, avente per oggetto l'Organizzazione nazionale per la gestione di crisi, definiva l'ambito d'intervento in caso di situazioni difficili, anche internazionali, che potessero mettere a rischio gli interessi nazionali. A tale scopo venivano costituiti:
  - il Comitato Politico Strategico (Cops), presieduto dal Presidente del consiglio dei Ministri , per l'indirizzo e la guida strategica nazionale nelle situazioni di crisi;
  - il Dipartimento delle informazioni per la sicurezza (Nisp), presieduto dal Sottosegretario di Stato alla Presidenza del consiglio dei Ministri , per il supporto del Cops e del suo Presidente, con funzioni di coordinamento interministeriale, acquisizione di notizie, programmazione, pianificazione operativa di contrasto, etc.
- Il D.lgs. n. 61 dell'11 aprile 2011, al fine di pervenire all'attuazione della citata Direttiva europea 2008/114/CE del Consiglio, stabiliva le procedure per l'individuazione e la designazione di Infrastrutture critiche europee (Ice) nei settori dell'energia e dei trasporti, nonché le modalità di valutazione della sicurezza delle stesse e le relative prescrizioni minime di protezione da minacce di varia natura, incluse quelle di origine tecnologica, attribuendo specifici compiti al Nisp, supportato da una specifica struttura responsabile, che il D.p.c.m. 17 maggio 2011 individuava nella Segreteria infrastrutture critiche, inserita nell'ambito dell'Ufficio del Consigliere militare della Presidenza del consiglio dei Ministri, con il compito di supportare il Nisp nelle attività tecniche e scientifiche riguardanti l'individuazione e la designazione delle Ice, nonché per i

rapporti con la Commissione europea e con analoghe strutture degli Stati membri dell'Ue.

- Il D Lgs. n. 70/2012 modificava il D.lgs 1° settembre 2003, n. 259 con l'inserimento dell'art. 16 bis che al comma 4, prevedeva l'individuazione del *Computer Emergency Response Team (Cert)* Nazionale presso il Mise, con compiti di prevenzione e supporto a cittadini e imprese nel fronteggiare incidenti informatici, sulla base di un modello cooperativo pubblico-privato.
- Il successivo D.p.c.m. n. 158 del 5 dicembre 2013 affidava all' Iscti-Iscom le attività di pertinenza dei Cert Nazionale, divenuto operativo il 5 giugno 2014. Quest'ultimo, prevalentemente invia bollettini di *early warning,* scambia informazioni con altri Cert e stipula accordi di collaborazione.
- Il D Lgs. n. 83 del 22 giugno 2012 convertito, con modificazioni, nella Legge n. 134 del 7 agosto 2012, istituiva l'Agenzia per l' Italia digitale (Agid) cui demandava, tra l'altro, le funzioni a suo tempo attribuite all' Iscti-lscom in materia di sicurezza informatica e di relative emergenze nonché quelle di coordinamento, indirizzo e regolamentazione tecnica già affidate a DigitPA.
- Con il D.p.c.m. 8 gennaio 2014 veniva approvato lo statuto dell'Agid e venivano affidate ad essa anche le funzioni di direzione e organizzazione del Cert della P.a., divenuto pienamente operativo il 3 marzo 2014.
- La Legge n. 133 del 7 agosto 2012 (Revisione del sistema di informazione per la sicurezza della Repubblica), poneva come primo obiettivo il rafforzamento della protezione cibernetica e della sicurezza informatica nazionale.

Su tale preesistente, variegato quadro normativo è intervenuto il D.p.c.m. del 24 gennaio 2013 (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale), che ha ritenuto:

- necessario definire un Quadro strategico nazionale che specifichi i ruoli che le istituzioni devono esercitare per assicurare la sicurezza cibernetica del Paese, coinvolgendo tutti gli attori pubblici e privati interessati;
- importante individuare gli Organi nazionali di riferimento per interagire con le corrispondenti autorità estere;
- dover procedere, per realizzare tale quadro, secondo un percorso graduale di razionalizzazione di ruoli, strumenti e procedure, con l'obiettivo di accrescere la sicurezza cibernetica del Paese, anche con interventi di carattere normativo;

- che nell'immediato, a legislazione vigente, possa svilupparsi un'azione comune tra le diverse attribuzioni istituzionali, assicurando anche l'apporto degli operatori privati interessati alla gestione dei sistemi e delle reti strategiche. A tal fine si definisce un'architettura istituzionale che si sviluppa su tre distinti livelli di intervento: 1) di indirizzo politico e di coordinamento strategico, per l'individuazione degli obiettivi volti a garantire la protezione cibernetica nazionale, anche attraverso l'elaborazione di un "Piano nazionale per lo spazio cibernetico" è per lo studio di normative tese al loro conseguimento; 2) di supporto a carattere permanente, di raccordo tra tutti gli Organi competenti, per l'attuazione degli obiettivi e delle linee d'azione indicate dalla pianificazione nazionale e per l'attivazione delle procedure di allertamento in caso di crisi; 3) di gestione delle crisi, con il compito di coordinare le attività di risposta e ripristino delle funzionalità dei sistemi coinvolti, avvalendosi delle componenti interessate.

L'architettura complessivamente delineata comprende i soggetti di seguito indicati:

- Il, il quale adotta, su proposta del (Cisr), il Quadro strategico nazionale (approvato nel dicembre 2013, unitamente al Piano Nazionale) per la sicurezza dello spazio cibernetico e dà attuazione, su deliberazione del Cisr, al piano nazionale per la protezione cibernetica e la sicurezza informatica, contenente gli obiettivi da conseguire e le linee d'azione da porre in essere per realizzare il Quadro strategico nazionale, emanando le necessarie direttive per la sua attuazione;
- Il Comitato Interministeriale per la Sicurezza della Repubblica, che propone al Presidente del consiglio dei Ministri il Quadro strategico nazionale, delibera il suddetto piano e ne sorveglia l'attuazione, favorisce la collaborazione tra soggetti istituzionali e privati, elabora gli indirizzi generali che gli Organismi di informazione per la sicurezza (Oois) devono perseguire, formula proposte di intervento normativo e svolge funzioni di consulenza al Presidente del consiglio dei Ministri in caso di crisi;
- L'Organismo collegiale di coordinamento del Dipartimento delle informazioni per la sicurezza (Dis), che supporta il Cisr nello svolgimento delle funzioni di cui sopra, verifica l'attuazione degli interventi previsti dal piano, coordina le attività di individuazione delle minacce cibernetiche, delle vulnerabilità, delle misure di sicurezza e delle *best practices* da adottare;
- Il Comitato scientifico, istituito presso la Scuola di formazione del Dipartimento delle informazioni per la sicurezza e composto da esperti nel settore della sicurezza

cibernetica, che propone sia ipotesi di intervento volte a migliorare gli *standard* e i livelli di sicurezza dei sistemi e delle reti, sia progetti di promozione e diffusione della cultura della sicurezza nel settore cibernetico;

- Gli Organismi di informazione per la sicurezza che svolgono la propria attività nel campo della sicurezza cibernetica secondo modalità e procedure previste dalla legge 124/2007 e si raccordano con P.a, università, enti di ricerca, erogatori di servizi di pubblica utilità, stipulando, in tal senso apposite convenzioni e accedendo ai loro archivi informatici secondo le modalità previste dal D.p.c.m. del 12 giugno 2009. In particolare:
  - il Direttore Generale del Dis, sulla base delle direttive del Presidente del consiglio dei Ministri e degli indirizzi e obiettivi individuati dal Cisr, cura il coordinamento delle attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica nazionale;
  - Il Dis supporta il Direttore Generale per l'espletamento delle attività, formula analisi e valutazioni sulla minaccia cibernetica e provvede alla trasmissione di informazioni rilevanti ai fini della sicurezza cibernetica al Nucleo per la sicurezza cibernetica e ai soggetti interessati; promuove la conoscenza sui rischi e la prevenzione cibernetica, avvalendosi del predetto Comitato scientifico;
  - Le Agenzie svolgono, in aderenza al loro mandato, agli indirizzi del Presidente del consiglio dei Ministri e alle linee di coordinamento stabilite dal Dis, le attività di ricerca e di elaborazione informativa in materia di protezione cibernetica e sicurezza informatica;
- Il Nucleo per la sicurezza cibernetica (Nsc) - il secondo livello dell'architettura delineata - è istituito in via permanente presso l'Ufficio del Consigliere militare del Presidente del consiglio dei Ministri, a supporto di quest' ultimo per gli aspetti relativi alla prevenzione e preparazione a eventuali situazioni di crisi. È presieduto dal Consigliere militare ed è composto da rappresentanti del Dipartimento delle informazioni per la sicurezza , dell' Agenzia informazione e sicurezza esterna, dell' Agenzia informazione e sicurezza interna, del ministero Affari Esteri, dei ministeri dell'Interno e della Difesa, dei Mise, del ministero economia e finanze, del Dipartimento della protezione civile, dell'Agenzia per l'Italia digitale e da un rappresentante dell'Ufficio centrale per la segretezza per gli aspetti relativi alla

trattazione di informazioni classificate. Il Nucleo svolge funzioni di raccordo tra le varie componenti dell'architettura e, in particolare:

- per la prevenzione e preparazione di situazioni di crisi, promuove la pianificazione operativa della contromossa a eventi cibernetici, mantiene attiva una Unità di allertamento per la risposta ad attacchi informatici, condivide informazioni con gli Organismi interessati relativamente ad allarmi, gestione delle crisi, violazioni della sicurezza informatica, promuove esercitazioni, cura i rapporti con Organismi internazionali *fatte* salve le competenze delle altre amministrazioni;
- ai fini delle attivazioni delle azioni di risposta e ripristino, in caso di eventi cibernetici, riceve le segnalazioni e dirama gli allarmi alle amministrazioni e agli operatori privati; provvede, quando l'evento non possa essere fronteggiato dalle singole amministrazioni, a dichiarare la situazione di crisi e ad attivare il Dipartimento delle informazioni per la sicurezza informando il Presidente del consiglio dei Ministri su quanto in atto.

- Il Dipartimento delle informazioni per la sicurezza costituisce il terzo livello dell'architettura istituzionale, in quanto funzionale all'ottimale gestione delle crisi di natura cibernetica. È presieduto dal Consigliere militare del ed è costituito dai rappresentanti delle amministrazioni indicate nel D.p.c.m. 5 maggio 2010, unitamente a un rappresentante del Mise e dell'Agid. Ha il compito di assicurare che le attività di reazione e stabilizzazione delle amministrazioni e degli enti coinvolti nella crisi cibernetica vengano espletate in maniera coordinata, avvalendosi del Cert Nazionale (istituito presso il Mise). Mantiene informato il Presidente del consiglio dei Ministri sulla crisi in atto, coordina l'attuazione delle sue determinazioni per il superamento di essa, raccoglie i dati relativi agli incidenti, fornisce informazioni ai soggetti interessati, assicura i collegamenti finalizzati alla gestione della crisi con omologhi Organismi di altri Stati o di Organizzazioni internazionali di cui l'Italia fa parte;
- gli operatori privati, che forniscono reti pubbliche o servizi di comunicazione e che gestiscono infrastrutture critiche informatizzate di rilievo nazionale ed europeo, comunicano al Nisp ogni significativa violazione della sicurezza dei propri sistemi informatici, utilizzando canali di trasmissione protetti, adottano le *best practices* finalizzate all'obiettivo della sicurezza cibernetica, forniscono informazioni agli Oois e consentono ad essi l'accesso alle banche dati di interesse ai fini della sicurezza

cibernetica di pertinenza e collaborano alla gestione delle crisi contribuendo al ripristino delle funzionalità dei sistemi e delle reti da essi gestiti.

Le azioni intraprese in ambito nazionale, in tema di prevenzione e contrasto alle minacce cibernetiche, non si limitano a quelle afferenti al complesso quadro legislativo e normativo sopra delineato; numerose, infatti, sono state le iniziative che, a vario titolo, hanno visto il coinvolgimento di organi pubblici.

Tra queste, si sottolinea che nel febbraio 2007, è stato costituito, presso l'Ufficio del Consigliere militare del Presidente del consiglio dei Ministri, il Tavolo interministeriale di coordinamento e indirizzo nel settore della Protezione delle infrastrutture critiche (cosiddetto Tavolo Pic). Nel corso del suo mandato, esso ha svolto, principalmente, attività tese all'approvazione della citata Direttiva europea del 2008 ed alla valutazione della necessità di migliorarne la protezione. Con l'istituzione del Nisp (2010) il Tavolo ha cessato le sue attività. Presso il menzionato Iscti-Iscom del Mise, nel 2011 è stato costituito il Tavolo tecnico per il coordinamento interministeriale dell'attività approntata nel settore della *cybersecurity;* nell'aprile 2013, da parte del Dipartimento delle informazioni per la sicurezza sono state intraprese le azioni necessarie per la stipula di apposite convenzioni per lo scambio di informazioni con le maggiori aziende italiane, in modo da formalizzare rapporti funzionali agli interessi del Paese. Il primo obiettivo di tali convenzioni è quello del contrasto al *cybercrime.* Nel dicembre 1989 è stato costituito il Consorzio Interuniversitario Nazionale per l'Informatica (Cini), posto sotto la vigilanza del Ministero dell'Istruzione, dell'Università e della Ricerca, cui aderiscono 39 università, che si pone quale principale punto di riferimento della ricerca accademica nazionale nell'informatica e nell'IT. In particolare, per quanto concerne la sicurezza informatica, nell'ambito del consorzio è stato creato (nel maggio 2014) un laboratorio nazionale di *cybersecurity* che vede collegati 240 dipartimenti universitari, con lo scopo di coordinare l'eccellenza accademica del comparto, promuovendo la ricerca in numerosi settori quali: la *System and network security*, la protezione delle infrastrutture critiche, *risk and malware analysis,* algoritmi crittografici etc. Nell'ottobre 2014, tra il Direttore Generale del Dis ed il Presidente del Cini è stato firmato un accordo di collaborazione triennale incentrato sulle iniziative del menzionato laboratorio. Nel maggio 2011 è stato inaugurato, presso l'Osservatorio per la sicurezza nazionale (progetto promosso dal Centro militare di studi strategici e da Selex-Finmeccanica) il Gruppo di lavoro *Cyberworld,* una compartecipazione tra pubblico e privato, con il compito di investigare e analizzare gli aspetti giuridici, tecnologici, economico-finanziari e sociologici del complesso mondo *cyber.*

I risultati di tale attività hanno costituito l'oggetto del volume Cyberworld (edito nel 2013). L'Osservatorio ha cessatol'attività nel 2014. Nel luglio 2011 è stato firmato un accordo tra il Direttore Generale del Dis e il Rettore dell'Università "Sapienza" allo scopo di promuovere la cultura della sicurezza informatica. Nell'ambito di tale partnership è stato creato il Centro di ricerca in *Cyber intelligence and information security* (Cis-Sapienza), quale organo multidisciplinare per lo sviluppo di metodologie e tecnologie d'avanguardia per il contrasto delle minacce nel *cyber* spazio. A cura del Centro, nel gennaio 2015, è stato presentato il Report italiano di *cybersecurity* 2014, dal titolo "Consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione", nel quale vengono esposti i risultati dell'indagine svolta in collaborazione con l'Agid e il Dis, presso circa trecento pubbliche amministrazioni a livello nazionale, regionale e locale, tesa a valutare i livelli di consapevolezza della problematica *cyber,* organizzativi e di difesa, addivenendo ad una lista di raccomandazioni. Nell'ambito dello stesso accordo figurano anche i master di secondo livello in tema di "Sicurezza delle informazioni e informazione strategica" attivati dall'Ateneo con la collaborazione della Scuola di formazione del Dis. In chiusura vanno ricordati anche i *Computer Emergency Response Team* che operano in ambito nazionale, per il fondamentale ruolo svolto presso gli utenti in termini di aggiornamento sulle minacce, di assistenza qualificata e di supporto in caso di cyber attack. Oltre al Cert Nazionale (per privati e imprese) ed al Cert p.a., si citano anche i seguenti per l'ampia platea di pubblici utenti da questi supportata:

- il Cert Difesa, creato presso lo Stato maggiore Difesa, che collega e coordina i Cert delle singole Forze Armate al fine di fornire assistenza ai fruitori nella difesa delle reti telematiche e che s'interfaccia, oltre che con quelli nazionali, anche con il Cert Nato;
- il Cert- Garr (Gruppo per l'armonizzazione delle reti della ricerca), attivato nel 1999 per il supporto alla rete telematica italiana dell'Università e della ricerca che collega oltre duemila siti per fornire connettività ad altissime prestazioni alla comunità accademica.

2. L. 48/2008 e le modifiche al codice di procedura penale

Le modifiche apportate al codice di procedura penale dalla Legge n. 48 del 2008 consistono essenzialmente in un adeguamento attraverso operazioni di "chirurgia lessicale" su disposizioni processuali già vigenti. In particolare, gli artt. 8, 9 e 11 della citata novella hanno

modificato i seguenti istituti:

- ispezioni e rilievi tecnici (art. 244, 2°comma c.p.p.)
- esame di atti, documenti e corrispondenza presso banche (art. 248, 2°comma c.p.p.)
- doveri di esibizione e consegna (art. 256, 1°comma c.p.p.)
- obblighi e modalità di custodia (art. 259, 2°comma c.p.p.)
- sigilli e vincolo delle cose sequestrate (art. 260,1°e 2° comma c.p.p.)
- acquisizione di plichi e corrispondenza (art. 353, 1°e 2° comma c.p.p.)
- accertamenti urgenti e sequestro (art. 354, 2° comma c.p.p.).

Per ciascun istituto il legislatore ha ampliato l'oggetto della norma attraverso l'inserimento di espressioni che rimandano ad attività legate al trattamento di "dati, informazioni e programmi informatici" e ha sottolineato l'importanza della salvaguardia dell'integrità dei dati stessi, utilizzando diciture come *«[…] Adottano misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»*[50], le quali diventano, di fatti, canoni operativi imprescindibili per l'operatore di polizia.

a. Casi e forme delle ispezioni e delle perquisizioni

Il nucleo della riforma in materia processuale rappresenta dalla modifica delle disposizioni relative alle ispezioni ed alle perquisizioni: in entrambi i casi viene offerto un "paradigma" sul corretto *modus operandi* da seguirsi nelle operazioni di accesso al *computer* oggetto d'indagine, sottolineando la necessità della salvaguardia dell'integrità dei dati digitali che assurge, quindi, a canone operativo imprescindibile. È frequente, infatti, la precisazione circa la necessità di adottare *«Misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»*[51] a sostegno di un duplice obiettivo: da un lato, garantire la genuina acquisizione di elementi probatori che potranno assumere in seguito valenza di prova, dall'altro, sul fronte delle garanzie difensive, permettere un controllo sul lavoro degli inquirenti, il quale deve necessariamente prendere le mosse dalla verifica sulle procedure acquisitive. È stato osservato[52] che la locuzione sopra richiamata appare come "norma processuale in bianco" attraverso un implicito richiamo alle *best practices* del settore [53], senza però indicare a quale fra le molteplici esistenti ci si debba riferire. Il legislatore mostra una certa indifferenza qualitativa fra le plurime

[50] Comma 2 dell'art 244 c.p.p. così modificato dal comma 1 dell'art. 8, L. 18 marzo 2008, n. 48, che ha ratificato la Convenzione del Consiglio d'Europa sulla criminalità informatica.

[51] Art. 244, comma 2 c.p.p.

[52] Braghò G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici* in Lupària L., *Sistema penale e criminalità informatica*, Giuffrè, 2009, p. 187.

[53] Braghò G., *L'ispezione e la perquisizione di dati,* cit., p. 188.

procedure, lasciando margine d'azione e di scelta al *forenser* che concretamente porrà in essere le operazioni secondo la tecnica preferita senza che tale scelta comporti alcuna "trappola della legittimità[54] ", sempreché il risultato acquisito rispetti il vincolo della formula normativa sopra richiamata.

Tradizionalmente l'ispezione e la perquisizione sono operazioni classiche di ricerca della prova. L'attività tipica dell'*inspicere* si sostanzia nell'osservazione di persone, luoghi, cose onde accertare tracce o altri effetti materiali del reato (art. 244, comma 1 c.p.p.); di contro, l'attività tipica del *perquirere* si caratterizza per essere volta all'individuazione e acquisizione del corpo del reato o delle cose ad esso pertinenti, spesso qualificandosi come attività prodromica rispetto al sequestro probatorio (art. 247, comma 1° del c.p.p.).

La novella in discorso ha interessato entrambi gli istituti: tuttavia, il disegno originario di legge approvato dal Consiglio dei Ministri nel maggio 2007 aveva previsto un mero ampliamento dell'oggetto delle rispettive attività, senza prevedere le opportune garanzie di affidabilità imposte dalla Convenzione sul *Cybercrime*. Fortunatamente, e grazie all'apporto degli specialisti intervenuti in sede di stesura, si è posta concretamente l'attenzione sulla problematica più delicata che si ravvisa in dette operazioni: la preservazione della *scena criminis* informatica. Si è, quindi, inserita al 2° comma dell'art. 244 c.p.p. la possibilità per l'autorità giudiziaria di disporre l'ispezione *«Anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e la loro inalterabilità»*[55]; per quel che riguarda la materia delle perquisizioni, il successivo art. 247 c.p.p., al comma 1-*bis* stabilisce che *«Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»*[56]. In sostanza, quindi, *«Qualora l'*objectum *da "scrutare" o "frugare", per dirla con Cordero, sia un sistema informatico devono essere adottate misure tecniche dirette ad assicurare la conservazione dei dati originali e a impedirne l'alterazione»*[57]. Da qui due corollari di notevole importanza: il primo, la qualifica dell'attività ispettiva o perquisente in ambiente virtuale come attività potenzialmente e concretamente idonea a modificare in maniera irreversibile lo stato e il contenuto interno del dispositivo sottoposto alla misura; il secondo, per cui si riconosce *«La natura ontologicamente volatile e alterabile del dato digitale, su cui possono spesso incidere condotte involontarie atte a ingenerare*

---

54 Braghò G., *L'ispezione e la perquisizione di dati,* cit., p.189.

55 Art. 244, comma 2 c.p.p. così modificato dal comma 1 dell'art. 8, L. 18 marzo 2008, n. 48, cit.

56 Comma aggiunto dal comma 2 dell'art. 8, L. 18 marzo 2008, n. 48, cit.

57 Lupària L., *Ratifica della Convenzione* Cybercrime *del Consiglio d'Europa*, in *Diritto Penale e Processo,* 2008, p. 697.

fenomeni di "inquinamento" e la conseguente necessità di impiegare "standard operating procedure" idonee a garantire la genuinità dell'accertamento»[58]. Adattare le due figure all'ambiente virtuale su cui andranno a operare non è sempre agevole, considerando soprattutto che a livello tecnico le attività in esame possono essere attuate attraverso procedure essenzialmente analoghe sfumando in concreto la linea di demarcazione fra i due istituti.

Posto che, come detto, l'attività ispettiva è diretta alla ricerca visiva tesa all'individuazione di tracce o effetti materiali del reato, in quali termini è possibile parlare di ispezione informatica? Quali possono essere le modalità attuative?

A livello informatico esplorare un sistema alla ricerca di dati e tracce informatiche inerenti ai fatti oggetto dell'ispezione comporta irrimediabilmente l'alterazione dei dati di sistema e dei metadati relativi ai *files* oggetto di attenzione da parte degli inquirenti. Parte della dottrina[59] ha infatti sottolineato come l'attività ispettiva in ambiente informatico dovrebbe limitarsi ad osservare il sistema descrivendolo nei suoi particolari, ad esempio rilevando la presenza di periferiche collegate, accesso alla rete attivo, presenza di *software* in funzione, partizioni logiche nascoste e rese visibili da meccanismi di autorizzazione connessi allo *status* dell'utilizzatore (ad esempio amministratore di sistema e chiavi di cifratura). Altra parte,[60] invece, ne incoraggia l'utilizzo soprattutto con riguardo a reati di lieve entità (ad esempio diffamazione a mezzo internet, diffusione di virus) o per casi dove è necessario acquisire solo una piccola parte dei dati contenuti nei dispositivi, rappresentando il sequestro dell'intero contenuto operazione non rispondente al principio di proporzionalità con riguardo al fine (ad esempio nei casi di acquisizione presso terzi di dati rilevanti). Si osserva[61] come questa possibilità soffra comunque di due limiti importanti: il primo, di natura temporale, legato all'impossibilità di poter analizzare in maniera accurata grande quantità di dati, tralasciandone giocoforza l'accuratezza e completezza. Il secondo, legato al rispetto delle garanzie difensive. Rientrando, infatti, nella categoria degli accertamenti irripetibili, le operazioni ispettive dovranno essere condotte secondo lo schema previsto dall'art. 360 c.p.p. Sebbene l'accertamento verrà condotto da operatori tecnici appartenenti alla polizia giudiziaria in contraddittorio con la parte interessata, eventualmente alla presenza di consulenti tecnici di parte, i risultati così ottenuti saranno cristallizzati in verbali con la conseguente utilizzabilità piena in dibattimento. Resta preclusa la

---

58 Lupària L., *Ratifica della Convenzione* Cybercrime, cit., p. 690

59 Aterno S., *Modifiche al titolo III del terzo libro del codice di procedura penale*, in Corasaniti G. Corrias - Lucente G. *, Cybercrime, responsabilità degli enti, prova digitale*, Cedam, 2008, p. 206 ss.

60 Costabile G., Scena criminis, *documento informatico e formazione della prova penale*, in *Diritto dell'informatica,* 2005, p. 531 ss.

61 Braghò G., *L'ispezione e la perquisizione di dati,* cit., p. 170.

possibilità da parte dell'indagato di esperire *ex post* una nuova analisi sugli stessi supporti e sullo stesso oggetto, in quanto i risultati saranno necessariamente diversi, stante la modificazione dell'ambiente *target* operata anteriormente dal *cyber* investigatore. In realtà, *«Prevalendo le finalità di descrizione e rilevazione di dati oggettivi, non comportando alcuna apprensione, mediante sequestro, del bene oggetto di ricerca»* [62], l'ispezione finalizzata all'acquisizione condotta *ex* art. 360 c.p.p. appare una via non praticabile, dovendosi quindi preferire la prima soluzione. Ad avallare tale tesi è altresì il dato normativo che individua nel sistema informatico o telematico l'ambito di intervento ispettivo, più ampio rispetto alla disciplina della perquisizione che invece si rivolge a dati, informazioni o programmi: la *ratio* della norma sembra infatti rimarcare il fine ultimo delle attività costituito dall'osservazione del sistema e al più all'accertamento in ordine all'esistenza nel sistema medesimo di determinate applicazioni. Il panorama si complica ulteriormente nel caso di utilizzo delle cosiddette *preview*: attraverso l'utilizzo di *software ad hoc* viene permesso agli inquirenti in sede d'ispezione, ma anche di perquisizione, di poter analizzare in maniera grossolana il contenuto di un dispositivo per poi scegliere il materiale interessante e, se del caso, procedere a sequestro del dato. Si osserva, tuttavia, come tale operazione debba essere condotta da personale altamente qualificato, stante l'alto rischio di alterazione dei contenuti con conseguente dispersione di una possibile prova e, altresì, debba essere valutata caso per caso non rappresentando ad oggi operazione di *routine* applicabile indiscriminatamente a qualsiasi fattispecie concreta[63]. Parte della dottrina[64] ne suggerisce un uso attento e calibrato a seconda dell'indagine in essere: ad esempio, se si procede per pedopornografia *online*, sarà rilevante il materiale detenuto con dolo (presente e non cancellato) all'interno della memoria per cui la *preview* potrebbe rappresentare un'opportunità utile al fine di evitare il sequestro di materiale "neutro" rispetto al reato per cui si procede; di contro, la confutazione di *alibi informatici* necessita l'apprensione di tutti i dati memorizzati per poter ricostruire, anche attraverso l'ausilio di macchine[65], le attività poste in essere dalla stessa e sudi essa e quindi, in questa ipotesi, tale strumento appare inidoneo ai fini dell'accertamento.

Le perquisizioni, come noto, possono essere svolte durante le indagini preliminari

---

62 Costabile G., *Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Cyberspazio e diritto,* 2010, pag. 478.

63 Aterno S., Cajani F., Costabile G. - Mattiucci M., Mazzaraco G., *Computer Forensics e indagini digitali,* Vol. 1, Experta 2011, pag. 18.

64 Aterno S., Cajani F., Costabile G., Mattiucci M., Mazzaraco G., *Computer Forensics e indagini digitali*, Vol. 1, Experta, 2011,cit., p. 20.

65 Utilizzate per ricostruire fedelmente attività o comportamenti *hardware* e *software* al fine di avallare o contestare fatti a carico (tesi accusatorie) o a discarico (tesi difensive) dell'imputato. Cfr., più diffusamente, Nicosia G., Caccavella D., *Macchine virtuali e sistema della prova nel processo civile e penale*, in *Diritto dell'Internet*, 2008, 5, p. 525 ss.

secondo due distinte modalità: solitamente, a seguito d'iniziativa del pubblico ministero, il quale le dispone con decreto motivato prevedendo altresì se vadano eseguite personalmente ovvero vadano delegate ad ufficiali di polizia giudiziaria (art. 247 c.p.p.). Può però accadere che, sempre in sede d'indagini preliminari, la p.g. possa dar luogo personalmente e di propria iniziativa a perquisizione locale o personale nei casi di flagranza del reato o evasione (art. 352 c.p.p.). In quest'ultima ipotesi, essendo la perquisizione atto coercitivo potenzialmente lesivo dei diritti di cui agli artt. 13 e 14 della Costituzione, essa necessita, *ex post*, di convalida da parte del p.m. entro le 48 ore successive per accertarne il fondamento: in caso contrario, i risultati così ottenuti e cristallizzati all'interno del verbale di perquisizione saranno inutilizzabili. Con la previsione di cui al nuovo comma 1*bis* dell'art. 247 c.p.p. il legislatore contempla poteri più invasivi per gli investigatori, statuendo altresì che *«Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».*[66] Sulla questione si rimarca l'importanza rivestita dalla sicurezza informatica, scienza che si pone in un rapporto ambivalente di rimedio-ostacolo alle procedure di informatica forense[67]. Il punto relativo alle misure di sicurezza rende ancor più garantita la figura del "domicilio informatico" alla quale sembrano estendersi tutte le garanzie previste per il "domicilio tradizionale".

In parallelo, attraverso la modifica apportata all'art. 354 c.p.p., si prevede, in tema di accertamenti urgenti da parte della p.g., che la stessa, prima dell'intervento del pubblico ministero, sia tenuta alla conservazione dello stato dei luoghi e delle cose pertinenti al reato (1° comma) e, in relazione a dati, informazioni, programmi, sistemi informatici o telematici, sia tenuta all'adozione di misure tecniche o prescrizioni necessarie ad assicurarne la conservazione, impedirne l'alterazione e l'accesso, provvedendo ove possibile alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità (2° comma). In sostanza, nell'ambito delle attività in questione, la p.g. dovrà limitarsi a porre in essere azioni volte alla preservazione e assicurazione del quadro probatorio originario.

Ciò che è importante sottolineare, trattandosi di attività prodromica rispetto al sequestro, è la necessità che la perquisizione, anche in via informatica, sia opportunamente giustificata e

---

66 Comma aggiunto dal comma 2 dell'art. 8, L. 18 marzo 2008, n. 48, cit.

67 Si può pensare alla sicurezza informatica come ostacolo, rappresentato dallo studio di sistemi di sicurezza sempre più sicuri eventualmente in uso sui dispositivi interessati; o come rimedio, rappresentato dallo studio di tecniche *hacking* utili per forzare dette misure e acquisire più informazioni possibili.

legata al *thema probandum*, attraverso l'individuazione del fatto storico, di natura penalmente rilevante, in cui assume importanza e decisività l'elemento informatico. In mancanza, non sarebbe possibile accertare l'esigenza probatoria sottesa al provvedimento, né la riconduzione del dispositivo al corpo del reato o a cosa ad esso pertinente: si ravviserà, quindi, non più un mezzo di ricerca della prova, bensì uno strumento discutibile di ricerca di notizie di reato. Un'importante opportunità è appunto resa dalla *preview* dei contenuti, come sottolineato in precedenza. In ogni caso, tali attività, sia di *preview* sia perquisenti in senso stretto, dovranno essere condotte con le cautele previste dall'art. 247, comma 1*bis* c.p.p.: potranno consistere in operazioni di tipo *live* o *dead* a seconda dello scenario che concretamente si manifesterà agli occhi degli inquirenti. Diverso, infatti, è il trattamento tecnico da riservare a dispositivi rinvenuti in modalità *off* o *on*: si pensi al caso di ritrovamento sulla scena del crimine di due *computers*, di cui solo uno acceso. Nel caso di *computer* spento gli inquirenti, qualora lo ritengano necessario, potranno esaminarne preliminarmente il contenuto e procedere eventualmente al sequestro dell'intero *hard-disk* o di alcune parti attraverso il ricorso alle procedure previste: ciò che preme rilevare è che in tale ipotesi il rischio di alterabilità dei dati presenti è più basso rispetto al caso opposto, sempreché in via preliminare siano adottate le cautele previste dalle *best practices*. La questione risulta invece più complessa nel caso in cui il dispositivo sia acceso e collegato alla rete: in questa ipotesi la prescrizione prevista dall'art. 247, comma 1*bis* c.p.p. acquista un peso ed una rilevanza ancor più imprescindibile, stante l'alto tasso di vulnerabilità del sistema dato dalla sua dinamicità. "Frugare" all'interno di un sistema attivo è attività molto rischiosa che interessa sia la genuinità dei dati rinvenuti al momento dell'atto, sia il tema delle garanzie difensive, rappresentandosi come attività sostanzialmente non ripetibile. Ciò comporta il richiamo dell'art. 360 c.p.p. in tema di accertamenti urgenti[68] i quali, tuttavia, non sempre possono essere praticati, vuoi per la natura stessa dell'istituto che è e resta tipico atto d'indagine a sorpresa, vuoi per impossibilità legate alle caratteristiche del caso concreto (se si procede contro ignoti, se vi è una quantità enorme di dati da acquisire, se il *target* è rappresentato per esempio da *service provider*, istituti bancari, gestori di telefonia e in generale in tutti i casi in cui possano sorgere problemi sulla qualità del servizio reso dal soggetto interessato dalla perquisizione).

[68] Apre l'ampio dibattito sulla ripetibilità o meno degli accertamenti. In argomento, cfr. più diffusamente Aterno S., Cajani F., Costabile G., Mattiucci M., Mazzaraco G., *Computer Forensics e indagini digitali,* cit., p. 27; Novario F.*, L'attività d'accertamento tecnico difensivo disposta su elementi informatici e la sua ripetibilità*, in *Cyberspazio e diritto*, pp. 75-87; Aterno S.*, La computer forensics tra teoria e prassi: elaborazioni dottrinali e strategie processuali*, in *Cyberspazio e diritto*, pp. 425-440.

b. La perquisizione online

A seguito della sentenza della Corte Costituzionale Tedesca (*Bundesverfassungsgericht*) del 27 febbraio 2008 è esplosa una nuova questione legata alla legittimità circa l'utilizzo di tecnologie sempre più evolute e invisibili in sede d'indagine, rappresentate nel caso concreto dalle cosiddette "perquisizioni *online*". La vicenda ha destato una forte attenzione non solo a livello nazionale ma anche europeo, costituendo un notevole precedente legato al discutibile utilizzo di avanzate tecnologie di controllo da parte degli apparati statali. Più nel dettaglio, l'episodio ha per oggetto una norma contenuta all'interno della Legge sulla protezione della Costituzione del *North Rhein Westfalia* (VSG), in particolare il capitolo 5 comma 2, n. 11 che autorizzava il Verfassungsschutzbehörde, organismo di intelligence a "protezione della Costituzione", a effettuare due tipi di attività: un monitoraggio segreto su quanto accade in internet e l'accesso a sistemi informatici attraverso un meccanismo di intrusione a mezzo *Trojan*, sempre in modalità silente[69]. A livello tecnico, esistono essenzialmente due modelli di monitoraggio delle attività che più si avvicinano al concetto di perquisizione virtuale: la cosiddetta *online search* o *one time copy* ovvero l' appostamento informatico (l'*online surveillance*)[70]. La prima consiste *«nell'installazione occulta, in un determinato sistema informatico (ad esempio in un server, in un personal computer, in uno smartphone, in un tablet), di un "programma-spia" (in gergo denominato trojan horse) capace di monitorare il flusso di dati che coinvolgono l'apparecchio spiato»*[71]. Grazie all'utilizzo del cosiddetto *sniffer*[72] o attraverso l'intrusione di programmi particolari, come appunto il *trojan-horse* oggetto della vicenda, tali operazioni sono rese tecnicamente possibili[73]. È evidente come gli strumenti in questione siano fortemente invasivi della sfera privata e di libertà dei soggetti nei cui confronti siano utilizzati, tenuto conto, fra l'altro, della loro caratteristica peculiare rivestita dal fatto di essere, informaticamente parlando, "innocui": il soggetto "attenzionato", infatti, nulla può sospettare in tal senso, non provocando detti *software* alcun tipo di interferenza qualitativa sulle

---

69 Così Flor R., *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del* Bundesverfassungsgericht*,* in *Cyberspazio e diritto,* p. 363.

70 Trogu M., *Sorveglianza e "perquisizioni" on-line su materiale informatico*, in *Le indagini atipiche,* 2016, p. 434.

71 Trogu M., *Sorveglianza e "perquisizioni" on-line su materiale informatico*, cit., p. 434.

72 Per *sniffing* si intende l'attività di intercettazione passiva dei dati che transitano in una rete telematica. Tale attività può essere svolta sia per scopi legittimi, come l'individuazione di problemi di comunicazione o la prevenzione di tentativi di intrusione, che per scopi illeciti, come l'intercettazione fraudolenta di dati personali). I programmi utilizzati a tali scopi, detti *sniffer*, offrono inoltre funzionalità di analisi del traffico.

73 Secondo Cass. pen., sez. VI, 10 marzo 2016 (dep. 6 aprile 2016), n. 13884, in *penalecontemporaneo.it*., «*se il decreto che dispone l'intercettazione di conversazioni o comunicazioni attraverso l'installazione in congegni elettronici di un virus informatico debba indicare, a pena di inutilizzabilità dei relativi risultati, i luoghi ove deve avvenire la relativa captazione; in mancanza di tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in concreto solo le captazioni che avvengano in luoghi di privata dimora al di fuori dei presupposti indicati dall'art. 266, comma 2, codice procedura penale. Se possa comunque prescindersi da tale indicazione nel caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata».*

prestazioni rese dal dispositivo interessato, *computer* o connessione internet che sia, e sollevando quindi forti perplessità circa il loro utilizzo, soprattutto da un punto di vista difensivo.

Numerose, infatti, sono state le censure mosse dalla Corte Costituzionale tedesca che, con la ricordata sentenza del 27 febbraio 2008, ha dichiarato incostituzionale la norma che consentiva l'utilizzo di quello che è stato ribattezzato come "*Trojan di Stato*". *In primis* la Corte ha al riguardo sottolineato come l'utilizzo delle nuove tecnologie in generale - quindi non solo di quelle oggetto di scrutinio da parte della sentenza - debba necessariamente bilanciarsi con la necessità di salvaguardia dei diritti fondamentali della persona, riconducibili per l'ordinamento tedesco all'art. 10 della Legge Fondamentale. Successivamente, ha esaminato la questione di una possibile estensione al sistema informatico della previsione di cui all'art. 13 della Legge Fondamentale, che tutela la inviolabilità del domicilio: posto che la norma costituzionale garantisce uno spazio di dignità ai singoli e che l'intrusione prevista dal VSG va oltre la semplice acquisizione di meri dati privati, permettendo una completa "profilazione" dell'utente, ad avviso del Giudice delle leggi la protezione sopra richiamata deve necessariamente estendersi anche al sistema informatico. Ciò rafforza quel "diritto all'autodeterminazione informativa" che *«va oltre la tutela della privacy e non si limita a informazioni sensibili per natura ma conferisce alla persona, in linea di principio, il potere di determinare, in sé, la divulgazione e l'utilizzo dei suoi dati personali, anche se connotati da un contenuto informativo minimo, che amplia la tutela della libertà della vita privata».*[74] La Corte, invero, amplia il contenuto di tale diritto, creandone di fatto uno "nuovo" diritto alla riservatezza e integrità del sistema informatico o telematico, cui offre una "prosecuzione di tutela" proprio perché attraverso esso l'individuo moderno traspone ed esplica parte della propria personalità e in forza di ciò deve essere tutelato contro l'accesso segreto.

Per quanto riguarda la seconda attività, assimilabile alla *one time copy*, la Corte ha censurato il dettato normativo, non rispondente a "chiarezza e determinatezza" stante l'impossibilità di ricavarne i presupposti applicativi dalla formulazione che si risolve in una "clausola di salvezza" inidonea a regolarne gli effetti in un caso delicato come questo. In particolare, è stato ravvisato un controllo smodato e pervasivo dei sistemi informatici dei cittadini senza che ciò venga ad essere sufficientemente giustificato, anche alla luce del principio di proporzionalità. Di per sé ciò non implica l'impossibilità totale da parte delle Autorità di avvalersi dello strumento *de quo*; al contrario, tale eventualità deve rappresentare un'eccezione, per cui deve essere necessaria un'idonea giustificazione, rappresentata da adeguati beni giuridici primari da tutelare come la

[74] Flor R., *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht,* cit., p. 369.

vita, l'incolumità fisica, la libertà personale e collettiva), la cui minaccia può provocare serie ricadute sulle fondamenta dello Stato. Qualora ciò avvenga, e si renda quindi necessario il ricorso a tali procedure investigative invasive, si dovrà comunque procedere ad una sorta di "compensazione di rappresentanza" degli interessi da parte del soggetto sottoposto a procedimento.

La vicenda della *Online Durchsuchung* può essere assimilata, volendo tentare un parallelismo con la disciplina processuale italiana, alle attività di contrasto alla pedopornografia *online*, pur rappresentandosi come *tertium genus* fra ispezione e perquisizione[75]. Alcuni studiosi si sono interrogati, all'indomani della sentenza in commento, sulla possibile cittadinanza all'interno del panorama giuridico italiano di dette perquisizioni *online.*[76] A tale quesito hanno dato risposta negativa, stante non solo l'attuale cornice normativa di riferimento di cui al codice di rito, ma anche, e soprattutto a seguito delle sentenze della Corte Costituzionale n. 348 e n. 349 del 2007, nonché n. 39 del 2008, che hanno riconosciuto ai principi CEDU valore di "norma interposta" rispetto alle leggi ordinarie, assurgendo così, sia pure in modo indiretto, a parametro di legittimità, pur non avendo rango costituzionale. A livello codicistico, non rientrando in alcuna delle categorie tipizzate dal legislatore, le attività in questione potrebbero al limite essere annoverate tra gli strumenti di indagine atipici o innominati. Poiché, come visto, le procedure *de quibus* minano la riservatezza della vita privata, bene giuridico protetto da riserva di legge, il ricorso alle stesse si porrebbe però in contrasto con quanto affermato dall'orientamento prevalente nella giurisprudenza di legittimità, inaugurato con il famoso "Caso Prisco", nel quale si è stabilita l'illegittimità di una determinata attività investigativa qualora questa assuma i caratteri dell'atipicità andando a incidere su un bene giuridico protetto da riserva di legge. *A fortiori*, gli arresi della Corte Europea dei Diritti dell'Uomo le richiamate sentenze di legittimità sui principi Corte Europea dei Diritti dell'Uomo, sulla valenza del canone di cui all'art. 8 C.E.D.U., che tutela il rispetto della vita privata e familiare, assumono un'ulteriore valenza rafforzatrice del su riferito indirizzo esegetico nazionale, *«anche se in misura ridotta rispetto ad altri strumenti di sorveglianza quali le intercettazioni di comunicazioni»*[77]. Ne consegue, quindi, che *«se le perquisizioni online fossero effettuate in un procedimento penale italiano, dovrebbero essere dichiarate inammissibili come prova perché, non previste dalla legge, verrebbero a incidere su un bene giuridico - la*

---

[75] In realtà si è osservato come anche nel caso tedesco sia improprio parlare di perquisizione, in quanto la vicenda appare come attività di vera e propria "intrusione autorizzata dall'ordinamento": così Aterno S. ,Corasaniti F., Corrias Lucente G., *Cybercrime*, *responsabilità degli enti, prova digitale,* cit., p. 214.

[76] Flor R., *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht,*cit., p. 305.

[77] Trogu M., *Sorveglianza e "perquisizioni" on-line su materiale informatico*, cit., p. 448.

riservatezza della vita privata - la cui lesione, alla luce del nuovo combinato costituzionale-sovranazionale (…) esige la previa determinazione, da parte del legislatore ordinario, dei casi e dei modi di aggressione a quel bene.»[78]

c. Il sequestro probatorio

Altra importante modifica che va segnalata riguarda l'istituto del sequestro probatorio, anch'esso interessato dall'intervenuta evoluzione tecnologica.

In particolare, all'art. 260 c.p.p. si prevede la possibilità da parte delle autorità di assicurare le cose sequestrate anche attraverso l'apposizione di sigilli di carattere elettronico o informatico, idonei ad indicare il vincolo imposto a fini di giustizia. Tale previsione recepisce a livello processuale la certificazione fra copia e originale tramite procedure informatizzate, ossia le cosiddette *hash functions*; inoltre, al 2° comma, la disposizione *de qua* estende la presunzione di deperibilità e alterazione prevedendo la possibilità di effettuare copia dei dati d'interesse su adeguati supporti mediante procedura che ne assicuri la conformità all'originale e la sua immodificabilità.

Il sequestro rappresenta l'istituto processuale che, con riferimento alla specifica tematica che qui ci occupa, più ha fatto discutere e che continua tutt'oggi a generare profili di maggior criticità. Per molto tempo dottrina e giurisprudenza si sono confrontate, in momenti diversi, sulla possibile qualificazione del *computer* quale corpo del reato o cosa pertinente al reato. È chiaro che il vincolo pertinenziale fra reato e supporto informatico sussisterà ogni qualvolta esso potrà qualificarsi come "arma del delitto" (si pensi ai reati informatici "propri", in cui la condotta avviene ed è diretta verso dispositivi informatici). Di contro, nei casi in cui il calcolatore rappresenti cosa pertinente al reato, ossia strumento per risalire attraverso le tracce ivi presenti alle fasi preparatorie e alla condotta assunta in concreto dal soggetto indagato, tale automatismo non può operare, dovendosi caso per caso analizzare il ruolo svolto da esso all'interno della vicenda. La questione ruota attorno al "vincolo pertinenziale" esistente fra i dati digitali e i supporti in cui gli stessi risultano memorizzati. In passato la giurisprudenza dominante affermava come *«non sarebbe possibile individuare supporti o elementi informatici che, sottoposti a sequestro, si possano ritenere non necessari per gli accertamenti di natura tecnica»*[79]. L'assunto avallava prassi distorsive ed ingiustificate che, basandosi su asseriti vincoli pertinenziali[80], conducevano a sequestri indiscriminati di materiale neutro rispetto al *computer,* come stampanti, tastiere, schermi, *mouse* e finanche tappetini *mouse-pads*.

---

78 Buso D., Pistolesi D., *Le perquisizioni e i sequestri informatici*, in Ruggeri F., Picotti L., *Nuove tendenze della giustizia penale di fronte alla criminalità informatica*, Giappichelli, 2011, p. 200.

79 Tribunale Riesame, Perugia, ord. 25 ottobre 2006, in *leggiditalia.it.*

80 Cass. sent. 5 marzo 2008, n. 13792, in *Dirittoitalia.it*, 2012; Cass. sent., 3 aprile 2008, n. 18897, *in Dirittoitalia.it.*

Ciò ha indotto alcuni Autori ad ironizzare su tale condotta, definendola come attinente ad un principio di precauzione secondo cui *«non sapendo bene con cosa si ha a che fare, meglio eccedere e prendere tutto ciò che, genericamente, ricade nella nozione di hardware»*[81].

La giurisprudenza minoritaria, aveva a suo tempo avvertito come *«gli accessori non possono ritenersi rientranti nel concetto di corpo del reato, non essendo cose mediante le quali è stato commesso il reato»*[82].

Inoltre, può osservarsi come estendere il sequestro all'intero elaboratore risulti lesivo sotto due aspetti: il primo di natura economico-sociale, stante il ruolo decisivo che tale strumento assume nella quotidiana vita di ciascuno di noi. Il secondo legato alla potenziale incidenza (anche negativa per l'indagato) dei dati rinvenuti all'interno che non si pongano in un rapporto di connessione rispetto ai fatti contestati. Si osserva, quindi, come più che di sequestro fisico legato al disco rigido (unità sola rilevante ai fini dell'acquisizione) si debba correttamente parlare di sequestro logico di dati, attraverso la creazione di *bit stream images* capaci di riportare fedelmente il contenuto dello stesso attraverso una sorta di fotografia dell'intero sistema.

Essendo ormai consolidato a livello di prassi il ricorso alla duplicazione garantita da possibili alterazioni e immodificabilità del contenuto delle memorie, sorge un'ulteriore questione legata ai contenuti rinvenuti. Sul punto si scontrano diverse esigenze: da un lato, l'interesse pubblico all'acquisizione di elementi utili per l'indagine nell'ottica della ricerca della verità processuale, dall'altro il diritto dell'indagato al rispetto dei suoi diritti, difensivi, ma anche e soprattutto l'effettiva garanzia delle libertà costituzionalmente previste. Netta è la posizione della Cassazione che, con la sentenza n. 735/2007, ha affermato come l'acquisizione indiscriminata di informazioni, *rectius* "dati", contenuti all'interno della memoria di un *computer* non può e non deve risolversi in una distorsione delle attività d'indagine volte alla ricerca della *notitia criminis*. In un caso analogo ha sostenuto espressamente che *«l'atto acquisitivo, non individuando in maniera chiara e specifica il legame intercorrente fra il reato per cui si procedeva e l'azione di sequestro dell'intera memoria informatica, si è risolto in una acquisizione indiscriminata (…)»*[83] generando l'illegittimità del sequestro stesso.

La Legge n. 48 del 2008, è intervenuta anche in tema di sequestro di corrispondenza, incidendo sia sull'art. 254 c.p.p. (sequestro di corrispondenza) che sull'art. 353 c.p.p. (acquisizione di plichi o corrispondenza). Come noto, il tema è di grande delicatezza, stante la protezione costituzionale posta dall'art. 15 della Carta fondamentale, che impone il rispetto di una duplice garanzia rappresentata dalla riserva di legge e dalla riserva di giurisdizione.

---

81 Monti A., *No ai sequestri indiscriminati di* computer, in *Diritto dell'Internet,* 2007, 3, p. 268.

82 Tribunale Riesame, Venezia, ord. 6 ottobre 2000, in *leggiditalia.it.*

83 Logli A., *Commento alla sentenza n. 753/2007*, in *Cass. pen.*, 2008, 7-8, pp. 2956-2957.

In particolare, l'art. 254 c.p.p. prevede la possibilità da parte dell'autorità giudiziaria di disporre il sequestro di corrispondenza quando abbia fondato motivo di ritenere che la corrispondenza diretta o riferibile all'imputato possa avere una qualche relazione con il reato per cui si procede. Le novità apportate dalla citata Legge n. 48 possono essere lette sotto tre differenti profili. In primo luogo vi è stato un ampliamento dei soggetti coinvolti dal sequestro, nel senso che accanto ai tradizionali servizi postali e telegrafici sono stati richiamati più genericamente i fornitori di servizi postali, telegrafici, telematici e di telecomunicazione, poiché sempre più non solo gli *Internet Service Provider* ma anche i tradizionali servizi postali sono offerti al grande pubblico mediante la modalità elettronica. Si veda, infatti, come sul punto anche la stessa normativa internazionale accolga una definizione "omnicomprensiva" di fornitore di servizi quale « *Any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service.»* (art. 1 *Code of Conduct*). In seconda battuta si stabilisce a chiare lettere l'equiparazione fra inoltro tradizionale e inoltro telematico (letteralmente *« (…) anche se inoltrati per via telematica»*[84]): alla luce di ciò, potrà qualificarsi legittimo il provvedimento di sequestro che abbia per oggetto qualsiasi comunicazione inviata o ricevuta dall'indagato mediante l'utilizzo di strumenti elettronici. Da ultimo, il secondo comma dell'art. 254 c.p.p. fa riferimento al caso in cui qualora al sequestro provveda un ufficiale di p.g., questi è tenuto alla sola presa in consegna degli oggetti di corrispondenza sequestrati, *«senza aprirli o alterarli e senza prendere altrimenti conoscenza del loro contenuto»*. Con l'espressione "alterarli" si fa un implicito rinvio alla forma informatica della comunicazione e, in conseguenza, anche alle norme che ne permettono l'acquisizione mediante procedure che ne garantiscano l'immodificabilità del contenuto (una su tutte la funzione di *hashing)*. Sul fronte del sequestro a iniziativa della p.g., l'art. 353 c.p.p. prevede in generale la facoltà per la stessa di acquisire plichi sigillati. Nel caso di comunicazioni elettroniche è interessante la novità rappresentata dall'apprensione del contenuto della comunicazione in casi urgenti: qualora, infatti, sussista un pericolo di dispersione a causa del ritardo, l'ufficiale di p.g., può chiedere al p.m. l'autorizzazione all'apertura *«e l'accertamento del contenuto»*; sul punto la dottrina lamenta *«un vuoto difficilmente colmabile»,*[85] rappresentato dalla mancanza del richiamo alla forma elettronica, non praticabile mediante interpretazione estensiva del successivo terzo comma della norma. Qui si prevede, infatti, in maniera esplicita che in caso di «oggetti di corrispondenza, anche se in forma

[84] Logli A., *ibidem.*

[85] Cajani F., Aterno S., *Aspetti giuridici comuni delle indagini informatiche*, in Aterno S., Cajani F., Costabile G. Mattiucci M., Mazzaraco G., *Computer forensics e indagini digitali,* cit., p. 484.

elettronica o inoltrati per via telematica», qualora sussistano ragioni di urgenza, gli agenti possono ordinare al gestore del servizio di sospenderne l'inoltro per poterli "congelare". Se entro le quarantotto ore successive il p.m. non ne dispone il sequestro, potrà proseguirsi con l'ordinaria trasmissione.

Inquadrati i termini del problema dal punto di vista normativo, non resta che analizzare la questione del sequestro di corrispondenza da un punto di vista pratico. Ci si riferisce in particolare alle problematiche connesse all'utilizzo di programmi di gestione della posta elettronica (*Outlook Express* nella versione *Windows*, *Mail* nella versione *Macintosh*). Il frequente utilizzo delle *e-mail* ha portato, infatti, accanto all'uso delle tradizionali applicazioni *live* fornite dai gestori di posta elettronica (*msn-hotmail, yhaoo-yhaoomail, google-googlemail*), alla diffusione di numerosi *software ad hoc* per la ricezione e gestione della posta in entrata e in uscita, attraverso meccanismi di transito diretto al *computer*. La questione ruota intorno al trattamento giuridico da riservarsi in sede di acquisizione del dato mediante tecniche forensi.

In particolare, l'acquisizione di messaggi di posta contenuti all'interno di programmi subiscono lo stesso trattamento se contrassegnati come "letti" o "nuovi"? La dottrina, sul punto, argomenta in maniera diversa: tuttavia è concorde nel ritenere che l'acquisizione di messaggi "in uscita" debba avvenire nel rispetto degli art. 254 e 353 del codice di rito. Lo scontro di posizioni è dato dal rinvenimento di messaggi aperti e nuovi presenti sul programma gestionale o su *browser* aperto all'indirizzo legato al gestore di posta elettronica in modalità remota. La posizione più garantista[86] ritiene applicabile ai messaggi non letti la procedura dettata dall'art 254 c.p.p. con conseguente acquisizione garantita contro alterazioni e trasmissione al p.m., il quale, successivamente ne valuterà la sequestrabilità. Di contro, per i messaggi aperti, la garanzia sopra ricordata non sembrerebbe applicabile in quanto non integrerebbe l'ipotesi di corrispondenza "chiusa" o "sigillata". Per arginare in parte la lacuna e per ragioni di coerenza si è argomentato come anche la *password* inserita all'interno delle impostazioni relative al programma gestionale di posta possa assumere valore di "sigillo", estendendo anche a questa ipotesi l'applicabilità dell'art. 353 c.p.p. L'argomentazione, forzata, parte del presupposto che, nel configurare il programma, l'utente fornirà *Id* e *password* d'accesso corrispondenti all'*account* di posta creato presso il proprio gestore: nei successivi accessi il programma non richiederà nuovamente tali informazioni, poiché saranno memorizzate come impostazioni di configurazione di base. È chiaro che qualora la p.g. acceda al dispositivo o rinvenga lo stesso già in funzione, potrà rilevare la presenza del programma gestionale in uso

[86] A. Logli, *Commento alla sentenza n. 753/2007*, cit., pp. 2957-2958.

già impostato, libero da qualsiasi misura di sicurezza atta a prevenirne l'apprensione.

La tesi sicuramente è forzata ma, in ragione della delicatezza della materia, risulta per i sostenitori l'unica via percorribile per non creare trattamenti differenziati ingiustificati in un settore così delicato come quello della segretezza delle comunicazioni. Da un diverso punto di vista, forse più "inquisitorio", altra parte distingue nettamente il trattamento. Seguendo l'impostazione della Cassazione[87], la ripartizione fra *mail* aperta e mail chiusa così come visivamente rappresentato dal programma, in termini giuridici, risulta fuorviante. L'evidenziazione grafica della "posta in arrivo" non fornisce, da un punto di vista giuridico, certezza sull'intervenuta conoscenza o meno del contenuto da parte del destinatario[88]. Sul punto, infatti, sembrerebbe potersi applicare l'art. 45, comma 2° del codice dell'amministrazione digitale il quale prevede che *«Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.»* Sulla base di queste considerazioni non vi sono elementi a contrario che possano giustificare un diverso trattamento, e quindi in conseguenza si esclude l'applicabilità dell'art. 254 c.p.p. Di questo avviso è la stessa giurisprudenza di Cassazione, la quale ritiene che *«in materia di sequestro di corrispondenza l'art. 254 c.p.p. è norma speciale rispetto alla disciplina dei sequestri, in quanto attiene a materia presidiata dall'art. 15 Costituzione e dall'art. 8 della Convenzione Europea dei Diritti dell'Uomo e pertanto è applicabile al solo sequestro della corrispondenza "in corso di spedizione"».* In sostanza, quindi, qualora in occasione di un sequestro le autorità ritrovassero all'interno di un *computer* elementi di corrispondenza telematica pertinenti all'indagine potranno liberamente prenderne visione ed estrarne copia alla stregua di qualsiasi altro dato informatico presente nel dispositivo. Diversamente, in ordine all'applicabilità delle garanzie previste dagli artt. 254 c.p.p. e 353 c.p.p. è necessario che la corrispondenza di cui al sequestro sia *«trasmessa nel sistema di telecomunicazione e che, temporaneamente e prima dell'invio del destinatario, si trovi conservata e memorizzata presso il fornitore di servizio»*[89].

Da ultimo, si segnala un'ulteriore possibilità di sequestro disciplinata dal nuovo art. 254 *bis* c.p.p.: il sequestro di dati presso fornitori di servizi. Si prevede un onere di collaborazione fra autorità giudiziaria e gestori di servizi informatici, telematici o di telecomunicazioni, soggetti

---

87 Cass., sez. VI, 10 dicembre 2009, n. 47009, in *leggiditalia.it*.

88 Si veda l'opzione permessa dalla maggior parte dei programmi di gestione di contrassegnare, anche in un momento successivo, posta aperta come "messaggio non letto", ricostruendo visivamente la busta chiusa accanto al messaggio selezionato.

89 Cajani F., Aterno S., *Aspetti giuridici comuni delle indagini informatiche*, in Aterno S., Cajani, F. Costabile G. Mattiucci G., Mazzaraco M., *Computer forensics e indagini digitali*, cit., p. 487.

all'azione coattiva di apprensione dei dati mediante copia degli stessi su adeguato supporto e, in conseguenza, sempre più destinatari di obblighi di collaborazione, consegna, e conservazione prolungata dei dati di traffico. Diverse sono le critiche che vengono mosse alla disposizione *de qua*: da un lato, si sottolinea come essa appaia discutibile addossando, di fatto, *«incombenti "investigativi" a soggetti che assumono una posizione delicata quali individui a rischio di concorso nel reato commesso dal cliente (...), facendosi portatori di quel* privilege against self-incrimination *di chi rischia di far emergere la propria responsabilità»*[90]; dall'altro, si evidenzia la possibile sovrapposizione della previsione del sequestro di dati di traffico o ubicazione all'analoga disciplina contenuta nel Codice della *Privacy* all'art. 132 in tema di *data retention*. Si è proposta, al riguardo, una interpretazione restrittiva - invero non priva di forzature - secondo cui l'art. 254 *bis* c.p.p. disciplinerebbe il *quomodo*, ma non *l'an* del decreto di sequestro, andando solamente a riempire i contenuti operativi dell'art. 254 c.p.p. di cui costituirebbe una specificazione.[91]

[90] Lupària L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, in *Diritto Penale e Processo,* 2008, 6, p. 699.
[91] Lupària L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, in *Diritto Penale e Processo,* cit., p. 701.

CAPITOLO TERZO

Le prove informatiche[92]

A questo punto della trattazione, occorre soffermarsi più specificamente sulla natura delle cosiddette "prove digitali", distinte dalle "prove tradizionali".

Si seguirà un approccio che cerchi di focalizzare l'attenzione più sui principi che regolano la materia che sui tecnicismi, il cui approfondimento non solo esulerebbe dai limiti del presente studio, ma sarebbe soggetto ad una rapida obsolescenza. Onde favorire la chiarezza espositiva, si cercherà, dunque, di ridurre al minimo gli aspetti tecnologici, che però appaiono una componente imprescindibile per una corretta disamina della materia.

1. Le principali fonti di prova

Le prove digitali possono essere classificate in base alla loro accessibilità da parte dell'utente. Si possono definire in tale dominio quelle prove che sono direttamente accessibili dall'*user*. Si noti che ciò non fa riferimento ad uno specifico luogo fisico o ad un insieme di dispositivi fisici, ma all'insieme di strumenti a cui l'utente ha un accesso informatico diretto. Tra questi si possono considerare alcuni dispositivi fisici, che possono anche essere collocati in differenti luoghi, ad esempio: i *computers* dell'ufficio, di casa e il portatile, il telefono cellulare, ed una serie di memorie *USB*. Sono nel dominio dell'utente anche gli strumenti remoti che sono disponibili in rete e che in alcuni casi hanno una collocazione fisica ignota; tra questi, le caselle di posta elettronica memorizzate nei *server* dei *provider* o gli spazi di memorizzazione disponibili nella cosiddetta *cloud* [93]. Analogamente, si possono definire estranee al dominio dell'*user* le prove che consistono in strumenti informatici che non sono accessibili dall'utente.

Ad esempio, tutte quelle prove che sono in internet e genericamente *online*. In altri termini, per accedere alle prove estranee al dominio di un utente è necessario fare ricorso ai terzi nel cui dominio ricadono queste prove.

È interessante notare come la fisicità non abbia alcun rilevo ai fini di questa classificazione.

---

92 Liberamente tratto da Delfini F., Finocchiaro G., *Diritto dell'informatica*, UTET giuridica, anno 2014.

93 Questi aspetti saranno analizzati nel Cap, 3 par. 5.

Si consideri un *computer* portatile aziendale che, pur essendo nel pieno possesso fisico dell'utente, non è gestito da quest'ultimo, ma dai servizi informatici aziendali. In questo caso avrebbe il pieno controllo di alcune parti del disco rigido, ossia quelle che gli sono state assegnate come semplice *user*, ma non potrebbe accedere alle parti del disco che sono di pertinenza dell'amministratore di sistema. Quindi, il disco rigido di quel *computer* portatile sarebbe solo parzialmente nel dominio dell'utente, mentre il resto rientrerebbe nel dominio dell'amministratore di sistema.

L'utente, però, potrebbe sfruttare il suo controllo fisico dell'apparato per operarvi con strumenti specifici che permettano di "scavalcare" il sistema operativo e quindi potrebbe accedere ai dati nel dominio dell'amministratore.

Un *file* potrebbe anche essere nel dominio di più *users*, come nel caso di documenti condivisi tra più utenti oppure di *file* accessibili da tutti gli utenti di un sistema.

Il contenuto di un documento, o più genericamente di un *file*, dipende esclusivamente dalla sequenza temporale di scritture e quindi di modifiche compiute su di esso. Normalmente, i sistemi informatici non tengono traccia dell'intera successione di scritture, ma solo del loro esito complessivo[94].

Per mezzo di specifici sistemi *software* si può tenere traccia di ogni singola modifica apportata a *files* prestabiliti.

Questi strumenti sono detti di *versioning* e vengono solitamente utilizzati nello sviluppo di *software* oppure nella scrittura a più mani di documenti[95].

L'operazione di modifica di un *file* può essere conseguenza esplicita di una azione volontaria dell'utente, o di automatismi che possono essere sia del sistema operativo sia di altri programmi in esecuzione. Ad esempio, sia il sistema operativo sia diversi altri programmi, tengono traccia cronologica di eventi considerati rilevanti.

Queste tracce sono memorizzate in appositi *files*, detti *files di log*: mano a mano che si verificano eventi rilevanti la loro registrazione viene aggiunta al *file di log* relativo al tipo di evento[96]. In un certo senso essi costituiscono una sorta di "giornale di bordo" delle attività rilevanti del *computer*. Sono solitamente estranei al dominio degli utenti, e sono gestiti in modo

---

[94] In questo caso il termine *computer* è da considerarsi in una accezione più generale, che comprende sia *l'hardware* sia il sistema operativo.

[95] Tra i più diffusi strumenti di *versioning* si possono considerare, ad esempio, *CVS (http://cvs.nongnu.org) e Subversion (http://subversion.apache.org)* ed anche la modalità "revisione" fornita da molti programmi di scrittura.

[96] Tutti gli accessi, ossia la data e l'ora in cui ogni utente entra nel sistema, ovvero effettua il cosiddetto *login*, e di quando lo lascia, ovvero quando effettua il *logout*. In diversi casi il sistema ha anche un file di *log* per ogni stampa effettuata che contiene dati quali i nomi dell'utente e del *file* stampato, l'ora, la lunghezza del *file* ed altro ancora.

automatizzato indipendentemente dalla volontà di questi ultimi. Possono inoltre subire continue modifiche o anche essere cancellati a seguito delle regolari attività di manutenzione eseguite autonomamente dal sistema operativo.

Solitamente, gli utenti hanno un accesso limitato ai *files di log*, che spesso si riduce unicamente alla loro lettura. In generale, un utente generico ha diverse limitazioni alle azioni che può compiere, sia per evidenti ragioni di sicurezza e riservatezza, sia per motivi di integrità del sistema. I sistemi operativi moderni prevedano la presenza di molti utenti, e quindi forniscono dei sistemi automatici per evitare possibili interferenze fra questi. Costituiscono una rilevante eccezione molti apparati ad uso prevalentemente personale, quali i telefoni cellulari evoluti, detti *smartphones*, e i cosiddetti *tablet computers*. Come sarà illustrato di seguito, questi apparati sono *computers* a tutti gli effetti, ma sia la loro potenza sia la loro modalità di utilizzo favoriscono l'adozione di un sistema operativo per singolo utente.

Per migliorare la loro efficacia, molti programmi gestiscono autonomamente dei dati temporanei nelle memorie permanenti: questi dati costituiscono la cosiddetta memoria *cache*. Ad esempio, i *browser*[97] per navigare nel *web* utilizzano una *cache* per memorizzare le pagine visitate di recente: in questo modo non è più necessario ricaricarle se l'utente volesse rivederle a breve, così come non sarebbe necessario ricaricare tutti gli elementi comuni alle pagine di uno stesso sito visitate in sequenza.

Diversi siti *web* memorizzano piccole quantità di dati direttamente nel *computer* degli utenti che li visitano: questi dati prendono il nome di *cookies*. Un *cookie* può contenere dati identificativi dell'utente quando questi accede a siti che richiedono una *password*, quali ad esempio quelli di posta elettronica o di *home-banking*, ma anche dati per il tracciamento delle abitudini di navigazione dell'utente. Solitamente i *browser* permettono all'utente di gestire i *cookie*s, ad esempio si può decidere di non accettarli mai, di accettarli solo da alcuni siti, di cancellarli all'uscita dal *browser*, e molto altro. Esistono moltissimi programmi di gestione dei *cookie*s nei più diffusi sistemi operativi e *browser*. La navigazione in *internet*, quindi, lascia tracce numerose e differenziate nella memoria stabile del dispositivo utilizzato.

Tutti i sistemi operativi prevedono un utente privilegiato, detto anche *root* o *superuser*, che non ha vincoli né all'esecuzione di programmi, né all'accesso ai *file*s. La presenza di un utente senza vincoli è particolarmente utile per amministrare completamente il sistema.

Nel corso del normale funzionamento di un sistema informatizzato, l'utente *superuser* entra

[97] Fra tutti vale la pena menzionare *Firefox (http://www.firefox.com)* di Mozilla, *Internet Explorer* di Microsoft *(http://windows.microsoft.com/it-it/internet-explorer/download-ie), Chrome* di Google *(https://www.google.com/it/chrome/), Safari* di Apple *(http://www.apple.com/it/safari) e Opera* della omonima società *(http://www.opera.com).*

in gioco solo per compiere operazioni straordinarie quali, ad esempio, l'aggiunta di nuovi utenti e l'installazione di nuovi programmi.

Gli altri utenti sono gli utilizzatori normali e solitamente non hanno possibilità e responsabilità di amministrazione del sistema.

Diversi sistemi hanno una o più copie periodiche di *backup* dei dati, che sono salvate su memorie esterne. Le copie di *backup* hanno lo scopo di memorizzare una copia dei dati allo stato attuale, in modo da poterli recuperare se questi dovessero andare persi o essere danneggiati a causa di malfunzionamenti del sistema, di incidenti, oppure di una azione incauta dell'utente. Questi sistemi sono automatizzati ed in alcuni casi possono permettere di ricostruire la storia delle modifiche apportate nel tempo ad ogni singolo *file*. Essi possono costituire un interessante caso di passaggio di dominio: sino a che un utente può fare tutte le modifiche che ritiene ad un documento, questo resta nel suo dominio, mentre la copia del *file* che è nel *backup* non è più modificabile da parte dell'utente, e quindi è estranea alla sua disponibilità. Per ripristinare la copia di un *file* contenuto in un *backup* è necessario che l'utente faccia ricorso all'amministratore di sistema, che effettua il ricollocamento di una copia di quel *file* all'interno del dominio dell'utente.

2. I dispositivi fisici

Per meglio comprendere molte peculiarità delle prove informatiche, è necessario considerare alcune caratteristiche tecnologiche proprie dei *computer* , rilevanti ai fini del presente studio. I *files* sono memorizzati in memorie cosiddette "stabili" o "permanenti", come ad esempio: i dischi rigidi, i CD, i DVD e le memorie *USB*[98]. Questi supporti conservano il loro contenuto anche quando il *computer* è spento. Altro tipo di memorie sono quelle definite "volatili", come ad esempio, la memoria centrale di un *computer*, detta anche *RAM*[99].

Le memorie volatili perdono il loro contenuto quando il dispositivo viene spento, mentre sono utilizzate intensamente durante il suo funzionamento[100].

---

[98] I cosiddetti *floppy disk* si basano sulla stessa tecnologia magnetica dei dischi rigidi, anche se meccanicamente meno raffinata, e hanno una capacità nettamente ridotta rispetto a questi ultimi. Sono oramai praticamente in disuso.

[99] Questa memoria contiene i programmi in esecuzione e i dati su cui questi operano. Un programma può essere eseguito solo quando memorizzato nella RAM.

[100] La differente tecnologia di memorizzazione diventa evidente nel caso di una imprevista interruzione di corrente elettrica al *computer*: tutto il lavoro fatto, ma non ancora "salvato" sul disco rigido, viene perso irrimediabilmente.

Solitamente, il contenuto delle memorie volatili è estraneo al dominio dell'utente ed è completamente gestito dal sistema operativo e dai programmi in uso. Il tempo di persistenza dei dati in una memoria è funzionale al loro ruolo. I dati temporanei necessari all'esecuzione di un programma possono avere una persistenza di alcune frazioni di secondo, mentre i dati in un archivio che viene consultato molto raramente possono arrivare ad avere una persistenza che abbraccia tutta la vita fisica della memoria[101].

È importante illustrare brevemente lo schema logico della memorizzazione dei *files* in un disco rigido[102]. In estrema sintesi, può essere rappresentato come una grande cassettiera[103], di cui ogni cassetto, tecnicamente chiamato settore*,* è solitamente capace di memorizzare *512 Byte.* Ogni *file* memorizzato sul disco è quindi contenuto in una sequenza di settori logicamente concatenati fra loro.

Il disco ha un sommario che indica solo il primo settore di ogni *file*, mentre ogni altro settore della sequenza indica il suo successore; l'ultimo settore del *file* non ha alcun successore. Esso non è necessariamente memorizzato in settori contigui[104].

Il sommario del disco contiene anche gli indici dei primi settori delle liste di quelli liberi*,* e di quelli danneggiati[105]. Quando un *file* viene cancellato, il sistema operativo, per eseguirne velocemente la cancellazione, si limita a modificare solo alcuni indici, aggiungendo alla catena dei settori liberi quelli che contenevano il *file*, e a cancellarne dal sommario solo il nome e l'indice al suo primo settore.

Tutti i dati contenuti nei settori del *file* cancellato restano sul disco, ma non sono più accessibili come dati organizzati.

---

[101] La RFC 3227 *Guiddines for Evidence Collection and Archiving* consultabile all'URL *http://wtmv.rfc-editor.org/rfcjrfc3227.txt,* elenca le memorie volatili in base a quanto velocemente cambiano i dati in esse contenuti. Le *Request For Comment,, RFC,* letteralmente "Richiesta di Commento", sono una sorta di *memorandum* di argomento informatico proposte internazionalmente da scienziati e ricercatori sia per una revisione fra pari *(peer review)* sia per diffondere nuove idee e concetti. Le RFC sono pubblicate dalla *Internet Society,* organizzazione *non-profit* internazionale per la promozione dell'accesso e dell'utilizzo di *internet* e possono essere vagliate dalla *Internet Engineering Task Force (IETF),* che ha il compito di sviluppare e proporre *standard* e "*test practices*" per *internet*.

[102] Un disco rigido è in realtà composto da una pila di dischi rotanti in solido sullo stesso asse. Le superfici di questi dischi sono magnetizzabili per mezzo di una testina di lettura e scrittura che può muoversi radialmente rispetto all'asse di rotazione. I *files* sono memorizzati sulla superficie di un disco in ***tracce*** concentriche, suddivise a loro volta in *settori,* che possono contenere *512 byte.* Il disco contiene un indice che indica il primo settore di ogni *file*, il primo della lista dei settori liberi e il primo della lista dei settori danneggiati.

[103] Un disco rigido da *1TB*, misura attualmente molto comune nei *personal computer* da scrivania, ha una capacità equivalente ad una mensola piena di libri lunga approssimativamente 10Km.

[104] Questa tecnica di memorizzazione permette una gestione flessibile della memorizzazione dei *files*. La sua dimensione non interferisce con la memorizzazione degli altri *files*.

[105] Considerare una lista di settori danneggiati permette di escluderli dall'utilizzo e di aumentare l'affidabilità del disco. Una tecnica per nascondere dati su disco prevede di aggiungere alla lista dei settori danneggiati anche quelli che contengono i *files* che si vuole tenere segreti.

La metodologia di cancellazione dei *files* appena descritta implica che lo spazio "vuoto" di un disco rigido può contenere molti dati, che sono stati "cancellati" ma non eliminati dal disco. Le tecniche di recupero dei *files* cancellati sfruttano proprio questa peculiarità[106]. Un'altra conseguenza della metodologia di memorizzazione dei *files* su disco è che l'ultimo settore di un *file* potrebbe non essere completamente riempito dai dati del *file* e potrebbe contenere ancora dati precedenti che non siano stati sovrascritti completamente.

I dischi rigidi sono le memorie permanenti attualmente più comuni e si basano su una tecnologia di tipo magnetico. Iniziano a diffondersi le memorie permanenti a stato solido, dette *SSD*[107]*,* ma attualmente sono montate solo su una parte ancora poco rilevante dei *computer* disponibili. Queste memorie si basano sulla stessa tecnologia elettronica che viene utilizzata per le memorie *USB*, detta memoria *flash*. Oltre alla velocità superiore rispetto ai dischi tradizionali, la caratteristica principale degli SSD è che i *transistor* utilizzati per memorizzare i dati possono supportare un numero massimo di scritture, dopo le quali non offrono più garanzie di funzionamento affidabile. Di conseguenza, la memoria *SSD* evita di insistere sempre sulle stesse celle per memorizzare i *files* e cerca di utilizzarle uniformemente. Un primo effetto di questa tecnica consisterebbe nel fatto che anche dopo un breve periodo di utilizzo tutta la memoria *SSD* conterrebbe dati, siano essi attuali o obsoleti. Lo scenario si complica considerando che per riscrivere dati in una locazione della SSD solitamente è necessario che questa sia vuota, ossia occorre cancellarla prima di ogni riscrittura. Se la cancellazione del contenuto di una cella di memoria fosse effettuata in occasione di ogni riscrittura rallenterebbe sensibilmente le sue prestazioni complessive. Per ovviare a questi inconvenienti la SSD, autonomamente dal sistema operativo e nei suoi momenti di pausa, cancella le locazioni di memoria che contengono dati obsoleti. Tale caratteristica rende molto complessa la ricerca di prove digitali in una SSD, perché questa potrebbe cancellarle autonomamente, a seguito delle sue usuali operazioni di *routine,* anche semplicemente perché viene collegata ad un alimentatore elettrico. Più passa il tempo, più la memoria SSD modifica il suo contenuto cancellando dati divenuti obsoleti. È evidente che le memorie SSD possono creare fortissime limitazioni alla estensione delle indagini forensi. Le tecniche e gli strumenti di indagine forense fanno tradizionalmente riferimento a memorie di tipo magnetico, e sono quasi del tutto inefficaci nel

---

[106] Non sempre un *file* può essere recuperato, dipende dal sistema operativo e da come questo utilizza i settori dello spazio disponibile. In generale, se i settori che contenevano un *file* cancellato non sono stati riutilizzati il *file* continua a essere memorizzato sul disco. Alcuni sistemi operativi forniscono meccanismi di "cancellazione sicura", che scrivono anche diverse volte i settori dei *files* cancellati con sequenze di dati senza significato. La stessa metodologia è utilizzata anche da specifici programmi di cancellazione.

[107] Acronimo dall'inglese *Solid State Drive.*

caso di memorie a stato solido, che fanno del dinamismo il fulcro della loro efficienza funzionale.

Un sistema informatico costituisce un ambiente estremamente dinamico, anche quando non compaiono segni evidenti di attività il sistema operativo è comunque in esecuzione e spesso lo sono anche altri programmi[45]. Questi programmi in continua esecuzione modificano lo stato del sistema, ovvero possono modificare i contenuti di *files* ed i dati nelle memorie volatili. Si consideri che in molti casi il sistema operativo può attivare ulteriori programmi, non ancora in esecuzione, a seguito di scadenze temporali[46].

Mai come in questo caso l'aspetto fisico è del tutto ininfluente: un *computer* in funzione non subisce modifiche fisiche nel corso delle sue elaborazioni di dati. Le operazioni di raccolta di prove digitali sono particolarmente delicate. L'ideale sarebbe poter fare l'equivalente di una sorta di "fotografia" al contenuto istantaneo di tutte le memorie del *computer* facendone una copia fedele. Purtroppo questo non è praticabile a causa del continuo dinamismo dell'ambiente e se fosse attuato produrrebbe risultati diversi in momenti diversi. Si consideri che persino la semplice lettura del contenuto di un disco rigido potrebbe modificare lo stato di alcune memorie e di zone del disco riservate ai programmi di *auto test* e di monitoraggio che vengono attivati all'accensione del disco. Il miglior approccio praticabile per acquisire i dati in una memoria stabile è quindi quello di duplicarli tramite copia, limitando il più possibile le inevitabili interferenze e modifiche. La copia delle memorie volatili presenta caratteristiche completamente differenti, perché il loro contenuto si perde dopo lo spegnimento del sistema, e quindi raramente si ha la possibilità di poterle copiare. Nel caso in cui il sistema informatico fosse ancora in funzione, si potrebbe fare un *dump* della memoria, ovvero una sorta di "fotografia" per salvarne il contenuto in un *file* nella memoria stabile.

Sempre nel caso di un sistema in funzione, occorre considerare che anche il regolare spegnimento tramite le usuali procedure può provocare la modifica dei dati. Molti sistemi prevedono l'esecuzione automatica di specifici programmi in questa fase; essi potrebbero alterare, anche pesantemente, il contenuto dei *files* nelle memorie stabili. In alcuni casi è quindi preferibile uno spegnimento poco ortodosso del sistema ancora accesso, quale quello di togliere l'alimentazione elettrica, per preservare il più possibile il contenuto delle memorie stabili.

a. Documenti e files

Quanto appena descritto fa riferimento a dati "in chiaro" ossia esplicitamente accessibili

sia in forma di dati sia in forma di metadati che molti programmi inseriscono nei loro documenti. Oltre a questi, si possono considerare anche dati di origine diversa, che sono rimasti "impigliati" nelle pieghe dei sistemi informatici. Tra questi vale la pena menzionare i più comuni, quali i dati negli spazi liberi[108] e in quelli *slack*[109] dei dischi rigidi, nei *files* temporanei dei programmi[110], nei *files* di *swap* della memoria[111] e di *ibernazione*[54], e i dati fisici, non più accessibili logicamente, che restano sotto forma di tracce lasciate dai meccanismi di scrittura[112]. Tutti questi dati possono essere memorizzati in un disco rigido senza essere palesemente manifesti. Diversi programmi ad ampia diffusione inseriscono nei documenti con il proprio formato un'ampia gamma di informazioni aggiuntive, che prendono il nome di "metadati". Ne sono un esempio due dei formati maggiormente diffusi: *Microsoft Word e Adobe PDF*. Ad esempio i dati necessari a *Word* per le formattazioni, per le revisioni e per i commenti sono memorizzati come metadati all'interno del *file* che contiene il testo. Ulteriori metadati, ad esempio relativi all'autore e alle date di creazione e modifica, possono essere trovati nelle proprietà del documento e sono inseriti automaticamente dal programma[113]. In realtà, i documenti di molti

---

[108] Come illustrato in precedenza, gli spazi liberi possono contenere parti di *files* cancellati, o anche *files* ancora integri, i cui settori non siano stati ancora utilizzati, e quindi sovrascritti, da altri *file*s.

[109] Lo spazio eccedente la lunghezza di un *file* rispetto alla capacità della catena di settori che lo contiene prende il nome di spazio *slack*. In alcuni casi, quando un disco è di grande capacità può contenere talmente tanti settori che non sono indirizzabili individualmente nell'indice sommario. Per ovviare a questo problema il sistema operativo raggruppa i settori e considera questi gruppi, detti *cluster,* come una sorta di macrosettore atomico. Quello che può accadere è che l'ultimo *cluster* della catena che contiene un *file* potrebbe avere anche più settori con i dati di *file*s precedenti.

[110] Molti programmi utilizzano *files* temporanei per memorizzare lo stato dell'elaborazione prima che questo venga salvato dall'utente in forma compiuta. Ad esempio alcuni *files* temporanei potrebbero contenere la storia delle modifiche apportate ad un documento in modo da abilitare la funzione di "annulla" da parte dell'utente.

[111] Diversi dispositivi mobili dispongono di una modalità, cosiddetta di *ibernazione*, che consente al sistema operativo di salvare sul disco rigido l'intero contenuto della memoria RAM e del processore in modo da riattivarsi molto velocemente, senza riaccendere il dispositivo, e ripristinare lo stato subito prima dell'ibernazione.

[112] Ognuna delle testine di lettura/scrittura dei dischi rigidi tradizionali è montata su un braccio mobile che la posiziona sul settore del disco da leggere o scrivere, che nel frattempo ruota sotto di essa. Per quanto la meccanica coinvolta sia di grande precisione, la testina non è mai posizionata esattamente nello stesso punto del piatto sottostante. Il risultato finale è che ai margini fisici del settore possono restare tracce dei dati precedentemente memorizzati. Per accedere a queste tracce è necessario utilizzare sofisticate tecniche *hardware*.

[113] Sono noti diversi casi di documenti rilasciati ufficialmente che contenevano dati che non si intendeva rendere pubblici. Nel 2003 il governo inglese rilasciò un documento *word* sullo stato degli armamenti dell'Iraq che si rivelò essere un plagio di alcune fonti accademiche. Una analisi dei metadati del documento portò all'identificazione degli autori e causò un notevole imbarazzo internazionale al governo inglese. Nel 2005, a seguito del tragico incidente in zona di guerra che costò la vita a Nicola Calipari, il comando militare statunitense pubblicò un documento PDF di 45 pagine il cui testo era stato ampiamente coperto da rettangoli neri per ragioni di segretezza. I rettangoli neri del documento erano però nei metadati dello stesso e con il

applicativi, quali ad esempio *Word* e *Write* di *OpenOffice* sono *files* compressi con metodologia *standard*[114], che contengono una struttura di cartelle e sotto-cartelle con i dati e i metadati del documento. Gli applicativi compiono *runtime* le operazioni di compressione e decompressione dei propri *files*. Diversi applicativi dispongono di linguaggi di programmazione interna, detti linguaggi di *script,* che permettono di associare ad ogni documento veri e propri programmi che consentono anche di modificare automaticamente il documento a cui sono associati ogni volta che questo viene aperto. In altri termini, il contenuto di un *file* potrebbe apparire dinamico e non costante nel tempo. Ad esempio, molti *word processor* permettono di inserire automaticamente la data corrente in un documento, quindi aprendo il documento in giorni diversi si ottiene un documento diverso. In questi casi occorre evidenziare che il documento contiene sia il testo sia un programma, e questo insieme non varia nel tempo; quello che varia è risultato dell'esecuzione del programma all'apertura del *file*, ossia quello che viene *mostrato* del contenuto del documento[115].

b. Accesso ai files

L'accesso ai *files* di un apparato è regolato dal sistema operativo. A seconda del grado di raffinatezza del sistema si possono avere diversi gradi di accessibilità ad un *file*, ovvero delle operazioni che l'utente può compiere su di esso. Usualmente ci sono almeno tre tipi di accesso, che possono essere combinati tra loro: lettura, scrittura, esecuzione. I primi due tipi di accesso sono auto-esplicativi, mentre il terzo è necessario per eseguire i programmi. I tipi di accesso sono usualmente associati ai permessi di accesso*,* anche questi gestiti dal sistema operativo. Questi ultimi stabiliscono quale utente ha diritto di accedere al *file* e quali operazioni può compiere su di esso.

Sia i tipi di accesso sia le metodologie di gestione di essi dipendono dal sistema operativo in uso. Ad esempio, nei sistemi operativi della famiglia *Unix* i tre tipi di accesso sono applicati

---

classico "copia e incolla" fu particolarmente semplice leggere l'intero contenuto, che conteneva, fra l'altro anche i nomi dei militari coinvolti. Per maggiori dettagli: *http://www.corriere.it/Primo_Piano/Cronache/2005/05_Maggio/01/omissis.shtml.*

[114] Ad esempio, i *files .docx* contengono diverse cartelle al cui interno risiedono molti *files*, tutto questo compresso in formato *ZIP*, che può essere anche direttamente decompresso con il relativo programma *standard.*

[115] Gli esempi riportati in questa sezione potrebbero dare l'impressione che solo i documenti di testo contengono metadati. In realtà moltissimi tipi di documento li contengono. I programmi di produttività individuale (*word processing*, fogli di calcolo e presentazione) utilizzano insiemi molto simili di metadati. I dispositivi per scattare fotografi e digitali solitamente inseriscono nei *file* anche metadati con le coordinate geografiche e l'ora in cui la fotografia è stata scatta. Molti altri esempi potrebbero essere riportati, ma non si intende appesantire ulteriormente la trattazione.

anche alle cartelle, così come i permessi di accesso che sono distinti in: proprietario del *file*, ossia l'utente che lo ha creato, i gruppi a cui appartiene il proprietario[116] e tutti gli altri. Il proprietario del *file* ne stabilisce i permessi di accesso, che rispecchiano la gerarchia di memorizzazione. Ad esempio, se un *file* che tutti possono leggere e scrivere è collocato in una cartella in cui può scrivere solo il proprietario, nessun altro utente può modificare il *file*, ma quelli che hanno i permessi di lettura della cartella potrebbero copiarlo e poi modificare la copia. I meccanismi di memorizzazione dei dati nelle memorie di massa sono particolarmente complessi, come accennato in precedenza, e dipendono anche dalla tecnologia del supporto fisico. Per questi motivi il sistema operativo fornisce uno strato di astrazione, detto *file System*, che offre un'interfaccia uniforme per la gestione delle memorie permanenti[117]. Una memoria di massa può essere suddivisa in parti, dette partizioni, indipendenti fra loro, ognuna delle quali può essere strutturata secondo un diverso *file System*. Spesso un sistema operativo può gestire più di un tipo di *file System*. È ciò che si fa carico di gestire i metadati di memorizzazione e di associarli ai *files* e alle cartelle. Considerare un *file* al di fuori del suo contesto può diminuirne pesantemente il valore probatorio. La necessità del contesto per la corretta analisi dei documenti informatici appare chiara anche in questo scenario. Il ruolo del contesto è quello di stabilire, quanto meno, se un *file* era nel dominio dell'utente; oltre a ciò, esso potrebbe fornire gli elementi per stabilire se l'utente ha realmente effettuato un accesso significativo al *file*. Ad esempio, si possono considerare i *files di log*, che sono documenti di solo testo in formato *ASCII*, senza nessun metadato o formattazioni particolari. In altri termini, sono documenti che possono essere creati o modificati con un semplice *editor* di testo[118]. I tipi di accesso e gli utenti autorizzati alla modifica del *file* sono metadati gestiti dal sistema operativo nel *file System*; il *file di log* in sé non contiene questi metadati. La completezza e puntualità dei metadati di accesso dipende dal sistema in uso, ma senza di questi, ovvero senza contesto, il *file di log* non avrebbe un alto valore probatorio.

---

[116] I gruppi di utenti sono definiti dall'amministratore del sistema e identificano utenti con caratteristiche analoghe.

[117] Ci sono diversi *file system*, ognuno corrispondente a differenti esigenze. Per *personal computer* si possono citare almeno i seguenti *file system*. I primi PC con il *DOS* utilizzavano il *FAT* (*File Allocation Table) file system*, che ha subito molte evoluzioni ed è stato poi utilizzato da *Windows*. Le nuove generazioni di Windows utilizzano *NTFS* (*New Technology File System*), che è stato sviluppato appositamente. I *computer* Macintosh utilizzano diverse evoluzioni di *HFS* (*Hierarchical File System*). La famiglia dei sistemi operativi Unix utilizza *UFS* (*Unix File Sistem*) e una serie di sue varianti a seconda del sistema operativo. Per le memorie di massa distribuite si utilizzano *NFS* (*Network File System*) e *AFS* (*Andrew File System*). Molti di questi *file system* forniscono versioni *journaled*.

[118] Un *editor* di testo è un programma che gestisce *files* di solo testo. A differenza di un *word processor*, che inserisce anche metadati di formattazione nel documento, un *editor* è estremamente diretto e permette di gestire l'esatto contenuto del *file*, carattere per carattere.

Diverse versioni moderne di *file System* implementano una tecnologia, detta *journaled,* che gestisce un *file di log* per tutte le modifiche fatte ad ogni *file*. Questa tecnologia permette operazioni più veloci sul disco e lo protegge da eventuali incoerenze in caso di guasti. I sistemi *journaled* tengono quindi traccia completa delle modifiche effettuate recentemente a ogni *file*.

c. Dispositivi mobili

In questa categoria consideriamo telefoni cellulari e *tablet,* escludendo i *personal computers* portatili, che non presentano particolarità rilevanti rispetto quelli da scrivania. I telefoni cellulari di ultima generazione, denominati *smartphones,* sono in grado di eseguire programmi (le cosiddette *apps*), di collegarsi ad *internet* come se fossero un *computer* (sia tramite *WiFi* sia tramite rete telefonica), seppure con uno schermo più piccolo, di ricevere il segnale di posizionamento geografico del sistema *GPS*, di fare fotografie e filmati in alta definizione, di riprodurre musica e filmati (inoltre sono anche in grado ovviamente di fare telefonate e scambiare SMS e MMS). Questa tipologia di apparati ha iniziato a diffondersi negli ultimi anni dello scorso secolo e si sta rapidamente affermando presso un numero sempre maggiore di utenti. Solitamente gli *smartphones* dispongono di una tecnologia denominata *multitouch* per l'interazione con l'utente[119]. Gli *smartphones* possono essere considerati dei *computers* a tutti gli effetti e in questa sede rilevano le peculiarità dal punto di vista delle prove informatiche. I cosiddetti *tablet* sono veri e propri *computers* portatili[120] caratterizzati dalla stessa modalità *multitouch* di interazione utilizzata da molti *smartphone* ; solitamente non hanno una tastiera fisica integrata ma ne hanno una "virtuale" mostrata alla bisogna direttamente sullo schermo. Rispetto agli *smartphone* hanno uno schermo più grande e spesso non sono in grado di effettuare telefonate, anche se possono disporre di una connessione cellulare per i dati. I sistemi operativi dei *tablet* possono essere di due tipologie: quelli in uso anche nei *personal computer*, oppure quelli *post-PC,* sviluppati appositamente per questi apparati[121].

---

[119] È oramai considerato *standard* l'uso contemporaneo di più dita sullo schermo, ad esempio per ingrandire o ruotare quanto mostrato. Operazioni più complesse, sempre effettuate toccando e muovendo le dita sullo schermo, prendono il nome di *gesture*.

[120] Per avere un quadro della potenza degli attuali *tablet* si pensi che l'iPad 2, lanciato nel 2011, aveva la potenza di calcolo del *Cray 1*, il supercomputer più potente al mondo nella metà degli anni Ottanta dello scorso secolo e sarebbe restato tra i primi cinquecento supercomputer per una decina di anni. La notizia che prende spunto da uno studio dell'autorevole analista numerico Jack Dongarra, fu riportata, tra gli altri anche dal *Wall Street Journal*: *http://blogs.wsj.com/tech-europe/2011/05/11/ipad-2-more-powerful-than-1990ssupercomputer*.

[121] Della categoria dei sistemi operativi per PC utilizzati anche su *tablet* giova menzionare QNX (http://www.qnx.com) e i due Microsoft Windows 8 *(http://windows.microsoft.com/it-it/windows-8/features#t1=music)* e RT *(http://windows.microsoft.com/it-it/windows/rt-welcome)*.
I sistemi operativi post-PC più importanti sono Apple iOS *(http://www.apple.com/it/ios/ios7/)* e Google Andorid *(http://www.android.com)*. Tutti questi sistemi operativi offrono il *multitasking*.

I *tablet* presentano diverse peculiarità rispetto ai *computer* tradizionali per quanto riguarda l'indagine forense. Solitamente, sono apparati "chiusi" fisicamente, in cui non è possibile rimuovere la memoria di massa, come è invece possibile nei *computer* tradizionali. Inoltre, è molto complesso, e spesso impossibile, reperire dati cancellati perché essa è spesso del tipo SSD e in molti casi i dati sono immagazzinati per mezzo di *files* di *database*. Le tecnologie costruttive dei *tablet* e degli *smartphones* rendono spesso impossibile accedere ai dati con il dispositivo spento. L'accensione di questi dispositivi mobili causa l'esecuzione automatica di molti programmi, e quasi sempre la connessione ad i*nternet*. Entrambe queste evenienze sono indesiderabili perché causano delle modifiche ai dati memorizzati, che possono anche essere rilevanti.

I dati che possono essere reperiti su un dispositivo mobile sono di diverse tipologie e sono generati in automatico sia dal sistema operativo sia da molte *apps* in relazione ai comportamenti dell'utente. Gli *smartphone*s contengono tutti gli SMS inviati e ricevuti che non siano stati cancellati, e l'elenco delle telefonate più recenti. Molti apparati mobili tengono anche una traccia temporale dei luoghi dove sono stati. In molti casi anche le fotografie scattate contengono metadati descrittivi. Spesso gli utenti utilizzano questi dispositivi anche come agenda e rubrica telefonica, quindi i relativi dati sono memorizzati nel dispositivo. Anche la *SIM* dell'operatore telefonico può contenere dati rilevanti, oltre agli identificativi dell'utente.

Molti dispositivi mobili hanno in essere dei meccanismi di *backup* automatico. Questi *backup* possono essere memorizzati sia su *personal computer* sia *online* su appositi servizi di *cloud computing,* che saranno analizzati di seguito. I *backup* solitamente contengono una copia completa di tutti i dati sul dispositivo, memorizzati secondo un schema privato di ogni costruttore, e possono anche essere crittografati.

d. Altre possibili fonti di prova

Ci sono diversi dispositivi che possono contenere prove digitali. Ad esempio le macchine fotografiche digitali possono inserire dati GPS di posizionamento geografico e di orario nei metadati associati alle fotografie. Alcune stampanti memorizzano un *log* delle operazioni di stampa più recenti. Anche i *fax* basati su tecnologia digitale mantengono un *log*. Tutti questi dispositivi possono contenere prove, ma non è possibile descriverli in modo generale; ognuno di essi ha caratteristiche peculiari, rispettando comunque i principi generali qui descritti.

3. La posta elettronica

L'accesso alla posta elettronica solitamente avviene tramite un programma specifico oppure tramite il *web*. I programmi per la lettura stessa possono avere diverse modalità per la conservazione dei messaggi, che coinvolgono il *server* di posta ed il dispositivo locale. Si va da un approccio che prevede di conservare tutti i messaggi sul *server*, senza ritenere nulla in locale, a quello opposto, che prevede di salvare tutto localmente senza lasciare alcun messaggio nel *server*, passando per una serie di metodiche intermedie. La scelta delle modalità di gestione della *web mail* dipende dagli scenari di utilizzo, che prevedono diversi parametri, tra cui il numero dei dispositivi utilizzati, il loro grado di connettività e la loro capacità di memoria permanente[122]. L'utente ha comunque la possibilità di gestire completamente i messaggi indipendentemente dall'apparato in cui vengono memorizzati. In alcuni casi i *server* di posta offrono anche servizi di *backup*. L'affidabilità delle informazioni fomite da un messaggio di posta elettronica è variabile. I messaggi contengono una intestazione, detta *header,* che tra l'altro indica il mittente, il destinatario e tutti i *server* che il messaggio ha attraversato sul percorso per giungere a destinazione. Il mittente di un messaggio di posta elettronica potrebbe falsificare i suoi dati o anche utilizzare *server* di anonimizzazione per offuscare i suoi dati di origine. Un messaggio potrebbe, al contrario, anche essere certificato quando si utilizzino specifici servizi che forniscono carattere di terzo fidato*,* garantendo diverse proprietà altrimenti non certe, quali l'identità del mittente, l'ora e la data di invio, l'ora e la data di ricezione del messaggio. Ad esempio, la Posta Elettronica Certificata*,* detta *PEC,* garantisce tra l'altro le data e ora di spedizione e consegna ed anche che il messaggio e i suoi allegati non siano stati modificati.

4. I *social networks*

Quando una persona si iscrive ad un *social network* solitamente crea un profilo, talvolta con fotografie e dettagli anagrafici, che diviene una sorta di sua identità elettronica. Queste informazioni possono essere falsificate e potrebbero anche arrivare a non rispecchiare alcuna persona reale. Solitamente i *social networks* forniscono anche possibilità di scambio di messaggi

[122] Un esempio di pagine *web* dinamiche sono quelle che richiedono l'interrogazione di un *database.* Ad esempio si considerino le pagine restituite da un motore di ricerca: queste vengono generate automaticamente al momento della richiesta dell'utente e non sono già preparate dal *server* in attesa che qualcuno, forse, le richieda.

tra utenti. Altra caratteristica sono le pagine principali, a volte definite bacheca, dove l'utente pubblica fotografie e messaggi che altri utenti possono leggere. Spesso gli utenti si classificano fra loro in base a diversi livelli, autorizzando di conseguenza l'accesso alla bacheca e alle informazioni più riservate. Tutti i dati pubblicati in un *social network* risiedono sui *server* del servizio, e l'utente ne conserva un controllo piuttosto limitato.

5. *Cloud computing*

Il cosiddetto *cloud computing* indica l'uso di applicazioni e servizi remoti per mezzo di *internet*. Principio fondante del *cloud computing* è che trasformano i servizi informatici in una comune utenza, così come l'energia elettrica o l'acqua potabile. La prima conseguenza è che l'utente si abbona ai servizi informatici, che diventano disponibili *online,* e paga in base all'uso che ne fa[123]. Per accedere ai servizi informatici l'utente ha bisogno di un sistema per collegarsi ad *internet* e per eseguire un semplice *client* del servizio[124]. La computazione si svolge altrove, sui *server* del fornitore del servizio, e l'apparato utilizzato dall'utente svolge il solo ruolo di interfaccia verso il servizio. Il *cloud computing* è un modello estremamente flessibile, che può essere facilmente adottato sia da un singolo utente sia da una azienda, ed è facile prevedere che avrà una ampia diffusione nei prossimi anni.

Il termine *"cloud"* - parola inglese che significa "nuvola" - deriva dalla già citata rappresentazione a forma di nuvola di *internet*. Nello specifico, il termine evidenzia che le applicazioni e i servizi sono accessibili solo tramite *internet*, dove sono in essere. In altri termini, nel *cloud computing* sono difficilmente determinabili sia le collocazioni fisiche degli apparati che forniscono come servizio, sia le loro implementazioni tecnologiche.

A seconda delle funzionalità offerte dai servizi di *cloud computing* si possono riconoscere tre differenti modelli di utenza[125]: il *software,* detto *SaaS* (acronimo dall'inglese *Software as a Service),* la piattaforma, detto *PaaS* (*Platform as a Service),* l'infrastruttura, detto *IaaS* (I*nfrastructure as a Service).* Il modello SaaS prevede che l'utente non installi il *software* sul suo sistema locale, ma che lo

[123] Una sintetica ed efficace presentazione può essere trovata in Barret S. R. T. B., *Computer Forensics Jump Start (2nd ed.),* Indianapolis, Indiana (USA), 2011, p.118.

[124] Ad esempio, all'utente può essere sufficiente uno *smartphone*, un *tablet* o un *computer* portatile non particolarmente potente.

[125] Così come sono classificate dall' Istituto Nazionale degli Standard e della Tecnologia Statunitense, NIST (*National Institute of Standards and Technologies*), nelle raccomandazioni pubblicate in Grance P.M.T. , *The NIST Definition of Cloud Computing,* Gaithersburg, MD (USA), 2011 (disponibile *Online* presso *http:llcsrc.nist.gov/publicationslnistpubsl800-145jSP800-145.pdf).*

utilizzi tramite *internet*[126]. Il modello PaaS stabilisce che l'utente definisca le caratteristiche sia *hardware* sia *software* del servizio completo che intende utilizzare[127]. Nel modello IaaS l'utente affitta le risorse di cui ha bisogno, ad esempio la capacità della rete, lo spazio di memorizzazione, e la potenza di calcolo[128].

A seconda del tipo di utenza le responsabilità gestionali, e quindi il dominio amministrativo, si spostano dall'utente al *provider*. Nel modello di utenza IaaS, l'utente affida a quest'ultimo la gestione della rete, della memoria e del server, che vengono solitamente gestiti con tecniche di virtualizzazione, mentre restano a suo carico gli altri elementi. Nel modello di utenza PaaS, il *provider* si fa carico anche della gestione delle basi di dati, delle applicazioni *web* e dello sviluppo del *software*. Il modello della utenza SaaS, demanda al *provider* anche la gestione degli applicativi, dei dati e dei servizi. Sostanzialmente, in questo modello l'utente gestisce solo il sistema che utilizza per accedere ai servizi.

I servizi di *cloud computing* possono essere forniti secondo quattro modalità, che si differenziano per il tipo di implementazione: *pubblica, privata, ibrida, condivisa.* I *cloud* pubblici sono accessibili tramite *internet*; tutte le infrastrutture, tranne quelle necessarie all'utente per accedere alla rete, sono fisicamente collocate in uno o più centri di calcolo del *provider*, che provvede alla loro gestione e agli aggiornamenti. I *cloud* privati, per contro, hanno sia le infrastrutture sia il *software* interni al dominio aziendale dell'utente e non sono accessibili dall'esterno; solitamente conservano la caratteristica dinamicità dei servizi *cloud,* ossia possono aumentare o diminuire le risorse utilizzate dall'utente in base alle sue richieste; offrono un livello di sicurezza superiore a quelle pubbliche. I *cloud* ibridi sono una combinazione delle due precedenti, e solitamente utilizzano la parte privata per questioni di sicurezza e riservatezza. I *cloud* condivisi possono assumere una qualsiasi delle configurazioni precedenti e sono

---

[126] Questi servizi di *cloud computing* offrono delle vere e proprie applicazioni, solitamente di produttività personale. Tra le più diffuse è opportuno menzionare le cosiddette *Google Apps Qittp://www.google.itlintx/it/enterprise/apps/business/)* ed il recente *Office 365* (*http:jjoffice.microsoft.com/it-TT)* che offrono, tra l'altro, applicazioni per la posta e la produttività individuale.

[127] Solitamente questi sono servizi più complessi e articolati, orientati principalmente al mondo aziendale, tra cui vale la pena menzionare *Amazon EC2* (*http://aws.amazon.com/ec2/*), IBM*SmartCloud* (*http://www-05.ibm.com/it/cloud/*) e *ArubaCloud* (*http://www.cloud.it/en/home.aspx*) (consultati giugno 2016).

[128] Alcuni servizi forniscono spazio di memorizzazione remoto, che in molti casi viene visto dall'utente come se fosse un disco rigido esterno collegato al proprio sistema. Solitamente, per accedere al proprio spazio di memorizzazione sulla *cloud* l'utente può installare un apposito programma nel sistema utilizzato, oppure ricorrere direttamente ad un *browser* per il *web*. Diversi di questi servizi offrono meccanismi automatici di *backup* e di *versioning* dei *file.* Giova evidenziare che l'accesso al proprio spazio remoto può essere effettuato da molteplici apparati, e che può anche essere condiviso con altri utenti. Tra i servizi di questo tipo vale la pena menzionare:
Dropbox (*https://www.dropbox.com*), *Apple iCloud* (*https://www.icloud.com*), *Microsoft SkyDrive* (*http://windows.microsoft.com/it-it/skydrive/download*), *Amazon Cloud Drive* (*http://www.amazon.it/gp/feature.html?ie=UTF8&docId=1000657443)*, e *Google Drive* (*http://www.google.com/intl/it/drive/about.html*).

caratterizzati dagli utenti che ad essi accedono: questi formano delle "comunità" che condividono scopi e intenti.

La caratteristica peculiare dei servizi di *cloud computing* è che i sistemi utilizzati dal *server* per fornire questi servizi sono accessibili *online,* e spesso sono implementati per mezzo di macchine virtuali complesse, che sono in esecuzione su *hardware* condivisi. In altri termini, l'aspetto fisico degli apparati informatici diventa sostanzialmente inaccessibile, rendendo praticamente inapplicabili le classiche tecniche di indagine forense. Ad esempio, si consideri quanto precedentemente illustrato in merito alla cancellazione di *files* da un disco magnetico tradizionale: questo resta memorizzato sul disco sino a quando non viene sovrascritto. Invece, la cancellazione di un *file* che risiede su un "disco" nel *cloud* comporta la scomparsa quasi istantanea della corrispondenza tra il *file fisico,* memorizzato sui dischi del *provider*, ed il *file logico,* a cui l'utente fa riferimento sul disco nel *cloud.* Giova evidenziare che anche la collocazione fisica dei centri di calcolo del *provider* potrebbe giocare un ruolo importante perché questi potrebbero essere nel territorio di altre nazioni. Ad ulteriore dimostrazione che il *cloud computing* offre aspetti innovativi, vale la pena menzionare una funzionalità fornita automaticamente da *Dropbox*: qualsiasi *file* cancellato dal disco *cloud* resta disponibile trenta giorni per un suo eventuale ripristino.

6. Il trattamento delle prove

Le buone pratiche per il trattamento delle prove digitali si possono sintetizzare con l'acronimo *PICI,* che deriva dalle parole inglesi *Preservation* (*conservazione), Isolation* (*isolamento), Correlation (relazione*) e *Logging (registrazione cronologica).* La conservazione ha lo scopo di evitare alterazioni dei dati acquisiti e prevede di farne opportuni duplicati di lavoro. L'isolamento fa riferimento agli strumenti di analisi, che è raccomandabile siano isolati sia dai dati analizzati, per evitare di esserne contaminati[129], sia dal mondo esterno, per evitare comunicazioni impreviste e incontrollate da parte del sistema in analisi. L'isolamento può essere complesso da realizzare qualora si analizzino sistemi informatici durante il loro funzionamento. È auspicabile mettere in relazione i dati raccolti con fonti esterne e indipendenti, in modo da poterli validare e ridurre il rischio di falsificazioni.

[129] Ad esempio, il sistema analizzato potrebbe contenere dei *malware*, come *virus* o altro, che potrebbe infettare gli strumenti utilizzati per l'analisi, compromettendone il corretto funzionamento.

È anche necessario eseguire una completa registrazione cronologica sia delle azioni compiute sulle prove sia dei relativi attori. In questo modo si possono documentare compiutamente sia le operazioni non ripetibili sia quelle replicabili, cosicché queste ultime possano essere eventualmente rieseguite. Una prova ha un valore differente a seconda del dominio entro cui ricade. Se è esterno a quello dell'utente, allora ha tanto più valore quanto più è affidabile il responsabile del dominio. Se una prova è nel dominio dell'utente, allora il suo valore probatorio dipende da quanto si può accertare rispetto alle modifiche che l'utente potrebbe avere compiuto: non è detto che l'utente abbia modificato una prova, anche se aveva la possibilità di farlo. Ad esempio, si pensi al sequestro di un *computer*: non è detto che siccome i *files* erano nel dominio dell'utente allora abbiano una bassa valenza probatoria, anzi il motivo del sequestro è proprio quello di acquisire prove prima che queste possano essere modificate o cancellate.

a. Acquisizione e conservazione delle prove digitali

Una investigazione di carattere digitale può essere scomposta in tre fasi: *acquisizione, ricerca* e *ricostruzione*. L'acquisizione prevede l'identificazione di tutte le possibili fonti di prove digitali e la loro conservazione**;** la ricerca ha lo scopo di identificare le prove digitali; la ricostruzione quello di supportare o confutare le ipotesi investigative. Le ultime due fasi sono anche dette "analisi delle prove".

L'investigazione può essere svolta in due modalità: *dead* oppure *live*. La prima prevede di interagire con sistemi non in funzione, tramite strumenti consolidati, in un ambiente affidabile e circoscritto; la seconda prevede di interagire con sistemi mentre sono in funzione, approfittando anche della loro operatività per trovare le prove.

Le prove digitali devono essere identificate in quanto tali per poter essere acquisite. Non è sempre facile stabilire dove potrebbero risiedere: l'informatica permea la quotidianità delle persone, sia direttamente sia indirettamente, e alcune tracce informatiche delle nostre azioni potrebbero essere anche in dispositivi inusuali. Ad esempio, si considerino le indicazioni di posizionamento *GPS* e di ora e data che molte fotocamere inseriscono nelle fotografie scattate, oppure anche alcune stampanti dotate di disco rigido che conservano un *log* dettagliato delle stampe effettuate.

In base al tempo di persistenza dei dati nelle memorie e alla natura di queste ultime, ci sono tre possibili modalità di acquisizione delle prove informatiche: sequestro, copia e intercettazione.

Nel caso di dispositivi spenti, dotati di memorie permanenti, il sequestro *dell'hardware* è il primo passo per l'acquisizione delle prove; in questo caso tutti i dati contenuti nel dispositivo vengono acquisiti assieme all'*hardware*.

In altri casi il sequestro fisico potrebbe essere inadeguato o impossibile, ad esempio quando occorra acquisire dati contenuti in memorie volatili o in memorie stabili di apparati che devono restare in funzione. In queste ipotesi per acquisire le prove è possibile utilizzare la duplicazione dei dati su una memoria permanente esterna. La tecnica di duplicazione dei dati viene utilizzata anche successivamente ad un sequestro per preservare l'originale, ossia per evitarne possibili corruzioni a seguito di analisi successive.

Il sequestro di apparecchiature elettroniche richiede specifiche metodologie per conservare al meglio le prove digitali[130]. Uno degli aspetti più delicati è costituito dalla gestione di *computer*, o apparati in genere, che siano accesi e funzionanti. Ci sono almeno due possibili metodologhe: la prima prevede di staccare direttamente l'alimentazione elettrica senza interagire con l'apparecchiatura**;** la seconda contempla alcune interazioni con il sistema, che devono essere ampliamente descritte e documentate, che hanno lo scopo di salvaguardare il contenuto volatile della *RAM*. Quest'ultima metodologia è particolarmente critica, perché comporta la palese alterazione del sistema in esame, quindi occorre valutare con estrema attenzione se sia il caso di correre il rischio di apportare modifiche sostanziali per recuperare i dati nelle memorie volatili.

Quando i dati siano in transito, ad esempio sul cavo di una rete o tra le antenne di una rete senza fili, non ci sono oggetti fisici cui fare riferimento **:** per acquisirli è necessario intercettarli, ovvero copiarli mano a mano che questi transitano, senza interferire nella trasmissione. Anche in questo caso si può pensare di fare una duplicazione dei dati intercettati per evitare possibili inquinamenti successivi.

b. Duplicazione

Da quanto appena illustrato emerge che il ruolo della duplicazione dei dati appare centrale sia nell'acquisizione sia nella successiva analisi delle prove informatiche.

La duplicazione sfrutta una caratteristica del mondo digitale, già citata in precedenza, in cui la copia di un dato digitale è indistinguibile dal suo originale. Nel caso delle memorie permanenti, l'originale è costituito dall'intero contenuto della memoria, compresi spazi "vuoti"

130 United States Secret Service, *Best Practices for Seizing Electronic Evidences A pocket Guide for First Responders,* vol. 3, disponibile *online* all'indirizzo: *https://www.ncjrs.gov/App/Publications/abstract.*

e *files* cancellati. Esistono diverse tecnologie, dette di *bitstream copy,* che permettono di duplicare il contenuto di un disco *bit* per *bit*. Il processo di duplicazione solitamente prevede di "smontare" fisicamente la memoria dal dispositivo originale per collegarla ad appositi apparati di duplicazione. Nel duplicare il contenuto di una memoria permanente occorre adottare delle misure, dette di *write blocking,* per evitare che il processo di copia possa alterare l'originale andando a memorizzarci dei dati. Particolarmente complessa risulta la copia di molteplici dischi rigidi quando questi siano connessi fra loro e configurati per essere visti dal sistema operativo come un unico disco logico: questa tecnologia è detta *raid disk*. Lo scopo di un disco *raid* è di usare diversi dischi connessi tra loro per ottenere una o più tra le seguenti evenienze: tolleranza ai guasti, miglioramento delle prestazioni e scalabilità. L'aspetto critico è che un disco *raid* può essere realizzato a diversi livelli, sia di astrazione sia di complessità; quindi ne esistono numerose implementazioni che sono sostanzialmente incompatibili fra loro. La duplicazione di un *raid disk* deve dunque essere strutturata opportunamente per rispecchiare sia il contenuto completo di ognuno dei singoli dischi che lo compongono sia il loro insieme logico.

Come già accennato in precedenza, data l'estrema "fragilità" delle prove informatiche, un ruolo fondamentale nella loro raccolta è la documentazione completa delle operazioni svolte[131]. Partendo dalle modalità della prima acquisizione, la documentazione riporterà la descrizione e i riferimenti temporali di ognuna delle operazioni compiuta sulle prove[132].

c. Autenticità

Si dice che una prova acquisita è autentica quando corrisponde a quella originale. Purtroppo, per le prove digitali potrebbe essere impossibile confrontare la copia acquisita rispetto ai dati originali. Si pensi ad esempio ai dati contenuti in una memoria volatile, che sono spesso in rapido cambiamento nel corso del normale funzionamento di un *computer*. La copia di questi dati corrisponde ad una sorta di "fotografia" della memoria in quel preciso momento, ma quei dati possono cambiare molto velocemente, e quindi viene meno il concetto di dati "originali" rispetto ai quali confrontare la copia. Questo fenomeno è ancora più marcato nel caso del traffico su una qualsiasi rete di comunicazione, a maggior ragione su *internet*, che è esclusivamente dinamico e deve essere "catturato" mentre i dati sono in transito.

In generale, si può affermare che i dati "catturati" sono autentici se non sono stati successivamente modificati.

---

131 L'importanza della documentazione è ampiamente sottolineata, tra gli atri, in Bejtlich R., *Real Digital Forensics. Computer Security and Incident Response*, Upper Saddle River, New Jersey (USA), 2006, pp. 166 - 169.

132 Si v., Bejtlich R., *Real Digital Forensics. Computer Security and Incident Response*, cit., p. 178.

Uno strumento ulteriore per garantire l'autenticità delle prove acquisite è la cosiddetta "catena di custodia delle prove informatiche", ossia la documentazione della sequenza cronologica di tutte le azioni operate su di esse e dei loro autori.

d. Integrità

L'integrità di una prova informatica è costituita dal fatto che questa non ha subito modifiche rispetto a quanto originariamente acquisito, e quindi si basa sulla autenticità della prova. Per verificare l'integrità di un duplicato occorrerebbe fare una confronto *bit* per *bit* con l'originale. È una tecnica comunemente accettata quella di confrontare le impronte dei *files*, dette anche *hash*: se le impronte dei dati originali e del loro duplicato coincidono allora i dati sono identici. In questi casi è sufficiente disporre dell'*hash* dell'originale.

I programmi per elaborare le impronte si basano su calcoli matematici e prendono in *input* un *file* per produrre una sequenza di caratteri con lunghezza prefissata, detta impronta o *hash* del *file*. Ripetendo più volte l'operazione di *hash* sullo stesso *file* si ottiene sempre lo stesso risultato, ma data l'impronta non è possibile risalire al *file* originale. Due *file* che differiscono anche solo di un carattere hanno impronta molto diversa fra loro. È altamente improbabile, anche se teoricamente possibile, che due *files* diversi abbiano la stessa impronta: qualora si verificasse questa eventualità si parlerebbe di collisione delle impronte. Attualmente i metodi più comunemente usati per il calcolo dell'impronta di un *file* sono *MD5 e SHA-1,* che sono diversi fra loro.

Per verificare l'integrità delle prove una delle prime azioni compiute su di esse è il calcolo delle loro impronte, che poi vengono conservate autonomamente. Per verificare l'integrità delle prove sarà quindi necessario calcolarne nuovamente l'impronta e confrontarla con quella calcolata originariamente. Solo se il *file* originale non ha subito modifiche le due impronte coincideranno. Analogamente, si calcola l'impronta anche dei duplicati: solo se questa coincide con quella dei dati originali il duplicato è identico a questi.

Giova evidenziare come l'affidabilità della metodologia di verifica dell'integrità basata sulle impronte si fondi, a sua volta, sulla corretta custodia delle stesse. Potrebbe accadere, infatti, che dopo una alterazione dei dati originali ne venga calcolata nuovamente l'impronta per sostituirla a quella originale. Ovviamente questa nuova impronta confermerebbe l'integrità dei dati alterati, ma solo perché alterata a sua volta.

7. Il tempo

La quasi totalità degli apparati digitali è equipaggiata con un orologio che segna la data e l'ora. Queste informazioni sono solitamente utilizzate dal sistema operativo per "marcare" sia i *files*, per indicarne data e ora di creazione e di modifica più recente, sia gli eventi registrati nei *files di log,* per indicare quando sono accaduti. La gestione dell'orologio di sistema è solitamente automatizzata, in alcuni casi l'apparato può sincronizzarsi con specifici "*server* di tempo", che forniscono l'ora di riferimento. La sincronizzazione può essere periodica ed effettuata anche con molta frequenza. L'orologio di sistema è solitamente alimentato da una piccola batteria, detta tampone*,* che gli permette di continuare a segnare l'orario anche quando il *computer* è spento[133].

A dispetto di quanto appena illustrato, il tempo di sistema potrebbe essere del tutto inaffidabile. In alcuni casi anche l'utente generico può modificare esplicitamente l'ora e la data, mentre il *superuser* può farlo in ogni caso. Per impostare l'ora e la data tramite *server* di tempo occorre stabilire il fuso orario in cui si trova l'apparato ed un *server* di riferimento. Modificando uno di questi parametri si cambia l'orario di sistema. Negli apparati di mobilità, quali ad esempio i navigatori *GPS*, i telefoni cellulari e i *tablet computers*, solitamente un automatismo interno rileva la posizione geografica e stabilisce il fuso orario corrente. Il meccanismo di sincronizzazione dell'orario può essere disattivato, in modo tale che data e ora possono essere stabiliti direttamente dall'utente: questa operazione solitamente è preclusa all'utente generico ed è possibile solo per il *superuser*.

I sistemi operativi associano ad ogni *file* e cartella[134] dei riferimenti temporali composti da data e ora[135]; i riferimenti temporali più comuni si riferiscono alla generazione del *file*, all'ultima modifica del contenuto, all'ultimo accesso, all'ultima modifica degli attributi. Quali di questi sono implementati dipende dal sistema operativo usato[136].

---

[133] Solitamente, una prima sincronizzazione può essere effettuata all'accensione del sistema, mentre le successive possono avere una frequenza giornaliera, ma che in alcuni casi può arrivare ad essere oraria, o addirittura minore. In molti altri i telefoni cellulari possono ricevere il segnale orario direttamente dalla compagnia telefonica anche assieme ad ogni chiamata ricevuta.

[134] Nei sistemi operativi di alcuni dispositivi mobili, quali *smartphone* e *tablet,* la metafora della cartella è stata abbandonata, e l'utente non accede più direttamente ai *file*s su disco, ma può farlo solo attraverso le applicazioni che li hanno generati.

[135] Il formato non è definito a priori, ma l'orario è solitamente approssimato al minuto, anche se il più delle volte l'orologio di sistema può arrivare a discriminare discernere, contare, calcolare i centesimi o i millesimi di secondo.

[136] I sistemi operativi derivati da Unix solitamente utilizzano i riferimenti temporali di ultimo accesso e di ultima modifica sia del contenuto sia degli attributi; a questi Linux aggiunge anche il riferimento di cancellazione. I sistemi operativi Microsoft utilizzano i riferimenti di: creazione, modifica degli attributi, ultimo accesso, ultima scrittura.

Si noti che molti di essi indicano l'ultima volta che una certa azione è stata compiuta sul *file* o sulla cartella, e questo dato sostituisce il precedente: Ne consegue che dai riferimenti temporali non è possibile ricostruire casi potrebbe anche essere possibile confrontare a posteriori l'orario interno al dispositivo con quello di una sorgente terza e affidabile. Ad esempio, il programma per la posta elettronica potrebbe marcare con l'ora locale ogni messaggio di posta inviato, e questa potrebbe essere confrontata con la marcatura temporale che il *server* di posta appone alla stessa *mail* prima di instradarla. Il confronto fra i due orologi sarebbe quindi relativo al momento dell'invio della messaggio di posta elettronica, ma da la cronistoria di un *file* o di una cartella[137].

In alcuni questo confronto nulla si potrebbe dedurre sul tempo locale prima e dopo tale evento. I riferimenti temporali presentano diverse criticità probatorie. Ad esempio, il riferimento temporale dell'ultimo accesso viene aggiornato anche a seguito della sola lettura di un *file*. Considerando che l'interfaccia grafica del sistema operativo deve leggere i *files* di una cartella per visualizzarne l'icona, anche la semplice apertura di una cartella può modificare i riferimenti temporali dell'ultimo accesso ai *files* in essa contenuti. Vale la pena rilevare che diverse operazioni automatiche, quali la scansione con un *antivirus* ed il *backup*, modificano il riferimento dell'ultimo accesso ai *files*. Potrebbe anche accadere che la data di generazione risulti più recente di quella dell'ultima modifica dello stesso *file*. Questa evenienza, ad esempio, si può presentare quando un *file* viene prima generato su un *computer* e successivamente copiato in un altro. Nel secondo *computer* la data di generazione è quella della copia, mentre quella dell'ultima modifica potrebbe rimanere la data originale. Un'altra criticità è che non tengono conto dell'utente che ha effettuato l'azione a cui fanno riferimento. Inoltre, possono essere modificati anche tramite appositi comandi messi a disposizione dai sistemi operativi. In conclusione, i riferimenti temporali sono tracce informatiche molto complesse da valutare.

[137] In realtà i *file system* cosiddetti *journaled*, ad esempio quello in uso da Mac OsX, tengono traccia anche della cronistoria "recente" di un *file* o di una cartella.

CAPITOLO QUARTO

Il contrasto internazionale alla criminalità informatica: verso una politica di *cyber security*[138]

Pare opportuno, giunti a questo punto della trattazione, tracciare una panoramica europea sulle crescenti sfide che si originano nel dominio cibernetico il quale, pur generando molte opportunità di sviluppo, è causa di vulnerabilità alla sicurezza e all'economia degli Stati nazionali. Il contesto europeo resta fondamentale per la piena comprensione degli sviluppi italiani in materia, dal momento che le dinamiche nazionali degli Stati membri sono in molti casi guidate dalle politiche comunitarie.

La *cyber security* in Europa rappresenta allo stato attuale un vero *work in progress*. L'approccio europeo alla sicurezza cibernetica è avanzato in questi anni a passi relativamente lenti, soprattutto se paragonati a quelli di Paesi come Stati Uniti o Regno Unito. Ciò è in gran parte dovuto all'assetto stesso dell'Unione che, ovviamente, deve mettere d'accordo molti e più diversi punti di vista nazionali. L'Unione Europea ha, quindi, registrato un ritardo nella formulazione di una propria strategia. Nel 2013 ne è stata approvata una apprezzabile nella prospettiva di un'auspicabile evoluzione delle capacità dell'Unione Europea di affrontare adeguatamente la questione della *cybersecurity*. La tematica necessita infatti di un'adeguata trattazione non solo a livello nazionale ma anche e soprattutto a livello UE, considerato che la *cybersecurity* è per definizione una questione che travalica i confini nazionali e necessita di una gestione multinazionale.

1. Le innovazioni in materia di cooperazione contro i reati informatici transnazionali

L'Unione Europea ha iniziato ad occuparsi di *cybersecurity* agli inizi del 2000. I primi documenti hanno cercato di individuare le aree di priorità in ambito di sicurezza delle reti e appaiono significativi proprio per l'idea che forniscono dell'impostazione e delle priorità originarie dell'Unione.

Merita mettere in evidenza che il termine specifico "*cybersecurity*" non compare all'interno di questi primi documenti e non comparirà fino all'elaborazione della relazione del 2008

[138] Cencetti C., *Cybersecurity: Unione europea e Italia: Prospettive a confronto*, Edizioni nuova cultura, Roma, 2014.

sull'implementazione della strategia europea in materia di sicurezza del 2003. Fino a quel momento, infatti, si parla di *cybercrime* e di protezione dei dati personali e delle infrastrutture critiche, senza esplicito riferimento al concetto più comprensivo di *cybersecurity*.

Nel 2000 la Commissione ha elaborato una comunicazione sul *cybercrime*[139] che tratta due questioni fondamentali della *cybersecurity*: la sicurezza delle infrastrutture dell'informazione e la lotta al crimine informatico. Questi macro-aspetti della *cybersecurity* costituiscono il nocciolo duro della visione europea, che dal 2000 mantiene queste due priorità in cima alla *to do list* per la sicurezza cibernetica.

Nel 2001 la Commissione ha presentato un documento[140] interamente dedicato alla definizione della NIS (*Network and Information Security*), che si propone la realizzazione di una politica europea in materia. Il testo - approvato nel mese di giugno, ovvero prima dell'attentato alle torri gemelle - testimonia la volontà autonoma dell'Unione di seguire un proprio percorso in questo campo. All'interno del documento si trova una definizione della NIS, che viene intesa come «*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*»[141].

Di seguito alla definizione, il documento presenta un quadro generale delle minacce alla sicurezza che possono impattare sulla NIS. Queste sono classificate in base alla loro natura e non anche all'ordine di importanza e sono costituite da:

1) intercettazioni delle comunicazioni;
2) accesso non autorizzato a computer e reti informatiche;
3) caduta della rete;
4) esecuzione di *software* "maligni" che modificano o distruggono i dati;
5) usurpazione di identità;
6) incidenti ambientali ed eventi imprevisti.

Mentre risulta abbastanza chiaro comprendere i primi due punti, è forse necessario spiegare cosa si intende con gli altri.

---

[139] Commissione europea, *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica.* eEurope 2002 (COM(2000)890), 26 gennaio 2001.

[140] Commissione europea, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo* (COM(2001)298), 6 giugno 2001.

[141] Commissione europea, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo* (COM(2001)298), 6 giugno 2001, par.2.1.

Il terzo punto si riferisce ai cosiddetti "*disruptive attack*", i quali comportano l'interruzione delle funzioni di un'infrastruttura, che può essere anche un'infrastruttura critica[142]. Tale interruzione colpisce i fruitori del servizio e, nel caso di una infrastruttura critica, può interessare il sistema Paese nel suo complesso, con possibilità di gravi danni economici.

Il quarto punto è rappresentato dall'esecuzione di *software* maligni in grado di infettare i computer per provocare anche la modifica o la distruzione di dati. Questa è una realtà nota alla maggioranza degli utenti di internet. Il costo associato a questi attacchi risulta tutt'altro che trascurabile. Ne può conseguire l'usurpazione di identità, che non solo arreca danni all'immagine dei diretti interessati, ma può mascherare come affidabili siti, blog e quant'altro in realtà contiene appunto *software* maligni in grado di introdurre *virus* nelle pagine personali degli utenti che vi accedono.

Infine, la categoria degli "incidenti ambientali ed eventi imprevisti" comprende tutti quei casi che sfuggono alla volontà umana. Spesso, questi derivano da eventi naturali, quali catastrofi o incidenti, ma possono anche presentarsi come diretta conseguenza dell'errore umano. L'inevitabile correlazione tra reti cibernetiche e reti fisiche comporta tale tipo di problematiche, molto difficili da contrastare. Come ha sostenuto David Omand, segretario permanente dell'Home Office del Regno Unito, *«l'interruzione di un servizio è più probabile sia dovuta ad un incidente ambientale piuttosto che ad un attacco deliberato, pertanto la distinzione tra minacce maligne ed eventi accidentali si rivela meno importante che la definizione dei tempi massimi previsti per il recupero del servizio»*[143].

Nei primi anni 2000 altri due documenti hanno segnato l'inizio di un interesse europeo per le dinamiche scaturite dal processo di digitalizzazione: il documento del 2000 eEurope[144] e quello del 2002 eEurope 2005[145].

Tali atti si inseriscono all'interno della visione rappresentata dalla strategia di Lisbona del 2000, intesa a fare dell'Europa, entro il 2010, l'economia basata sulla conoscenza *«più competitiva e più dinamica del mondo»*[146]; essi esprimono inoltre la necessità per il Vecchio continente di

---

[142] Lo sviluppo, la sicurezza e la qualità della vita nei paesi industrializzati dipendono sempre più dal funzionamento, continuo e coordinato, di un insieme di infrastrutture che, per la loro importanza, sono definite infrastrutture critiche. Con questo termine si intende un sistema, una risorsa, un processo, un insieme, la cui distruzione, interruzione o anche parziale o momentanea indisponibilità ha l'effetto di indebolire in maniera significativa l'efficienza e il funzionamento normale di un Paese, ma anche la sicurezza e il sistema economico-finanziario e sociale, compresi gli apparati della pubblica amministrazione centrale e locale.

[143] Omand D., *The steps needed to protect the EU's critical infrastructure against cyber-attack*, in *Europe's World*, *No. 25*, 2013, in *http://europesworld.org/?p=176.p.*, pp. 112-118.

[144] Commissione europea, eEurope *Una società dell'informazione per tutti* (COM(2000)130), 8 marzo 2000.

[145] Commissione europea, eEurope 2005: *una società dell'informazione per tutti* (COM(2002)263), 28 maggio 2002.

[146] Commissione europea, eEurope 2005: *una società dell'informazione per tutti* (COM(2002)263),cit.

dotarsi di moderni servizi pubblici offerti sulla rete e di un'affidabile infrastruttura di protezione dell'informazione.

Nel 2002 sono state approvate tre importanti direttive in materia di NIS: la direttiva 2002/21/CE, che ha istituito un quadro normativo comune per le reti ed i servizi di comunicazione elettronica; la direttiva 2002/19/CE, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate e all'interconnessione delle medesime; e la direttiva 2002/20/CE, in tema di autorizzazioni per le reti ed i servizi di comunicazione elettronica.

Nel 2003 l'Unione Europea ha elaborato una propria strategia in materia di sicurezza. In questa non si fa menzione del termine "*cybersecurity*", ma si individua una *«dipendenza europea da un'infrastruttura interconnessa nel settore dei trasporti, dell'energia, dell'informazione ed altri, e la conseguente vulnerabilità dell'Europa sotto questo profilo»*[147].

La appena menzionata strategia europea per la sicurezza è ancora in vigore, non essendo mai stata modificata né aggiornata. Dopo una relazione sulla sua implementazione nel 2008[148], il progetto di una nuova strategia non è mai giunto a termine, lasciando in vigore il testo del 2003. Una revisione del documento sarebbe auspicabile, in considerazione del fatto che le minacce alla sicurezza sono in continua evoluzione, proprio come dimostra l'emergere della questione *cyber* negli ultimi dieci anni: il peso crescente che questo tema sta acquisendo a livello globale meriterebbe di essere citato all'interno di ogni strategia di sicurezza, anche dell'Unione europea. Il termine "*cybersecurity*" compare per la prima volta proprio nel testo in lingua inglese[149] della suddetta relazione del 2008 , ma resta ancora fuori da quello della strategia di sicurezza ufficialmente in vigore.

2. La strategia dell'Unione Europea per la *Cyber* sicurezza

Nel 2013 si è arrivati all'approvazione della Strategia dell'Unione europea per la *cyber* sicurezza (7 febbraio 2013). Il documento è frutto del lavoro congiunto della Commissione e dell'Alto Rappresentante per gli affari esteri e la politica di sicurezza e illustra la visione dell'UE

147 Consiglio dell'Unione europea, *Un'Europea sicura in un mondo migliore. Strategia europea in materia di sicurezza,* 12 dicembre 2003, p. 2.

148 Consiglio dell'Unione europea, *Relazione sull'attuazione della strategia europea in materia di sicurezza. Garantire sicurezza in un mondo in piena evoluzione* (S407/08), 11 dicembre 2008.

149 La versione in italiano riporta la traduzione "sicurezza informatica".

sul tema della *cyber* security e le azioni necessarie da intraprendere, per garantire la sicurezza di tutti i cittadini e degli stati. Solito errore: troppe ripetizioni. Evitarle, usare dei sinonimi, delle perifrasi.

Nella sua parte iniziale, la strategia cerca di mettere in evidenza il peso del cosiddetto fattore ICT[150] nell'era moderna, il quale costituisce ormai un aspetto fondamentale della vita sociale e della crescita economica dei paesi europei, nonché una risorsa critica sulla quale poggia gran parte del settore industriale. La dipendenza di quest'ultimo e di molte delle infrastrutture critiche nazionali dai sistemi digitalizzati e da internet in generale cresce sempre più; e di conseguenza aumentano anche i rischi. Pertanto, viene dichiarato per l'Europa l'obiettivo di dotarsi degli strumenti necessari per poter prevenire ed eventualmente reagire a possibili attacchi di natura cibernetica, in grado di recare notevoli danni e di attentare alla sicurezza dei Paesi.

Scopo principale della strategia, è quello di garantire uno spazio cibernetico "aperto e sicuro", che sia accessibile a tutti e, allo stesso tempo, dotato degli strumenti adeguati per assicurare la riservatezza dei dati e delle informazioni in esso contenuti. Compito dell'Unione è promuovere l'applicazione di principi, norme e valori che sono già validi nella dimensione fisica, anche in quella digitale. Diritti fondamentali, democrazia e stato di diritto dovrebbero essere tutelati anche nel *cyber* spazio. Questi principi sono elencati all'interno della strategia:

1) protezione dei diritti fondamentali, della libertà di espressione, dei dati personali e della *privacy*;
2) accesso alla rete garantito per tutti;
3) *multi-stakeholder governance* democratica ed efficiente;
4) responsabilità condivisa tra tutti gli attori coinvolti.

Il rispetto di questi "*core values*" appare indispensabile per la messa in atto delle azioni necessarie a raggiungere gli obiettivi che la strategia si prefigge. In particolare, il documento delinea tre priorità fondamentali per poter fronteggiare le minacce provenienti dal *cyber* spazio:

1) ridurre drasticamente il *cibercrimine*;
2) sviluppare una politica e capacità di ciberdifesa connesse alla Politica di sicurezza e di difesa comune (PSDC);

[150] L'ICT, acronimo di *Information Communication Technology*, è la scienza che studia in modo integrato i sistemi di elaborazione, trasformazione e trasmissione dell'informazione. Quindi comprende l'insieme delle nuove tecnologie che consente di trattare e scambiare le informazioni. L'ICT è costituita da diverse aree, quali informatica, elettronica e telecomunicazioni ed è alla base dell'evoluzione tecnologica odierna: nell'economia, nella produzione industriale e nella vita di tutti i giorni. È paragonabile ad una vera e propria rivoluzione: la Rivoluzione ICT. L'impatto che questa sta avendo è pari a quello della rivoluzione industriale, trasformando radicalmente il modo in cui lavoriamo, viaggiamo, comunichiamo e viviamo.

3) creare una politica internazionale coerente dell'Unione europea sul ciberspazio e promuovere i valori costitutivi dell'UE.

La prima priorità consiste nella lotta massiva al *cybercrime*, il quale rappresenta oggi la causa maggiore di perdite di tipo economico, soprattutto a danno del settore privato. Ridurre il *cybercrime* è probabilmente l'obiettivo più urgente in questo ambito, poiché è necessario per garantire la protezione dei cittadini, dal punto di vista economico e non solo. Frodi telematiche, violazione dei dati personali, furto della proprietà intellettuale e dell'identità digitale, spionaggio industriale: questi fenomeni sono all'ordine del giorno e causano danni economici estremamente rilevanti e probabilmente sotto-stimati. Nel 2012 il quaranta per cento della popolazione europea si è dichiarato preoccupato per una possibile manipolazione dei propri dati personali e il trentotto per cento per la sicurezza dei pagamenti *online*[151].

La seconda priorità apre all'ambizione di creare una politica di *cyberdefence*,

che sia inquadrata all'interno della PSDC; la terza proietta invece la questione

della *cybersecurity* sul piano internazionale, a testimonianza del fatto che solo una proficua collaborazione a livello globale può portare a risultati importanti, nella sfida contro le minacce asimmetriche provenienti dal *cyber* spazio.

a. La lotta al cybercrime

Il crimine informatico rappresenta la piaga peggiore per la sicurezza delle reti e delle informazioni, in termini di portata e di danni economici. Secondo uno studio commissionato da McAfee nel 2013, costa all'economia mondiale dai trecento miliardi a un miliardo di miliardi di dollari all'anno[152]. Ciò che merita veramente attenzione, però, è l'analisi degli effetti di questi numeri sul commercio, la tecnologia e il benessere globale.

Un sondaggio di Eurobarometro, ad esempio, evidenzia come circa il trentotto per cento degli utenti di internet, temendo di poter essere coinvolto in problematiche inerenti pagamenti *online*, abbia modificato il proprio comportamento: il diciotto per cento ha diminuito i propri acquisti *online*, mentre il quindici per cento ha ridotto le proprie transazioni di *home banking*[153].

Il *cybercrime* ha acquisito negli ultimi anni un peso significativo ed una notorietà sempre più diffusa all'interno della società civile: secondo lo stesso sondaggio di Eurobarometro, il 73%

---

[151] European Commission, *Special Eurobarometer 390: Cyber Security Report,* in *http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf,* luglio 2012, p. 25.

[152] Lewis J., Baker S. *, The Economic Impact of Cybercrime and Cyber Espionage, Santa Clara*, in *http://csis.org/node/45446 McAfee*, luglio 2013, p. 5.

[153] European Commission, *Special Eurobarometer 390: Cyber Security Report*, cit., p. 28.

circa della popolazione dell'UE ha visto o sentito qualcosa riguardo il *cybercrime* negli ultimi dodici mesi e circa il 59% ne ha avuto notizia dalla televisione[154]. Questi dati costituiscono una media delle percentuali dei vari Paesi membri, i quali presentano situazioni alquanto differenziate tra loro. In Italia, per esempio, si registra un tasso relativamente basso di informazione al riguardo: solo il 51% della popolazione nazionale ha sentito parlare di *cybercrime* dai mezzi di comunicazione o in sedi più informali, a fronte di un 40% che ne è totalmente all'oscuro. Infine, il 59% della popolazione europea si sente non adeguatamente o affatto informato sui rischi associati al *cybercrime*, mentre solo il 7% se ne dichiara ben consapevole[155]. Anche in questo caso, le percentuali variano a seconda dei contesti nazionali: paesi come Danimarca, Svezia e Finlandia registrano tassi di consapevolezza elevati, fino al 73%; mentre altri, come l'Italia, superano di poco il 20%.

Le differenziazioni sopra riportate dipendono in maniera significativa anche dalla diversa diffusione del crimine informatico nei vari contesti nazionali. La lotta al *cybercrime* necessita di adeguati strumenti e, in particolare, di legislazioni forti ed efficaci, di meccanismi di *law enforcement* e di buone capacità tecnico-operative. In tutto questo, l'UE può coordinare l'attività dei singoli Stati, facilitando un approccio collaborativo che metta insieme le autorità giudiziarie e gli *stakeholder*, ai vari livelli dell'Unione.

b. Cyberdefence policy

Per fronteggiare le minacce provenienti dal *cyber* spazio, l'Unione dovrebbe dar vita ad una politica di sicurezza cibernetica, inserita nell'ambito della Politica di sicurezza e difesa comune. Secondo quanto si legge nella strategia, lo sviluppo della *cyberdefence* dovrebbe concentrarsi sulle attività di *«individuazione, risposta e recupero nei confronti di* cyber *minacce sofisticate»* per *«aumentare la resilienza dei sistemi informativi e di comunicazione che supportano gli interessi della difesa e della sicurezza nazionale degli Stati membri»*[156]

La *cyberdefence*, quindi, si presenta rilevante al fine di tutelare la difesa e gli interessi di sicurezza nazionale degli Stati membri. Per garantire un'adeguata *cyberdefence*, è necessario coinvolgere tutti gli aspetti del processo di *capability development*: «la dottrina, la leadership, l'organizzazione, il personale, la formazione, la tecnologia, l'infrastruttura, la logistica e l'interoperabilità»[157].

---

154 European Commission, *Special Eurobarometer 390: Cyber Security Report*, cit., pp. 34-35.
155 European Commission, *Special Eurobarometer 390: Cyber Security Report*, cit., p. 37.
156 Commissione europea, *Strategia dell'Unione europea per la cibersicurezza*, cit., p. 12.
157 Commissione europea, *Strategia dell'Unione europea per la cibersicurezza*, cit., p. 13

Questo processo è affidato all'Alto Rappresentante per gli affari esteri e la politica di sicurezza, agli Stati membri e all'Agenzia europea di difesa (EDA), in collaborazione con l'ENISA e l'Europol.

Per incrementare le capacità di difesa europee in ambito cibernetico è opportuno predisporre di adeguati fondi e, per questo motivo, si rivelano cruciali i progetti di finanziamento in Europa, in particolare nell'ambito di "Horizon 2020", programma quadro di ricerca e innovazione che dispone di circa ottanta miliardi di euro per il periodo 2014-2020.

Per quanto riguarda i finanziamenti alla *cybersecurity*, si deve fare riferimento ad almeno due aree distinte di tale programma: "*Secure societies. Protecting freedom and security of Europe and its citizens*" e "*ICT Research* & *Innovation*". Nella prima area vengono individuate le attività principali che l'Unione europea si impegna ad intraprendere per garantire la pace e la sicurezza dei suoi paesi membri. Tra queste attività compare anche l'avanzamento della *cybersecurity*. In questa sezione è presente il programma "*Digital Security: Cybersecurity, Privacy and Trust*", con a disposizione 47.040.000 euro per il 2014.

La seconda area riguarda lo sviluppo del settore ICT, che da solo rappresenta il 4,8% dell'economia europea[158]. La relativa sezione "*Leadership in enabling and industrial technologies*" contiene il programma "ICT 2014. *Information and Communications Technology*", con 125 milioni di euro per il 2014.

Nei giorni 19 e 20 dicembre 2013 il Consiglio europeo si è riunito per discutere, tra l'altro, della Politica di sicurezza e di difesa comune. Nelle conclusioni si è affermata l'importanza di favorire lo sviluppo della Politica di Sicurezza e di Difesa Comune (PSDC), così superando la frammentazione dei mercati europei della difesa, che incide negativamente sulla sostenibilità e competitività dell'industria europea della sicurezza e difesa. Il rafforzamento della PSDC richiede l'azione decisa di tutti i Paesi membri dell'Unione, in collaborazione coni suoi *partners* chiave: le Nazioni Unite e la NATO. Tale rafforzamento deve avvenire «in piena complementarità con la NATO nel quadro concertato del partenariato strategico fra l'UE e la NATO e nel rispetto dell'autonomia e delle procedure decisionali di ciascuno»[159].

Inoltre, per incrementare la sicurezza interna ed esterna all'Unione, il Consiglio ha chiesto l'elaborazione di un "Quadro strategico UE in materia di *cyber* difesa" per il 2014, coerentemente con gli sforzi della NATO, su proposta dell'Alto Rappresentante per gli affari esteri e la politica di sicurezza ed in collaborazione con la Commissione e l'EDA.

---

158 Reperibile in *http://ec.europa.eu/programmes/horizon2020/en/area/ict-research-innovation.*

159 Consiglio europeo, *Conclusioni del Consiglio europeo 19 e 20 dicembre 2013 - Politica di sicurezza e di difesa comune*, 19 dicembre 2013.

Nonostante, quindi, le problematiche associate a questo concetto, la sicurezza e la difesa del dominio *cyber* sono presentate nella strategia come due facce della stessa medaglia. L'EDA ha perciò il compito di promuovere lo sviluppo delle *capabilities* di *cyberdefence* a livello europeo, a cominciare dai singoli Stati.

L'agenzia ha commissionato alla Rand Corporation un'analisi dello sviluppo delle suddette *capabilities* in venti Stati membri. Lo studio, pubblicato nel marzo 2013, ha evidenziato «un quadro complesso e diversificato sia a livello UE che all'interno dei venti Paesi presi in esame»[160]. Il rapporto completo, con i profili dettagliati di questi Paesi, è classificato ma dalla parte resa pubblica si evince che gli Stati con maggiore familiarità con la *cybersecurity* sono anche quelli con *capabilities* più avanzate nel settore della difesa. Specificamente, gli aspetti di *leadership*, *personnel* e *interoperability* risultano abbastanza consolidati; mentre quelli di *doctrine*, *organisation* e training si trovano ancora ad un primo stadio di maturità. L'aspetto *facilities*, poi, appare indubbiamente quello più complesso e il suo sviluppo è stato definito pressoché inesistente. Lo studio propone infine l'elaborazione, nel breve-medio periodo, di una "*Roadmap for strengthening Cyber Defence i*n CSDP"[161].

A tale proposito ricordiamo che il Consiglio europeo del dicembre 2013 ha richiesto l'elaborazione entro il 2014 di un "Quadro strategico UE in materia di ciberdifesa", da realizzare su proposta dell'Alto Rappresentante ed in collaborazione con la Commissione e l'EDA.

Gli ultimi due organi rilevanti sono l'EC3 ed il CERT-EU, rispettivamente deputati alle risposte al *cybercrime* e ai *cyber attack*. Entrambi sono nati nel 2012 e sono divenuti operativi a partire dal 2013, per cui il loro reale apporto sarà valutabile solo quando avranno raggiunto maggiori livelli di operatività. Quello che è certo è che la loro realizzazione si è presentata come una componente necessaria, anche se non sufficiente, per la corretta gestione della *cybersecurity*.

c. International cyberspace policy

L'ultima priorità della strategia riguarda la cooperazione internazionale per la creazione di un *dossier* di raccordo per lo spazio cibernetico. La proiezione della questione *cyber* nelle relazioni esterne dell'Unione consentirebbe a quest'ultima di allacciare rapporti e stringere partenariati con attori internazionali, statali e non, attivi in questo settore.

---

[160] Brune S. et al., *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP. Unclassified Summary*, Santa Monica, Rand, 2013, p. 6, in *http://www.rand.org/pubs/research_reports/RR286.html.*

[161] European Defence Agency (EDA), *Factsheet Cyber Defence*, 19 novembre 2013, in *http://www.eda.europa.eu/info-hub/publications/publication-details/pub/factsheet-cyber-defence.*

Tra le cooperazioni auspicate, la strategia include quelle con Consiglio d'Europa, OCSE, Nazioni Unite, OSCE, NATO, Unione africana, ASEAN e OSA.

Una particolare attenzione viene poi rivolta alla cooperazione bilaterale con gli Stati Uniti, in special modo attraverso il Gruppo di lavoro UE-Stati Uniti su *cybersecurity* e *cybercrime*, istituito in occasione del vertice annuale UE-Stati Uniti del 2010. È significativo che nel corso di tale vertice, che dal 1990 costituisce un punto di forza della *partnership* transatlantica, le due potenze abbiano ritenuto importante creare un gruppo di lavoro specifico per la *cybersecurity* ed il *cybercrime*, il cui compito è preparare il dialogo ed il confronto in sede di vertice ufficiale. Ciò prova che questi temi sono entrati nella lista delle loro priorità.

Per quanto riguarda, invece, l'elaborazione di un dossier di raccordo internazionale, la strategia non auspica l'elaborazione di nuovi strumenti di diritto internazionale riferiti al *cyber*, bensì che siano estese portata e campo di applicazione di tre documenti specifici già esistenti: il Trattato internazionale sui diritti civili e politici, la Convenzione europea dei diritti dell'uomo e la Carta dei diritti fondamentali dell'Uomo. L'impegno dell'Unione dovrebbe volgere verso l'attuazione delle disposizioni ivi contenute, anche nel *cyber* spazio.

Infine, la strategia segnala la rilevanza della Convenzione di Budapest sul *cybercrime* del 2001, promossa dal Consiglio d'Europa e firmata da cinquantadue Paesi. Ad oggi la Convenzione è stata ratificata da quarantuno Stati, dei quali ventitré sono membri dell'UE[162]. La strategia definisce la Convenzione un importante strumento aperto alla firma anche di Paesi terzi; un modello per l'adozione di norme e regole nazionali ed un simbolo della volontà di cooperare a livello internazionale.

3. Organi Rilevanti

L'Unione europea ha progressivamente incaricato determinati suoi organi ed agenzie di occuparsi della questione della *cybersecurity*, procedendo all'assegnazione di compiti specifici in merito.

Allo stato attuale i più rilevanti sono:

- Commissione europea;
- Alto Rappresentante per gli affari esteri e la politica di sicurezza;

[162] I Paesi UE che non hanno ancora ratificato la convenzione *de qua* sono Grecia, Irlanda, Lussemburgo, Polonia e Svezia.
Si veda *http://conventions.coe.int/Treaty/Commun/ hercheSig.asp?NT=185&CM=&DF=&CL=ENG.*

- ENISA;
- EDA;
- EC3;
- CERT-EU.

La Commissione e, solo recentemente anche l'Alto Rappresentante, svolgono un ruolo importante nell'elaborazione di proposte e nella preparazione di documenti ufficiali riguardanti la *cybersecurity*.

La Commissione, in particolare, è stata protagonista dei primi documenti ufficiali dell'Unione in ambito *cyber*, contribuendo in maniera significativa all'evoluzione di questa tematica. Inoltre, una Direzione generale della Commissione - quella per le Reti di comunicazione, contenuti e tecnologia (CNET), detta DG CONNECT - è specificamente dedicata allo sviluppo delle tecnologie dell'informazione e delle comunicazioni, al fine di aumentare i posti di lavoro e favorire la crescita economica in Europa. La DG CONNECT partecipa al finanziamento del progetto "*Cybersecurity, privacy and trustworthy ICT: research and innovation*", nell'ambito del programma "Horizon 2020", con un bilancio di circa 136 milioni di euro per il biennio 2014-2015,

Una fondamentale agenzia europea per la *cybersecurity* è l'ENISA. Essa rappresenta il punto di riferimento principale per il coordinamento delle politiche *cyber* nazionali, proponendosi come tramite europeo ed attivatore di dialogo. Merita mettere in evidenza l'impegno dell'Agenzia nel promuovere il progresso delle capacità tecnologiche, condizione essenziale per una risposta adeguata agli attacchi di natura cibernetica. Questo impegno si traduce nella costruzione di un rapporto solido con i vari Governi nazionali e nell'organizzazione di esercitazioni.

Queste ultime, in particolare, come già accennato, costituiscono un modo molto importante di rafforzare la cooperazione, consentendo all'UE e alla comunità internazionale di riunire i maggiori esperti in ambito *cybersecurity*, sottoponendo loro complicati esempi di attacchi cibernetici, così da testare il grado di competenze acquisite e stimolare l'apprendimento secondo la tecnica del *learn by doing*. Le esercitazioni di questo tipo rientrano nella categoria dei cosiddetti *serious game*, ideati per consentire al personale coinvolto di accrescere le proprie abilità ed affinare le proprie strategie, attraverso la simulazione di eventi di crisi potenzialmente realizzabili nella realtà. I *serious game* possono trovare applicazione sia in ambito civile sia in ambito militare; quelli *cyber* si collocano a metà strada tra questi due settori, in linea con il duplice scopo cui possono essere destinati, già trattato in precedenza.

Durante le esercitazioni non ha alcuna importanza la nazionalità degli esperti, poiché tutti lavorano egualmente all'interno di una piattaforma, utilizzando modelli comuni di conoscenza. Ciò significa che, dopo ogni esercizio, il metodo di risoluzione che si rivela migliore diventa automaticamente il modello base per affrontare problemi più complessi. Tale metodo viene messo immediatamente a completa disposizione di tutti gli altri partecipanti, i quali possono così sfruttare il *know how* altrui per apportare il proprio contributo nello *step* successivo. Il metodo consente di raggiungere in tempo reale la soluzione più efficace, attraverso la piena condivisione dell'*expertise* a disposizione.

A livello europeo due esercitazioni sono state organizzate dall'ENISA ed altre dal *Cooperative Cyber Defence Centre of Excellence di Tallinn* (CCD COE). Tale centro è stato inaugurato nel maggio 2008 ed ha ottenuto pochi mesi dopo il patrocinio della NATO ed il riconoscimento dello *status* di organizzazione militare internazionale. È importante sottolineare che il CCD COE non è una struttura della NATO o dell'UE, ma un centro sorto per iniziativa dello Stato estone, che dal 2003 ha esercitato molte pressioni per ottenerne il patrocinio da parte dell'Alleanza Atlantica.

Il centro svolge oggi un ruolo particolare per quanto riguarda la formazione e l'addestramento dei tecnici/analisti informatici in materia di *cybersecurity*. Dal 2012 le esercitazioni organizzate dal CCD COE prendono il nome di *"Locked Shields"* e si svolgono con cadenza pressoché annuale.

Sempre secondo la logica dei *serious game*, più squadre hanno preso parte all'esercitazione, la quale è stata organizzata in modo tale che le "squadre blu" dovessero cooperare tra loro per rispondere a svariati attacchi da parte della "squadra rossa". Ogni squadra blu era composta da una serie di esperti IT e da due consulenti legali, aventi lo scopo di garantire il rispetto del diritto. Lo scenario prevedeva il dispiegamento di un certo numero di squadre, dietro mandato delle Nazioni Unite, a sostegno del governo di uno stato fittizio (Boolea), il quale si trovava a dover fronteggiare un'aspra guerra civile ed aveva chiesto l'intervento della comunità internazionale.

Compito delle squadre blu era rispondere agli attacchi di natura cibernetica rivolti contro i sistemi IT delle organizzazioni di aiuto locali e preservare l'integrità dei *network* militari. Le squadre avevano inoltre l'obbligo di tenere costantemente aggiornato il quartier generale, eseguire gli ordini da questo provenienti, e rispondere ai media. Paragonata all'esercitazione ENISA del 2012, *la Locked Shield* 2013 ha presentato problemi/esercizi più complessi e diversificati, soprattutto dal punto di vista dei *task*.

L'introduzione di due elementi aggiuntivi, i consulenti legali per gli aspetti del diritto e i media per l'opinione pubblica, ha permesso di rendere lo scenario più completo e realistico.

Secondo il rapporto dell'esercitazione del 2013, le squadre hanno riportato notevoli successi nelle attività di "*preventing*", "*detecting*" e "*mitigating*" degli attacchi, in confronto ai precedenti eventi.

Numerose altre esercitazioni sono state organizzate negli ultimi anni da altri attori internazionali, quali la NATO e gli Stati Uniti; ma quello che preme mettere in rilievo è che questa pratica va via via consolidandosi da circa 3 anni. Prima del 2010, infatti, non si registrano molti eventi del genere, in ogni caso caratterizzati da un tasso relativamente basso di partecipazione.

La pratica delle esercitazioni si rivela molto significativa sia per la messa in comune delle competenze informatiche sia perché costituisce l'occasione di una cooperazione internazionale. Eventi simili dovrebbero essere organizzati pure su scala nazionale, anche per permettere una più stretta collaborazione tra il settore pubblico e quello privato. Dal 2012 l'Italia organizza annualmente un'esercitazione nazionale denominata "CybIt", la quale, nella sua ultima edizione, ha visto anche la partecipazione di attori privati operanti nel settore energetico. Si auspica che questa pratica venga consolidata negli anni a venire, con un coinvolgimento più ampio del settore privato. Inoltre, sempre in Italia, si sta pensando di creare una sorta di "*Battle Lab*", grazie all'operato del Comando C4 Difesa, delle Forze Armate e di altri rilevanti *stakeholder*, così da permettere l'esercizio continuativo del personale in questione[163]. Quest'attività è stata già realizzata in alcuni Paesi, come Stati Uniti e Regno Unito, che hanno già inaugurato le proprie *"cyber units"*.

A partire da ottobre 2013, il Ministero della Difesa britannico ha lanciato una campagna di reclutamento per la costituzione di una futura "*Joint Cyber Reserve*", la quale avrà come obiettivo quello di garantire la sicurezza cibernetica entro i confini nazionali. Il personale invitato ad offrire la propria candidatura non deve necessariamente provenire dalle fila dell'apparato militare; anzi, le probabilità di coinvolgere esperti informatici al di fuori dell'ambiente militare sono più che elevate ed auspicate, dal momento che in ambito *cyber* una sinergia civile/militare si rende necessaria.

---

[163] Secondo Umberto Maria Castelli, comandante del Comando C4 Difesa del Ministero della Difesa, il "*Battle Lab*" dovrebbe svolgere la funzione di una vera e propria «palestra per addestrare un futuro esercito del cyber spazio» (dichiarazione rilasciata in occasione del seminario "Cooperare per crescere nella sicurezza", organizzato a Roma il 25 ottobre 2013 dall'Istituto superiore delle comunicazioni e delle tecnologie ISCOM).

A livello europeo, la costituzione di queste capacità aggregate e strutturate in ambito cibernetico potrebbe rappresentare un buon anello di congiunzione tra gli Stati membri e le istituzioni UE, tra le quali l'ENISA giocherebbe un ruolo primario.

L'Agenzia europea di difesa ha il compito di delineare la *cyberdefence* all'interno delle politiche di sicurezza europee. La stessa strategia di sicurezza cibernetica afferma che «le attività a favore della *cyber sicurezza* nell'Unione europea coinvolgono anche la dimensione della *cyber* difesa»[164] e che, come già riportato, «lo sviluppo di capacità di *cyber* difesa dovrebbe concentrarsi sulle attività di individuazione, risposta e recupero nei confronti di *cyber* minacce sofisticate»[165].

Nonostante, quindi, le problematiche associate a questo concetto, la sicurezza e la difesa del dominio *cyber* sono presentate nella strategia come due facce della stessa medaglia. L'EDA ha perciò il compito di promuovere lo sviluppo delle *capabilities* di *cyberdefence* a livello europeo, a cominciare dai singoli Stati. L'agenzia ha commissionato alla *Rand Corporation* un'analisi dello sviluppo delle suddette *capabilities* in venti Stati membri. Lo studio, pubblicato nel marzo 2013, ha evidenziato *«un quadro complesso e diversificato sia a livello UE che all'interno dei venti paesi presi in esame»*[166]. Il rapporto completo, con i profili dettagliati di questi Paesi, è "classificato", ma dalla parte resa pubblica si evince che gli Stati con maggiore familiarità con la *cybersecurity* sono anche quelli con *capabilities* più avanzate nel settore della difesa. Specificamente, gli aspetti di *leadership*, *personnel* e *interoperability* risultano abbastanza consolidati; mentre quelli di *doctrine*, *organisation* e *training* si trovano ancora ad un primo stadio di maturità. L'aspetto *facilities*, poi, appare indubbiamente quello più complesso e il suo sviluppo è stato definito pressoché inesistente. Lo studio propone infine l'elaborazione, nel breve-medio periodo, di una *«Roadmap for strengthening Cyber Defence in CSDP»*[167]. A tale proposito ricordiamo che il Consiglio europeo del dicembre 2013 ha richiesto l'elaborazione entro il 2014 di un "Quadro strategico UE in materia di *cyber* difesa", da realizzare su proposta dell'Alto Rappresentante ed in collaborazione con la Commissione e l'EDA.

Gli ultimi due organi rilevanti sono l'EC3 ed il CERT-EU, rispettivamente deputati alle risposte al *cybercrime* e ai *cyber attacks*. Entrambi sono nati nel 2012 e sono divenuti operativi a

---

164 Commissione europea, *Strategia dell'Unione europea per la cibersicurezza,* cit., p. 12.

165 Commissione europea, *Strategia dell'Unione europea per la cibersicurezza,* cit., p. 13.

166 Brune S., *Stocktaking study of military cyber defence capabilities in the European Union* milCyberCAP. Unclassified Summary, Santa Monica, Rand, 2013, p. 6, in *http://www.rand.org/pubs/research_reports/RR286.html.*

167 European Defence Agency (EDA), *Factsheet Cyber Defence*, 19 novembre 2013, in *http://www.eda.europa.eu/info-hub/publications/publication-details/pub/factsheetcyber-defence.*

partire dal 2013, per cui il loro reale apporto sarà valutabile solo quando avranno raggiunto maggiori livelli di operatività.

Quello che è certo è che la loro realizzazione si è presentata come una componente necessaria, anche se non sufficiente, per la corretta gestione della *cybersecurity*. L'EC3 ed il CERT-EU rappresentano, infatti, gli organi tecnici operativi dell'Unione, con il compito di rispondere concretamente ed efficacemente alle crisi di natura cibernetica. Il loro operato è, inoltre, fondamentale per il raccordo e la collaborazione con i loro corrispettivi nazionali, ove esistenti. Dell'EC3 segnaliamo uno studio redatto in collaborazione con *l'International Cyber Security Protection Alliance* (ICSPA) e pubblicato nel 2013 che offre una panoramica dei possibili sviluppi del crimine informatico negli anni a venire. L'obiettivo è anticipare il futuro del *cybercrime*, consentendo a governi, imprese e cittadini di prepararsi per le sfide e le opportunità del prossimo decennio[168]. Lo studio afferma che *«cybercrimes in 2020 will be adaptations of existing crimes to the technological developments of the next seven to eight years. […] Evolved threats to critical infrastructure and human implants will increasingly blur the distinction between cyber and physical attack».*[169]

Il documento considera inoltre la possibilità che nuovi crimini informatici possano, in futuro, causare danni psicologici alle vittime e prevede che la natura evoluta e maggiormente complessa del *cybercrime* richiederà una migliore definizione dei ruoli e delle responsabilità degli organi incaricati di indagare e combattere queste minacce. Lo studio propone quindi la messa in atto di procedimenti giudiziari o "quasi-giudiziari" nei confronti non solo degli autori degli attacchi, ma anche delle organizzazioni oggetto di questi, siano esse pubbliche o private. Ad esse spetterebbe infatti il dovere di ripristinare i servizi - pena il pagamento di sanzioni - e di applicare norme per la prevenzione del crimine. Oltre ad offrire un ampliamento della categoria dei crimini informatici, lo studio ha il pregio di evidenziare l'importanza dello sviluppo di adeguati meccanismi di *law enforcement*, per assicurare una corretta gestione del rischio e del danno, da parte di tutte le organizzazioni interessate.

Le istituzioni e gli organi dell'Unione descritti in questo paragrafo sono, attualmente, quelli maggiormente rilevanti per quanto riguarda la *cybersecurity* in Europa, ma è prevedibile che il panorama possa mutare negli anni a venire.

---

168 Europol and ICSPA, *Project 2020. Scenarios for the future of Cybercrime*, 25 September 2013, in *www.europol.europa.eu/content/project-2020-scenarios-future-cybercrime.*

169 Europol and ICSPA, *Project 2020. Scenarios for the future of Cybercrime*, cit. 25 settembre 2013, p. 7.

4. Elementi critici

È importante mettere in evidenza come la strategia europea di sicurezza cibernetica non arrivi a definire il lato più squisitamente tecnico/operativo della *cybersecurity*, ma ne stabilisca solo i profili essenziali, in linea con gli scopi ed obiettivi di ogni documento strategico.

Il documento, infatti, enuncia i valori chiave alla base dell'approccio europeo e le buone pratiche da seguire per raggiungere dei risultati significativi. *Core values* e *good practices* rappresentano le priorità europee in materia ed il punto di partenza per agire.

Quanto ai valori chiave, la strategia stabilisce l'importanza di agire sempre secondo un sentimento di responsabilità condivisa, il quale consenta di trattare la *cybersecurity* come una questione di portata globale.

Essenziale, infatti, è l'adozione di una prospettiva che valichi i confini nazionali e quelli europei, affinché la cooperazione internazionale possa essere efficace, in considerazione della natura tendenzialmente *borderless* delle problematiche cibernetiche. Proprio il concetto di cooperazione è alla base dell'intero documento. Tale cooperazione è intesa sia a livello nazionale, per ciò riguarda la creazione di *partnership* pubblico-private , sia a livello europeo, con riferimento all'importanza per gli Stati e per le rilevanti istituzioni ed agenzie dell'UE di comunicare ed agire insieme nell'ambito dell'Unione , sia, infine, a livello internazionale, con altri attori statali e non. Questa priorità rappresenta il *landmark* della strategia *cyber* dell'UE.

Affinché la cooperazione sia realizzabile, è opportuno che tutte le parti coinvolte sostengano e promuovano la creazione di strumenti di *confidence building*, basati sulla trasparenza e sull'*information sharing*.

Proprio quest'ultimo punto si rivela una condizione imprescindibile per la buona riuscita di una politica di *cybersecurity*, anche se, purtroppo, di non facile realizzazione.

Lo scambio delle informazioni resta un argomento piuttosto ostico, soprattutto in tema di sicurezza. La diffidenza che esiste non solo tra Stati sovrani, ma anche tra singolo Stato ed imprese private, spinge le parti a rifuggire dal dialogo aperto e ad optare per la non condivisione delle informazioni. Tale scelta viene sempre percepita come un vantaggio sugli altri, secondo una logica realistica in cui il conflitto caratterizza la vera natura dei rapporti, siano essi tra individui o tra Paesi. Appare dunque molto difficile favorire il diffondersi su vasta scala di comportamenti collaborativi, ma non bisogna dimenticare che a volte cooperare in un ambito

nuovo può apparire molto più semplice che cercare un'intesa in un ambito tradizionalmente complicato.

Il *cyber* ha dalla sua parte la relativa novità. In una situazione generale in cui tutti gli attori principali cominciano a rapportarsi con una problematica per la prima volta, ci sono buone probabilità che questi decidano di operare insieme, per trarne reciproco vantaggio. Ora, è vero che non tutti gli attori si trovano nella stessa situazione - anzi, molte e significative sono le differenze in questo senso - ma è anche vero che nessuno si trova in possesso dell' "arma nucleare" in grado di tenere tutti gli altri sotto scacco. La scelta cooperativa potrebbe rivelarsi non impossibile, come dimostrano le sempre più frequenti occasioni di incontro tra Stati, organizzazioni internazionali e compagnie private.

Attualmente, in Europa, l'*information sharing* può essere definito unidirezionale: non esiste un obbligo per le autorità di fornire informazioni al settore privato, il quale, al contrario, ha il dovere di fare rapporto alle autorità. A questo proposito, Troels Oerting, direttore dell'EC3, ha affermato nel marzo 2013 che il meccanismo di info *sharing* in Europa dovrebbe assomigliare a quello statunitense, essere cioè una strada a doppio senso, in cui le informazioni fluiscono in ambedue le direzioni[170].

Vi è un altro aspetto problematico della cooperazione: il dominio *cyber* è per sua natura difficilmente contenibile all'interno di confini precisi, anche se le opinioni al riguardo divergono. È piuttosto diffusa l'idea secondo la quale il *cyber* costituirebbe un "*global common*". I sostenitori di questa tesi considerano lo spazio cibernetico come un bene comune, in quanto tale sottoposto al regime di *res communis omnium*, che presuppone l'inappropriabilità del bene e la sua libertà d'uso[171].

Il dibattito sul tema è molto acceso ed alcuni non condividono questa impostazione, soprattutto in considerazione del fatto che il *cyber* spazio risulta in larghissima parte posseduto da privati. Gli aspetti regolativi di internet, ad esempio, sono interamente appannaggio di un ente internazionale no-profit, l'ICANN (*International Corporation for Assigned Names and Numbers*). L'ICANN ha il compito di gestire l'assegnazione degli indirizzi IP, nell'ambito del sistema di nome di dominio (DNS). Da un lato, l'assegnazione di un codice identificativo per ogni singolo

---

[170] Intervento di *Troels Oerting* al dibattito "*What next for European cyber-security?*", organizzato a Bruxelles il 19 marzo 2013 dalla *Security* & *Defence Agenda* (SDA). SDA, in *Cyber-security: Problems outpace solutions*, dicembre 2013, p. 9, consultabile al link: *http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3620/categoryId/62/Cybersecurity-Problems-outpacesolutions.aspx*.

[171] Pisa R., *L'accesso ad internet: un nuovo diritto fondamentale?*, in Treccani Magazine, 7 gennaio 2010, consultabile in *http://www.treccani.it/magazine/diritto/approfondimenti/diritto_internazionale_e_comparato/2_Pisa_internet.html*.

dispositivo elettronico permette ai computer di rintracciarsi ed interagire tra di loro; dall'altro, l'assegnazione dei domini *"com", "net"* oppure *"org"* consente agli utenti di individuare i siti *web*. Il DNS è quindi alla base del funzionamento di internet, e l'immenso potere di controllo e gestione di questo sistema è appartenuto fino ad oggi a questo ente internazionale, in seguito ad un contratto stipulato con il Dipartimento per il Commercio degli Stati Uniti.

Quanto detto è in contrasto con la tesi del *cyber* spazio inteso come *global common* ed apre scenari più complessi, non esenti da logiche di competizione per il "comando e controllo".

La questione della natura dello spazio cibernetico è tuttora molto discussa, mal prestandosi ad un suo inquadramento nei principi tradizionali di diritto internazionale. In particolare, l'apparente mancanza di fisicità del *cyber space* rende difficile l'applicazione di concetti tipici del diritto del mare e del diritto dello spazio (luna e corpi celesti), aprendo a nuove possibilità di definizione ancora non previste a livello giuridico.

L'ex presidente, dell'Istituto Affari Internazionali, in un intervento del febbraio 2012 , ha precisato che un *global common* può essere dichiarato tale solo qualora sia regolato dal diritto internazionale generale. In caso contrario, il bene rimane "globale", ma non può essere considerato comune. Un *cyber* spazio del tipo *global common* non è compatibile con le logiche nazionali di competizione per l'acquisizione di una superiorità strategica in questo campo. Tanto meno gli Stati sembrano intenzionati a firmare una nuova Convenzione internazionale in difesa della natura comune dello spazio cibernetico. Appare pertanto difficile sostenere la tesi che il dominio *cyber* costituisca un *global common.* [172]

Una tesi diversa è sostenuta dal direttore del programma di Tecnologie strategiche del *Center for Strategic and International Studies* (CSIS), il quale in un intervento del settembre 2011 ha sostenuto che lo spazio cibernetico non può essere considerato un *common*, ma piuttosto un "condominio", in cui tutti i proprietari condividono la stessa struttura, dotata di poche regole e di un debole organo di governo.

Secondo tale impostazione, il *cyber* spazio possiede dei confini entro i quali gli Stati si sentono, o si sentiranno a breve, legittimati a rivendicare la propria sovranità. Alcuni governi hanno infatti paragonato il ciberspazio al mare territoriale, accessibile dall'esterno ma soggetto al proprio controllo.

---

[172] Silvestri S., *Speaking notes, documento NIAG a Finmeccanica su Cyber security e cooperazione internazionale*, 6 febbraio 2012. Il NIAG (*NATO Industrial Advisory Group*) è un gruppo consultivo per gli aspetti industriali della Conferenza dei direttori nazionali degli armamenti (CNAD) della NATO e dei principali gruppi di armamenti, a cui ha preso parte una delegazione italiana di rappresentanti delle principali aziende nazionali operanti in vari settori tecnologici della difesa.

L'estensione della sovranità nazionale al dominio cibernetico avrebbe come conseguenza quella di ridefinirne l'architettura, con le sue regole e la sua *governante*, prospettiva questa che si rivela molto più probabile di quanto possa sembrare. [173]

L'amministratore delegato del *Data Security Council of India* (DSCI), ha affermato in un articolo del giugno 2012 che lo spazio cibernetico è allo stesso tempo un *global common* ed una risorsa nazionale. Si tratterebbe, infatti, di un bene comune di nuovo tipo, ancora privo di un regime formale di regolamentazione, ma in grado di offrire una vasta gamma di servizi a cittadini. Ciò dovrebbe spingere i governi a concludere accordi internazionali in questo campo, che non necessariamente debbono assumere la forma di trattati, considerata la persistente generale difficoltà nel comprendere appieno le dinamiche del ciberspazio. [174]

Il dibattito sulla natura dello spazio cibernetico è tutt'altro che teorico, essendo alla base della cooperazione internazionale. È quindi prioritario chiarire le intenzioni della comunità internazionale in riferimento alla gestione della *governance* della dimensione cibernetica: la cooperazione internazionale è possibile solo in un'ottica di approccio *multi-stakeholder*, basato sulla partecipazione attiva di tutti gli attori interessati, pubblici e privati. La strategia europea di sicurezza cibernetica ha gettato le basi per un'auspicata evoluzione verso una più articolata politica europea di *cybersecurity*, che stabilisca chiaramente le regole da rispettare ed istituisca precisi meccanismi di comunicazione tra le parti.

Si discute, in particolare, sull'eventualità di stabilire degli *standard* o *security label* a livello europeo, validi in tutti gli Stati membri. Il testo della strategia afferma l'importanza di stabilire *«norme di sicurezza promosse dall'industria»*[175] in virtù del *know how* consolidato posseduto dal settore privato in questo campo. Tale atteggiamento potrebbe rivelarsi significativo se affiancato da un'efficace attività di regolamentazione da parte delle istituzioni politiche. Comincia a farsi strada l'idea che sia necessario un intervento pubblico più coercitivo, sia a livello nazionale che europeo. Secondo questa prospettiva, spetterebbe all'Unione stessa il compito di fissare degli *standard* obbligatori di sicurezza e di predisporre tutte le misure atte a garantire una costante collaborazione tra il settore pubblico e quello privato e tra i governi e le istituzioni europee.

Le opinioni al riguardo, però, divergono: oltre alla suddetta impostazione, c'è chi sostiene che la *cybersecurity* sia essenzialmente un processo auto-generantesi appannaggio del solo settore

---

[173] Lewis J., *Rethinking Cybersecurity. A Comprehensive Approach, Speech at the Sasakawa Peace Foundation*, Tokyo, 12 settembre 2011, in *http://csis.org/node/32513*.

[174] Kamlesh B., *Globar cyber commons. Addressing cyber security issues*, in Neurope, 3 giugno 2012, in *http://www.neurope.eu/node/114509*.

[175] Commissione europea, *Strategia dell'Unione europea per la cybersicurezza*, cit., p.14.

privato e chi crede che gli *standard* di sicurezza debbano essere fissati a livello globale e non regionale[176].

Quale che sia il livello decisionale, la messa in pratica dei suddetti *standard* di sicurezza appare, oggi, una priorità per la *cybersecurity* in generale. In quest'ottica si inserisce anche la necessità di creare un meccanismo di *incident reporting* che sia obbligatorio e non volontario. La questione della resistenza operata dal settore privato potrebbe essere parzialmente risolta tramite l'istituzione dell'anonimato oppure la classificazione di certe informazioni, le quali sarebbero così note solo alle istituzioni governative e non anche al pubblico. Questo punto di vista è stato presentato anche dall'ex Ministro britannico per la sicurezza e la lotta al terrorismo che ha affermato*: «I would very much like to see a mandatory reporting system with anonymisation and not leading to a criminal investigation in every case»*[177]. Lo stesso, che attualmente ricopre il ruolo di rappresentante speciale del Governo britannico presso il settore industriale per gli affari di *cybersecurity*, ha inoltre più volte sottolineato l'esigenza di un vero e proprio "*mentality shift*"[178]: l'obiettivo, ha affermato, è far sì che i singoli e le aziende vedano la *cybersecurity* come un "*enabler of their business*"[179], in considerazione del fatto che i maggiori danni prodotti dal *cybercrime* sono di natura economica. Affinché ciò sia possibile è importante pensare la *cybersecurity* al di là delle mere logiche di *business continuity*, in uno sforzo di rinnovata mentalità e atteggiamento costruttivo. Coinvolgere il settore privato significa anche promuovere il concetto di sicurezza funzionale, che si prefigge la continuazione delle funzioni chiave della società moderna. Per inserire la *cybersecurity* all'interno di questa visione è necessario allontanare il settore privato da un'impostazione individualista e renderlo consapevole dell'impatto del *cyber* sulla vita economica del Paese intero.

Tenendo tutto questo bene a mente, è auspicabile che l'Unione compia presto i prossimi passi nella direzione di una maggiore definizione della politica di *cybersecurity* e di un potenziamento degli strumenti già posti in essere. In parallelo, è fondamentale che anche gli Stati seguano lo stesso esempio, così che tutti i vari livelli di *governance* europea godano di una buona consapevolezza situazionale e di adeguate *capabilities* e procedure.

---

176 Neville-Jones P., *Security* & *Defence Agenda (SDA), Cyber-security: Problems outpace solutions*, cit., p. 9.

177 Neville-Jones P., *Security* & *Defence Agenda (SDA), Where cyber-security is heading*, ottobre 2012, p. 65, in: *http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3412/New-SDAcyber-report.aspx*.

178 Neville-Jones P., *Security* & *Defence Agenda (SDA), Where cyber-security is heading*, cit p. 67.

179 Neville-Jones P., *Security* & *Defence Agenda (SDA), Where cyber-security is heading*,cti, p. 61.

Bibliografia

- *Alma M., Perroni C., Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici,* in *Dir. pen. Proc.,* 1997;
- Atemo S., *Il reato di accesso abusivo a sistema informatico tra reato di danno e reato di pericolo*, in *www.penale.it*;
- Aterno S, *Le misure di sicurezza nel reato di accesso abusivo: l'agente deve averle neutralizzate, commento a sentenza della Cassazione sul reato di accesso abusivo*, in *Diritto dell'Internet*, 1, 2008, Ipsoa;
- Aterno S., Cajani F., Costabile G., Mattiucci M., Mazzaraco G., *Computer Forensics e indagini digitali,* Vol. 1, Experta 2011;
- Aterno S., Corasaniti F., Corrias Lucente G., *Cybercrime, responsabilità degli enti, prova digitale,* Lucente*,* Padova, 2009;
- Aterno S., *Modifiche al titolo III del terzo libro del codice di procedura penale*, in Corasaniti G., Corrias Lucente G., *Cybercrime, responsabilità degli enti, prova digitale*, Cedam, 2008;
- Bejtlich R., *Real Digital Forensics. Computer Security and Incident Response*, Addison-Wesley; ottobre 2005;
- Braghò G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici* in Lupària L., *Sistema penale e criminalità informatica*, Giuffrè, 2009;
- Brune S., *Stocktaking study of military cyber defence capabilities in the European Union*, milCyberCAP. Unclassified Summary, Santa Monica, Rand, 2013;
- Brune S., *Stocktaking study of military cyber defence capabilities in the European Union* milCyberCAP. Unclassified Summary, Santa Monica, Rand, 2013;
- Buso D., Pistolesi D., *Le perquisizioni e i sequestri informatici*, in Ruggeri F., Picotti L., *Nuove tendenze della giustizia penale di fronte alla criminalità informatica*, Giappichelli, 2011;
- Casey E., *Digital evidence and computer crime. Forensic Science, computer and the internet,* Elsevier Academic Press, Second Edition, 2004;
- Cencetti C., *Cybersecurity: Unione europea e Italia: Prospettive a confronto,* Edizioni nuova cultura, Roma, 2014;
- Clifford R. D., *Cybercrime: the investigation, prosecution and defense of a computer-related crime,* Durham, NC: Carolina Academic, 3th edition, 2010;
- Costabile G., *Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Cyberspazio e diritto,* 2010;
- Delfini F., Finocchiaro G., *Diritto dell'informatica,* UTET giuridica, anno 2014;

- Flor R., *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht,* in *Cyberspazio e diritto,* 2012;
- Kamlesh Bajaj, *Globar cyber commons. Addressing cyber security issues,* in *Neurope, 3 giugno 2012, http://www.neurope.eu/node/114509;*
- Leman-Langlois S. (editing), *Technocrime,* Routledge, 2010;
- Lewis J., Baker S., *The Economic Impact of Cybercrime and Cyber Espionage,* Santa Clara, McAfee, luglio 2013;
- Lewis J., *Rethinking Cybersecurity. A Comprehensive Approach, Speech at the Sasakawa Peace Foundation*, Tokyo, 12 settembre 2011;
- Logli A., *Commento alla sentenza n. 753/2007*, in *Cass. pen.*, 2008;
- Lupària L., *Ratifica della Convenzione Cybercrime del Consiglio d'Europa*, in *Diritto Penale e Processo,* 2008;
- *Lusitano D., In tema di accesso abusivo a sistemi informatici o telematici*, in *Giur. it.,* 1998;
- Mantovani F., *Diritto Penale, delitti contro la persona*, I. ed. Cedam, 1995;
- Monti A., *No ai sequestri indiscriminati di computer*, in *Diritto dell'Internet,* 2007;
- Moore R., *Cybercrime: investigating high-technology computer crime,* Anderson publishing, 2nd edition, 2011;
- Nicosia G., Caccavella D., *Macchine virtuali e sistema della prova nel processo civile e penale*, in *Diritto dell'Internet*, 2008;
- Omand D., *The steps needed to protect the EU's critical infrastructure against cyber-attack*, in *Europe's World*, *No. 25*, 2013;
- Pawlak P., *Riding the digital wave, The impact of cyber capacity building on human development,* Report n. 21, dicembre 2014;
- Pecorella C., *Il diritto penale dell'informatica*, Padova, 2006;
- Pica G., v. *Reati informatici e telematici,* in *Dige. Disc. pen. eco.,* Aggiomam. I, 2000;
- Piciotti L., S*istematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati***,** in *Id. (a cura di), Il diritto penale dell'informatica nell'epoca di Internet*, Cedam, Padova, 2004;
- Pisa R*., L'accesso ad internet: un nuovo diritto fondamentale?,* in Treccani Magazine, 7 gennaio 2010;
- Salvadori I., *Hacking, cracking e nuove forme di attacco ai sistemi d'informazione. Profili di diritto penale e prospettive de jure condendo***,** in *Ciber. Dir.,* 2008;
- Security & Defence Agenda (SDA), *Where cyber-security is heading*, ottobre 2012;
- Sfeber U., *The intemational handbook for computer crime. Computer-Related Economie Crime and the Infringements of Privacy*, New York, 1986;
- Sieber U., *Organised crime in Europe: thè threat of cyber crime,* Situation Report 2004, Council of Europe Publishing, 2005;

- Smith R. G., Grabosky P., Urbas G., *Cyber criminals on trial,* Cambridge, 2004;
- Trogu M., *Sorveglianza e "perquisizioni" on-line su materiale informatico*, in *Le indagini atipiche,* (a cura di) Scalfati A., Giappichelli Editore,2014;

Fonti giuridiche

- Cass., sez. VI, 4 ottobre 1999, n 3554, Piersanti, in *Cass. pen., 2*000, p. 2990 e., disponibile anche sul sito *ictlex.net*.
- Cass., sez. VI, 5 marzo 2008, n 13792, in *Dirittoitalia.it*.
- Cass., sez. VI, 10 dicembre 2009, n° 47009, in leggiditalia.it.
- Cass., sez.VI, 3 aprile 2008, n 18897 , *in Dirittoitalia.it.*
- Cass., sez. fer., 16 dicembre 2013, n. 50620, c.c. 12 dicembre 2013, Preite.
- Cass., sez. VI, 14 dicembre 1999, n. 3067, in Cass. pen., 2000.
- Cass., sez. V , 6 luglio 2007, n. 31135, in *Dirittoitalia.it*.
- Cass., sez. VI, 14 dicembre1999, n. 3067, in Cass. pen., 2000.
- Cass., sez. V , 6 luglio 2007, n. 31135, in *Dirittoitalia.it*.
- Cass., sez. VI, 14 dicembre1999, n. 3067, in Cass. pen., 2000.
- Cass., sez. V , 6 luglio 2007, n. 31135, in *Dirittoitalia.it*.
- Commissione europea, *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica,* eEurope 2002 (COM(2000)890), 26 gennaio 2001.
- Commissione europea, eEurope 2005: *una società dell'informazione per tutti* (COM(2002)263), 28 maggio 2002.
- Commissione europea, eEurope. *Una società dell'informazione per tutti* (COM(2000)130), 8 marzo 2000.
- Commissione europea, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo* (COM(2001)298), 6 giugno 2001.
- Commissione europea, *Strategia dell'Unione europea per la cybersicurezza,* luglio 2012.
- Consiglio europeo, *Relazione sull'attuazione della strategia europea in materia di sicurezza. Garantire sicurezza in un mondo in piena evoluzione* (S407/08), 11 dicembre 2008.
- Consiglio europeo, *Conclusioni del Consiglio europeo 19 e 20 dicembre 2013 - Politica di sicurezza e di difesa comune*, 19 dicembre 2013.
- Consiglio europeo, *Un'Europea sicura in un mondo migliore. Strategia europea in materia di sicurezza,* 12 dicembre 2003.

- Tribunale Riesame, Perugia, ord. 25 ottobre 2006, in *leggiditalia.it.*
- Tribunale Riesame-, Venezia, ord. 6 ottobre 2000, in *leggiditalia.it.*