ACI Informatica S.p.A.

MODELLO DI ORGANIZZAZIONE

DI GESTIONE E DI CONTROLLO

Ex DECRETO LEGISLATIVO 8 giugno 2001 n. 231

e successive integrazioni e modificazioni

Approvato con delibera de Consiglio di Amministrazione del 29 marzo 2004
Aggiornato con delibere del Consiglio di Amministrazione del:

- 12 dicembre 2007 (vers. 2)
- 16 novembre 2009 (vers. 3)
- 27 marzo 2012 (vers. 4)
- 10 settembre 2013 (vers. 5)
- 19 gennaio 2016 (vers. 6)

INDICE

PARTE SPECIALE pag.

PARTE GENERALE

1. IL DECRETO LEGISLATIVO N.231/2001

1.1. Sintesi della normativa

Il D.Lgs. 8 giugno 2001 n. 231, ha introdotto per la prima volta nel nostro ordinamento la responsabilità cd. "amministrativa" degli enti (così intendendosi anche le associazioni e gli enti pubblici economici) per alcuni reati commessi, nel loro interesse o vantaggio, da determinati soggetti, preposti, dipendenti o anche solo in rapporto funzionale con l'ente stesso, responsabilità che va ad aggiungersi a quella della persona fisica che ha realizzato effettivamente il reato.

La finalità che il legislatore ha voluto perseguire è quella di coinvolgere il patrimonio della Società e, in definitiva, gli interessi economici dei soci, nella punizione di alcuni illeciti penali, realizzati da amministratori e/o dipendenti nell'interesse o a vantaggio dell'azienda, in modo tale da richiamare i soggetti interessati ad un maggiore controllo della regolarità e della legalità dell'operato aziendale, anche in funzione preventiva.

Secondo il principio di legalità, solo i reati espressamente indicati dal decreto generano la responsabilità degli enti; si tratta, per quanto qui maggiormente interessa, di reati nei confronti della Pubblica Amministrazione (italiana, straniera o comunitaria) specificamente indicati in seguito[1], di quelli societari oggetto della revisione normativa operata dal D.Lgs. 11 aprile 2002 n. 61 (quali false comunicazioni sociali, operazioni in pregiudizio ai creditori, etc.)[2], dei reati informatici, di quelli in materia di diritti d'autori e antinfortunistica, etc., come specificatamente indicato nel seguito.
E' bene precisare che la responsabilità amministrativa dell'ente sorge quando la condotta sia stata posta in essere da soggetti legati all'ente da particolari relazioni funzionali, che sono descritte in due categorie: quella facente capo ai "soggetti in cd. posizione apicale"[3] e quella riguardante i "soggetti sottoposti all'altrui direzione"[2].
Le sanzioni previste dalla legge a carico dell'ente responsabile sono*:*

- sanzioni pecuniarie,
- sanzioni interdittive,

[1] sulla base dell'originaria previsione degli artt. 24-25 D.lgs. 231/2001

[2] mentre la legge delega 300 del 2000 già prevedeva l'estensione ai reati connessi all'ambiente ed alla infortunistica del lavoro.

[3] Precisamente interessa amministratori, anche di fatto, loro rappresentanti, direttori generali, preposti a sedi secondarie ed, in caso di organizzazione divisionale, direttori di divisione.

[2] Si intendono persone che agiscono sotto la direzione o la vigilanza delle persone esercenti le funzioni sopra indicate come apicali, in ciò comprendendosi anche soggetti non dipendenti dell'ente, quali agenti, collaboratori, consulenti.

- confisca,
- pubblicazione della sentenza.

Le sanzioni pecuniarie e la confisca vengono sempre applicate, mentre la sanzione interdittiva e la pubblicazione della sentenza sono previste solo per alcune tipologie di reato.
Sono sanzioni interdittive:

- interdizione dall'esercizio dell'attività,
- sospensione o revoca delle autorizzazioni, licenze, concessioni che siano funzionali alla commissione dell'illecito,
- divieto di contrattare con la Pubblica Amministrazione,
- esclusione dalle agevolazioni, finanziamenti, contributi e sussidi e l'eventuale revoca di quelli già concessi,
- divieto di pubblicizzare beni o servizi.

In sostituzione della interdizione dell'esercizio dell'attività, il giudice può nominare un commissario giudiziale per un periodo pari alla durata della misura che sarebbe stata applicata nei casi in cui:

- l'ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;
- l'interruzione dell'attività dell'ente può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione.

Tali sanzioni limitano notevolmente la libertà di azione dell'ente e sono generalmente temporanee. Di norma esse vengono irrogate:

- in caso di reiterazione dell'illecito;
- se l'ente ha tratto un profitto di rilevante entità;
- ove vengano evidenziate gravi carenze organizzative.

La normativa in oggetto è applicata, secondo le regole della procedura penale in quanto compatibili, nell'ambito del processo penale.
Stante l'ampia previsione normativa, il regime di responsabilità di cui si tratta, si applica anche ad ACI Informatica S.p.A..

Con riferimento specifico alla tipologia di reati, destinati a comportare il suddetto regime di responsabilità amministrativa a carico degli Enti, il Decreto, nel suo testo originario (artt. 24 e 25), si riferiva ad una serie di reati commessi nei rapporti con la P.A., dei quali si darà sintetica descrizione nella parte speciale, per completezza qui di seguito elencati:

- corruzione per un atto d'ufficio (art. 318 c.p.);
- corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
- corruzione in atti giudiziari (art. 319-ter c.p.);
- istigazione alla corruzione (art. 322 c.p.);
- concussione (art. 317 c.p.);

- peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis c.p.);
- malversazione a danno dello Stato (art. 316-bis c.p.).
- indebita percezione di erogazioni da parte dello Stato (art. 316-ter c.p.);
- truffa in danno dello Stato o di altro ente pubblico (art. 640, 2° comma, n. 1 c.p.);
- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- frode informatica (art. 640-ter c.p.).

Alcune fattispecie di reato di cui sopra sono state modificate/integrate con Legge 6 novembre 2012 n. 190 e con Legge 27 maggio 2015 n. 69. La Parte speciale del presente Modello tiene conto di tali interventi normativi.

L'art. 6 della Legge 23 novembre 2001, n. 409, recante "Disposizioni urgenti in vista dell'introduzione dell'euro", ha inserito l'art. 25-bis, che mira a punire gli Enti per i delitti previsti dal codice penale in materia di "falsità in monete, in carte di pubblico credito e in valori di bollo". Tale rubrica è stata modificata includendo anche la "falsità in strumenti o segni di riconoscimento ad opera dell'art. 15, comma 7, della Legge 23 luglio 2009, n. 99.

Nell'ambito della riforma del diritto societario, l'art. 3 del D.Lgs. 11 aprile 2002 n. 61, in vigore dal 16 aprile 2002, ha introdotto il nuovo art. 25-ter, estendendo il regime della responsabilità amministrativa degli Enti ai c.d. reati societari, così come configurati dallo stesso D.Lgs. n. 61/2002, dei quali si darà sintetica descrizione nella stessa parte speciale, mentre di seguito per completezza si ricordano:

- false comunicazioni sociali (art. 2621 c.c.);
- false comunicazioni sociali delle società quotate (art. 2622, commi 1 e 3, c.c.);
- falso in prospetto (art. 2623, commi 1 e 2, c.c.), *ora abrogato*;
- impedito controllo (art. 2625, comma 2, c.c.);
- indebita restituzione dei conferimenti (art. 2626 c.c.);
- illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- illecite operazioni sulle azioni o quote sociali proprie o della Società controllante (art. 2628 c.c.);
- operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- omessa comunicazione del conflitto d'interessi (art. 2629 bis c.c.);
- formazione fittizia del capitale (art. 2632 c.c.);
- indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- illecita influenza sull'assemblea (art. 2636 c.c.);
- aggiotaggio (art. 2637 c.c.);
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.).

Lo stesso art. 25-ter è stato poi modificato dalla Legge 28 dicembre 2005, n. 262, che ha, tra l'altro, inserito tra i reati presupposto l'art. 2629-bis c.c. in tema di omessa comunicazione del

conflitto di interessi, nonché dalle leggi 6 novembre 2012 n. 190 e 27 maggio 2015, n. 69, per quanto riguarda i reati societari.

L'art. 3 della Legge 14 gennaio 2003, n. 7, ha introdotto nel Decreto l'art. 25-quater, che inserisce nel novero dei reati presupposto per l'applicazione delle sanzioni agli Enti, i "delitti con finalità di terrorismo o di eversione dell'ordine democratico" previsti dal codice penale, dalle leggi speciali o comunque che siano stati posti in essere in violazione della convenzione internazionale per la repressione del finanziamento del terrorismo tenutasi a New York il 9 dicembre 1999.
In relazione alle attività svolte e per le modalità operative tale previsione non costituisce reato presupposto di interesse di ACI Informatica.

Successivamente, l'art. 5 della Legge 11 agosto 2003, n. 228 ha aggiunto agli altri l'art. 25-quinquies riguardante i delitti contro la personalità individuale, quali a titolo d'esempio, la riduzione in schiavitù e la tratta di persone; in materia attinente a questa, la Legge 9 gennaio 2006, n.7 ha inserito l'art. 25-quater.1 che punisce gli enti nella cui struttura è commesso il delitto di cui all'art. 583-bis c.p. (in tema di pratiche di mutilazione degli organi genitali femminili).
In relazione alle attività svolte e per le modalità operative tale previsione non costituisce reato presupposto di interesse di ACI Informatica.

Con la legge comunitaria 2004, in particolare con l'art. 9 comma 3, Legge 18 aprile 2005, n. 62 è stato aggiunto l'art. 25-sexies concernente i reati di abuso di informazioni privilegiate e di manipolazione del mercato, previsti dalla parte V, titolo I bis, capo II, del Testo Unico di cui al D.Lgs. 24 febbraio 1998, n. 58.
In relazione alle attività svolte e per le modalità operative tale previsione non costituisce reato presupposto di interesse di ACI Informatica.

Ancora, l'art. 10 della Legge 16 marzo 2006, n. 146 prevede la responsabilità degli Enti secondo il D. Lgs. 231/2001, con riferimento ad un ulteriore elenco di fattispecie, che debbono tuttavia presentare le caratteristiche del "reato transnazionale":

- associazione per delinquere (art. 416 c.p.);
- associazione di tipo mafioso (art. 416 bis c.p.);
- associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater, D.P.R. 23-1-1973 n. 43);
- associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9-10-1990 n. 309);
- disposizioni contro le immigrazioni clandestine (art. 12 commi 3, 3 bis, 3 ter e 5, D.lgs. 25-7-1998 n. 286);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.);
- favoreggiamento personale (art. 378 c.p.).

Si richiede, per qualificare come transnazionali i reati sopra elencati, (oltre alla punibilità del fatto commesso con la reclusione non inferiore nel massimo a quattro anni) il coinvolgimento di un gruppo criminale organizzato. Inoltre il reato transnazionale è tale in quanto commesso alternativamente in più di uno Stato; ovvero pianificato, diretto o controllato in uno Stato diverso da quello della effettiva commissione; commesso in un solo Stato, ma attraverso l'attività di un gruppo criminale organizzato operante in diversi Stati; ovvero commesso in un solo Stato, ma producendo effetti sostanziali in un altro Stato.

L'art. 9 della Legge 3 agosto 2007, n. 123, così come sostituito dall'art. 300 del D.Lgs. 9 aprile 2008 n. 81, ha inserito l'art. 25-septies per l'omicidio colposo e le lesioni colpose, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro. Trattasi in particolare delle seguenti norme:

- morte di una persona per colpa in violazione delle norme sulla prevenzione degli infortuni sul lavoro (art. 589 c.p.);
- lesioni e lesioni gravi per colpa in violazione delle norme sulla prevenzione degli infortuni sul lavoro (art. 590 c.p.)

Successivamente, l'art. 63 del D.Lgs. 21 novembre 2007, n. 231 ha aggiunto l'art. 25-octies che riguarda:

- ricettazione (art. 648 c.p.);
- riciclaggio (art. 648 bis c.p.);
- impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.).

Con Legge 15 dicembre 2015, n. 186 "Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché il potenziamento della lotta all'evasione fiscale - Disposizioni in materia di autoriciclaggio", entrata in vigore il 1° gennaio 2015, sono stati operati interventi modificativi ed inserito il reato di auto riciclaggio (art. 648 – ter 1. del c.p.).

In particolare, la citata legge ha apportato alcune modifiche al codice penale, sia provvedendo all'inasprimento delle pene pecuniarie per i delitti di riciclaggio e reimpiego, di cui agli articoli 648 –bis, primo comma, e 648-ter, sia introducendo all'art. 648-ter 1 il nuovo reato di autoriciclaggio, con pene diversificate a seconda della gravità del reato presupposto e con la previsione della non punibilità delle condotte nelle quali il denaro, i beni o altre utilità vengono destinati alla "mera utilizzazione o al godimento personale" .

Il citato intervento normativo ha comportato la modifica dell'art. 25-octies del D.lgs. 231/2001 includendo la nuova fattispecie tra i reati presupposto.

Ne consegue la possibilità di sanzionare gli enti i cui dipendenti (apicali e non) dopo aver commesso o concorso a commettere un delitto non colposo, impieghino, sostituiscano, trasferiscano, in attività, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione del precedente delitto, in modo da ostacolare concretamente l'identificazione della provenienza delittuosa. Ciò qualora sussista un interesse o vantaggio dell'ente stesso.

Conseguentemente, il presente Modello è integrato con l'introduzione in un apposito capitolo del reato di autoriciclaggio i cui effetti, come detto, si ripercuotono anche sulla Società.

Nell'anno 2008 i reati presupposto sono ulteriormente aumentati con l'inserimento ad opera dell'art. 7 della Legge 18 marzo 2008, n. 48 dell'art. 24 bis. Le fattispecie previste concernono:

- documenti informatici (art. 491 bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici. (art. 615 quarter c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quarter c.p.);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 quarter c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.).

Con successiva Legge 15 luglio 2009, n. 94, è stato inserito l'art. 24 ter (Delitti di criminalità organizzata) che concerne:

- associazione per delinquere (art. 416, comma 6, c.p.)
- associazione di tipo mafioso (art. 416 bis c.p.);
- scambio elettorale politico-mafioso (art. 416 ter c.p.);
- sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.);
- associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 Testo unico D.P.R. 9/10/1990 n. 309).

In relazione alle attività svolte e per le modalità operative tale previsione non costituisce reato presupposto di interesse di ACI Informatica.

Ancora, l'art. 15 della Legge 23 luglio 2009, n.99 ha aggiunto l'art. 25 novies in materia di violazione del diritto d'autore di cui agli artt. 171, 1° comma, lett. a-bis) e 3° comma, 171 bis, 171 ter, 171 septies, 171 octies della Legge 22 aprile 1941, 633.

L'art. 4 della Legge 3 agosto 2009, n. 116, ha aggiunto l'art. 25 decies in tema di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria, così come previsto all'art. 377 bis del cod. penale.
In relazione alle attività svolte e per le modalità operative tale previsione non costituisce reato presupposto di interesse di ACI Informatica.

Successivamente, il D.Lgs. n. 121, del 7 luglio 2011, ha introdotto l'art. 25 undecies (Reati ambientali). Tale disposizione richiama le seguenti fattispecie di reato, quali a titolo semplificativo e non esaustivo:

- uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727 bis c.p.);
- distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733 bis c.p.);
- attività di gestione di rifiuti non autorizzata (art. 256 del D.Lgs. 3 aprile 2006 n. 152);
- scarico di acque reflue senza autorizzazione (art. 137 del D.Lgs. 3 aprile 2006 n. 152);
- inquinamento del suolo (art. 257 del D.Lgs. 3 aprile 2006 n. 152);
- violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 del D.Lgs. 3 aprile 2006 n. 152);
- traffico illecito di rifiuti e attività organizzate per il traffico illecito di rifiuti (artt. 259 e 258 del D.Lgs. 3 aprile 2006 n. 152);
- importazione ed esportazione di specie animali e vegetali in via di estinzione (art. 1 della L. 7 febbraio 1992 n. 150);
- inquinamento doloso e colposo (artt. 8 e 9 del D.Lgs. 6 novembre 2007 n. 202).

In tale contesto si inquadra anche l'art. 192 del D.Lgs. 152/2006 in tema di divieti di abbandono e deposito incontrollato di rifiuti sul suolo e nel suolo (comma 1), nonché di immissione di rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali e sotterranee (comma 2).

Con la Legge 22 maggio 2015 n. 68 "Disposizioni in materia di delitti contro l'ambiente", è stato integrato l'art. 25 – undicies del D.Lgs. 231/01 dedicato ai reati ambientali, introducendo i seguenti illeciti:

- Inquinamento ambientale (art. 452 – bis c.p.)
- Morte o lesioni come conseguenza del delitto di inquinamento ambientale (art. 452 – ter c.p.)
- Disastro ambientale (art. 452 – quater c.p.)
- Delitti colposi contro l'ambiente (art. 452- quinquies c.p.)
- Traffico e abbandono di materiale ad alta radioattività (art. 452 – sexies c.p.)
- Impedimento del controllo (art. 452 – septies c.p.)

Ai reati sopra citati, sono collegati i seguenti articoli che regolano le seguenti situazioni:

- circostanze aggravanti (delitti associativi finalizzati al compimento di illeciti ambientali – art. 452 – octies c.p.), aggravante ambientale (art. 452 - novies c.p.), ravvedimento operoso (art. 452 - decies c.p.), confisca (art. 452 - undicies c.p.), ripristino dello stato dei luoghi (art. 452 - duodecies c.p.), omessa bonifica (art. 452 – terdecies c.p.)

Il D.Lgs. n. 109/2012 ha aggiunto l'art. 25-duodecies relativamente all'impiego di cittadini di paesi terzi il cui soggiorno è irregolare.

In pratica, è estesa la responsabilità agli Enti, quando lo sfruttamento di manodopera irregolare supera certi limiti, in termini di numero di lavoratori (maggiori di tre), età (minori in età lavorativa) e condizioni lavorative (sfruttamento), nei termini stabiliti dall'art. 22, comma 12 bis del D.Lgs. 25 luglio 1998, n. 286, cd."Testo unico dell'immigrazione".

La Legge 6 novembre 2012, n. 190 ha:

- integrato l'art. 25 del D.Lgs. 231/01 (reati nei confronti della Pubblica Amministrazione) con il nuovo art. 319-quater c.p. in materia di induzione indebita a dare o promettere utilità, nonché riformulato alcune fattispecie di reato già previste, inasprendone peraltro le pene edittali (ad esempio per il reato di concussione, di corruzione per esercizio della funzione, etc.);

- inserito all'art. 25-ter del D.Lgs. 231/01 (reati societari) il ridefinito art. 2635 c.c. (limitatamente al comma 3), in materia di corruzione tra privati (rubricandolo alla lett. s-bis).

Per quanto attiene alla trattazione specifica dei singoli reati, nella Parte Speciale sono esaminate quelle fattispecie di reato che si ritiene possano verosimilmente trovare applicazione nei confronti di ACI Informatica. Trattasi, in particolare:

- **reati nei confronti della Pubblica Amministrazione** (artt. 316 bis, 316 ter, 640, comma 2, n.1, 640 bis, 640 ter, 317, 318, 319, 319 ter, 320, 321, 322, 322 bis, 317 e 319-quarter c.p.);
- **reati societari** (artt. 2621, 2621 bis, 2621 ter, 2622, 2625, 2626, 2627, 2628, 2629, 2629-bis, 2632, 2633, 2635, 2636, 2637, 2638 c.c. e artt. 184 e 185 D.Lgs. 58/98);
- **reati in materia di lavoro** (per violazioni di norma antinfortunistiche di cui agli art. 589 c.p.);
- **reati informatici** (artt. 491 bis, 640 ter, 615 ter, 615-quater, 615 quinquies, 617 quater, 617 quinquies, 635 bis, 635 ter, 635 quater, 635 quinquies, 640 quinquies c.p.);
- **reati in materia di diritti d'autore** (art.171, comma 1, lett. a bis, comma 3, 171-bis commi 1 e 2, Legge 22 aprile 1941, n.633 e s.m.i.);
- **reati ambientali** ovvero illeciti in materia di abbandono e deposito incontrollato di rifiuti sul suolo e nel suolo, nonché di immissione di rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali e sotterranee (art. 192 del D.Lgs. 152/2006 commi 1 e 2), delitti contro l'ambiente (artt. 452-bis, 452-ter, 452-quater, 452-quinquies, 452-sexies, 452-septies c.p.);
- **reati in materia di impiego** di cittadini di paesi terzi il cui soggiorno sia irregolare (art. 22, comma 12 bis, D.Lgs. 25 luglio 1998, n. 286 e s.m.i..)
- **reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio** (artt. 648, 648 bis, 648 ter e 648 ter.1 c.p.)

Per quanto concerne, invece, le altre categorie di reati, realizzabili mediante comportamenti obiettivamente estranei alla normale attività societaria, si ritiene adeguata quale misura preventiva l'osservanza del "Codice Etico" di ACI Informatica S.p.A.

1.2. L'adozione del Modello di Organizzazione, Gestione e di Controllo quale strumento di prevenzione ed esimente della responsabilità in capo all'azienda

Il decreto[3] esonera dalla responsabilità l'ente, qualora dimostri di aver adottato ed efficacemente attuato, prima della commissione del reato, modelli di organizzazione, gestione e controllo idonei a prevenire la realizzazione degli illeciti penali considerati[4]; tale esimente opera diversamente a seconda che i reati siano commessi da soggetti in posizione apicale o soggetti sottoposti alla direzione di questi ultimi[5].
Circa l'ipotesi di reati commessi da soggetti in posizione "apicale"[6], l'esclusione della responsabilità postula essenzialmente tre condizioni:

- che sia stato formalmente adottato quel sistema di regole procedurali interne costituenti il modello;
- che il modello risulti astrattamente idoneo a *"prevenire reati della specie di quello verificatosi"*;
- che tale modello sia stato attuato *"efficacemente prima della commissione del reato"*.

Le ulteriori condizioni previste dal decreto, possono essere considerate specificazioni dei requisiti di idoneità e di efficace attuazione o rappresentare una loro conferma.
Si richiede infatti:

- che sia stato affidato il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo, nonché di specifica professionalità;
- che le persone abbiano commesso il reato eludendo fraudolentemente i modelli di organizzazione e gestione, e non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di vigilanza [7].

Nel caso di reati commessi da soggetti sottoposti, la responsabilità dell'ente scatta se vi è stata inosservanza da parte dell'azienda degli obblighi di direzione e vigilanza; tale inosservanza è esclusa se l'ente ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati.

---

[3] Artt. 6 e 7 del D. Lgs. 231/2001.
[4] Si tratta per quanto riguarda l'ente, di una causa di esclusione della punibilità..
[5] Gli effetti positivi dell'adozione di questi modelli non sono limitati all'esclusione in radice della responsabilità dell'ente in caso di una loro attuazione in via preventiva rispetto alla commissione del reato da parte di propri rappresentanti, dirigenti o dipendenti. Infatti se adottati prima dell'apertura del dibattimento di primo grado essi possono concorrere ad evitare all'ente delle più gravi sanzioni interdittive (art. 17 lett. *b)*) (e di riflesso impedire la pubblicazione della sentenza di condanna) ed inoltre possono determinare una sensibile riduzione delle pene pecuniarie (art. 12). Anche la semplice dichiarazione di voler attuare tali modelli unitamente ad altre condizioni può implicare la sospensione delle misure cautelari interdittive eventualmente adottate in corso di causa (art. 49) e la revoca delle stesse in caso di effettiva attuazione di detti modelli, sempre in presenza delle altre condizioni (artt. 49 e 50).
[6] A norma dell'art. 5 soggetti in posizione apicale sono i titolari, anche in via di fatto, di funzioni di rappresentanza, amministrazione e direzione dell'ente o di una sua unità autonoma. Destinatari della norma saranno quindi amministratori, i legali rappresentanti a qualunque titolo, i direttori generali ed i direttori di divisioni munite di autonomia finanziaria.
[7] Infatti solo la elusione o il difettoso controllo possono spiegare la commissione del reato pur in presenza di modelli astrattamente idonei ed efficaci.

Quindi, sia nel caso di reati commessi da apicali che da sottoposti, l'adozione e la efficace attuazione da parte dell'ente del modello organizzativo, gestionale e di controllo è condizione necessaria[8], per evitare la responsabilità diretta dell'ente.

[8] Si nota comunque che il giudizio circa l'efficace attuazione del modello spetta al vaglio dell'Autorità giudiziaria, che ovviamente è autonomo.

1.3. I Codici di Comportamento delle associazioni di categoria

La legge consente alle Associazioni di categoria la individuazione di linee guida generali, definiti Codici di Comportamento, per la costruzione dei modelli organizzativi; anche se la legge non riconduce espressamente a tali linee guida un valore regolamentare vincolante né presuntivo[9], è di tutta evidenza come una corretta e tempestiva applicazione di tali linee guida diventerà punto di riferimento per le decisioni giudiziali in materia[10].

Nel caso di specie sono state prese in considerazione le **linee guida** sviluppate e pubblicate da **Confindustria** per le aziende associate[11].

[9] Infatti la legge non prevede né un obbligo di adozione delle linee guida da parte degli enti aderenti alla associazione di categoria né una presunzione per i giudici in sede di giudizio.
[10] Nella previsione legislativa l'adozione di un modello di organizzazione, gestione e controllo è prospettata in termini di facoltatività, non di obbligatorietà, tant'è che la mancata adozione non è soggetta ad alcuna sanzione, ma di fatto l'adozione di un modello è obbligatoria se si vuole beneficiare dell'esimente.
[11] "Linee Guida per la Costruzione dei Modelli di Organizzazione, Gestione e Controllo *ex* D. Lgs. 231/2001" del 31.03.2008, approvate da Confindustria il 7 marzo 2002 e, da ultimo aggiornate nel marzo 2014.

2. STRUTTURA ORGANIZZATIVA DI ACI INFORMATICA

2.1. L'attività

ACI Informatica, Società a partecipazione pubblica costituita nel 1960 è una Società per azioni, interamente controllata dall'Automobile Club d'Italia (ACI), Ente pubblico non economico senza scopo di lucro, deputato a rappresentare e tutelare gli interessi generali dell'automobilismo italiano. ACI Informatica è sottoposta, ai sensi degli artt. 2497 e segg. del codice civile, all'attività di direzione e coordinamento di ACI.
E' da segnalare, inoltre, che ACI Informatica svolge le attività di seguito indicate in regime di società "*in house*", conservando comunque la natura soggetto di diritto privato (Società per azioni) che svolge un'attività di servizi in regime privatistico ed è quindi soggetto all'applicazione del D.lgs. 231/2001.
ACI Informatica provvede all'espletamento nei confronti dell'Azionista di servizi informatici, di telecomunicazione, di marketing, nonché di qualsiasi attività a supporto e nell'interesse di ACI stesso.
Più in particolare, ACI Informatica è specializzata nella progettazione, sviluppo e gestione di sistemi informativi e procedure di elaborazione automatica dei dati inerenti il settore automobilistico ed ogni altro settore di interesse dell'ACI, nonchè nella gestione della rete commerciale e nell'utilizzazione del marchio "ACI" nei confronti dei singoli Automobile Club locali.
L'attività precipua della Società, ossia la gestione informatica degli archivi e la relativa assistenza, viene svolta principalmente nei confronti di ACI e, in proporzione minima, in favore di altri soggetti collegati a quest'ultimo (Società partecipate, etc.); così come l'attività commerciale svolta dalla Direzione Sviluppo Commerciale Rete ACI (ex Divisione ACI Rete).
In sostituzione delle separate convenzioni per i servizi informatici e per i servizi di marketing che hanno cessato ogni effetto alla data del 31 dicembre 2014, è entrata in vigore la nuova convenzione, con effetto dal 1° gennaio 2015 e scadenza 31 dicembre 2023, con cui si disciplina l'affidamento *in house* dei servizi strumentali informatici e non, ivi comprese le attività di marketing e lo sviluppo della Rete ACI, su sistemi di proprietà ACI e di terzi, nonché l'esecuzione di commesse anche a favore di terzi di interesse di ACI.
ACI Informatica gestisce, quindi, alcuni sistemi informativi complessi diffusi sul territorio, quali:

- il sistema di informatizzazione del P.R.A., attraverso il collegamento in rete dei dipartimenti provinciali dell'ACI;
- il sistema di riscossione e controllo delle tasse automobilistiche per conto delle Regioni convenzionate con l'ACI;
- il sistema che consente la gestione dei soci ed il controllo della rete di vendita.

2.2. La Società e la sua organizzazione

La struttura organizzativa aziendale è articolata come segue:

- il **Presidente** del Consiglio di Amministrazione;
- in posizione trasversale rispetto al Presidente e al Consiglio di Amministrazione, è collocato l'Organismo di Vigilanza e il Collegio Sindacale;
- alla Presidenza rispondono la Direzione Affari Societari e Legali e la Funzione Internal Auditing.
- la Direzione Generale risponde alla Presidenza e sovrintende oltre che alle Direzioni Amministrative e del personale, alle Direzioni tecniche (Sviluppo Commerciale Rete ACI, Demand, Sviluppo software, Esercizio, Servizi, Applicazioni PRA e Tasse, ICT e Servizi).

L'azienda è certificata ISO 9001 e ISO 27001 (Sicurezza Informatica) ed in tale contesto dispone di un articolato Manuale della Qualità, nonché di un Manuale della Sicurezza.
La struttura dei poteri aziendali di ACI Informatica riserva sostanzialmente all'intero Consiglio di Amministrazione gli indirizzi e gli orientamenti cui ispirarsi per le strategie di intervento della Società; l'approvazione del bilancio e del budget; l'approvazione dei contratti comportanti impegni superiori ai limiti di spesa attribuiti al Direttore Generale. Gli Organi societari esercitano i loro poteri nel rispetto ed in coerenza con i principi generali di governo definiti ACI, unico socio, ed esplicitati nel documento "Regolamento di *Governance* delle società controllate da ACI" del 16 marzo 2011.

Al Presidente è riservata, tra l'altro, la rappresentanza della Società, anche in giudizio.

Ad altri responsabili aziendali sono conferiti sostanzialmente i necessari poteri di gestione.
L'articolazione delle deleghe aziendali è riportata in specifico allegato al presente Modello.

3. IL MODELLO DI ACI INFORMATICA

3.1. Finalità, Elaborazione ed Approvazione del Modello

Sebbene l'adozione del Modello rappresenti una facoltà e non un obbligo, ACI Informatica S.p.A. ha deciso di procedere con l'elaborazione e costruzione del presente Modello, al duplice fine di adeguarsi alle finalità di prevenzione indicate dal Legislatore e di proteggere, dagli effetti negativi derivanti da una inopinata applicazione di sanzioni, gli interessi dei Soci, degli Amministratori e, in ultima analisi, di tutta l'azienda nel suo insieme.
ACI Informatica S.p.A. ritiene inoltre che l'adozione del Modello costituisca una opportunità importante di verifica, revisione ed integrazione dei processi decisionali ed applicativi aziendali, nonché dei sistemi di controllo dei medesimi, rafforzando l'immagine di correttezza e trasparenza alla quale si è sempre orientata l'attività aziendale.
A tal fine il Consiglio di Amministrazione, avvalendosi dell'assistenza e consulenza delle strutture aziendali nonché di professionisti esterni, ha dato avvio nel 2003 al lavoro di analisi e di preparazione del Modello, lavoro che si è articolato nelle seguenti fasi:

- Identificazione delle aree di rischio aziendali; questa fase ha comportato l'identificazione dei processi operativi nelle varie aree di attività aziendale, mediante l'esame della documentazione aziendale di rilievo ed interviste mirate con i soggetti chiave nell'ambito della struttura aziendale, nonché la verifica di tali processi operativi alla luce delle fattispecie di illecito previste dalla normativa di cui si tratta (fase di **mappatura dei processi a rischio**).
- Verifica delle procedure operative e di controllo esistenti a livello aziendale ed identificazione delle azioni di miglioramento, individuando modifiche ed integrazioni necessarie/opportune (fase di ***gap analysis***).
- Individuazione dei soggetti ai quali conferire l'incarico di **Organismo di Vigilanza** e di *Compliance Manager.*
- **Predisposizione del Modello** e di alcuni rilevanti componenti autonomi, quali il Codice Etico, prevedendo l'aggiornamento progressivo e periodico delle singole procedure e protocolli aziendali operativi.

Successivamente, così come previsto al paragrafo 3.3, si è provveduto ad avviare le attività di aggiornamento del Modello in merito a:

- integrazione delle aree sensibili rilevate nell'attività di ACI Informatica rispetto a quelle presenti nella prima versione del Modello;
- formalizzazione di specifici standard di controllo per le aree sensibili;
- verifica dell'allocazione, all'interno della struttura organizzativa di ACI Informatica, delle responsabilità relative ai processi sensibili individuati rispetto ai reati contemplati dal Modello;
- aggiornamento della Parte Speciale reati e rischi con l'introduzione dei nuovi reati presupposto inseriti nel Decreto di approvazione del Modello;

- aggiornamento delle aree sensibili già mappate per verificare se vi siano rischi specifici per il compimento di reati di recente introduzione e, sempre alla luce delle innovazioni legislative, verifica del possibile rinvenimento di nuove aree di rischio.

3.2 Obiettivi del Modello

Con l'adozione del Modello, ACI Informatica S.p.A. si pone l'obiettivo principale di disporre di un sistema strutturato di procedure e controlli che riduca, tendenzialmente eliminandolo, il rischio di commissione dei reati rilevanti, e degli illeciti in genere, nei processi a rischio.
Infatti la commissione dei reati rilevanti, e dei comportamenti illeciti in genere, è comunque contraria alla volontà di ACI Informatica S.p.A., come dichiarato nel Codice Etico e qui confermato, e comporta sempre un danno per la Società, anche se essa possa apparentemente ed erroneamente essere considerata nell'interesse o a vantaggio della medesima.
Il Modello, quindi, predispone gli strumenti per il monitoraggio dei processi a rischio, per una efficace prevenzione dei comportamenti illeciti, per un tempestivo intervento aziendale nei confronti di atti posti in essere in violazione delle regole aziendali, e per l'adozione dei necessari provvedimenti disciplinari di sanzione e repressione.

3.3 Verifica ed Aggiornamento del Modello

Il Modello è stato espressamente costruito per ACI Informatica S.p.A., sulla base della situazione concreta delle attività aziendali e dei processi operativi. Esso è uno strumento vivo e corrispondente alle esigenze di prevenzione e controllo aziendale; in conseguenza, è necessario procedere alla periodica verifica della rispondenza del modello alle predette esigenze, provvedendo quindi alle integrazioni e modifiche che si rendessero di volta in volta necessarie.
La verifica si rende inoltre necessaria ogni qualvolta intervengano modifiche organizzative aziendali significative, particolarmente nelle aree già individuate come a rischio.
Le verifiche sono svolte in collaborazione con l'Organismo di Vigilanza e, all'occorrenza, della assistenza di professionisti esterni. Le integrazioni e le modifiche che si rendessero di volta in volta necessarie o opportune sono proposte al Consiglio di Amministrazione che è competente e responsabile dell'adozione delle integrazioni e modifiche al Modello (Cfr. art. 6 comma 1 lett. A).
La modifica/integrazione degli allegati, di cui al punto 16, non comporta l'aggiornamento del Modello, salvo le ipotesi di modifiche significative, valutate di volta in volta, dell'organizzazione aziendale tali da incidere sull'operatività del Modello stesso.
L'aggiornamento e/o adeguamento del Modello è quindi principalmente effettuato in occasione di: i) novità legislative con riferimento alla disciplina della responsabilità degli enti per gli illeciti amministrativi dipendenti da reato; ii) revisione periodica del Modello anche in relazione a cambiamenti significativi della struttura organizzativa dell'ente e/o delle procedure aziendali; iii) significative violazioni del Modello e/o esiti di verifiche sulla sua efficacia o di esperienze di pubblico dominio del settore.

4. L'ORGANISMO DI VIGILANZA INTERNO

4.1. Individuazione dell'Organismo di Vigilanza

La normativa in questione impone, onde poter fruire dei benefici previsti dall'adozione ed attuazione del Modello, di affidare ad un organismo dell'ente il compito di vigilare sul funzionamento e sulla osservanza del Modello, nonché di curarne l'aggiornamento, attribuendo al medesimo organismo, ove non già presenti, autonomi poteri di iniziativa e controllo.
ACI Informatica S.p.A. ritiene che la costituzione di un organo collegiale apposito, al quale affidare tale funzione, possa meglio rispondere alle esigenze di autonomia e controllo richieste dalla normativa.

Il Consiglio di Amministrazione ha perciò provveduto alla costituzione *ad hoc* di un Organismo di Vigilanza di tipo collegiale, composto da due soggetti esterni alla Società, dei quali almeno uno abbia titolo di Revisore Contabile.

4.2. Poteri e Compiti dell'Organismo di Vigilanza

All'Organismo di Vigilanza sono attribuiti i seguenti poteri:
- chiedere informazioni in autonomia a tutto il personale dirigente e dipendente della Società, nonché a collaboratori e consulenti esterni alla stessa, avendo accesso alla documentazione relativa all'attività svolta nelle aree a rischio;
- ricevere periodicamente informazioni dai responsabili delle aree di rischio;
- proporre eventualmente l'applicazione delle sanzioni tra quelle previste dal sistema sanzionatorio in vigore per la prevenzione dei reati *ex* D. Lgs. 231/2001;
- avvalersi di consulenti esterni per il compimento di operazioni o verifiche tecniche e del supporto di eventuali funzioni della Società che si rendessero necessari, ciò anche con riferimento all'area dei reati informatici;
- proporre le modifiche ed integrazioni per l'aggiornamento del Modello.

Nell'ambito di tali generali poteri, l'Organismo di Vigilanza svolge i seguenti compiti:

- effettua periodicamente, di propria iniziativa o su segnalazioni da chiunque ricevute, verifiche su determinate operazioni o specifici atti posti in essere all'interno dell'azienda o dei soggetti esterni coinvolti nei processi a rischio. Nel corso di tali verifiche all'Organismo di Vigilanza dovrà essere consentito l'accesso a tutta la documentazione che ritenga necessaria per l'effettuazione della verifica stessa. Al termine di ogni verifica deve essere redatto un verbale che deve essere sottoposto per conoscenza ai vertici aziendali (Presidente o Assemblea);

- coordina con la Direzione Generale competente la formazione necessaria per la divulgazione del Modello e dei protocolli preventivi sulle attività a rischio al personale della Società e ad eventuali collaboratori esterni in stretto contatto con la Società stessa

(in tale attività può essere eventualmente supportato da ulteriori funzioni interne o da collaboratori esterni);

- predispone e mantiene aggiornata tutta la documentazione inerente il Modello e la documentazione necessaria al fine di garantire il funzionamento del Modello stesso (es. manuali, procedure, istruzioni). Predispone inoltre e tiene aggiornato un apposito quadro sinottico in cui vengono individuati tutti i flussi informativi che interessano l'Organismo di Vigilanza;
- riceve da parte dei diversi responsabili aziendali la documentazione inerente le attività a rischio e la conserva secondo le tempistiche e le modalità disciplinate nel quadro sinottico sopra menzionato;
- raccoglie e formalizza, secondo modalità standardizzate, e conserva eventuali informazioni e/o segnalazioni ricevute con riferimento alla commissione di reati (effettive o sospettate) o a violazioni del Codice Etico o del Modello. Le violazioni commesse vengono sottoposte ai vertici aziendali (Presidente o Assemblea) unitamente ad un'eventuale proposta di sanzione disciplinare, individuata in coordinamento con il Presidente;
- semestralmente redige una relazione scritta dell'attività svolta, del grado in cui il modello è attuato e di eventuali progetti da attivare per il miglioramento del modello stesso, e la sottopone ai vertici aziendali (Consiglio di Amministrazione).

Nella seduta del Consiglio di Amministrazione del 29 luglio 2015, è stato approvato il Regolamento dell'Organismo di Vigilanza, volto a disciplinare la composizione, il funzionamento e le procedure dell'Organismo stesso, garantendo un corretto funzionamento del Modello.

4.3. Reporting dell'Organismo di Vigilanza

L'Organismo di Vigilanza riferisce periodicamente ed all'occorrenza in merito all'attuazione del Modello e propone le modifiche ed integrazioni di volta in volta ritenute necessarie.
Sono assegnate all'Organismo di Vigilanza due linee di *reporting*:

- la prima prevede un *reporting* su base continuativa al Presidente;
- la seconda, su base periodica semestrale, nei confronti del Consiglio di Amministrazione.

In caso di violazione del Modello da parte degli Amministratori, l'Organismo di Vigilanza dovrà riportare direttamente e senza indugio all'intero Consiglio ed al Collegio Sindacale.

Stante la necessità di garantire l'indipendenza dell'Organismo di Vigilanza, laddove esso ritenga che per circostanze gravi e comprovabili sia necessario riportare direttamente all'Assemblea dei Soci informazioni che riguardano violazioni del Modello da parte del Consiglio di Amministrazione e del Collegio Sindacale, esso è autorizzato a farlo alla prima Assemblea utile.

Inoltre, il Consiglio di Amministrazione ha adottato alcune forme di tutela nei confronti dell'Organismo di Vigilanza per evitare rischi di ritorsioni a suo danno per l'attività svolta: in particolare è stato previsto che ogni atto modificativo o interruttivo del rapporto della Società con i soggetti che compongono l'Organismo di Vigilanza sia sottoposto alla preventiva approvazione del Consiglio di Amministrazione e, in caso di approvazione degli interventi modificativi o interruttivi adottati senza la unanimità di decisione, sia data adeguata informazione all'Assemblea dei Soci, alla prima occasione utile.

5. DIFFUSIONE DEL MODELLO E FORMAZIONE DELLE RISORSE

5.1. Nei confronti degli Apici e dei Dipendenti

Il presente Modello è oggetto di comunicazione a tutti i soggetti aziendali, secondo modalità e tempi definiti d'intesa con la Presidenza, tali da favorire la massima conoscenza delle regole comportamentali che l'azienda ha ritenuto di darsi.
Il Modello è disponibile e visionabile nella sua interezza presso il sito *intranet* aziendale.
L'Organismo di Vigilanza inoltre, d'intesa con la Direzione Generale, definisce programmi di formazione/informazione dei soggetti aziendali in funzione della qualifica ricoperta, dei poteri e delle deleghe attribuite, nonché del livello di rischio dell'area aziendale nella quale operano.

5.2. Nei confronti dei Fornitori e Collaboratori

La Società provvede all'informazione ai Fornitori e Collaboratori che operassero in aree e con attività a rischio, della esistenza delle regole comportamentali e procedurali di interesse.
Nei rapporti contrattuali con tali soggetti sono inserite apposite clausole di tutela dell'azienda in caso di contravvenzione alle predette regole comportamentali e procedurali.

6. SISTEMA DISCIPLINARE

6.1. Obiettivi del sistema disciplinare

Come espressamente richiesto dalla legge, un adeguato sistema sanzionatorio, commisurato alla violazione e con prioritario fine preventivo, è stato previsto per la violazione delle norme del Codice Etico, nonché delle procedure previste dal Modello.
L'applicazione delle sanzioni disciplinari prescinde dall'esito (o dall'avvio stesso) di un procedimento penale in capo alla Società, in quanto tali violazioni ledono il rapporto di fiducia instaurato con la Società, la quale, si ricorda, con l'adozione del Modello, persegue l'obiettivo di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela del patrimonio aziendale e della propria immagine nel mercato.

6.2. Struttura del sistema disciplinare

6.2.1. nei confronti dei Dipendenti

La violazione delle singole regole comportamentali del Codice Etico e del Modello costituisce illecito disciplinare, con gli effetti previsti dalla legge e dalla Contrattazione collettiva nazionale ed aziendale applicabile. I provvedimenti disciplinari applicabili, in ordine crescente di gravità, consistono, conformemente alle norme sopra richiamate, in

- richiamo verbale,
- ammonizione scritta,
- multa,
- sospensione dal lavoro e dalla retribuzione fino ad un massimo di 3 giorni,
- licenziamento.

I provvedimenti disciplinari sono irrogati, nel rispetto delle norme procedurali e sostanziali vigenti, dalla Direzione Generale su richiesta o segnalazione dell'Organismo di Vigilanza.

6.2.2. nei confronti dei Dirigenti

In caso di violazione, da parte di dirigenti, delle singole regole comportamentali del Codice Etico e del Modello, si provvederà ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro.
Quale specifica sanzione disciplinare, in considerazione della violazione del vincolo fiduciario che presiede alla natura del rapporto dirigenziale è prevista la possibilità del licenziamento del dirigente.
I provvedimenti disciplinari verso i dirigenti, proposti dal Direttore Generale, sono irrogati, nel rispetto delle norme procedurali e sostanziali vigenti, dal Presidente su richiesta o segnalazione dell'Organismo di Vigilanza.

Dell'emanazione di provvedimenti disciplinari verso i dirigenti deve essere informato il Consiglio di Amministrazione.

6.2.3. nei confronti degli Amministratori e dei Sindaci

In caso di violazioni commesse da parte di uno o più componenti del Consiglio di Amministrazione o del Collegio Sindacale, il Consiglio di Amministrazione e il Collegio Sindacale applicheranno adeguati provvedimenti, che possono consistere, in relazione alla gravità del comportamento, in:

- censura scritta a verbale,
- sospensione del diritto alla indennità di carica fino ad un massimo corrispondente a tre riunioni dell'organo,
- segnalazione all'Assemblea dei Soci per gli opportuni provvedimenti.

6.2.4. nei confronti dei Fornitori, Collaboratori e dei Partners commerciali

Le violazioni, da parte dei soggetti terzi, Fornitori, Collaboratori o Partners commerciali della Società, delle regole del Codice Etico e del presente Modello, comporta l'attivazione obbligatoria, su richiesta o segnalazione dell'Organismo di Vigilanza, delle clausole contrattuali sanzionatorie inserite nei relativi contratti.
Resta salvo il diritto dell'azienda a chiedere il risarcimento dei danni.

7. IL CODICE ETICO

L'adozione da parte della Società di principi etici rilevanti ai fini della trasparenza e correttezza dell'attività aziendale ed utili ai fini della prevenzione dei reati *ex* D.Lgs. 231/2001 costituisce un elemento essenziale del sistema di controllo preventivo.
Tali principi sono inseriti nel Codice Etico, che è parte integrante del presente Modello. Esso mira a raccomandare, promuovere o vietare determinati comportamenti, al di là ed indipendentemente da quanto previsto a livello normativo, definendo i principi di "deontologia aziendale" che la Società riconosce come propri e sui quali richiama l'osservanza di tutti i destinatari.

PARTE SPECIALE

8. REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE

8.1. I reati nei confronti della Pubblica Amministrazione richiamati dagli artt. 24 e 25 del D.Lgs. 231/2001

Si riporta, qui di seguito, una breve descrizione dei contenuti degli articoli del codice penale che disciplinano i reati nei confronti della Pubblica Amministrazione previsti nel corpo del D.Lgs. 231/2001.

Malversazione a danno dello Stato (art. 316-bis c.p.)
La norma punisce chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità.

Indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.)
La norma punisce chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee.

Truffa in danno dello Stato o di altro ente pubblico (art. 640, comma 2, n. 1, c.p.)
La norma punisce chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)
La norma punisce chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.

Frode informatica (art. 640-ter c.p.)
La norma punisce chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto.

Il reato è trattato anche nel capitolo 11 concernente i reati informatici richiamati dall'art. 24 del D.lgs. 231/01.

Concussione (art. 317 c.p.)
La norma punisce il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri costringe taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro o altra utilità.

Corruzione per l'esercizio della funzione (art. 318 c.p.)
La norma punisce il pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, , per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa.

Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)
La norma punisce il pubblico ufficiale che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa.

Corruzione in atti giudiziari (art 319-ter c.p.)
La norma punisce i reati di corruzione commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo.

Induzione indebita a dare o promettere utilità (art. 319 quater c.p.)

La norma punisce, salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

E' punito altresì chi da o promette denaro o altra utilità.

Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.)
Le disposizioni degli articoli 318 e 319 del codice penale si applicano anche se il fatto è commesso da persona incaricata di un pubblico servizio;

Pene per il corruttore (art. 321 c.p.)
Le pene stabilite nel primo comma dell'articolo 318, nell'articolo 319, nell'articolo 319-*bis*, nell'articolo 319-*ter* e nell'articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche, per disposizione della norma qui in esame, a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro o altra utilità.
In altri termini, il reato di corruzione è un reato a concorso necessario, in cui vengono puniti sia il corrotto che il corruttore.

Istigazione alla corruzione (art. 322 c.p.)
La norma punisce chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizioper l'esercizio delle sue funzioni o dei suoi

poteri , per indurlo a compiere, omettere o ritardare un atto del suo ufficio, ovvero indurlo a compiere un atto contrario ai suoi doveri, qualora l'offerta o la promessa non sia accettata.

Le pena previste si applicano al pubblico ufficiale, o all'incaricato di un pubblico servizio, che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri anche da parte di un privato per le finalità indicate dall'articolo 319.

Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e degli esteri (art. 322-bis c.p.)

La norma estende la punibilità dalle fattispecie degli artt. 314, 316, da 317 a 320 e 322, terzo e quarto comma, ai membri della Commissione delle Comunità europee e di funzionari delle Comunità europee e degli esteri.

8.2. Sanzioni in materia di reati nei confronti della Pubblica Amministrazione previste dal D.lgs. 231/01

Articolo 24 - *malversazione a danno dello Stato* (art. 316-bis c.p.)*, indebita percezione di erogazioni a danno dello Stato* (art. 316-ter c.p.)*, truffa* (art. 640, comma 2, n. 1, c.p.)*, truffa aggravata per il conseguimento di erogazioni pubbliche* (art. 640-bis c.p.), *frode informatica* (art. 640-ter c.p.):

- sanzioni pecuniarie: fino a cinquecento quote; se l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità la sanzione pecuniaria va da duecento a seicento quote;
- sanzioni interdittive: divieto di contrattare con la P.A.; esclusione da agevolazioni, finanziamenti o contributi: divieto di pubblicizzare beni o servizi.

Art. 25 Concussione, induzione indebita a dare o promettere utilità *(rubrica così modificata dall'art. 1, comma 77, lettera a),n.1, legge n. 190 del 2012).*

Articolo 25, primo comma - *corruzione per l'esercizio della funzione* (art. 318 c.p.)*, pene per il corruttore* (art. 321 c.p.), *istigazione alla corruzione* (art. 322, 1° e 3° comma, c.p.), *corruzione di persona incaricata di pubblico servizio* (art. 320 c.p.), *peculato, concussione, induzione indebita di dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle comunità europee e di Stati esteri* (art. 322-bis c.p.)*:*

- sanzioni pecuniarie: fino a duecento quote.

Articolo 25, secondo comma - *corruzione per un atto contrario ai doveri d'ufficio* (art. 319 c.p.)*, corruzione in atti giudiziari* (art 319-ter, 1° comma, c.p.)*, pene per il corruttore* (art. 321 c.p.), *istigazione alla corruzione* (art. 322, 2° e 4° comma, c.p.):

- sanzioni pecuniarie: pena base da duecento a seicento quote; se l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità la sanzione pecuniaria va da trecento a ottocento quote.

- sanzioni interdittive (per una durata non inferiore ad un anno): interdizione dall'esercizio dell'attività, sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, esclusioni da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, divieto di pubblicizzare beni o servizi.

Articolo 25, terzo comma – *concussione* (art. 317 e 319-bis c.p.) *corruzione per un atto contrario ai doveri d'ufficio aggravata* (art. 319 e 319-bis, c.p.)*, corruzione in atti giudiziari* (art 319-ter, 2° comma, c.p.)*, induzione indebita a dare o promettere utilità* (art.319-quater), *pene per il corruttore* (art. 321 c.p.):

- sanzioni pecuniarie: da trecento a ottocento quote quando dal fatto l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità e anche quando tali delitti sono stati commessi dalle persone indicate negli articoli 320 e 322-bis.

- sanzioni interdittive (per una durata non inferiore ad un anno): interdizione dall'esercizio dell'attività, sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, esclusioni da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, divieto di pubblicizzare beni o servizi.

8.3. Le attività, individuate come sensibili ai fini del D.Lgs. 231/2001 con riferimento ai reati nei rapporti con la Pubblica Amministrazione

L'art. 6, comma 2, lett. a) del D.Lgs. 231/2001 indica, come più volte ricordato, tra gli elementi essenziali del modello di organizzazione e di gestione, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.Lgs. 231/2001.

L'analisi dei processi aziendali di ACI Informatica ha consentito di individuare le attività che potrebbero essere considerate sensibili con riferimento al rischio di commissione di reati richiamati dagli artt. 24 e 25 del Decreto. Le attività sensibili identificate sono qui di seguito riportate.

1. ***Gestione dei rapporti in convenzione con ACI:*** il processo riguarda l'elaborazione, la negoziazione e la stipulazione dei rapporti contrattuali tra ACI Informatica S.p.A. e l'ente Automobile Club Italia (ACI) e che regolano le attività relative allo svolgimento di servizi informatici e commerciali per l'ACI e per la federazione degli Automobile Club Provinciali e per la rete delle delegazioni a marchio ACI presenti sul territorio nazionale.

La Convenzione in essere con ACI affida ad ACI Informatica i seguenti servizi strumentali :

- ✓ conduzione funzionale e gestione applicazioni;
- ✓ conduzione operativa e assistenza sistemistica delle infrastrutture ICT centrali e periferiche;
- ✓ servizi professionali specialistici a supporto di ACI;
- ✓ servizi non informatici;
- ✓ servizi per la gestione e lo sviluppo della Rete commerciale ACI;
- ✓ servizi MEV (Major Release) e sviluppo di nuove funzioni/applicazioni.

2. ***Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con enti della P.A. per la vendita di servizi mediante trattative private e gare ad evidenza pubblica:*** il processo riguarda la negoziazione e la stipulazione di contratti attraverso i quali ACI Informatica si propone agli enti della Pubblica Amministrazione al fine di:
   - vendere i propri servizi informatici;
   - realizzare accordi per la commercializzazione di prodotti/servizi presso i punti vendita ACI dislocati sul territorio nazionale.

3. ***Gestione di software pubblici o forniti da terzi per conto di soggetti pubblici per comunicare con la P.A.:*** il processo consiste nell'utilizzo di software pubblici per la trasmissione al Ministero delle Finanze delle dichiarazioni fiscali (per mezzo del sistema telematico ENTRATEL di proprietà del Ministero delle Finanze) e per la trasmissione all'INPS di denunce contributive, relative ad adempimenti previdenziali e ritenute a carico di ACI Informatica e del personale aziendale, mediante software UNIEMENS – aggregato e individuale, di proprietà dell'ente INPS.

4. ***Gestione del Contenzioso:*** il processo concerne la gestione dei procedimenti stragiudiziali e giudiziali attraverso i quali ACI Informatica giunge alla risoluzione delle controversie afferenti diverse materie (lavoro dipendente, rapporti di fornitura, gare ad evidenza pubblica), ivi compresi i criteri e le modalità di selezione del professionista esterno a cui affidare la difesa in giudizio della società.

5. ***Gestione dei rapporti con le Autorità pubbliche relativi ad attività di ispezione e controllo:*** si tratta dell'attività concernente la gestione dei rapporti con Soggetti Pubblici per aspetti riguardanti l'esecuzione di verifiche ed accertamenti in relazione agli adempimenti connessi all'applicazione di leggi e regolamenti relativi a: i) sicurezza ed igiene sul lavoro; ii) previdenza ed assistenza dei lavoratori dipendenti; iii) fisco e tributi.

6. ***Gestione degli Acquisti e del Patrimonio:*** si tratta dell'attività di negoziazione/ stipulazione e/o esecuzione di contratti per l'acquisizione di beni e servizi ai quali si perviene mediante procedure aperte, ristrette, negoziate o altre procedure.

Ci si riferisce, in particolare, ai processi di: i) acquisti di beni e servizi mediante procedure negoziate; ii) acquisti di beni e servizi mediante procedure ad evidenza pubblica; iii) gestione del patrimonio.

7. ***Gestione dei Flussi Finanziari:*** l'attività si riferisce alla gestione ed alla movimentazione delle risorse finanziarie relative all'attività di impresa.

8. ***Gestione delle Risorse Umane:*** si tratta delle attività relative alla gestione della selezione ed assunzione del personale, comprese le categorie protette, nonché della definizione e gestione del sistema premiante (MBO).

8.4. Il sistema dei controlli

Il sistema dei controlli identificato dalla Società prevede il rispetto di specifici principi di controllo relativi alle attività sensibili.

Le disposizioni e gli accorgimenti tecnici richiamati nel modello, sono di carattere meramente difensivo e sono volti ad accertare la commissione di eventuali comportamenti illeciti e non anche a consentire un controllo qualitativo-quantitativo sulla prestazione resa dai lavoratori.

8.4.1. Definizione del sistema dei controllo

I Principi di controllo posti a base degli strumenti e delle metodologie utilizzate possono essere classificati come di seguito indicato:

- **Regolamentazione**: si richiede l'esistenza di regole, linee guida, procedure formalizzate, o prassi consolidate, idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili, nonché modalità di archiviazione della documentazione rilevante.
- **Tracciabilità**: si richiede la documentabilità delle attività sensibili. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile *ex post*, anche tramite appositi supporti documentali.
- **Segregazione delle attività**: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- **Poteri autorizzativi e di firma**: si richiede la presenza dei seguenti requisiti in merito ai poteri autorizzativi e di firma: i) coerenza con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) definizione chiara e conoscenza all'interno della Società.
- **Codice Etico:** si richiede il rispetto del Codice Etico, nei suoi principi generali e con riferimento alle previsioni relative ad attività specifiche, già indicate nella parte speciale del modello organizzativo nelle sezioni dedicate ai reati presupposto.

8.4.2. Applicazione dei principi di controllo

Il sistema dei controlli prevede presidi specifici per ciascuna delle attività sopra elencate.

1. Gestione dei rapporti in convenzione con ACI

- *Regolamentazione*: sono individuati: i) ruoli, responsabilità e modalità operative connesse alle attività di definizione e negoziazione delle Convenzioni con ACI; ii) ruoli, responsabilità e modalità operative di verifica, rendicontazione e fatturazione dell'attività svolta in relazione alle Convenzioni: iii) ruoli, responsabilità e modalità operative connesse alla gestione delle attività della Convenzione.
- *Tracciabilità*: è prevista l'archiviazione delle comunicazioni intercorse fra ACI Informatica ed ACI in occasione della elaborazione dei contenuti contrattuali e della stipulazione di Convenzioni, delle lettere di offerta, dei Piani di Attività, dei documenti di controllo commessa, delle rendicontazioni e delle relative fatturazioni.
- *Segregazione dei compiti:* è prevista, per le attività di stipulazione di accordi e convenzioni con ACI, la separazione delle funzioni di autorizzazione, demandata al Consiglio di Amministrazione e sottoscritta dal Presidente, di esecuzione, affidata ad uno specifico Gruppo di Lavoro tecnico/amministrativo. In relazione alla gestione e alla rendicontazione delle Convenzioni è prevista la separazione delle funzioni di autorizzazione, demandata alla Direzione Generale, di esecuzione, demandata alla struttura tecnica e amministrativa e di controllo, esercitato dalla Direzione Generale e dalla Direzione Amministrazione, Finanza e Controllo.
- *Poteri autorizzativi e di firma:* è previsto che siano autorizzati ad intrattenere rapporti con ACI, solo i soggetti muniti di apposita procura o comunque specificamente individuati mediante atti di ripartizione interna di compiti operativi.
- *Codice Etico*: è richiesta l'osservanza dei principi indicati nel capitolo II ("Comportamento nella gestione degli affari", paragrafo A).

2. Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con enti della P.A. per la vendita di servizi mediante trattative private e gare ad evidenza pubblica

- *Regolamentazione*: sono individuati ruoli e responsabilità dei diversi attori coinvolti nei processi di: i) vendita di servizi informatici, con particolare riferimento alle attività di contatto con la clientela, predisposizione e sviluppo delle offerte commerciali, riesame ed approvazione delle offerte, contrattualizzazione del rapporto commerciale con il cliente; ii) vendita di servizi commerciali e di marketing, con particolare riferimento alle attività di individuazione della controparte commerciale, , contatto con il cliente e contrattualizzazione del rapporto commerciale.
- *Tracciabilità*: è previsto che: i) sia posta la massima attenzione affinché informazioni e dati indicati nella documentazione siano corretti e veritieri; ii) i processi siano documentati; iii)

la documentazione sia archiviata. E' inoltre prevista la conservazione in archivio della seguente documentazione inerente la vendita di servizi informatici e commerciali: contratti di vendita, richieste del cliente, allegati tecnici all'Offerta, lettere di offerta, comunicazioni di accettazione.

- *Segregazione dei compiti*: è prevista la separazione delle funzioni di autorizzazione, esecuzione e controllo, attribuite alle seguenti funzioni/ai seguenti soggetti: i) vendita di servizi informatici: l'autorizzazione è demandata ai soggetti muniti di apposita delega secondo i relativi limiti, l'esecuzione è demandata alla struttura aziendale responsabile dell'offerta, il controllo è demandato alla Direzione Amministrazione, Finanza e Controllo e alle Strutture Tecniche interessate; ii) vendita di servizi commerciali e di marketing: l'autorizzazione è demandata ai soggetti muniti di apposita delega secondo i relativi limiti, l'esecuzione alla Direzione Sviluppo Commerciale Rete ACI, il controllo alla Direzione Generale.
- *Poteri autorizzativi e di firma*: è richiesto che siano autorizzati ad intrattenere rapporti con acquirenti appartenenti alla Pubblica Amministrazione, o comunque con soggetti qualificabili come "pubblici" o "incaricati di pubblico servizio", solo i soggetti muniti di apposita procura (Presidente, Direttore Generale, altri soggetti delegati, nei limiti delle loro procure).
- *Codice Etico*: è richiesta l'osservanza dei principi di condotta indicati nel capitolo II ("Comportamento nella gestione degli affari", paragrafi B, D, E, F).

3. *Gestione di software pubblici o forniti da terzi per conto di soggetti pubblici per comunicare con la P.A.*

- *Regolamentazione*: sono individuati i soggetti deputati alla gestione dei software necessari all'invio dei dati al Ministero delle Finanze e all'INPS e le modalità di estrazione dei dati e di verifica, approvazione, caricamento a sistema ed invio delle dichiarazioni ai soggetti pubblici competenti.
- *Tracciabilità*: la tracciabilità del processo di trasmissione in esame, è garantita dalla registrazione ed archiviazione della seguente documentazione: dichiarazioni fiscali approvate e inviate, ricevute delle trasmissioni, modulo DM10, ricevute delle trasmissioni, nonché dei fogli di controllo della corrispondenza fra le dichiarazioni inviate e le operazioni di estrazione dati eseguite.
- *Segregazione dei compiti*: il protocollo prevede: i) in relazione alla trasmissione di dichiarazioni fiscali mediante software pubblico, la separazione dei compiti di autorizzazione all'invio delle dichiarazioni, rilasciata dal Collegio Sindacale e dalla Direzione Generale, di esecuzione dell'estrazione dati dai file aziendali, affidata alla struttura competente, di verifica/supervisione della Direzione Amministrazione, Finanza e Controllo; ii) in relazione alla trasmissione di dati relativi al trattamento pensionistico mediante software pubblico la separazione dei compiti di autorizzazione, fornita dalla Direzione Generale, di esecuzione, affidata all'Area Gestione Risorse Umane, di controllo, affidato alla Direzione del Personale.
- *Poteri autorizzativi e di firma:* è previsto che siano autorizzati ad intrattenere rapporti con soggetti appartenenti alla Pubblica Amministrazione solo i soggetti muniti di apposita

procura (Presidente, Direttore Generale) o comunque specificamente individuati mediante atti di ripartizione interna di compiti operativi.

- *Codice Etico*: è richiesta l'osservanza delle indicazioni comportamentali previste dai capitoli II ("Comportamento nella gestione degli affari", paragrafo E), IV ("Trattamento di informazioni interne").

4. *Gestione del Contenzioso*

- *Regolamentazione*: sono individuati i soggetti deputati alla gestione dei contenziosi giudiziali o stragiudiziali o procedimenti arbitrali.
- *Tracciabilità*: è prevista la conservazione di tutta la documentazione processuale e di tutti gli atti inerenti contenziosi aperti/chiusi, in particolare istanze ricevute, procure, note difensive, atti giudiziari, con divieto di cancellare o distruggere i documenti archiviati in modo che sia garantita la tracciabilità/verificabilità *ex post* dell'attività svolta.
- *Segregazione dei compiti*: è prevista una separazione dei compiti come di seguito indicato: i) contenzioso giudiziale: l'autorizzazione è demandata al Presidente, l'esecuzione è demandata al consulente legale esterno sotto la supervisione e controllo del Responsabile dell'Unità Organizzativa Societario e Legale; ii) contenzioso stragiudiziale: l'autorizzazione è demandata al Presidente, al Direttore Generale; l'esecuzione degli atti è di competenza del responsabile della struttura interessata dalla controversia, il controllo è rimesso al Responsabile della Direzione Societario e Legale.
- *Poteri autorizzativi e di firma:* il Presidente dispone delle procure alle liti per quanto concerne il contenzioso giudiziale. E' previsto che siano autorizzati ad intrattenere rapporti con soggetti appartenenti alla Pubblica Amministrazione, solo i soggetti muniti di apposita procura (Presidente, Direttore Generale) o comunque specificamente individuati mediante atti di ripartizione interna di compiti operativi.
- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari", paragrafo E).

5. *Gestione dei rapporti con le Autorità pubbliche relativi ad attività di ispezione e controllo*

- *Regolamentazione*: è prevista la regolamentazione dei rapporti con la Pubblica Amministrazione in occasione di verifiche/ispezioni/accertamenti/richieste di informazioni, con particolare riferimento ai soggetti autorizzati a ricevere le Autorità Ispettive, a produrre, controllare ed autorizzare la documentazione richiesta e alle modalità di verbalizzazione interna ed archiviazione delle relative risultanze.
- *Tracciabilità*: è prevista la predisposizione di verbali relativi alle ispezioni/verifiche/accertamenti/richieste di informazioni effettuate nei confronti della Società, l'archiviazione di tali documenti in fascicoli allegati a verbali emessi dalla Pubblica Amministrazione, l'invio degli stessi ad adeguato livello gerarchico e la successiva archiviazione degli stessi. In particolare, è prevista la necessità di conservare il verbale prodotto dall'Autorità ispettiva ed un verbale interno. Inoltre, è prevista (fermo restando quanto previsto dalla Parte Generale del presente Modello in ordine ai flussi informativi verso l'Organismo di Vigilanza) la necessità di segnalare: i) al Direttore Generale

competente l'avvio di un processo di verifica da parte di un'Autorità Pubblica ispettiva; ii) al superiore gerarchico eventuali criticità emerse nel corso di verifiche/ispezioni/accertamenti/informazioni.

- *Segregazione dei compiti:* è prevista la separazione delle funzioni di autorizzazione, demandata al Responsabile della Direzione competente, di esecuzione, affidata al soggetto delegato alla gestione dell'interfaccia con l'Autorità Ispettiva e di controllo affidato al Direttore Generale .
- *Poteri autorizzativi e di firma:* è previsto che siano autorizzati ad intrattenere rapporti con soggetti appartenenti alla Pubblica Amministrazione o comunque con soggetti qualificabili come "pubblici" o "incaricati di pubblico servizio" solo i soggetti muniti di apposita procura (Presidente, Direttore Generale, altri soggetti delegati).
- *Codice Etico:* è richiesta l'osservanza delle indicazioni comportamentali previste dal capitolo II ("Comportamento nella gestione degli affari").

6. *Gestione degli Acquisti e del Patrimonio*

6.1. Con riferimento all'attività di acquisto di beni e servizi, i protocolli specifici adottati sono i seguenti:

- *Regolamentazione*: è richiesta: i) l'esplicita previsione delle tipologie di procedimento di acquisto utilizzabili in conformità con la vigente normativa; ii) l'indicazione del ruolo e della responsabilità dei diversi attori coinvolti, con separazione di compiti fra l'Area deputata alla gestione degli aspetti negoziali e contrattuali, e la funzione richiedente, che cura l'individuazione delle specifiche tecniche del bene/servizio e verifica la corretta esecuzione della prestazione; iii) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; iv) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; v) l'archiviazione della documentazione rilevante.
- *Tracciabilità*: è richiesto che: i) sia posta la massima attenzione affinché informazioni e dati indicati nella documentazione siano corretti e veritieri; ii) i processi siano documentati; iii) la documentazione sia archiviata. L'utilizzo di supporto informativo per la gestione delle transazioni e dello scambio documentale (Lotus Notes, applicativo gestione richieste di acquisto, applicativo gestione contratti) garantisce la ricostruibilità ex post del processo di acquisto.
- *Segregazione dei compiti*: è richiesta separazione delle funzioni di autorizzazione, esecuzione e controllo, in ragione della differente tipologia di procedimento: i) *Acquisti mediante procedure negoziate (affidamenti diretti)*: il Consiglio di Amministrazione autorizza, fuori dai limiti di spesa delegati, i Direttore Generale e gli altri soggetti delegati, secondo i loro limiti di spesa, sottoscrivono il contratto, la struttura aziendale responsabile degli approvvigionamenti gestisce tecnicamente il processo, la Direzione Amministrazione, Finanza e Controllo supervisiona il processo; ii) *Acquisti mediante procedimento ad evidenza pubblica, ivi compreso il cottimo fiduciario:* il Direttore Generale e gli altri soggetti delegati, firmano per autorizzazione i documenti di gara e/o richieste di offerta, la struttura aziendale responsabile degli approvvigionamenti, con il supporto dell'Unità

Organizzativa Societario e Legale, espleta gli adempimenti di formalizzazione del procedimento, la Commissione di Gara valuta e propone l'aggiudicazione alla Direzionei Generale, il Contratto è emesso con firma dei soggetti muniti di potere; iii) *Acquisti per Cassa:* le uscite di cassa sono autorizzate dal Responsabile della Direzione Amministrazione, Finanza e Controllo, la gestione fisica della cassa e dei prelievi è rimessa al Responsabile della Cassa, l'autorizzazione al reintegro di Cassa è fornita diversamente dalla Direzione Generale.

- *Poteri autorizzativi e di firma:* la sottoscrizione dei contratti avviene nel limite di spesa. E' altresì previsto che il Presidente, il DirettoreGenerale e gli altri soggetti delegati, abbiano il potere di sottoscrivere contratti passivi, qualunque ne sia l'importo e l'oggetto, quando questi siano stipulati in relazione all'aggiudicazione di una gara ad evidenza pubblica, compresi gli acquisti in economia, indette da ACI Informatica.
- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari", paragrafo B).

6.2. Con riferimento all'attività di gestione del patrimonio, i protocolli specifici adottati sono i seguenti:

- *Regolamentazione*: sono previsti: i) i modi di consegna, accettazione, registrazione, inventariazione dei beni immobili e mobili, e gestione del registro beni ammortizzabili; ii) le modalità di dismissione dei beni mobili e immobili, attraverso alienazione o rottamazione; iii) il ruolo e la responsabilità degli attori coinvolti nel processo.
- *Tracciabilità*: è richiesto che: i) sia posta la massima attenzione affinché informazioni e dati indicati nella documentazione siano corretti e veritieri; ii) i processi siano documentati; iii) la documentazione sia archiviata. E' richiesto l'utilizzo dei sistemi informatici Lotus Notes e SCI e la registrazione di magazzino di tutte le relative movimentazioni.
- *Segregazione dei compiti*: è prevista la separazione delle funzioni.
- *Poteri autorizzativi e di firma*: è richiesto che siano titolati ad autorizzare atti di disposizione sul patrimonio solo i soggetti muniti di apposita procura (Presidente, Direttore Generale e Procuratori speciali).
- *Codice Etico*: è richiesta l'osservanza dei comportamenti indicati nei capitoli VI ("Libri contabili e registri societari") e VII ("Condotta societaria").

7. Gestione dei Flussi Finanziari

- *Regolamentazione*: sono individuati ruoli e responsabilità nella gestione dei flussi finanziari, per la disciplina degli aspetti concernenti: i) i soggetti coinvolti nel processo; ii) le modalità operative per la gestione di pagamenti ed incassi; iii) i meccanismi di controllo della regolarità delle operazioni, anche attraverso il coinvolgimento nel processo di soggetti appartenenti ad almeno due strutture aziendali differenti; iv) le attività di verifica della rendicontazione bancaria inerente le movimentazioni di fondi.
- *Segregazione dei compiti*: è prevista la separazione delle funzioni di autorizzazione, esecuzione e controllo, che sono affidate, a distinti soggetti/funzioni aziendali tra loro indipendenti.

- *Tracciabilità:* è prevista la completa tracciabilità di tutte le operazioni effettuate, l'archiviazione dei documenti di pagamento e di incasso nonché l'utilizzo di sistemi informatici idonei a tracciare ex-post l'iter del processo e le operazioni eseguite.
- *Poteri autorizzativi e di firma:* è richiesta un'autorizzazione formalizzata alla disposizione di pagamento, con limiti di spesa, vincoli e responsabilità.
- *Codice Etico*: è richiesta l'osservanza delle indicazioni comportamentali previste dai capitoli II ("Comportamento nella gestione degli affari"), VI ("Libri contabili e registri societari") e VII ("Condotta societaria").

8. *Gestione delle Risorse Umane*

- *Regolamentazione*: sono individuati ruoli e responsabilità dei diversi soggetti nelle attività di seguito indicate: i) selezione dei candidati; ii) reperimento dei *curricula*; iii) valutazione, "attitudinale" e "tecnica", del candidato iv) segregazione delle funzioni coinvolte nel processo di richiesta di assunzione personale e in quello di valutazione/selezione o promozione del personale stesso; v) archiviazione della documentazione rilevante.
- *Segregazione dei compiti*: è prevista una separazione dei compiti nelle diverse fasi del processo. E' prevista pertanto una distinta allocazione dei poteri autorizzativi e di controllo in fase di definizione del Budget, redatto dalla Direzione Generale nonché dalla Direzione Amministrazione, Finanza e Controllo, e delle attività di selezione ed assunzione delle risorse, gestite dall'Area Gestione Risorse Umane sotto la supervisione della Direzione del Personale e autorizzate dal Presidente o da diversa persona nell'ambito di eventuali poteri delegati
- *Procure e deleghe:* è richiesto che i contratti di lavoro siano sottoscritti soltanto da persone munite di apposita procura in tal senso, con specificazione di limiti di valore oltre i quali il contratto deve essere sottoscritto da soggetto di livello gerarchico superiore).
- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dai capitoli II ("Comportamento nella gestione degli affari", paragrafo C), III ("Salute, sicurezza, ambiente", paragrafo A), IV ("Trattamento di informazioni interne"), VIII ("Conflitti di interesse") e IX ("Valenza del *Codice Etico").*

9. REATI SOCIETARI

9.1. I reati societari richiamati dall'art 25 – ter del D.Lgs. 231/2001

Si riporta, qui di seguito, una breve descrizione dei contenuti degli articoli del codice civile che disciplinano i reati societari previsti nel corpo del D.Lgs. 231/2001 ai sensi degli artt.25-ter, così come riformulato dalla Legge 27 maggio 2015 n. 69 che si è limitata a prevedere l'entità della sanzione pecuniaria a carico dell'Ente in relazione alla commissione dei reati societari, e 25-sexies.

La Legge 27 maggio 2015, n. 69, in materia di delitti contro la pubblica amministrazione, di associazioni di tipo mafioso e di falso in bilancio, pubblicata in data 30 maggio 2015 (Gazzetta Ufficiale Serie Generale n.124 del 30-5-2015), si è prefissa di cambiare in maniera radicale i reati di false comunicazioni sociali con particolare riferimento al cd. "falso in bilancio".
Il fine del Legislatore è provvedere ad un sostanziale rimodellamento della fattispecie criminosa, inasprendo contestualmente le sanzioni sia a carico dei soggetti persone fisiche (amministratori, direttori generali, dirigenti preposti alla redazione di documenti contabili, sindaci e liquidatori) sia a carico delle società, sanzionabili ex D.lgs. 231/2001.
La maggiore novità riguarda la previsione di punibilità della fattispecie in esame come delitto e non più come contravvenzione.
Inoltre, uno dei principali cambiamenti riguarda la trasformazione del reato di false comunicazioni sociali da reato di danno a reato di pericolo. In altri termini, verranno sanzionati quei comportamenti che, seppure non immediatamente causativi di danni, pongono in essere una situazione in grado di determinarli.
Alle società non quotate, inoltre, grazie all'inserimento di una nuova disposizione normativa all'interno del codice civile, l'art. 2621 ter c.c., potrà non essere applicata la disciplina in esame in ipotesi di particolare tenuità del fatto.
Spetterà, tuttavia, al giudice valutare l'entità dell'eventuale danno cagionato alla società, ai soci o ai creditori.

False comunicazioni sociali (artt. 2621, 2621 – bis e 2621- ter c.c.)
La norma punisce, fuori dai casi previsti dall'art. 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore.

La pena si applica anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.

Vengono sanzionati quei comportamenti che, seppure non immediatamente causativi di danni, pongono in essere una situazione in grado di determinarli.

False comunicazioni sociali delle società quotate (art. 2622 c.c.)

La norma punisce gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico consapevolmente espongono fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore.

Impedito controllo (art. 2625 c.c.)

La norma punisce gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali.
Si tratta di un reato nella sola ipotesi in cui dalla condotta sopra descritta sia derivato un danno ai soci.

Formazione fittizia del capitale (art. 2632 c.c.)

Tale reato può consumarsi quando: viene formato o aumentato fittiziamente il capitale della Società mediante attribuzione di azioni o quote sociali in misura complessivamente superiore all'ammontare del capitale sociale; vengono sottoscritte reciprocamente azioni o quote; vengono sopravvalutati in modo rilevante i conferimenti dei beni in natura, i crediti ovvero il patrimonio della Società, nel caso di trasformazione.

Si precisa che soggetti attivi sono gli amministratori e i soci conferenti.

Indebita restituzione dei conferimenti (art. 2626 c.c.)

La "condotta tipica" prevede, fuori dei casi di legittima riduzione del capitale sociale, la restituzione, anche simulata, dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli.

Si precisa che soggetti attivi sono gli amministratori.

Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)

Tale condotta criminosa consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che per legge non possono essere distribuite.
Si precisa che la ricostituzione degli utili o delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Soggetti attivi del reato sono gli amministratori (reato proprio).

Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)

Il reato si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, che cagioni un danno ai creditori.
Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.
Soggetti attivi del reato sono i liquidatori.

Illecita influenza sull'Assemblea (art. 2636 c.c.)

La norma punisce chiunque, con atti simulati o fraudolenti determina la maggioranza in Assemblea allo scopo di procurare a sé o ad altri un ingiusto profitto.

Aggiotaggio (art. 2637 c.c.)
La norma punisce chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati, o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.

Ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di vigilanza (art. 2638 c.c.)
La norma punisce gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci ed i liquidatori di Società od enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazione, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare concernenti la situazione medesima. La punibilità è estesa anche nel caso in cui le informazioni riguardino beni posseduti o amministrati dalla Società per conto di terzi.
I soggetti sopra descritti sono altresì punibili, per il semplice ostacolo all'esercizio delle funzioni di vigilanza, attuato consapevolmente, in qualsiasi forma, anche omettendo le comunicazioni dovute alle autorità di vigilanza (2° comma).

Illecite operazioni sulle azioni o quote sociali o della Società controllante (art. 2628 c.c.)
La norma punisce gli amministratori che, fuori dai casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge o acquistano o sottoscrivono azioni o quote emesse dalla Società controllante cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.

Si fa presente che se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio, relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

Operazioni in pregiudizio dei creditori (art. 2629 c.c.)

La norma punisce gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra Società o scissioni, cagionando danno ai creditori.

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Omessa comunicazione del conflitto d'interessi (art. 2629 bis c.c.)

La fattispecie sanziona penalmente il precetto contenuto nell'art. 2391, comma 1, c.c., che prevede un obbligo informativo in capo all'amministratore, finalizzato a dare notizia in modo specifico e dettagliato ad amministratori ed al collegio sindacale, di ogni interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società precisandone la natura, i termini, l'origine e la portata. Nel caso invece si tratti di amministratore delegato, è stabilito inoltre, per quest'ultimo, un obbligo di astensione dal compimento dell'operazione.
Si fa presente che la punibilità della condotta risulta condizionata al verificarsi di un danno alla società o a terzi, derivante dalla violazione stessa.

Corruzione tra privati (art.263, comma 3, c.c.)

La fattispecie sanziona, salvo che il fatto non costituisca più grave reato, l'ente nel caso in cui un esponente apicale o un sottoposto abbia dato o promesso denaro o altra utilità ad amministratori, direttori generali, sindaci, dirigenti preposti alla redazione dei documenti contabili societari, liquidatori e persone sottoposte alla direzione o vigilanza di uno dei citati soggetti affinché questi realizzassero od omettessero atti inerenti il loro ufficio o gli obblighi di fedeltà, cagionando un nocumento alla loro società.
Di seguito si fornisce una breve descrizione dei reati richiamati dall'art. 25-*sexies* del d.lgs. 231 del 2001 che trovano prevalente applicazione per le società quotate:

Abuso di informazioni privilegiate (articolo 184 del d.lgs 58/1998 - Testo Unico della Finanza)

Il reato in oggetto può essere commesso da chiunque si trovi in possesso di informazioni, che possono definirsi privilegiate, in quanto assunte in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo di una società quotata, della partecipazione al capitale di una società quotata, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio. In particolare le condotte individuate dalla norma consistono in: a) acquisto, vendita o commissione di altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni privilegiate di cui si è in possesso; b) comunicazione di tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio; c)

raccomandare o indurre altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a).
Per informazione privilegiata si intende una 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 (art. 181 del D. lgs. 24 febbraio 1998, n. 58).

Manipolazione del mercato (articolo 185 del D.Lgs. 58/1998 -Testo Unico della Finanza)
La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari quotati.

9.2. Sanzioni in materia di reati societari previste dal D.Lgs. 231/01

Articolo 25 ter

false comunicazioni sociali (art. 2621 c.c.) e *delitto di corruzione tra privati (art. 2635, 3° comma, c.c.)*

- sanzione pecuniaria: da duecento a quattocento quote;

false comunicazioni sociali di lieve entità (art. 2621 bis c.c.)

- sanzione pecuniaria: da cento a duecento quote;

false comunicazioni sociali delle società quotate (art. 2622 c.c., 1° comma)

- sanzione pecuniaria: da quattrocento a seicento quote;

contravvenzione di illegale ripartizione degli utili e delle riserve (art. 2627 c.c.),

- sanzione pecuniaria: da duecento a duecentosessanta quote;

delitto di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, 1° e 2° comma)

- sanzione pecuniaria: da quattrocento a ottocento quote;

delitto di impedito controllo (art. 2625, 2° comma, c.c.), delitto di formazione fittizia del capitale (art. 2632 c.c.), delitto di illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)

- sanzione pecuniaria: da duecento a trecentosessanta quote;

delitto di operazioni in pregiudizio dei creditori (art. 2629 c.c.),indebita restituzione dei conferimenti (art. 2626 c.c.), delitto di formazione fittizia del capitale (art. 2632 c.c.), delitto di indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.), illecita influenza sull'Assemblea (art. 2636 c.c.), *operazioni in pregiudizio dei creditori* (art. 2629 c.c.)

- sanzione pecuniaria: da trecento a seicentosessanta quote;

delitto di aggiotaggio (art. 2637 c.c.), delitto di omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.),

- sanzione pecuniaria: da quattrocento a mille quote;

delitto di corruzione tra privati (art. 2635, 3° comma, c.c.), delitto di omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.),

In relazione ai reati di cui sopra, se l'ente ha conseguito un profitto di rilevante entità la sanzione pecuniaria è aumentata di un terzo.

Articolo 25 sexies - *abuso di informazioni privilegiate* (articolo 184 del d.lgs 58/1998 - Testo Unico della Finanza), *manipolazione del mercato* (articolo 185 del d.lgs 58/1998 -Testo Unico della Finanza):

- sanzione pecuniaria: da quattrocento a mille quote; se l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità la sanzione pecuniaria è aumentata fino a dieci volte.

9.3. Le attività, individuate come sensibili ai fini del D.Lgs. 231/2001 in ACI Informatica, con riferimento ai reati societari

L'art. 6, comma 2, lett. a) del D.Lgs. 231/2001 indica, come più volte ricordato, tra gli elementi essenziali del modello di organizzazione e di gestione, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.Lgs. 231/2001.

L'analisi dei processi aziendali di ACI Informatica, ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato societario richiamate dall'articolo 25-*ter* e 25-*sexies* del D.Lgs. 231/2001. Le attività sensibili identificate sono qui di seguito riportate:

1. **Predisposizione di bilanci, relazioni, comunicazioni sociali:** trattasi dell'attività inerente la predisposizione del bilancio di esercizio, di relazioni e prospetti allegati al bilancio e qualsiasi altro dato o prospetto relativo alla situazione economica, patrimoniale e finanziaria della Società richiesto da disposizioni normative.

2. **Conservazione di documenti su cui altri organi societari potrebbero esercitare il controllo:** si tratta dell'attività, svolta dagli amministratori della Società, necessaria a rendere disponibili ai Soci, al Collegio Sindacale e all'eventuale Società di revisione (qualora tale funzione non venga svolta dal Collegio Sindacale), le informazioni e/o documenti richiesti dagli stessi e/o necessari per lo svolgimento delle attività di controllo loro deputate. Il processo riguarda più in generale la gestione dei rapporti con i suddetti organi di controllo.

3. **Predisposizione di documenti ai fini delle delibere assembleari e del CdA:** l'attività in esame prevede la definizione dei flussi informativi, provenienti dalle funzioni aziendali coinvolte al fine di predisporre in tempo utile la documentazione e le informazioni necessarie per consentire al Consiglio di Amministrazione e all'Assemblea di esprimersi sulle materie di competenza sottoposte ad approvazione.

4. **Gestione sociale: gestione delle partecipazioni e delle operazioni sul capitale:** il processo in oggetto riguarda le attività, svolte principalmente dal Consiglio di Amministrazione della Società, finalizzate a gestire e formalizzare le operazioni di acquisizione/costituzione/cessione di partecipazioni, finalizzate alla crescita e allo sviluppo della Società, attraverso la condivisione di mercati e conoscenze nel settore informatico (es. Ancitel). Il processo riguarda inoltre le operazioni ordinarie e straordinarie sul capitale

sociale, tra le quali le più significative sono: riduzione di capitale sociale, ripartizione degli utili e delle riserve e restituzione dei conferimenti.

5. ***Gestione delle Vendite:*** si tratta dell'attività residuale di ACI Informatica di negoziazione/ stipulazione e/o esecuzione di contratti finalizzati alla vendita di servizi a privati.

6. ***Gestione dei Flussi Finanziari:*** l'attività si riferisce alla gestione ed alla movimentazione delle risorse finanziarie relative all'attività di impresa.

9.4. Il sistema dei controlli

Il sistema dei controlli identificato dalla Società prevede il rispetto di specifici principi di controllo relativi alle attività sensibili.
Le disposizioni e gli accorgimenti tecnici richiamati nel modello, sono di carattere meramente difensivo e sono volti ad accertare la commissione di eventuali comportamenti illeciti e non anche a consentire un controllo qualitativo-quantitativo sulla prestazione resa dai lavoratori.

9.4.1. Definizione del sistema di controllo

I Principi di controllo posti a base degli strumenti e delle metodologie utilizzate possono essere classificati come di seguito indicato:

- **Regolamentazione**: si richiede l'esistenza di regole, linee guida, di procedure formalizzate, o prassi consolidate, idonee a fornire principi di comportamento e modalità operative per lo svolgimento delle attività sensibili, nonché modalità di archiviazione della documentazione rilevante.
- **Tracciabilità**: si richiede la documentabilità delle attività sensibili. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile *ex post*, anche tramite appositi supporti documentali.
- **Segregazione delle attività**: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- **Poteri autorizzativi e di firma**: si richiede la presenza dei seguenti requisiti in merito ai poteri autorizzativi e di firma: i) coerenza con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) definizione chiara e conoscenza all'interno della Società.
- **Codice Etico:** si richiede il rispetto del Codice Etico, nei suoi principi generali e con riferimento alle previsioni relative ad attività specifiche, già indicate nella parte speciale del modello organizzativo nelle sezioni dedicate ai reati presupposto.

9.4.2. Applicazione dei principi controllo

Il sistema dei controlli prevede presidi specifici per ognuna delle attività sopra elencate.

1. Predisposizione di bilanci, relazioni, comunicazioni sociali

- *Regolamentazione*: è previsto che siano portate a conoscenza del personale coinvolto in attività di formazione/redazione del bilancio di esercizio, norme che definiscano con chiarezza i principi contabili da adottare per la definizione delle poste del bilancio di esercizio e le modalità operative per la loro contabilizzazione. I criteri di contabilizzazione devono essere costantemente allineati alla normativa vigente, a cura dell'Area competente, alla luce delle novità della disciplina civilistica e comunicate alle strutture interne coinvolte nella predisposizione dei dati di bilancio. E' richiesta altresì la predisposizione di specifiche istruzioni e tempistica da parte della Direzione Amministrazione, Finanza e Controllo da fornire alle Unità Organizzative aziendali interessate dal processo di chiusura contabile.
- *Tracciabilità*: Il responsabile di ciascuna funzione coinvolta nel processo deve garantire la tracciabilità delle informazioni contabili non generate in automatico dal sistema informatico; presso la Direzione Amministrazione, Finanza e Controllo sono debitamente archiviati tutti i documenti relativi a estrazioni contabili non eseguite automaticamente dai sistemi, comunicazioni inviate e ricevute dalle Unità Organizzative in fase di chiusura infrannuale o di bilancio, bozze di bilancio, allegati al bilancio, atti di approvazione dei documenti di bilancio e versioni definitive.
- *Segregazione dei compiti*: è previsto che i documenti di bilancio siano sottoposti ad un controllo eseguito a diversi livelli, attraverso la partecipazione di molteplici soggetti, quali la Direzione Amministrazione, Finanza e Controllo, il Collegio Sindacale, il Consiglio di Amministrazione, l'eventuale Società di Revisione (qualora tale funzione non venga più svolta dal Collegio Sindacale).
- *Poteri autorizzativi e di firma*: è prevista l'attribuzione formale di poteri interni/responsabilità (attraverso deleghe di funzione e disposizioni/comunicazioni organizzative) ai soggetti che intervengano nel processo di predisposizione dei bilanci, delle relazioni ed altre comunicazioni sociali.
- *Codice Etico*: è richiesta l'osservanza in particolare dei principi previsti nei capitoli VI e VII riguardanti i "Libri contabili e libri societari" e la "Condotta societaria".

2. *Conservazione dei documenti su cui altri organi societari potrebbero esercitare il controllo*

- *Regolamentazione:* sono individuate la definizione di compiti e ruoli in merito alla conservazione dei libri contabili, fiscali, sociali e dei registri bollati; sono previste modalità strutturate di custodia della documentazione contabile, fiscale, societaria e dei registri bollati.
- *Tracciabilità*: è richiesta la conservazione di tutta la documentazione rilevante.
- *Segregazione dei compiti*: è previsto il rispetto della segregazione dei compiti.
- *Poteri autorizzativi e di firma*: è prevista l'attribuzione formale di poteri interni/responsabilità (attraverso deleghe di funzione e disposizioni/comunicazioni organizzative) ai soggetti che intervengano nel presente processo.
- *Codice Etico:* è richiesta l'osservanza delle indicazioni contenute nel capitolo IV dedicato al "Trattamento di informazioni interne".

3. *Predisposizione di documenti ai fini delle delibere assembleari e del Consiglio di Amministrazione*

- *Regolamentazione*: sono identificati ruoli e responsabilità in merito alla definizione dell'ordine del giorno, alla predisposizione della documentazione destinata alle delibere assembleari e del Consiglio di Amministrazione, alla trasmissione anticipata dei documenti ai Consiglieri, alla trascrizione del verbale d'Assemblea e della documentazione societaria relativa all'attività degli altri organi sociali. E' previsto il supporto fornito dalla Direzione Societario e Legale.
- *Tracciabilità*: è prevista la forma scritta per i flussi di richiesta, verifica ed autorizzazione alla trasmissione dei documenti agli organi preposti. E' inoltre prevista la registrazione e l'archiviazione dei documenti di supporto alle deliberazioni degli organi sociali presso l'Unità di competenza.
- *Segregazione dei compiti*: è prevista una separazione delle funzioni per le strutture e gli organi aziendali coinvolti nelle attività di predisposizione, verifica ed autorizzazione dei documenti utilizzati ai fini delle delibere assembleari e del Consiglio di Amministrazione.
- *Poteri autorizzativi e di firma*: è prevista l'attribuzione formale di poteri interni/responsabilità (attraverso deleghe di funzione e disposizioni/comunicazioni organizzative) ai soggetti che intervengano nel presente processo.
- *Codice Etico:* è richiesta l'osservanza delle indicazioni comportamentali previste dal capitolo VI riguardante i "Libri contabili e i registri societari".

4. *Gestione sociale: gestione delle partecipazioni e delle operazioni sul capitale*

- *Regolamentazione*: sono previsti i ruoli e le responsabilità nella gestione del capitale sociale. Con particolare riferimento alla gestione delle partecipazioni, è prevista la definizione dei ruoli e delle responsabilità connesse alle attività di individuazione di iniziative di partnership, contatto con la controparte, analisi e valutazione delle ipotesi realizzative, deliberazione e costituzione delle partecipazioni.
- *Tracciabilità*: è prevista la predisposizione e l'archiviazione degli atti di delibera e dei relativi documenti predisposti a supporto.
- *Segregazione dei compiti*: è previsto che le attività di supporto di carattere tecnico-economico-legale siano eseguite dalle strutture aziendali competenti e le attività autorizzative e deliberative permangano in capo agli Organi Sociali.
- *Poteri autorizzativi e di firma*: è prevista l'attribuzione formale di poteri al Consiglio di Amministrazione e all'Assemblea.
- *Codice Etico: è prevista l'osse*rvanza delle indicazioni comportamentali previste dai capitoli IV, VI e VII riguardanti rispettivamente il "Trattamento di informazioni interne", i "Libri contabili e i registri societari" e la "Condotta societaria".

5. *Gestione delle vendite*

- *Regolamentazione*: è richiesta: i) l'indicazione del ruolo e della responsabilità dei diversi attori coinvolti nel processo, con separazione di compiti fra l'Area deputata alla gestione degli aspetti negoziali e contrattuali, e la funzione offerente, che cura l'individuazione delle specifiche tecniche del servizio e verifica la corretta erogazione della prestazione; ii) i livelli autorizzativi previsti per ciascuna fase del processo di vendita; iii) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; iv) l'archiviazione della documentazione rilevante.
- *Tracciabilità*: è richiesto che: i) sia posta la massima attenzione affinché informazioni e dati indicati nella documentazione siano corretti e veritieri; ii) i processi siano documentati; iii) la documentazione sia archiviata. L'utilizzo di supporto informativo per la gestione delle transazioni e dello scambio documentale (Lotus Notes, applicativo gestione contratti) garantisce la ricostruibilità ex post del processo di vendita.
- *Segregazione dei compiti*: è richiesta separazione delle funzioni di autorizzazione, esecuzione e controllo;
- *Poteri autorizzativi e di firma:* la sottoscrizione dei contratti avviene nel limite di spesa.
- *Codice Etico*: è richiesta l'osservanza dei principi e comportamenti indicati nel capitolo II ("Comportamento nella gestione degli affari", paragrafo B) e nel capitolo VI ("Libri contabili e registri societari") e VII ("Condotta societaria").

6. *Gestione dei Flussi Finanziari*

- *Regolamentazione*: sono individuati ruoli e responsabilità nella gestione dei flussi finanziari, per la disciplina degli aspetti concernenti: i) i soggetti coinvolti nel processo; ii) le modalità operative per la gestione degli incassi; iii) i meccanismi di controllo della regolarità delle operazioni, anche attraverso il coinvolgimento nel processo di soggetti appartenenti ad almeno due strutture aziendali differenti; iv) le attività di verifica della rendicontazione bancaria inerente le movimentazioni di fondi.
- *Segregazione dei compiti*: è prevista la separazione delle funzioni di autorizzazione, esecuzione e controllo, che sono affidate, a distinti soggetti/funzioni aziendali tra loro indipendenti.
- *Tracciabilità:* è prevista la completa tracciabilità di tutte le operazioni effettuate, l'archiviazione dei documenti di incasso nonché l'utilizzo di sistemi informatici idonei a tracciare ex-post l'iter del processo e le operazioni eseguite.
- *Poteri autorizzativi e di firma:* è prevista l'attribuzione formale di poteri interni/responsabilità (attraverso deleghe di funzione e disposizioni/comunicazioni organizzative) ai soggetti che intervengano nel presente processo.
- *Codice Etico*: è richiesta l'osservanza delle indicazioni comportamentali previste dai capitoli II ("Comportamento nella gestione degli affari"), VI ("Libri contabili e registri societari") e VII ("Condotta societaria").

10. REATI IN MATERIA DI LAVORO PER VIOLAZIONE DI NORMA ANTINFORTUNISTICHE

10.1. I reati in materia di lavoro richiamati dall'art 25-septies del D.Lgs. 231/2001

Si riporta, qui di seguito, una breve descrizione dei contenuti degli articoli del codice penale che disciplinano i reati in materia di lavoro nel corpo del D.Lgs. 231/2001 ai sensi dell'art. 25-septies.

Omicidio colposo (art. 589 c.p.)
La norma punisce la società qualora è cagionata la morte colposa di un lavoratore come conseguenza della violazione di norme per la prevenzione degli infortuni sul lavoro.

Lesioni personali colpose (art. 59, comma3, c.p.)
La norma punisce la società qualora sono cagionate lesioni o lesioni gravi colpose ad un lavoratore come conseguenza della violazione di norme per la prevenzione degli infortuni sul lavoro.

10.2. Sanzioni in materia di reati di lavoro per violazione di norme antinfortunistiche previste dal D.lgs. 231/01

Articolo 25 septies, primo e secondo comma - *omicidio colposo* (art. 589 c.p.):

- sanzioni pecuniarie: non inferiore a duecentocinquanta quote e non superiore a mille quote;
- sanzioni interdittive (per una durata non inferiore a tre mesi e non superiore ad un anno): interdizione dall'esercizio dell'attività, sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, esclusioni da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, divieto di pubblicizzare beni o servizi

Articolo 25 septies, terzo comma - *lesioni personali colpose* (art. 590 c.p.):

- sanzioni pecuniarie: non superiore a duecentocinquanta quote;
- sanzioni interdittive (per una durata non superiore a sei mesi): interdizione dall'esercizio dell'attività, sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, esclusioni da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, divieto di pubblicizzare beni o servizi.

10.3. Le attività, individuate come sensibili ai fini del D.Lgs. 231/2001 in ACI Informatica , con riferimento ai reati in materia di lavoro

L'art. 6, comma 2, lett. a) del D.Lgs. 231/2001 indica, come più volte ricordato, tra gli elementi essenziali del modello di organizzazione e di gestione, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.Lgs. 231/2001.

L'analisi dei processi aziendali di ACI Informatica, ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'articolo 25-septies del D.Lgs. 231/2001. Le attività sensibili sono identificate nei documenti aziendali di seguito riportati:

1. **Manuale per la tutela dei lavoratori nei luoghi di lavoro e valutazione di rischi:** trattasi del documento redatto ai sensi e per gli effetti del D. Lgs 81/08 contenente l'individuazione dei rischi e le misure intraprese.

2. **Manuale della sicurezza aziendale:** trattasi del documento contenente le finalità e le procedure aziendali per le aree coinvolte ed è così articolato:
   - Politica della sicurezza
   - Modello organizzativo della sicurezza
   - Gestione della documentazione di sicurezza
   - Gestione dell'incidente di sicurezza
   - Audit
   - Norme e procedura di sicurezza aziendale

10.4. Il sistema dei controlli

Il sistema dei controlli identificato dalla Società prevede il rispetto di specifici principi di controllo relativi alle attività sensibili.

Le disposizioni e gli accorgimenti tecnici previsti nel modello, sono di carattere meramente difensivo e sono volti ad accertare la commissione di eventuali comportamenti illeciti e non anche a consentire un controllo qualitativo-quantitativo sulla prestazione resa dai lavoratori.

10.4.1. Definizione principi del sistema di controllo

I Principi di controllo posti a base degli strumenti e delle metodologie utilizzate possono essere classificati come di seguito indicato:

- **Regolamentazione**: si richiede l'esistenza di regole, linee guida, di procedure formalizzate, nel rispetto del D.Lgs. 81/08 concernente la sicurezza e la salute dei lavoratori sul luogo di lavoro.
- **Tracciabilità**: si richiede la documentabilità delle attività del responsabile del servizio di prevenzione protezione e suo interagisce con le altre funzioni previste nel D.Lgs. 81/08.
- **Segregazione delle attività**: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- **Poteri autorizzativi e di firma**: si richiede la presenza dei seguenti requisiti: i) coerenza con le responsabilità organizzative e gestionali assegnate, ii) definizione chiara e conoscenza all'interno della Società.
- **Codice Etico:** si richiede il rispetto del Codice Etico, nei suoi principi generali e con riferimento alle previsioni relative ad attività specifiche, già indicate nella parte speciale del modello organizzativo nelle sezioni dedicate ai reati presupposto.

10.4.2. Applicazione dei principi controllo

Il sistema dei controlli prevede presidi specifici identificati nel manuale per la tutela dei lavoratori nei luoghi di lavoro e valutazione di rischi e in quello della sicurezza aziendale.

11. REATI INFORMATICI

11.1.A I reati informatici richiamati dall'art. 24 bis del D.lgs. 231/01, introdotti dalla Legge 48/08

Si riporta, qui di seguito, una breve descrizione dei contenuti degli articoli del codice penale che disciplinano i reati informatici previsti nell'articolo 24 bis del D.lgs. 231/01.

1. Inviolabilità del "domicilio informatico"

1. ***Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.).***

- ***Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)***

Le norme sono volte a proteggere il "domicilio informatico", che costituisce espressione ideale dell'area di rispetto pertinente al soggetto interessato, riconducibile, tra gli altri, all'articolo 14 della Costituzione.

Le norme puniscono chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza o vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo (articolo 615 ter); e chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee a tale scopo (articolo 615 quater).

Perché il reato si configuri è necessario che il sistema sia protetto da misure di sicurezza, di cui l'autore della violazione sia quanto meno consapevole. Non è invece indispensabile che vi sia un'effettiva violazione di tali misure.

Nel caso di detenzione e diffusione abusiva di codici di accesso l'agente deve avere la specifica finalità di procurare a sé o ad altri un profitto o di arrecare ad altri un danno.

- ***Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies).***

La norma punisce chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o a 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.

Il reato fa riferimento ai c.d. virus informatici, spyware o altri. La condotta - che può riguardare non solo la produzione, ma anche il commercio di programmi - deve essere

necessariamente realizzata con la specifica finalità di danneggiare i sistemi informatici oppure software o dati contenuti nei sistemi stessi.

Il reato è prodromico ad un evento dannoso, ma si configura indipendentemente dal fatto che il danno si verifichi.

Si può verificare il concorso con altri reati. Si citano a titolo di esempio: danneggiamento (art. 635 bis, ter, quater, quinquies c.p.); interruzione totale o parziale di comunicazioni (art. 617 quater c.p.); acquisizione illecita di informazioni (art. 167 d.lgs. 196/03).

2. Inviolabilità dei segreti

- ***Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)***

- ***Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatico o telematiche (art. 617 quinquies c.p.)***

Le norme puniscono chiunque: fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi ovvero le impedisce o le interrompe, oppure rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto della comunicazione (articolo 617 quater); installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi (articolo 617 quinquies).

La prima ipotesi criminosa punisce chiunque fraudolentemente intercetta, impedisce o interrompe comunicazioni relative a un sistema informatico o intercorrenti tra più sistemi; al secondo comma è punita invece la rivelazione al pubblico del contenuto di comunicazioni intercettate illecitamente.

L'installazione di apparecchiature destinate all'intercettazione, impedimento o interruzione configura un reato prodromico rispetto al precedente.

3. Danneggiamento

Con la legge 48 del 2008, il Legislatore ha operato un complessivo riordino delle fattispecie di danneggiamento informatico: da un lato distinguendo nettamente tra il danneggiamento di dati, programmi e informazioni e il danneggiamento dei sistemi informatici, come già previsto dalla Convenzione di Budapest; dall'altro differenziando il caso in cui il danneggiamento riguardi soggetti privati da quello in cui riguardi soggetti pubblici, o dati o sistemi di pubblica utilità.

Con riferimento alle condotte che investono soggetti pubblici, il Legislatore ha anche provveduto ad accorpare tutte le fattispecie di danneggiamento, collocandole fra i reati contro il patrimonio - così come il danneggiamento compiuto ai danni di privati - e includendovi le ipotesi di attentato a sistemi informatici di pubblica utilità, con la contestuale abrogazione

dell'articolo 420 commi 2 e 3 del Codice Penale – collocato tra delitti contro l'ordine pubblico – che in precedenza le conteneva.

- ***Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.) utilizzati dallo Stato o da un altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)***

Nel caso di *danneggiamento di dati, programmi e informazioni* la tutela non può essere limitata ai dati necessari per il funzionamento del sistema, ma deve estendersi a tutti i dati in esso contenuti. Il danneggiamento può essere compiuto mediante una serie di condotte alternative. Da notare che nel caso di dati utilizzati dallo Stato o da altro ente pubblico il reato è a consumazione anticipata - è punito qualunque fatto diretto a danneggiare - ed è aggravato dall'effettiva distruzione, deterioramento, cancellazione, alterazione o soppressione delle informazioni, dati o programmi derivante dalla condotta dell'agente (in sostanza sufficiente il tentativo).

- ***Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.) di pubblica utilità (art. 635 quinquies c.p.)***

Nel caso di *danneggiamento di sistemi informatici o telematici* è punito chiunque - mediante la distruzione, il deterioramento, la cancellazione, l'alterazione, la soppressione, l'introduzione o la trasmissione di dati, informazioni o programmi informatici – compia un fatto diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Il fatto può essere compiuto mediante diverse condotte, dirette a danneggiare, rendere inservibili o comunque ostacolare gravemente il funzionamento dei sistemi informatici. Anche in questo caso il reato è a consumazione anticipata ed è aggravato dall'evento, consistente nell'effettiva distruzione o danneggiamento del sistema, o nel fatto che esso sia reso, in tutto o in parte, inservibile.

4. Documento informatico e firma digitale

- ***Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)***

Si configura quando il soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge (articolo 32 del decreto legislativo 82/05) per il rilascio di un certificato qualificato di firma elettronica. Il reato in questione, riguardando esclusivamente i soggetti – persone fisiche o giuridiche – che prestano servizi di certificazione elettronica, si configura come un reato proprio; il rappresentante di un'impresa che non svolge tale attività potrà eventualmente concorrere nel fatto commesso dal certificatore.

Il legislatore ha ritenuto di assimilare la frode del certificatore alla frode informatica prevista dall'articolo 640 ter del Codice Penale: uguale è la collocazione sistematica, tra i reati contro il patrimonio mediante frode; uguale è la pena (massima) prevista. E' invece del tutto diversa la condotta individuata: nella frode informatica "semplice" si richiede l'alterazione del funzionamento del sistema o l'intervento non autorizzato su dati, informazioni o programmi; nella frode del certificatore, invece, è sufficiente la violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

- Falso documento informatico (art. 491 bis c.p.)

L'articolo 491 bis del Codice Penale è una norma di collegamento, che consente di estendere anche ai documenti informatici, pubblici o privati aventi efficacia probatoria, le disposizioni relative al falso documentale, commesso su un atto pubblico o su una scrittura privata. Al riguardo si può ricordare che il Codice dell'Amministrazione Digitale, da un lato definisce "documento informatico" la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti; dall'altro attribuisce piena efficacia probatoria ai documenti sottoscritti con firma digitale - o con altra firma elettronica qualificata - basata su un certificato valido. Il Codice, inoltre, introduce una presunzione di utilizzo da parte del titolare del dispositivo della firma elettronica qualificata e della firma digitale, con la conseguenza che il documento così sottoscritto si presume riconducibile al titolare, addossando a quest'ultimo l'onere di dimostrare che il dispositivo di firma è stato utilizzato da altri senza la sua autorizzazione. Tali principi si applicano sia ai documenti formati da privati, sia ai documenti formati da pubblici ufficiali, nonché ai documenti trasmessi con posta elettronica certificata.

Il D.lgs. 231/2001 non prevede la responsabilità amministrativa delle imprese per ogni falso documentale, ma soltanto con riferimento ad alcune fattispecie specificamente individuate. Si richiamano pertanto i reati di **falsità in monete, in carte di pubblico credito, in valori di bollo e strumenti o segni di riconoscimento**, richiamati dall'**articolo 25 bis** del D.lgs. 231/01:

- Monete: falsificazione (art. 453 c.p.), spendita e introduzione nello Stato (art. 453, 455, 457 c.p.), alterazione (art. 454 c.p.)

- Valori di bollo: falsificazione, introduzione nello Stato, acquisto, detenzione o messa in circolazione (art. 459 c.p.); uso di valori contraffatti o alterati (art. 464 c.p.)

- Filigrana: contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito e di valori di bollo (art. 460 c.p.), fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo e di carta filigranata (art. 461 c.p.)

11.1.B I reati informatici richiamati dall'art. 24 del D.lgs. 231/01

Si riporta, qui di seguito, una breve descrizione del contenuto dell'articolo del codice penale che disciplina il reato informatico previsto nell'articolo 24 del D.lgs. 231/01.

- Frode informatica (art. 640 ter c.p.)

La *frode informatica* (art. 640 ter c.p.) si configura quando vi sia l'alterazione del funzionamento di un sistema informatico o telematico oppure in caso di intervento senza diritto, con qualunque modalità, su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti.

Il reato si configura se il fatto è commesso a danno dello Stato o di altro ente pubblico e se ne derivi un profitto ingiusto.

Il reato è aggravato se il fatto è commesso con abuso della qualità di operatore di sistema.

11.2. Sanzioni in materia di reati informatici previste dal D.lgs. 231/01

Articolo 24 - *frode informatica* a danno dello Stato o di altro ente pubblico (art. 640 ter):

- sanzioni pecuniarie: pena base fino a cinquecento quote; se l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità la sanzione pecuniaria va da duecento a seicento quote.

- sanzioni interdittive: divieto di contrattare con la P.A.; esclusione da agevolazioni, finanziamenti o contributi: divieto di pubblicizzare beni o servizi.

Articolo 24 bis, primo comma - *accesso abusivo a sistema informatico e telematico* (art. 615 ter); *intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche* o *installazione di apparecchiature* destinate a tali attività (art. 617 quater e quinquies); *danneggiamento di informazioni, dati e programmi* ad uso privato o utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (artt. 635 bis e ter); *danneggiamento di sistemi informatici o telematici* ad uso privato o di pubblica utilità (635 quater e quinquies).

- sanzioni pecuniarie: da cento a cinquecento quote.

- sanzioni interdittive: interdizione dall'esercizio dell'attività; sospensione o revoca da autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi.

Articolo 24 bis, secondo comma - *detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici* (art. 615 quater); *diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico* (art. 615 quinquies)

- sanzioni pecuniarie: sino a trecento quote.

- sanzioni interdittive: sospensione o revoca da autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi.

Articolo 24 bis, terzo comma - *falso documento informatico* (art. 491 bis); *frode informatica del soggetto che presta servizi di certificazione elettronica* (art. 640 quinquies)

- sanzioni pecuniarie: sino a quattrocento quote.

- sanzioni interdittive: divieto di contrattare con la P.A.; esclusione da agevolazioni, finanziamenti o contributi; divieto di pubblicizzare beni o servizi.

11.3. Attività individuate come sensibili ai fini del D.Lgs. 231/01 con riferimento ai reati informatici

L'analisi dei processi aziendali condotta anche attraverso interviste al personale interessato, ha consentito di individuare diverse attività che devono essere considerate sensibili con riferimento al rischio di commissione di reati informatici. In alcuni casi si tratta di attività dirette alla gestione di rapporti tra la Società e soggetti esterni (soggetti convenzionati, Pubbliche Amministrazioni, privati); in altri casi si tratta di attività relative alla gestione della Società.

1. ***Gestione dei rapporti in Convenzione con ACI:*** il processo riguarda la progettazione, gestione ed esecuzione, nonché la fatturazione dei corrispettivi, inerenti ai rapporti contrattuali tra la ACI Informatica e l'ente Automobile Club Italia (ACI), che regolano le attività relative allo svolgimento di servizi informatici e commerciali per l'ACI, la Federazione degli Automobile Club Provinciali e la rete delle delegazioni a marchio ACI presenti sul territorio nazionale.
   Di seguito si individuano le attività regolate da Convenzioni con ACI, rinviando ai capi che seguono per l'approfondimento:
   - la progettazione, produzione e assistenza delle infrastrutture ACI;
   - l'erogazione dei servizi informatici alla Federazione ACI;
   - la realizzazione e conduzione di sistemi informatici: Pubblico Registro Automobilistico; la riscossione e controllo delle tasse automobilistiche nelle Regioni Convenzionate; la gestione soci e controllo rete di vendita;
   - l'erogazione, alla rete dei punti vendita a marchio ACI, di servizi amministrativi, commerciali e di marketing (promozione, comunicazione, pubblicità, eventi);

2. ***Esecuzione di contratti conclusi da ACI Informatica S.p.A. con enti della P.A. e società del gruppo*****:** il processo riguarda la gestione di appalti di servizi e forniture affidati alla Società, a seguito di trattativa privata o di procedure a evidenza pubblica, ed esecuzione di contratti per l'erogazione di servizi a enti della Pubblica Amministrazione attraverso i quali la Società fornisce:
   - servizi informatici;

- commercializzazione di prodotti e servizi presso i punti vendita ACI dislocati sul territorio nazionale.

3. ***Erogazione di servizi informatici o telematici:*** il processo riguarda l'erogazione di servizi informatici o telematici forniti in virtù di convenzioni o contratti:
   - ***gestione del sistema di protocollo:*** gestione del sistema di protocollo informatico e documentale fornito in modalità ASP;
   - ***servizi di connettività:*** fornitura di servizi IP (Full IP: voip, adsl, web services; sicurezza reti, connettività);
   - ***tracciamento con sistemi RFID: s***ervizi sul territorio – forniti con sistemi locali - e relativi alla sosta nei parcheggi, mediante rilevazione di dati effettuata tramite applicazione di tag RFID sugli autoveicoli (Abil Park, warning point; SIV, Acivar, Videopoint, ACIZTL, Bollino Blu);
   - ***Services Location Based:*** controllo veicoli (in particolare nell'ambito della gestione flotte aziendali) e infomobilità, basate sulla localizzazione;
   - ***pagamenti (intermediazione): g***estione tasse automobilistiche e quote associative per conto di persone fisiche e giuridiche (Bollo Auto: Bollo sereno, Bollo sicuro, Bollo net, grandi flotte, telebollo, socionet).

4. ***Sviluppo sistemi informatici:*** l'attività riguarda lo sviluppo di infrastrutture di rete e di software sia nell'ambito dei rapporti in convenzione - realizzazione di sistemi informatici centrali e periferici di ACI – che per uso interno. Il Manuale del sistema di gestione per la qualità fornisce la prescrizione e le indicazioni sull'organizzazione, sulle modalità e sulle procedure alle quali la Società deve attenersi per gestire la rispondenza dei processi di sviluppo alle norme UNI EN ISO 9001:2000 e ISO 27001.

5. ***Gestione sistemi informatici:*** l'attività riguarda la gestione e manutenzione delle risorse informatiche – hardware, software, infrastrutturale e di rete – sia per conto di terzi (in virtù di convenzioni o contratti) che per uso interno.
   In particolare: i) per le reti l'attività riguarda la gestione degli accessi e la manutenzione in efficienza; ii) per l'hardware l'attività riguarda la scelta delle risorse da acquistare, il collegamento con le infrastrutture di rete, le modalità di utilizzo, la collocazione in locali idonei e la protezione dell'area, lo smaltimento; iii) per il software l'attività riguarda la scelta dei prodotti da acquisire, l'installazione, l'aggiornamento, l'utilizzo.

6. ***Archiviazione informatica e gestione di banche dati:*** l'attività riguarda le modalità di archiviazione di informazioni, dati e documenti, e gestione della modalità di accesso agli archivi pubblici, da parte di soggetti convenzionati o pubbliche autorità, e agli archivi di uso interno, da parte di dipendenti e collaboratori, nonché delle procedure di sicurezza.

8. ***Gestione del sistema di protocollo informatico e gestione documentale:*** l'attività riguarda il servizio di gestione del sistema di protocollo informatico e dei documenti per uso interno.

8. Internet e posta elettronica: il processo riguarda la modalità di accesso ad internet da parte

del personale, sia per quanto riguarda la navigazione, sia per quanto riguarda il download/upload di applicazioni.
Si fa riferimento all'uso di caselle di posta elettronica aziendale, nei rapporti interni e nei rapporti con l'esterno, in particolare in relazione all'invio di comunicazioni aventi efficacia probatoria.

9. ***Gestione dei Flussi Finanziari:*** l'attività si riferisce alla gestione ed alla movimentazione delle risorse finanziarie relative all'attività di impresa.

10. ***Gestione di flussi informativi con la P.A.:*** il processo consiste nell'utilizzo di software pubblici – o forniti da terzi per conto di soggetti pubblici – per comunicare con la Pubblica Amministrazione. In particolare ci si riferisce alla trasmissione al Ministero delle Finanze delle dichiarazioni fiscali (per mezzo del sistema telematico ENTRATEL del Ministero delle Finanze) e alla trasmissione all'INPS di denunce contributive, relative ad adempimenti previdenziali e ritenute a carico di Società e del personale aziendale (mediante software dell'INPS).

11. ***Gestione Acquisti e Patrimonio:*** si tratta dell'attività di gestione del patrimonio e delle attività connesse con l'approvvigionamento di beni e servizi.
Ci si riferisce, in particolare, ai processi di: i) acquisizione di beni e servizi informatici, ai quali si perviene mediante procedure a evidenza pubblica, a trattativa privata, in economia o per acquisto diretto; ii) acquisizione di beni e servizi mediante procedure di gara on-line; iii) acquisto di beni e servizi su piattaforma tecnologica CONSIP.

12. ***Gestione sociale:*** il processo riguarda la gestione di attività sociali con sistemi informatici: i) gestione della contabilità e predisposizione del bilancio; ii) dematerializzazione, archiviazione e conservazione di documenti relativi alle sedute degli Organi sociali; iii) convocazione di assemblee e consigli di amministrazione, sedute in teleconferenza, verbalizzazione elettronica; iv) iscrizione e materializzazione di titoli azionari.

13. ***Gestione delle Risorse Umane:*** si tratta delle attività relative alla gestione della selezione e dell'assunzione di personale informatico e dell'individuazione degli amministratori di sistema.

11.4. Il sistema dei controlli

Il sistema dei controlli si basa sull'identificazione di criteri e procedure di carattere generale e sulla loro applicazione alle attività sensibili.
Al riguardo si precisa che:

- l'individuazione delle competenze e delle responsabilità delle risorse umane dipende dalle modalità e dagli ambiti di intervento sul sistema informatico, distinguendo fra utenti del sistema informatico e personale esperto, qualificabile come operatore o amministratore di sistema;
- le attività di controllo sull'adempimento delle procedure e sul funzionamento del modello riguardano sia gli aspetti organizzativi sia il sistema informatico;
- le disposizioni e gli accorgimenti tecnici previsti nel modello, sono di carattere meramente difensivo e sono volti ad accertare la commissione di eventuali comportamenti illeciti e non anche a consentire un controllo qualitativo-quantitativo sulla prestazione resa dai lavoratori.

11.4.1. Definizione del sistema di controllo

I criteri e le procedure di controllo riguardano le persone e i sistemi informatici e sono organizzati secondo la suddivisione di seguito indicata:

- **Regolamentazione:** si richiede l'esistenza di regole, linee guida, procedure formalizzate, o prassi consolidate - sia per il personale che per i sistemi informatici - idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili, nonché modalità di archiviazione della documentazione rilevante. Si richiede l'esistenza di criteri per l'individuazione delle figure tecniche addette alla gestione dei sistemi informatici e per l'assegnazione delle utenze personali, applicative e di sistema, e delle relative abilitazioni per l'accesso al sistema e agli ambienti.

- **Segregazione dei compiti:** si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.

- **Poteri autorizzativi e di firma:** con riferimento ai sistemi informatici, i criteri adottati per l'individuazione dei soggetti a cui sono attribuiti i poteri devono essere definiti e trasparenti. Si richiede la presenza dei seguenti requisiti in merito ai poteri autorizzativi e di firma: i) coerenza con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) definizione chiara e conoscenza all'interno della Società; iii) emissione di certificati di firma elettronica, laddove utilizzati, o dispositivi idonei per la validazione dei documenti informatici, coerenti con i poteri conferiti; iv) rilascio e utilizzo di caselle di posta elettronica, laddove utilizzate, coerente con le funzioni e i poteri conferiti; v) assegnazione di utenze personali e di abilitazioni per l'accesso al sistema informatico, reti e ambienti conforme alle funzioni attribuite e alle mansioni svolte.

- **Sicurezza:** si richiede che le procedure di sicurezza riguardino da un lato i sistemi e le procedure informatiche – hardware, software, reti – dall'altro le risorse umane,

comprese le procedure per l'assegnazione e la gestione di utenze e abilitazioni e per la conservazione delle credenziali di accesso.

- **Tracciabilità:** al solo ed esclusivo fine di carattere difensivo volto ad accertare la commissione di eventuali comportamenti illeciti possono essere documentati – tramite supporti cartacei e informatici non modificabili – per consentire di verificare ex post i processi di decisione, autorizzazione e svolgimento di attività sensibili. In particolare, possono essere tracciate: le attività svolte, la gestione documentale (documenti cartacei e informatici), le comunicazioni e le interazioni della Società con l'esterno e all'interno della Società. La definizione dei sistemi di tracciabilità non potrà comunque estrinsecarsi in un controllo remoto sulla qualità e sulla quantità della prestazione fornita dai lavoratori.

- **Codice Etico:** si richiede il rispetto del Codice Etico, nei suoi principi generali e con riferimento alle previsioni relative ad attività specifiche, già indicate nella parte speciale del modello organizzativo nelle sezioni dedicate ai reati presupposti. Si richiede inoltre il rispetto delle previsioni relative all'uso delle risorse informatiche (capo V).

11.4.2. Applicazione dei principi di controllo

Nella fase di applicazione il sistema dei controlli prevede presidi specifici per ciascuna delle attività individuate come attività a rischio.

1. Gestione dei rapporti in convenzione con ACI

- *Regolamentazione:* sono individuati: i) ruoli, responsabilità e modalità operative connesse alla gestione delle attività informatiche previste dalle Convenzioni; ii) requisiti tecnici necessari per lo svolgimento delle attività di progettazione e sviluppo dei sistemi informatici e di erogazione dei servizi; iii) ruoli, responsabilità e modalità operative di verifica, rendicontazione e fatturazione dell'attività svolta in relazione alle Convenzioni.

- *Segregazione dei compiti:* in relazione alla gestione (progettazione, erogazione servizi e assistenza) e alla rendicontazione (controllo e fatturazione) delle attività svolte in convenzione, è prevista la separazione delle funzioni di autorizzazione (demandata alla Direzione Generale), di esecuzione (demandata alla struttura tecnica e amministrativa) e di controllo (esercitato dalla Direzione Generale e dalla Direzione Amministrazione, Finanza e Controllo.

- *Poteri autorizzativi e di firma*: è previsto che siano autorizzati a intrattenere rapporti con i soggetti convenzionati solo coloro che sono muniti di apposita procura o comunque specificamente individuati mediante atti di ripartizione interna di compiti operativi.

- *Sicurezza:* le procedure di sicurezza riguardano i sistemi – hardware, software e reti – utilizzati per la progettazione, sviluppo ed erogazione di servizi informatici.

- *Tracciabilità*: è prevista l'archiviazione delle comunicazioni intercorse fra ACI Informatica ed ACI in occasione dell'esecuzione della convenzione. E' richiesto il controllo della rendicontazione e fatturazione dei servizi informatici erogati. Al solo ed esclusivo fine di carattere difensivo volto ad accertare la commissione di eventuali comportamenti illeciti, è consentita la conservazione delle informazioni relative agli accessi informatici, in conformità con quanto previsto per la tutela della privacy dei dipendenti.

- *Codice Etico:* è richiesta l'osservanza dei principi indicati nel capitolo II ("Comportamento nella gestione degli affari", paragrafo A) e nel capitolo V ("Uso delle risorse informatiche").

2. Esecuzione di contratti conclusi da ACI Informatica S.p.A. con enti della P.A.

- *Regolamentazione:* sono previste regole, linee guida, procedure formalizzate, o prassi consolidate - sia per il personale che per i sistemi informatici - idonee a fornire principi di comportamento, modalità operative relative alla gestione dei contratti conclusi dalla Società, nonché modalità di archiviazione della documentazione rilevante.

- *Segregazione dei compiti:* è applicato il principio di separazione delle attività tra chi richiede, chi autorizza, chi esegue e chi controlla.

- *Poteri autorizzativi e di firma: i criteri adottati per l'individuazione dei soggetti* a cui sono attribuiti i poteri sono definiti e trasparenti. E' prevista la presenza dei seguenti requisiti in merito ai poteri autorizzativi e di firma: i) coerenza con le responsabilità organizzative e gestionali assegnate; ii) definizione chiara e conoscenza all'interno della Società; iii) emissione di certificati di firma elettronica, laddove previsti, coerenti con i poteri conferiti.

- *Sicurezza:* le procedure di sicurezza riguardano i sistemi – hardware, software e reti – utilizzati per la progettazione, sviluppo ed erogazione di servizi informatici.

- *Tracciabilità:* è prevista l'archiviazione della documentazione contrattuale e contabile delle comunicazioni intercorse fra Società e clienti in occasione dell'esecuzione della convenzione. E' previsto il controllo della rendicontazione e fatturazione dei servizi informatici erogati. Al solo ed esclusivo fine di carattere difensivo volto ad accertare la commissione di eventuali comportamenti illeciti è consentita la conservazione delle informazioni relative agli accessi informatici, in conformità con quanto previsto per la tutela della privacy dei dipendenti.

- *Codice Etico:* è richiesta l'osservanza dei principi indicati nel capitolo II ("Comportamento nella gestione degli affari", paragrafo B, D, E, F) e nel capitolo V ("Uso delle risorse informatiche").

3. Erogazione di servizi informatici e telematici

- *Regolamentazione:* sono previste regole e procedure - sia per il personale che per i sistemi informatici – per la progettazione, sviluppo ed erogazione dei servizi; sono previste procedure per la gestione delle transazioni economiche e per la trasmissione e l'archiviazione delle ricevute di pagamento.

- *Segregazione dei compiti:* si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.

- *Poteri autorizzativi e di firma:* si richiede l'individuazione delle figure autorizzate alla gestione delle attività relative all'erogazione dei servizi.

- *Sicurezza:* le procedure riguardano in particolare la sicurezza della rete, anche con riferimento alle necessità di continuità nell'erogazione, e la sicurezza dei dati trattati in ragione dei servizi erogati.

- *Tracciabilità:* con riferimento ai servizi di connettività sono previste procedure di conservazione dei dati di traffico a norma di legge.

- *Codice Etico:* è richiesta l'osservanza delle indicazioni comportamentali previste dai capitoli II ("Comportamento nella gestione degli affari", paragrafo A, D, E), IV ("Trattamento di informazioni interne") e nel capitolo V ("Uso delle risorse informatiche").

4. Sviluppo sistemi informatici

- *Regolamentazione:* sono definite le procedure per apertura, avvio, conduzione, erogazione, monitoraggio, chiusura, rendicontazione della progettazione e manutenzione di soluzioni informatiche.

- *Segregazione dei compiti:* si richiede l'applicazione del principio di separazione delle attività tra chi richiede, chi pianifica e progetta lo sviluppo e chi verifica la congruenza tra gli obiettivi, il prodotto realizzato e i risultati di progettazione.

- *Poteri autorizzativi e di firma:* i criteri adottati per l'individuazione dei soggetti a cui sono attribuiti poteri e responsabilità devono essere definiti e trasparenti. In merito ai poteri autorizzativi e di firma si richiedono i seguenti requisiti: i) coerenza con le responsabilità organizzative e gestionali assegnate; ii) definizione chiara e conoscenza all'interno della Società; iii) emissione di certificati di firma elettronica, laddove previsti, coerenti con i poteri.

- *Sicurezza:* la sicurezza investe in particolare il processo di sviluppo nonché le aree in cui si svolge l'attività.

- *Tracciabilità:* al solo ed esclusivo fine di carattere difensivo, volto ad accertare la commissione di eventuali illeciti è consentita la tracciabilità delle richieste e dei dati e requisiti di base per la progettazione, delle attività svolte e delle relative verifiche, che

non potrà comportare un controllo quantitativo-qualitativo in remoto della prestazione fornita dai lavoratori. È prevista inoltre la tracciabilità delle richieste di correzione di anomalie e dei relativi interventi.

- *Codice Etico:* è richiesta l'osservanza dei principi indicati nel capitolo IV ("Trattamento di informazioni interne"); V ("Uso delle risorse informatiche").

5. Gestione sistemi informatici

- *Regolamentazione:* è prevista la regolamentazione delle procedure di gestione: i) *hardware*: pianificazione dei bisogni, acquisizione, manutenzione, smaltimento; ii) *software:* acquisto di software disponibile sul mercato e regole di installazione, progettazione e sviluppo di software autoprodotto, manutenzione e aggiornamento; iii) *reti:* gestione e accesso interno e remoto alla rete interna, acceso a internet; iv) accesso aree protette.

- *Segregazione dei compiti:* si richiede l'applicazione del principio di separazione delle attività tra chi richiede l'acquisto, l'installazione o la manutenzione e chi esegue gli interventi.

- *Poteri autorizzativi e di firma:* sono definiti e resi noti i criteri per l'individuazione degli amministratori e degli operatori di sistema e le autorizzazioni per lo svolgimento delle attività. Sono definiti e resi noti i criteri per l'assegnazione delle utenze personali, applicative e di sistema, e delle relative abilitazioni per l'accesso al sistema, anche esterno, e agli ambienti.

- *Sicurezza:* la sicurezza riguarda le aree in cui sono collocati i sistemi; i PC forniti al personale; le reti. Per quanto riguarda le risorse umane: sono utilizzate procedure di assegnazione gestione e conservazione delle credenziali di accesso; è regolato l'accesso alle aree protette, alle postazioni (blocco automatico tramite screen saver protetto da password), alla rete interna, a internet. Il sistema è dotato di antivirus, il cui aggiornamento è centralizzato e non richiede l'intervento dei singoli utenti.

- *Tracciabilità:* sono tracciate le richieste di intervento (installazione, manutenzione, assistenza) e le attività di installazione dei programmi, degli interventi, anche di manutenzione, degli accessi al sistema, in modo che ciò non comporti un controllo quantitativo-qualitativo in remoto della prestazione fornita dai lavoratori.

- *Codice Etico:* è richiesta l'osservanza dei principi indicati nel capitolo III ("Salute, sicurezza, ambiente"), capitolo IV ("Trattamento di informazioni interne") e capitolo V ("Uso delle risorse informatiche").

6. Archiviazione informatica e gestione di banche dati

- *Regolamentazione:* archiviazione dati e documenti, individuazione dei soggetti autorizzati ad accedere e/o a gestire le banche dati, a consultare, elaborare, eliminare

informazioni.

- *Segregazione dei compiti:* si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.

- *Poteri autorizzativi e di firma:* **c**on riferimento ai sistemi informatici i criteri adottati per l'individuazione dei soggetti a cui sono attribuiti i poteri devono essere definiti e trasparenti. Si richiede la presenza dei seguenti requisiti in merito ai poteri autorizzativi e di firma: i) coerenza con le responsabilità organizzative e gestionali assegnate; ii) definizione chiara e conoscenza all'interno della Società; iii) emissione di certificati di firma elettronica, laddove previsti, coerenti con i poteri.

- *Sicurezza:* la sicurezza investe sistemi – hardware, software, reti – e procedure informatici. Sono individuati i criteri di accesso ad ambienti e banche dati e sono utilizzate procedure di assegnazione gestione e conservazione delle credenziali di accesso.

- *Tracciabilità:* si richiede che lo svolgimento delle attività sensibili sia tracciato. Il processo di decisione, autorizzazione e svolgimento delle attività sensibili deve essere verificabile ex post, anche tramite appositi supporti documentali. Deve restare traccia del work flow documentale. Traccia documentale cartacea o procedura per rendere non modificabili i documenti informatici.

- *Codice Etico:* è richiesta l'osservanza dei principi indicati nel capitolo IV ("Trattamento di informazioni interne"), nel capitolo VI ("Libri contabili e registri societari") e nel capitolo V ("Uso delle risorse informatiche).

7. Gestione del sistema di protocollo informatico e gestione documentale

- *Regolamentazione:* sono individuate: regole per attribuire la riconducibilità e la non alterabilità dei documenti informatici; modalità di dematerializzazione e archiviazione della documentazione rilevante e per la gestione del protocollo informatico.

- *Segregazione dei compiti:* si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.

- *Poteri autorizzativi e di firma:* **c**on riferimento ai sistemi informatici i criteri adottati per l'individuazione dei soggetti a cui sono attribuiti i poteri devono essere definiti e trasparenti. Si richiede la presenza dei seguenti requisiti in merito ai poteri autorizzativi e di firma: i) coerenza con le responsabilità organizzative e gestionali assegnate; ii) definizione chiara e conoscenza all'interno della Società; iii) emissione di certificati di firma elettronica, laddove utilizzati, coerenti con i poteri, iv) rilascio e utilizzo di caselle di posta elettronica, laddove utilizzate, coerente con le funzioni e i poteri conferiti.

- *Sicurezza:* sono previsti strumenti di gestione documentale che permettano di

mantenere la stabilizzazione temporale e l'integrità complessiva. Sono individuati i criteri di accesso al sistema e sono utilizzate procedure di assegnazione gestione e conservazione delle credenziali di accesso.

- *Tracciabilità:* la creazione e la modifica dei documenti informatici che hanno valore probatorio deve essere tracciata con strumenti che permettano di risalire al titolare della gestione documentale o all'autore del documento o della modifica.

- *Codice Etico:* è richiesta l'osservanza dei principi indicati nei capitoli IV ("Trattamento di informazioni interne") e V ("Uso delle risorse informatiche).

8. Internet e posta elettronica

- *Regolamentazione:* sono individuate le procedure alle quali deve attenersi il personale nell'uso di email aziendale, nell'accesso a internet.

- *Segregazione dei compiti:* le mail ufficiali (sostitutive della carta) devono essere autorizzate e realizzate in situazioni e con modalità predefinite; l'utilizzo di account di posta elettronica ufficiali è legato all'effettivo titolare.

- *Poteri autorizzativi e di firma:* per la trasmissione elettronica di documenti o messaggi vincolanti per la Società - consentita in virtù dei poteri conferiti o in esecuzione di disposizioni espressamente impartite - si deve prevedere l'utilizzo di sistemi di validazione e trasmissione sicuri (ad esempio: firma digitale e trasmissione a mezzo di posta elettronica certificata).

- *Sicurezza:* Internet: è attivo un meccanismo di filtraggio dei siti internet che previene l'accesso e il download non di carattere aziendale; posta elettronica: il sistema aziendale è dotato di tutti i meccanismi software antispam e antivirus atti a mettere i sicurezza l'intero sistema.

- *Tracciabilità:* al solo ed esclusivo fine di carattere difensivo volto ad accertare la commissione di eventuali comportamenti illeciti è prevista la possibilità di un controllo aggregato del traffico in entrata e in uscita che non potrà comportare un controllo qualitativo e quantitativo della prestazione fornita dai lavoratori.

- *Codice Etico:* è richiesta l'osservanza dei principi indicati nel capitolo II ("Comportamento nella gestione degli affari", paragrafo A, B, C, D, E), nel capitolo IV ("Trattamento di informazioni interne") e nel capitolo V ("Uso delle risorse informatiche).

9. Gestione dei Flussi Finanziari

- *Regolamentazione:* sono individuati ruoli e responsabilità nella gestione dei flussi finanziari, per la disciplina degli aspetti concernenti: i) i soggetti coinvolti nel processo; ii) le modalità operative per la gestione di pagamenti e incassi; iii) i meccanismi di controllo della regolarità delle operazioni, anche attraverso il

coinvolgimento nel processo di soggetti appartenenti ad almeno due strutture aziendali differenti; iv) le attività di verifica della rendicontazione bancaria inerente le movimentazioni di fondi.

- *Segregazione dei compiti:* è prevista la separazione delle funzioni di autorizzazione, esecuzione e controllo, che sono affidate, a distinti soggetti/funzioni aziendali tra loro indipendenti.

- *Poteri autorizzativi e di firma:* è richiesta un'autorizzazione formalizzata alla disposizione di pagamento, con limiti di spesa, vincoli e responsabilità e l'attribuzione di poteri di accesso e gestione del sistema informatico coerente con tali limiti. La soglia di approvazione delle spese deve essere indicata nei dispositivi di firma e nei profili informatici e resa nota all'interno della Società.

- *Sicurezza:* la sicurezza investe: sistemi – hardware, software, reti – e procedure informatici; identificazione e autenticazione; politiche di accesso a sistemi e banche dati (coerenti con privacy); politica di conservazione delle credenziali di accesso.

- *Tracciabilità:* è prevista la completa tracciabilità di tutte le operazioni effettuate, l'archiviazione dei documenti di pagamento e di incasso nonché l'utilizzo di sistemi informatici idonei a tracciare ex-post l'iter del processo e le operazioni eseguite.

- *Codice Etico:* è richiesta l'osservanza delle indicazioni comportamentali previste dai capitoli II ("Comportamento nella gestione degli affari"), VI ("Libri contabili e registri societari"), VII ("Condotta societaria") e nel capitolo V ("Uso delle risorse informatiche").

10. Gestione di flussi informativi con la P.A.

- *Regolamentazione:* sono individuati i soggetti deputati alla gestione dei software necessari all'invio dei dati al Ministero delle Finanze e all'INPS e le modalità di estrazione dei dati e di verifica, approvazione, caricamento a sistema e invio delle dichiarazioni ai soggetti pubblici competenti.

- *Segregazione dei compiti:* il protocollo prevede: i) in relazione alla trasmissione di dichiarazioni fiscali mediante software pubblico, la separazione dei compiti di autorizzazione all'invio delle dichiarazioni, rilasciata dal Collegio Sindacale e alla Direzione Generale, di esecuzione dell'estrazione dati dai file aziendali, affidata alla struttura competente, di verifica/supervisione della Direzione Amministrazione, Finanza e Controllo; ii) in relazione alla trasmissione di dati relativi al trattamento pensionistico mediante software pubblico la separazione dei compiti di autorizzazione, fornita dalla Direzione Generale, di esecuzione, affidata all'Area Gestione Risorse Umane, di controllo, affidato alla Direzione del Personale.

- *Poteri autorizzativi e di firma:* con riferimento ai sistemi informatici i criteri adottati per l'individuazione dei soggetti a cui sono attribuiti i poteri devono essere definiti e

trasparenti. Si richiede la presenza dei seguenti requisiti in merito ai poteri autorizzativi e di firma: i) coerenza con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) definizione chiara e conoscenza all'interno della Società; iii) emissione di certificati di firma elettronica, laddove previsti, coerenti con i poteri.

- *Sicurezza:* la sicurezza investe sistemi – hardware, software, reti – e procedure informatici e, in particolare, i flussi informativi. I rischi sono: danneggiamento di dati/sistemi, diffusione di virus, introduzione dati falsi, alterazione dati dei sistemi. Identificazione e autenticazione; politiche di accesso a sistemi e banche dati (coerenti con privacy); politica di conservazione delle credenziali di accesso.

- *Tracciabilità:* la tracciabilità del processo di trasmissione in esame è garantita dalla registrazione e dall'archiviazione della seguente documentazione: dichiarazioni fiscali approvate e inviate, ricevute delle trasmissioni, modulo DM10, ricevute delle trasmissioni, nonché dei fogli di controllo della corrispondenza fra le dichiarazioni inviate e le operazioni di estrazione dati eseguite.

- *Codice Etico:* è richiesta l'osservanza delle indicazioni comportamentali previste dai capitoli II ("Comportamento nella gestione degli affari", paragrafo E), IV ("Trattamento di informazioni interne") e nel capitolo V ("Uso delle risorse informatiche").

11. Gestione Acquisti e Patrimonio

a) Acquisto di beni e servizi

- *Regolamentazione:* è richiesto: i) il rispetto delle tipologie di procedimento di acquisto previste in conformità con la vigente normativa; ii) l'indicazione del ruolo e della responsabilità dei diversi attori coinvolti, con separazione di compiti fra l'Area deputata alla gestione degli aspetti negoziali e contrattuali e la funzione richiedente, che cura l'individuazione delle specifiche tecniche del bene/servizio e verifica la corretta esecuzione della prestazione; iii) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; iv) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal *sistema informati*co aziendale; v) l'archiviazione della documentazione rilevante.

- *Segregazione dei compiti:* è richiesta la separazione delle funzioni di autorizzazione, esecuzione e controllo, in ragione della differente tipologia di procedimento: i) *Acquisti mediante procedure negoziate*: il Consiglio di Amministrazione autorizza, fuori dai limiti di spesa delegati, il Direttore Generale e gli altri soggetti delegati, secondo i limiti di spesa, sottoscrivono il contratto, la struttura aziendale responsabile degli approvvigionamenti gestisce tecnicamente il processo, la Direzione Amministrazione, Finanza e Controllo supervisiona il processo; è previsto il supporto fornito dalla Direzione Societario e Legale; ii) *Acquisti mediante procedimento ad evidenza pubblica, ivi compreso il cottimo fiduciario*: il Direttore Generale e gli altri soggetti delegati firmano per autorizzazione i documenti di gara e/o le richieste di offerta, la struttura

aziendale responsabile degli approvvigionamenti, , con il supporto della Direzione Societario e Legale, espleta gli adempimenti di formalizzazione del procedimento, la Commissione di Gara valuta e propone l'aggiudicazione alla Direzione Generale, il Contratto è emesso con firma dei soggetti muniti di potere; iii) *Acquisti per Cassa:* le uscite di cassa sono autorizzate dal Responsabile della Direzione Amministrazione, Finanza e Controllo, la gestione fisica della cassa e dei prelievi è rimessa al Responsabile della Cassa, l'autorizzazione al reintegro di Cassa è fornita diversamente dalla Direzione Generale.

- *Poteri autorizzativi e di firma:* la sottoscrizione dei contratti avviene nel rispetto delle deleghe. E' altresì previsto che il Direttore e gli altri soggetti delegati abbiano il potere di sottoscrivere contratti passivi, qualunque ne sia l'importo e l'oggetto, quando questi siano stipulati in relazione all'aggiudicazione di una gara a evidenza pubblica indetta dalla Società.

- *Sicurezza:* sono adottate procedure di sicurezza relative a sistemi – hardware, software, reti – e procedure informatici. Identificazione e autenticazione; politiche di accesso a sistemi e banche dati (coerenti con privacy); politica di conservazione delle credenziali di accesso.

- *Tracciabilità:* è richiesto che: i) sia posta la massima attenzione affinché le informazioni e i dati indicati nella documentazione siano corretti e veritieri; ii) i processi siano documentati; iii) la documentazione sia archiviata. L'utilizzo di supporto informativo per la gestione delle transazioni e dello scambio documentale (Lotus Notes, applicativo gestione richieste di acquisto, applicativo gestione contratti) garantisce la ricostruibilità ex post del processo di acquisto.

- *Codice Etico:* è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari" paragrafo B) e nel capitolo V ("Uso delle risorse informatiche").

b) Gestione del patrimonio

- *Regolamentazione:* sono previsti: i) i modi di consegna, accettazione, registrazione, inventariazione dei beni immobili e mobili, e la gestione del registro beni ammortizzabili; ii) le modalità di dismissione dei beni mobili e immobili, attraverso alienazione o rottamazione; iii) il ruolo e la responsabilità degli attori coinvolti nel processo.

- *Segregazione dei compiti:* si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.

- *Poteri autorizzativi e di firma:* è richiesto che siano titolati ad autorizzare atti di disposizione sul patrimonio solo i soggetti muniti di apposita procura (Presidente e Direttore Generale e altri soggetti delegati).

- *Sicurezza:* la sicurezza investe sistemi – hardware, software, reti – e procedure

informatici. Identificazione e autenticazione; politiche di accesso a sistemi e banche dati (coerenti con privacy); politica di conservazione delle credenziali di accesso.

- *Tracciabilità:* è richiesto che: i) sia posta la massima attenzione affinché informazioni e dati indicati nella documentazione siano corretti e veritieri; ii) i processi siano documentati; iii) la documentazione sia archiviata. E' richiesto l'utilizzo dei sistemi informatici Lotus Notes e SCI e la registrazione di magazzino di tutte le relative movimentazioni.
- *Codice Etico:* è richiesta l'osservanza dei comportamenti indicati nei capitoli VI ("Libri contabili e registri societari"), VII ("Condotta societaria") e nel capitolo V ("Uso delle risorse informatiche").

12. Gestione delle Risorse Umane

- *Regolamentazione:* sono individuati ruoli e responsabilità dei diversi soggetti nelle attività di seguito indicate: i) selezione dei candidati; ii) reperimento dei *curricula*; iii) valutazione, "attitudinale" e "tecnica", del candidato (dipendente, consulente, personale a cottimo) iv) segregazione delle funzioni coinvolte nel processo di richiesta di assunzione personale e in quello di valutazione/selezione o promozione del personale stesso; v) archiviazione della documentazione rilevante; vi) previsione di formazione e aggiornamento. **utente** (informatico): istruito e tracciato, nei limiti previsti e già precisati; **sviluppatore**: certificato (sviluppa secondo criteri predefiniti conformemente alle esigenze; acquista oggetti esterni); **amministratore**: consapevole e, con riferimento alle attività sensibili, controllato e tracciato nei limiti previsti e già precisati (log entrata/uscita; identificazione/autenticazione).

- *Segregazione dei compiti:* è prevista la separazione dei compiti nelle diverse fasi del processo. E' prevista pertanto una distinta allocazione dei poteri autorizzativi e di controllo in fase di definizione del Budget, redatto dalla Direzione Generale competente e/o dalla Direzione Amministrazione, Finanza e Controllo, e delle attività di selezione e assunzione delle risorse, gestite dall'Area Gestione Risorse Umane sotto la supervisione della Direzione del Personale autorizzate dal Presidente.

- *Poteri autorizzativi e di firma:* è richiesto che i contratti di lavoro siano sottoscritti soltanto da persone munite di apposita procura in tal senso, con specificazione di limiti di valore oltre i quali il contratto deve essere sottoscritto da un soggetto di livello gerarchico superiore.

- *Sicurezza:* Sono previste: politiche di accesso a sistemi e banche dati (coerenti con la normativa sulla privacy); procedure di identificazione e autenticazione; procedure per il rilascio di dispositivi di firma digitale; procedure di conservazione delle credenziali di accesso e di sostituzione in caso di *turn over* o dimissioni.

- *Tracciabilità:* l'accesso al sistema e lo svolgimento delle attività sensibili sono tracciati. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali. Deve restare traccia del

workflow documentale.

- *Codice Etico:* è richiesta l'osservanza dei principi stabiliti dai capitoli II ("Comportamento nella gestione degli affari", paragrafo C), III ("Salute, sicurezza, ambiente", paragrafo A), IV ("Trattamento di informazioni interne"), VIII ("Conflitti di interesse"), IX ("Valenza del Codice Etico") e nel capitolo V ("Uso delle risorse informatiche")

13. Gestione attività societarie

- *Regolamentazione:* la regolamentazione riguarda: i) *bilancio*: procedure/modalità operative per la gestione contabile e la predisposizione della documentazione di bilancio (gestione data base, flussi informatici e informativi); ii) *conservazione libri e documenti*: dematerializzazione, archiviazione, conservazione, compiti, modalità, controllo; iii) *documenti relativi alle assemblee e c.d.a*: ruoli odg, predisposizione documenti preparatori, verbali; iv) *gestione partecipazioni*: archiviazione e conservazione documenti.

- *Segregazione dei compiti:* si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.

- *Poteri autorizzativi e di firma:* con riferimento ai sistemi informatici i criteri adottati per l'individuazione dei soggetti a cui sono attribuiti i poteri devono essere definiti e trasparenti. Si richiede la presenza dei seguenti requisiti in merito ai poteri autorizzativi e di firma: i) coerenza con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) definizione chiara e conoscenza all'interno della Società; iii) emissione di certificati di firma elettronica, laddove utilizzati, coerenti con i poteri.

- *Sicurezza:* la sicurezza investe sistemi – hardware, software, reti – e procedure informatici. Identificazione e autenticazione; politiche di accesso a sistemi e banche dati (coerenti con privacy); politica di conservazione delle credenziali di accesso.

- *Tracciabilità:* si richiede che lo svolgimento delle attività sensibili sia tracciato. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali. Deve restare traccia del work flow documentale.

- *Codice Etico:* è richiesta l'osservanza dei principi indicati nel capitolo IV ("Trattamento di informazioni interne"), nel capitolo VI ("Libri contabili e registri societari"), nel capitolo VII ("Condotta societaria") e nel capitolo V ("Uso delle risorse informatiche).

12. REATI IN MATERIA DI DIRITTO D'AUTORE

12.1. I reati in materia di diritto d'autore richiamati dall'art. 25 novies del D.lgs 231/2001,

L'art. 25-novies contempla alcuni reati previsti dalla c.d. Legge sul Diritto d'Autore (L. 22 aprile 1941 n. 633 e s.m.i.) e, in particolare, risultano richiamate le fattispecie di cui agli artt. 171, comma 1 lett. a-bis e comma 3**,** 171 bis**,** 171 ter, 171 septies e 171 octies.
L'analisi condotta sull'attività istituzionale di ACI Informatica, ha evidenziato che le fattispecie di reato di cui all'art. 25 novies, rilevanti per la Società sono quelle previste dagli artt. :

- 171, comma 1, lett. a-bis;
- 171, comma 3;
- 171 bis, commi 1 e 2.

Si ritiene non trovino, invece, applicazione i reati contemplati agli artt. 171-ter, 171_septies e 171 octies.

Si provvede, pertanto, a fornire qui di seguito una breve descrizione delle sole fattispecie sopra richiamate ritenute rilevanti per la Società.

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171, comma 1 lett. a bis)

La norma, con riferimento al reato già introdotto dalla L. n. 43 del 2005, punisce chiunque, mette a disposizione del pubblico, immettendola in un sistema di rete telematiche mediante connessioni di qualsiasi genere, un'opera d'ingegno protetta o parte di essa.

La norma tutela l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere frustrate le proprie aspettative di guadagno in casi di libera circolazione della propria opera in rete.

La ratio della norma è quella di responsabilizzare le aziende che, nel gestire le proprie reti telematiche, mettono a disposizione del pubblico opere protette dal diritto d'autore, inducendole a predisporre controlli più accurati sui contenuti che "transitano" nei loro sistemi informatici.

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171, comma 3)

La norma punisce le condotte di cui all'art. 171, primo comma, lett.a bis, ove commesse su un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera stessa, qualora ne risulti offesa all'onore o alla reputazione dell'autore.

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-bis, comma 1)

La disposizione, introdotta dal D.Lgs. 489/1992, al comma 1, punisce la condotta di chiunque abusivamente duplichi, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende o detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla SIAE.

La punibilità sussiste anche se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di una programma o di un elaboratore.

La norma è volta alla tutela del software in generale intendendosi, a norma dell'art. 2 della citata Legge sul diritto d'autore, i programmi per elaboratore, in qualsiasi forma espressi, purché originali, quale risultato della creazione intellettuale dell'autore, mentre risultano esclusi dalla tutela le idee i principi che sono alla base di un programma, compresi quelli alla base delle sue interfacce.

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171, bis, comma 2)

La disposizione, introdotta dal D.Lgs. n. 169/99, al comma 2, punisce chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE, riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca dati in violazione delle disposizioni di cui agli artt. 64-quinquies e 64-sexies della L. 633/1941, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni cui agli artt. 102 bis e 102 ter della citata legge, ovvero distribuisce, vende o concede in locazione una banca dati.

La norma, è diretta alla tutela delle banche dati, per esse intendendosi a norma dell'art. 2 della citata Legge sul Diritto d'Autore, le raccolte di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo.

12.2. Sanzioni in materia di Diritto d'Autore previste dal D.Lgs. 231/01

A norma dell'art. 25-novies , in relazione alla commissione dei reati sopra elencati si applicano all'ente le sanzioni pecuniarie fino a cinquecento quote e le sanzioni interdittive, per una durata non superiore ad un anno, previste dall'art. 9, comma 2, del D.Lgs. 231/01, ovvero:

- l'interdizione dall'esercizio dell'attività;
- la sospensione o la revoca delle autorizzazioni licenze o concessioni funzionali alla commissione dell'illecito;
- il divieto di contrattare con la pubblica amministrazione,salvo che per ottenere le prestazioni di un pubblico servizio;

- l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi.

12.3. Le attività, individuate come sensibili ai fini del D.Lgs. 231/2001 in ACI Informatica, con riferimento a reati in materia di diritto d'autore

L'art. 6, comma 2, lett. a) del D.Lgs. 231/2001 indica, come più volte ricordato, tra gli elementi essenziali del modello di organizzazione e di gestione, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.Lgs. 231/2001.

L'analisi dei processi aziendali di ACI Informatica, condotta anche attraverso interviste al personale interessato, ha consentito di individuare le attività sensibili nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'articolo 25-*novies* del D.Lgs. 231/2001 o che potrebbero essere strumentali alla loro commissione quali specificatamente:

- accesso alla rete internet e utilizzo del software aziendale.
- acquisto e gestione licenze software nell'attività d'impresa.

Pertanto, sono individuate le attività sensibili negli ambiti di seguito riportati.

1 ***Internet:*** il processo riguarda la modalità di accesso ad internet da parte del personale ed, in particolare, il download/upload di applicazioni in conformità alle disposizioni societarie in uso, nonché l'utilizzo del software licenziato.

2. Gestione Acquisti e Patrimonio: si tratta dell'attività di gestione del patrimonio e delle attività connesse con l'approvvigionamento di software.
Ci si riferisce, in particolare, ai processi di: i) acquisizione di software, ai quali si perviene mediante procedure ad evidenza pubblica, a trattativa privata, in economia o per acquisto diretto; ii) acquisizione di software mediante procedure di gara on-line; iii) acquisto di beni e servizi su piattaforma tecnologica CONSIP.

12.4. Il sistema dei controlli

Il sistema dei controlli si basa sull'identificazione di criteri e procedure di carattere generale e sulla loro applicazione alle attività sensibili.
Al riguardo si precisa che:

- l'individuazione delle competenze e delle responsabilità nell'ambito degli acquisti e della gestione del patrimonio dipende dalla tipologia di beni acquistati ;
- le attività di controllo sull'adempimento delle procedure e sul funzionamento del modello riguardano sia gli aspetti relativi all'acquisizione, installazione e gestione delle licenze d'uso sia le modalità di utilizzo della rete internet nell'ambito aziendale;

- le disposizioni e gli accorgimenti tecnici previsti nel modello, sono di carattere meramente difensivo e sono volti ad accertare la commissione di eventuali comportamenti illeciti e non anche a consentire un controllo qualitativo-quantitativo sulla prestazione resa dai lavoratori.

12.4.1. Definizione del sistema di controllo

I criteri e le procedure di controllo riguardano le persone e i sistemi informatici e sono organizzati secondo la suddivisione di seguito indicata:

- **Regolamentazione:** si richiede l'esistenza di regole, linee guida, procedure formalizzate, o prassi consolidate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili, nonché modalità di archiviazione della documentazione rilevante.

- **Segregazione dei compiti:** si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.

- **Poteri autorizzativi e di firma:** con riferimento all'acquisizione, gestione e utilizzo delle licenze software i criteri adottati per l'individuazione dei soggetti a cui sono attribuiti i poteri devono essere definiti e trasparenti. Si richiede la presenza dei seguenti requisiti in merito ai poteri autorizzativi e di firma: i) coerenza con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) definizione chiara e conoscenza all'interno della Società; iii) assegnazione di software, di utenze personali e di abilitazioni per l'accesso al sistema informatico, reti e ambienti conforme alle funzioni attribuite e alle mansioni svolte.

- **Sicurezza:** si richiede che le procedure di sicurezza riguardino da un lato i sistemi e le procedure informatiche – hardware, software, reti – dall'altro le risorse umane, comprese le procedure per l'assegnazione di software e la gestione di utenze e abilitazioni e per la conservazione delle credenziali di accesso.

- **Tracciabilità:** al solo ed esclusivo fine di carattere difensivo volto ad accertare la commissione di eventuali comportamenti illeciti possono essere documentati – tramite supporti cartacei e informatici non modificabili – per consentire di verificare ex post i processi di decisione, autorizzazione e svolgimento di attività sensibili. In particolare, possono essere tracciate: le attività svolte, la gestione documentale (documenti cartacei e informatici), le comunicazioni e le interazioni della Società con l'esterno e all'interno della Società. La definizione dei sistemi di tracciabilità non potrà comunque estrinsecarsi in un controllo remoto sulla qualità e sulla quantità della prestazione fornita dai lavoratori.

- **Codice Etico:** si richiede il rispetto del Codice Etico, nei suoi principi generali e con riferimento alle previsioni relative ad attività specifiche, già indicate nella parte speciale

del modello organizzativo nelle sezioni dedicate ai reati presupposti. Si richiede inoltre il rispetto delle previsioni relative all'uso delle risorse informatiche (capo V).

12.4.2. Applicazione dei principi di controllo

Nella fase di applicazione il sistema dei controlli prevede presidi specifici per ciascuna delle attività individuate come attività a rischio.

1. Internet e utilizzo software aziendale

- *Regolamentazione:* sono individuate le procedure: i) alle quali deve attenersi il personale nell'accesso a internet ed, in particolare in relazione alle attività di download/upload di applicazioni ii) di variazione delle configurazioni dei software in uso; iii) di installazione di software, forniti esclusivamente dalla società, da parte del personale autorizzato.

- *Segregazione dei compiti:* si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.

- *Poteri autorizzativi e di firma:* sono definiti e resi noti i criteri per l'assegnazione del software e delle utenze personali, applicative e di sistema, e delle relative abilitazioni per l'accesso al sistema.

- *Sicurezza:* la sicurezza riguarda: le aree dove sono collocati i sistemi, i PC forniti al personale, le reti. Per quanto riguarda le risorse umane, sono utilizzate procedure di assegnazione e conservazione delle credenziali d'accesso; è regolato l'accesso alle aree protette, alle postazioni e alla rete interna nella rete internet dove è attivo un meccanismo di filtraggio dei siti internet che previene l'accesso e il download non autorizzati e non di carattere aziendale;

- *Tracciabilità:* al solo ed esclusivo fine di carattere difensivo volto ad accertare la commissione di eventuali comportamenti illeciti è prevista la possibilità di un controllo sull'uso pertinente della rete internet che non potrà comportare un controllo qualitativo e quantitativo della prestazione fornita dai lavoratori.

- *Codice Etico:* è richiesta l'osservanza dei principi indicati nel capitolo V ("Uso delle risorse informatiche).

2. Acquisti Licenze e loro gestione

a) Acquisto licenze software di base (sistemi operativi, etc.) o applicativo (per la programmazione, data base, funzionamento macchine, etc.) nell'ambito del sistema centrale (Data Center) o delle postazioni di lavoro (PDL)

- *Regolamentazione:* è richiesto: i) il rispetto delle tipologie di procedimento di acquisto previste in conformità con la vigente normativa; ii) l'indicazione del ruolo e della responsabilità dei diversi attori coinvolti, con separazione di compiti fra l'Area deputata alla gestione degli aspetti negoziali e contrattuali e la funzione richiedente, che cura l'individuazione delle specifiche tecniche del bene/servizio e verifica la corretta

esecuzione della prestazione; iii) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; iv) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale (SCI e Lotus Notes); v) l'archiviazione della documentazione rilevante.

- *Segregazione dei compiti:* è richiesta la separazione delle funzioni di autorizzazione, esecuzione e controllo, in ragione della differente tipologia di procedimento: i) *Acquisti mediante procedure negoziate*: il Consiglio di Amministrazione autorizza fuori dai limiti di spesa delegati, il Direttore Generale e gli altri soggetti delegati, secondo i loro limiti di spesa, sottoscrivono il contratto, la struttura aziendale responsabile degli approvvigionamenti gestisce tecnicamente il processo, la Direzione Amministrazione, Finanza e Controllo supervisiona il processo; ii) *Acquisti mediante procedimento ad evidenza pubblica, ivi compreso il cottimo fiduciario*: il Direttore Generale e gli altri soggetti delegati, firmano per autorizzazione i documenti di gara e/o richieste di offerta, la struttura aziendale responsabile degli approvvigionamenti, con il supporto dell'Unità Organizzativa Societario e legale, espleta gli adempimenti di formalizzazione del procedimento di selezione del fornitore, la Commissione di Gara valuta e propone l'aggiudicazione alla Direzione Generale è il contratto è emesso con firma dei soggetti muniti di potere; il contratto stipulato di cui ai precedenti punti i) e ii) deve prevedere con dettaglio le modalità di acquisizione delle licenze d'uso e di installazione dei software nonché specifiche clausole che garantiscono la non violazione di diritti d'autore, brevetti industriali e in genere privativa altrui, con manleva a favore della Società; iv) *Acquisti per Cassa*: le uscite di cassa sono autorizzate dalla Direzione Amministrazione, Finanza e Controllo, la gestione fisica della cassa e dei prelievi è rimessa al Responsabile della Cassa, l'autorizzazione al reintegro di Cassa è fornita diversamente dalla Direzione Generale.

- *Poteri autorizzativi e di firma:* la sottoscrizione dei contratti avviene nel limite di spesa. E' altresì previsto La Direzione Generale e gli altri soggetti delegati abbiano il potere di sottoscrivere contratti passivi, qualunque ne sia l'importo e l'oggetto, quando questi siano stipulati in relazione all'aggiudicazione di una gara a evidenza pubblica indetta dalla Società.

- *Sicurezza:* nei contratti sono inserite clausole che disciplinano espressamente: i) l'acquisizione della titolarità delle licenze d'uso dei prodotti software; ii) l'acquisizione dei diritti nascenti in modo perpetuo, illimitato ed irrevocabile, iii) le garanzie che il fornitore presta in materia di rispetto della normativa sul diritto d'autore e di altri diritti allo stesso connesso; è previsto il monitoraggio periodico dei fornitori anche attraverso un processo di riqualificazione.

- *Tracciabilità:* è richiesto che: i) sia posta la massima attenzione affinché le informazioni e i dati indicati nella documentazione siano corretti e veritieri; ii) i processi siano documentati; iii) la documentazione sia archiviata. L'utilizzo di supporto informativo per la gestione delle transazioni e dello scambio documentale (Lotus Notes, applicativo gestione richieste di acquisto, applicativo gestione contratti, sistema di contabilità aziendale SCI) garantisce la ricostruibilità ex post del processo di acquisto**.**

- *Codice Etico:* è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari" paragrafo B) e nel capitolo V ("Uso delle risorse informatiche").

b) Gestione licenze software

- *Regolamentazione:* sono previsti: i) i modi di consegna del software acquistato ("materiale in azienda" ovvero "online" con la messa a disposizione da parte del fornitore dei codici di attivazione/accesso, in conformità agli accordi e previsioni contrattuali, ii) le modalità di accettazione (da parte dell'Ufficio Patrimonio, se la consegna è stata materiale, ovvero dalla struttura richiedente all'atto dell'installazione, per consegne on line), di registrazione, inventariazione dei software, e di gestione del registro beni ammortizzabili; iii) di assegnazione e installazione del software acquistato; iv) le modalità di dismissione del software, attraverso alienazione o rottamazione; v) il ruolo e la responsabilità degli attori coinvolti nel processo; vi) l'archiviazione della documentazione rilevante e la tracciabilità di ogni attività, sia on line che con prospetti interni.

- *Segregazione dei compiti:* si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla in relazione alla tipologia di software acquisiti. Inoltre il controllo, oltre che essere effettuato dal personale interno (in mancanza di programmi informatici a ciò deputati), è eseguito anche dai fornitori che eseguono controlli periodici sui software installati e sulla congruità dei codici d'accesso assegnati.

- *Poteri autorizzativi e di firma:* è richiesto che siano titolati ad autorizzare atti di disposizione sul patrimonio solo i soggetti muniti di apposita procura (Presidente e Direttore Generale e altri soggetti delegati) o comunque specificamente individuati mediante atti di ripartizione interna di compiti operativi.

- *Sicurezza:* la sicurezza investe i sistemi – hardware, software, reti – e le procedure informatiche, nonché le risorse umane comprese le procedure di identificazione e autenticazione; le politiche di accesso a sistemi e banche dati (coerenti con privacy); la politica di conservazione delle credenziali di accesso.

- *Tracciabilità:* è richiesto che: i) sia posta la massima attenzione affinché informazioni e dati indicati nella documentazione siano corretti e veritieri; ii) i processi siano documentati; iii) la documentazione sia archiviata; iv) sia ammonito il personale sull'importanza di effettuare continui e accurati controlli. E' richiesto l'utilizzo dei sistemi informatici Lotus Notes e SCI e la registrazione di magazzino di tutte le relative movimentazioni.
- *Codice Etico:* è richiesta l'osservanza dei comportamenti indicati nei capitoli VI ("Libri contabili e registri societari"), VII ("Condotta societaria"), VIII ("Conflitti di interesse") e nel capitolo V ("Uso delle risorse informatiche")

13. REATI IN MATERIA AMBIENTALE

13.1. Reati in materia ambientale

Con l'entrata in vigore del D. Lgs. 7 luglio 2011 n. 121, "Attuazione della direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della direttiva 2009/123/CE che modifica la direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni", è stata estesa la responsabilità amministrativa dell'ente, ferma restando la responsabilità penale della persona fisica che ha materialmente commesso il reato, anche ai "reati ambientali", in quanto il citato D. Lgs. n. 121/2011 ha previsto, tra l'altro, l'inserimento nel D. Lgs. n . 231/01 dell'art. 25-undecies su detta specifica materia.
Il citato art. 25 undecies ha subito delle modifiche a seguito dell'entrata in vigore della Legge 22 maggio 2015 n. 68 "Disposizioni in materia di delitti contro l'ambiente", che ha apportato delle modifiche all'entità delle sanzioni pecuniarie conseguenti alla violazione degli artt. 452 (bis, quater, quinquies, sexies, octies), a decorrere dal 29 maggio 2015.
Tale intervento normativo inserisce nel Codice Penale un nuovo Titolo, VI-bis, dedicato ai delitti contro l'ambiente all'interno del quale sono stati previsti cinque nuovi reati: inquinamento ambientale, disastro ambientale, traffico e abbandono di materiale di alta radioattività, impedimento del controllo.

In tale contesto è da segnalare, infine, l'art. 192 del D.Lgs. 152/2006 (cosiddetto "*Codice ambientale*") in tema di divieto di abbandono di rifiuti. Il citato art. 192 prevede espressamente che se "la responsabilità del fatto illecito sia imputabile ad amministratori o rappresentanti di persona giuridica", la persona giuridica risponde in solido, secondo le previsioni del D.Lgs. 231/01.
Una buona parte di tali reati è configurato dalla Legge stessa come reato-presupposto atto a far scattare la responsabilità amministrativa dell'ente, con conseguente modificazione e integrazione dell'articolo 25-undecies del decreto legislativo 8 giugno 2001 n.231.

L'analisi condotta su tutte le ipotesi di cui sopra ha rilevato che alla fattispecie di interesse per ACI Informatica di cui all'art. 192 del D.Lgs. 152/2006, si aggiungono i nuovi cd. Ecoreati, introdotti dalla Legge 68/2015.

Si provvede di seguito a fornire una descrizione delle fattispecie.

Divieto di abbandono (art. 192 del D.Lgs. 152/2006)

La norma disciplina il divieto di abbandonare o depositate in modo incontrollato i rifiuti sul suolo e nel suolo. Il divieto è esteso anche all'immissione di rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali e sotterranee; la norma, inoltre, obbliga l'autore della violazione a procedere alla loro rimozione, al loro avvio al recupero o allo smaltimento ed al ripristino dello stato dei luoghi in solido con il proprietario e con i titolari di diritti reali o personali di godimento sull'area.

La violazione deve essere imputabile a titolo di dolo o di colpa, in base agli accertamenti effettuati, in contraddittorio con gli autori, dai soggetti preposti al controllo, «*il sindaco, aggiunge il predetto articolo, dispone, con ordinanza, le operazioni a tal fine necessarie e il termine entro cui provvedere, decorso il quale procede all'esecuzione in danno dei soggetti obbligati ed al recupero delle somme anticipate*».
Il requisito della colpa può consistere anche nell'omissione delle cautele e degli accorgimenti che l'ordinaria diligenza suggerisce ai fini di un'efficacia custodia del sito interessato.
In particolare, il comma 4 del citato art. 192 richiama espressamente il D.Lgs. 231/2001 in materia di responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, prevedendo che "*qualora la responsabilità del fatto illecito sia imputabile ad amministratori o rappresentanti di persona giuridica ai sensi e per gli effetti del comma 3, sono tenuti in solido la persona giuridica ed i soggetti ed i soggetti che siano subentrati nei diritti della persona stessa*".

Inquinamento ambientale (art. 452-bis c.p.)

Tale reato punisce chiunque abusivamente cagiona una compromissione o un deterioramento significativi e misurabili:
1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sotto-suolo;
2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna.

Distaccandosi dal modello di illecito costruito sull'esercizio di attività inquinante in difetto di autorizzazione ovvero in superamento dei valori soglia, la previsione risulta costruita come delitto di evento e di danno, dove l'evento di danno è costituito dalla compromissione o dal deterioramento, significativi e misurabili, dei beni ambientali specificamente indicati.

In quanto concepito come reato a forma libera ("chiunque… cagiona…"), l'inquinamento nella sua materialità può consistere non solo in condotte che attengono al nucleo duro - acque, aria e rifiuti – della materia, ma anche mediante altre forme di inquinamento o di immissione di elementi come ad esempio sostanze chimiche, OGM, materiali radioattivi e, più in generale, in qualsiasi comportamento che provochi una immutazione in senso peggiorativo dell'equilibrio ambientale.

Inoltre, l'inquinamento potrà essere cagionato sia attraverso una condotta attiva, ossia con la realizzazione di un fatto considerevolmente dannoso o pericoloso, ma anche mediante un comportamento omissivo improprio, cioè con il mancato impedimento dell'evento da parte di chi, secondo la normativa ambientale, è tenuto al rispetto di specifici obblighi di prevenzione rispetto a quel determinato fatto inquinante dannoso o pericoloso.

Disastro ambientale (art. 452-quater c.p.)

Tale reato si ravvisa se si provoca l'alterazione irreversibile dell'equilibrio di un ecosistema o se l'eliminazione delle conseguenze nocive risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali o se si offende la pubblica incolumità

Delitti colposi contro l'ambiente (art. 452-quinquies c.p.)

L'ipotesi si ravvisa nel momento in cui i reati di cui agli artt. 452-bis e quarter, sono commessi per colpa, comportando una riduzione delle pene previste da un terzo a due terzi.

Se dalla commissione dei fatti di cui sopra deriva il pericolo di inquinamento ambientale o di disastro ambientale le pene sono ulteriormente diminuite di un terzo.

Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.)

Tale reato punisce chi abusivamente cede, acquista, riceve, trasporta, importa, esporta, procura ad altri, detiene, trasferisce, abbandona o si disfa illegittimamente di materiale ad alta radioattività.

Circostanze aggravanti (art. 452-octies c.p.)

L'articolo in oggetto prevede l'aumento delle pene qualora taluno dei delitti individuati venga commesso in forma associata (artt. 416 e 416 bis), così come se dell'associazione fanno parte pubblici ufficiali o incaricati di pubblico servizio che esercitano funzioni o svolgono servizi in materia ambientale.

13.2. Sanzioni in materia di reati ambientali

Divieto di abbandono (art. 192 del D.Lgs. 156/2006)

La violazione deve essere imputabile a titolo di dolo o di colpa, in base agli accertamenti effettuati, in contraddittorio con essi, dai soggetti preposti al controllo, «*il sindaco, aggiunge il predetto articolo, dispone, con ordinanza, le operazioni a tal fine necessarie e il termine entro cui provvedere, decorso il quale procede all'esecuzione in danno dei soggetti obbligati ed al recupero delle somme anticipate*».
Il requisito della colpa può consistere anche nell'omissione delle cautele e degli accorgimenti che l'ordinaria diligenza suggerisce ai fini di un'efficacia custodia del sito interessato.

In particolare, il comma 4 del citato art. 192 richiama espressamente il D.Lgs. 231/2001 in materia di responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, prevedendo che "*qualora la responsabilità del fatto illecito sia imputabile ad amministratori o rappresentanti di persona giuridica ai sensi e per gli effetti del comma 3, sono tenuti in solido la persona giuridica ed i soggetti ed i soggetti che siano subentrati nei diritti della persona stessa*".

In relazione alla commissione dei nuovi reati ambientali del codice penale, nell'art 25-undecies del D.LLgs. 231/01, sono previste le seguenti sanzioni per i reati presupposto:

Inquinamento ambientale (art. 452 – bis c.p.)
-sanzioni pecuniarie: da duecentocinquanta a seicento quote.

Disastro ambientale (art. 452 – quater c.p.)

-sanzioni pecuniarie: da quattrocento a ottocento quote.

Delitti colposi contro l'ambiente (in riferimento all'art. 452 quinquies c.p.)

- sanzioni pecuniarie: da duecento a cinquecento quote

Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.)

-sanzioni pecuniarie: da duecentocinquanta a seicento quote.

Circostanze aggravanti (art. 452 –octies c.p.)

-sanzioni pecuniarie: da trecento a mille quote.

Per i reati di inquinamento ambientale (art. 552 bis c.p.) e di disastro ambientale (art. 452 quater c.p.) si applichino, oltre alle sanzioni pecuniarie ivi previste, le sanzioni interdittive previste dall'articolo 9 del D.Lgs. 231/01, stabilendo una durata massima di 1 anno in relazione al delitto di inquinamento.

Nell'ipotesi colposa, le sanzioni pecuniarie e interdittive sono ridotte di un terzo.

La legge 68/2015 non richiama nei confronti degli enti la possibilità del ravvedimento operoso prevista all'art. 452 decies c.p.

Pertanto sarà applicabile l'attenuante dell'art. 12 del D.Lgs.231/01 che prevede che la sanzione pecuniaria venga ridotta da un terzo alla metà se prima dell'apertura del dibattimento l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è efficacemente adoperato in tal senso.

13.3. Le attività individuate come sensibili ai fini del D.Lgs. 231/2001 in ACI Informatica, con riferimento ai reati ambientali

L'art. 6, comma 2, lett. a) del D.Lgs. 231/2001 indica, come più volte ricordato, tra gli elementi essenziali del modello di organizzazione e di gestione, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.Lgs. 231/2001.

L'analisi dei processi aziendali di ACI Informatica ha consentito di individuare le attività sensibili nel cui ambito potrebbero astrattamente realizzarsi gli illeciti richiamati dall'art.192 del D.Lgs. 152/2006 e dai nuovi ecoreati, o che potrebbero essere strumentali alla loro commissione.

Le attività sensibili identificate sono: la raccolta (intesa come ogni operazione di prelievo, cernita e raggruppamento dei rifiuti per il loro trasporto) e la gestione (intesa come segregazione o deposito temporaneo, trasporto, recupero e smaltimento dei rifiuti, compreso il controllo di queste operazioni) di rifiuti aziendali, quali: toner, carta, cartucce per stampanti, hardware e altri componenti elettrici o elettronici, alluminio, plastica, vetro, rifiuti tossici o pericolosi, etc,

anche qualora venga svolta da soggetti terzi (ad esempio: fornitori, imprese di pulizia o di manutenzione del verde incaricate dalla Società).
Tali attività sono regolamentate da specifica procedura aziendale denominata "Trattamento rifiuti speciali" integrata anche con riferimento alla fase di scelta del fornitore, alla fase di esecuzione e controllo, all'esatta individuazione dei ruoli e delle responsabilità dei soggetti coinvolti.

Inoltre, ulteriore attività sensibile è quella inerente il processo di selezione del fornitore a cui affidare il servizio di raccolta e gestione dei rifiuti aziendale. Tale processo si inquadra nell'ambito della "**Gestione degli Acquisti e del Patrimonio**" per quanto concerne sia l'obbligo di individuare il fornitore dopo l'esperimento di procedure aperte, ristrette, negoziate o altre procedure, nel rispetto delle specifiche procedure aziendali denominate "Approvvigionamenti", "Acquisti in economia- cottimo fiduciario", nonché delle Linee Guida "Ciclo di vita dell'affidamento di appalti di servizi e forniture attraverso procedura ad evidenza pubblica per ACI Informatica S.p.A.", della "Disposizione Organizzativa - Acquisti in Economia" e della "Procedura Approvvigionamento – adozione schema determina a contrarre", sia per quanto riguarda la gestione del processo di rottamazione dei beni aziendali.

13.4. Il sistema dei controlli

Il sistema dei controlli identificato dalla Società prevede il rispetto di specifici principi di controllo relativi alle attività sensibili.

Le disposizioni e gli accorgimenti tecnici previsti nel modello, sono di carattere meramente difensivo e sono volti ad accertare la commissione di eventuali comportamenti illeciti e non anche a consentire un controllo qualitativo-quantitativo sulla prestazione resa dai lavoratori.

13.4.1. Definizione principi del sistema di controllo

I Principi di controllo posti a base degli strumenti e delle metodologie utilizzate possono essere classificati come di seguito indicato:

- **Regolamentazione**: si richiede l'esistenza di regole, linee guida, di procedure formalizzate, nel rispetto delle leggi vigenti in materia ambientale, del Codice Etico e dei principi generali di comportamento presenti nel Modello, che dovranno definire con particolare attenzione il processo di selezione del fornitore in possesso dei necessari requisiti morali e tecnico-professionali nonché delle necessarie autorizzazioni previste dalla normativa, ed individuare con puntualità i ruoli e le responsabilità dei soggetti coinvolti, anche con riferimento a colui a cui compete l'attività di verifica e validazione.
- **Tracciabilità**: si richiede che: i) la documentabilità delle attività dei soggetti coinvolti e dei responsabili delle attività di "gestione" dei rifiuti aziendali; ii) il processo sia identificato e analiticamente definito; iii) sia ammonito il personale sull'importanza di adottare comportamenti tali da evitare, anche solo potenzialmente, anche a titolo di concorso o di tentativo, la commissione degli illeciti; iv) vengano effettuati continui e accurati controlli anche nei confronti di soggetti terzi.

- **Segregazione delle attività**: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- **Poteri autorizzativi e di firma**: si richiede la presenza dei seguenti requisiti: i) coerenza con le responsabilità organizzative e gestionali assegnate, ii) definizione chiara e conoscenza all'interno della Società.
- **Codice Etico:** si richiede il rispetto del Codice Etico, nei suoi principi generali e con riferimento alle previsioni relative ad attività specifiche, già indicate nella parte speciale del modello organizzativo nelle sezioni dedicate ai reati presupposto.

13.4.2. Applicazione dei principi controllo

Il sistema dei controlli prevede presidi specifici individuati nella procedura organizzativa "Trattamento rifiuti speciali" .
In materia ambientale sono fissati, inoltre, i seguenti principi comportamentali di carattere generale, applicabili a tutti i Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività sensibili rispetto ai reati ambientali.
Agli stessi è richiesto di:

- verificare che i fornitori di servizi connessi alla gestione dei rifiuti, ove richiesto dal D.Lgs. 152/2006 e dalle ulteriori fonti normative e regolamentari, dichiarino e diano, in ogni caso, evidenza, in base alla natura del servizio prestato, del rispetto della disciplina in materia di gestione dei rifiuti e di tutela dell'ambiente;
- accertare, prima dell'instaurazione del rapporto, la rispettabilità e l'affidabilità dei
-fornitori di servizi connessi alla gestione dei rifiuti, anche attraverso l'acquisizione e la verifica delle comunicazioni, certificazioni e autorizzazioni in materia ambientale da questi effettuate o acquisite a norma di legge, astenendosi dall'avviare rapporti con i fornitori che non offrano garanzie di onorabilità e serietà professionale;
-inserire nei contratti stipulati con i fornitori di servizi connessi alla gestione dei rifiuti
-specifiche clausole attraverso le quali i fornitori si impegnino nei confronti di ACI Informatica a mantenere valide ed efficaci per l'intera durata del rapporto contrattuale le autorizzazioni prescritte dalla normativa per lo svolgimento dell'attività di gestione dei rifiuti.
- inserire nei contratti stipulati con i fornitori di servizi connessi alla gestione dei rifiuti specifiche clausole attraverso le quali ACI Informatica possa riservarsi il diritto di
- verificare periodicamente le comunicazioni, certificazioni e autorizzazioni in materia ambientale, tenendo in considerazione i termini di scadenza e rinnovo delle stesse;
- aggiornare periodicamente l'archivio delle autorizzazioni, iscrizioni e comunicazioni acquisite dai fornitori terzi e segnalare tempestivamente alla funzione preposta ogni variazione riscontrata;
- smaltire le sostanze lesive non rigenerabili né riutilizzabili, nel rispetto delle norme contro l'inquinamento;
- conferire i beni durevoli contenenti le sostanze lesive, al termine della loro durata operativa, a centri di raccolta autorizzati;
- impiegare esclusivamente personale specializzato nelle attività di estrazione, raccolta ed isolamento delle sostanze lesive;
- assicurarsi che i fornitori di servizi che operano nei siti conoscano e rispettino le procedure aziendali in materia ambientale.

È fatto espresso divieto ai Destinatari di:

- abbandonare o depositare in modo incontrollato i rifiuti ed immetterli, allo stato solido o liquido, nelle acque superficiali e sotterranee, in violazione delle procedure aziendali;
- miscelare categorie diverse di rifiuti pericolosi (oppure rifiuti pericolosi con quelli non pericolosi);
- violare gli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari per la gestione dei rifiuti;
- effettuare o predisporre attività organizzate per il traffico illecito di rifiuti;
- falsificare o alterare il certificato di analisi dei rifiuti, anche utilizzato nell'ambito del SISTRI – Area Movimentazione;
- falsificare o alterare qualsiasi documento da sottoporre a Pubbliche Amministrazioni o Autorità di controllo ovvero omettere di comunicare tempestivamente informazioni o dati su fatti o circostanze che possano compromettere la salute pubblica;
- astenersi dall'intrattenere rapporti con gestori di rifiuti che, sulla base di notizie acquisite, possano non dare garanzia di serietà;
- disperdere nell'ambiente le sostanze lesive;
- consumare, importare, esportare, detenere e commercializzare le sostanze lesive, secondo modalità diverse da quelle disciplinate dalla vigente normativa.

14. REATI IN MATERIA DI IMPIEGO DI STRANIERI PRIVI DEL PERMESSO DI SOGGIORNO

14.1. Reati in materia di impiego di stranieri privi del permesso di soggiorno richiamati dall'art. 25-duodecies del D.Lgs. 231/01

Il D.Lgs. 109/2012 ha ampliato il catalogo dei reati che possono generare una responsabilità diretta dell'ente inserendo nel D.Lgs. 231/01 l'art. 25-duodecies in merito all'impiego di lavoratori stranieri senza o irregolare permesso di soggiorno, richiamando la fattispecie prevista all'art. 22, comma 12-bis del D.Lgs. 25 luglio 1998, n. 286.

In pratica, è estesa la responsabilità agli Enti, quando lo sfruttamento di manodopera irregolare supera certi limiti, in termini di numero di lavoratori (maggiori di tre), età (minori in età lavorativa) e condizioni lavorative (sfruttamento), nei termini stabiliti dall'art. 22, comma 12 bis del D.Lgs. 25 luglio 1998, n. 286, cd."Testo unico dell'immigrazione".

14.2. Sanzioni in materia di impiego di stranieri privi del permesso di soggiorno previste dal D.Lgs. 231/01

In relazione alla commissione del delitto di cui all'art. 22, comma 12-bis, del D.Lgs. 286/98, si applica all'ente:

-sanzioni pecuniarie: da cento a duecento quote, entro il limite di 150.000 euro.

14.3. Le attività individuate come sensibili ai fini del D.Lgs. 231/2001 in ACI Informatica, con riferimento ai reati in materia di impiego di stranieri privi del permesso di soggiorno

L'art. 6, comma 2, lett. a) del D.Lgs. 231/2001 indica, come più volte ricordato, tra gli elementi essenziali del modello di organizzazione e di gestione, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.Lgs. 231/2001.

L'analisi dei processi aziendali di ACI Informatica ha consentito di individuare quale attività sensibile quella riferita alla '**Gestione delle Risorse Umane**'.
Trattasi dell'attività concernente la gestione della selezione ed assunzione del personale, nonché tutta l'attività di gestione del rapporto di lavoro con le risorse individuate.
Tale attività è regolamentata anche da specifica procedura aziendale denominata "Gestione assunzioni".

14.4. Il sistema dei controlli

Il sistema dei controlli identificato dalla Società prevede il rispetto di specifici principi di controllo relativi alle attività sensibili.

Le disposizioni e gli accorgimenti tecnici richiamati nel modello, sono di carattere meramente difensivo e sono volti ad accertare la commissione di eventuali comportamenti illeciti e non anche a consentire un controllo qualitativo-quantitativo sulla prestazione resa dai lavoratori.

14.4.1. Definizione dei principi di controllo

I Principi di controllo posti a base degli strumenti e delle metodologie utilizzate possono essere classificati come di seguito indicato:

- **Regolamentazione**: si richiede l'esistenza di regole, linee guida, procedure formalizzate, o prassi consolidate, idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili, nonché modalità di archiviazione della documentazione rilevante.
- **Tracciabilità**: si richiede la documentabilità delle attività sensibili. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile *ex post*, anche tramite appositi supporti documentali.
- **Segregazione delle attività**: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- **Poteri autorizzativi e di firma**: si richiede la presenza dei seguenti requisiti in merito ai poteri autorizzativi e di firma: i) coerenza con le responsabilità organizzative e gestionali assegnate; ii) definizione chiara e conoscenza all'interno della Società.
- **Codice Etico:** si richiede il rispetto del Codice Etico, nei suoi principi generali e con riferimento alle previsioni relative ad attività specifiche, già indicate nella parte speciale del modello organizzativo nelle sezioni dedicate ai reati presupposto.

14.4.2. Applicazione dei principi di controllo

Il sistema dei controlli prevede presidi specifici individuati nelle procedure e prassi aziendali.

- *Regolamentazione*: sono individuati ruoli e responsabilità dei diversi soggetti nelle attività di seguito indicate: i) selezione dei candidati; ii) reperimento dei *curricula*; iii) valutazione, "attitudinale" e "tecnica", del candidato; iv) segregazione delle funzioni coinvolte nel processo di richiesta di assunzione personale e in quello di valutazione/selezione o promozione del personale stesso; v) gestione amministrativa del contratto di lavoro e sua aderenza alla normativa di settore; vi) archiviazione della documentazione rilevante.
- *Segregazione dei compiti*: è prevista una separazione dei compiti nelle diverse fasi del processo. E' prevista pertanto una distinta allocazione dei poteri autorizzativi e di controllo in fase di definizione del Budget, redatto dalla Direzione Generale nonché dalla Direzione Amministrazione, Finanza e Controllo, nelle attività di selezione ed assunzione delle risorse, nonché nella gestione amministrativa del contratto di lavoro, spettante all'Area Gestione Risorse Umane sotto la supervisione della Direzione del Personale e autorizzata dal Presidente o da diversa persona nell'ambito di eventuali poteri delegati,
- *Procure e deleghe:* è richiesto che i contratti di lavoro siano sottoscritti soltanto da persone munite di apposita procura in tal senso, con specificazione di limiti di valore oltre i quali il contratto deve essere sottoscritto da soggetto di livello gerarchico superiore).

- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dai capitoli II ("Comportamento nella gestione degli affari", paragrafo C), III ("Salute, sicurezza, ambiente", paragrafo A), IV ("Trattamento di informazioni interne"), VIII ("Conflitti di interesse") e IX ("Valenza del *Codice Etico").*

La Società non consente alcuna forma di lavoro irregolare rispetto alla normativa vigente. Pertanto, nel caso di lavoratori stranieri non verranno presi in considerazione soggetti non in regola con la normativa relativa all'immigrazione (ad esempio privi di permessi di soggiorno, ovvero il cui permesso sia scaduto – e per il quale non si sia richiesto il rinnovo – revocato o annullato).

15. REATI IN MATERIA DI RICETTAZIONIE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA, NONCHE' AUTORICICLAGGIO

15.1. I Reati richiamati dall'art. 25-octies del D.Lgs. 231/01

La Legge 15 dicembre 2014, n. 186 ha ampliato le fattispecie di reato previste dall'art. 25 – octies del D.Lgs. 231/01, includendo al comma 5 dell'art. 3 la nuova fattispecie di "autoriciclaggio" tra i reati presupposto della responsabilità amministrativa "da reato" degli enti.

Il reato di **autoriciclaggio** è definito nell'art. 648-ter.1 del codice penale punisce " chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa"**.**

L'art. 648 ter.1 prevede un trattamento sanzionatorio per chi ricicla in prima persona, cioè sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo da egli commesso (o che ha concorso a commettere), ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.
Ne consegue pertanto la possibilità di sanzionare gli enti i cui soggetti, apicali o meno, dopo aver commesso o concorso a commettere un delitto non colposo, impieghino, sostituiscano, trasferiscano, in attività, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione del precedente delitto, in modo da ostacolare concretamente l'identificazione della provenienza delittuosa

La norma dunque è chiaramente volta non solo ad azzerare i risvolti economici del reato presupposto compiuto a monte dal reo ma, altresì, a contrastare dette condotte svolte per mezzo o attraverso la copertura di una persona giuridica.

Un esimente a tale reato è prevista nel caso in cui il denaro, i beni o le altre utilità derivanti dal reato vengano destinati al mero godimento o utilizzo del reo e, quindi, non al riutilizzo in attività economiche, finanziarie, imprenditoriali o speculative.

Il generico riferimento al "delitto non colposo" quale reato – base dell'autoriciclaggio ha dato luogo a dubbi interpretativi al momento non risolti dalla giurisprudenza. Infatti, non è chiaro se l'eventuale responsabilità dell'ente è limitata ai casi in cui il reato – base dell'autoriciclaggio rientra tra i reati presupposto di cui al catalogo del D.Lgs. 231/01, ovvero se esso possa considerarsi anche in presenza di fattispecie diverse, come ad esempio i reati tributari che non costituiscono reato-presupposto del D.Lgs. 231/01.
In assenza di una concreta presa di posizione sull'argomento da parte della giurisprudenza, in via prudenziale sono innanzitutto considerati rilevanti i reati con matrice comune all'autoriciclaggio, quali la ricettazione (art. 684 c.p.), il riciclaggio (art. 648 bis c.p.) e l'impiego di denaro, di beni o utilità di provenienza illecita (art. 648 – ter c.p.).

Occorre considerare, peraltro, che se l'autoriciclaggio ha quale base i "delitti non colposi" previsti dal catalogo del D.Lgs. 231 i presidi di comportamento già posti in essere possono risultare efficaci anche per la prevenzione dell'autoriciclaggio.
Se, invece, la provenienza del denaro è riconducibile a reati non rientranti del D.Lgs. 231/01, come quelli tributari ad esempio, l'attenzione è posta oltre che al controllo sulla provenienza del denaro, soprattutto sulle modalità di utilizzo dello stesso cercando di individuare comportamenti anomali o non ordinari dei flussi di denaro.

Di seguito la descrizione delle fattispecie dei reati di matrice comune all'autoriciclaggio.

- **Ricettazione** (art. 648 c.p.): costituito dalla condotta di chi, fuori dei casi di concorso nel reato, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare.
- **Riciclaggio** (art. 648-bis c.p.): costituito dalla condotta di chi, fuori dei casi di concorso nel reato, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.
- **Impiego di denaro, beni o utilità di provenienza illecita** (art. 648-ter c.p.): costituito dalla condotta di chi, fuori dei casi di concorso nel reato e dei casi previsti dagli artt. 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

15.2. Sanzioni in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio dal D.Lgs. 231/01

In relazione alla commissione del reati di cui agli artt. 648, 648-bis, 648-ter e 648-ter1. Del codice penale, richiamati dall'art. 25-ocietes del D.lgs. 231/01, si applicano all'ente:

-sanzione pecuniaria: da duecento a ottocento quote.

-sanzione pecuniaria da quattrocento a mille quote: nel caso in cui il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni.

-sanzioni interdittive previste dall'art.9, comma 2, del D.Lgs. 231/2001, per una durata non superiore a due anni,

15.3. Le attività individuate come sensibili ai fini del D.Lgs. 231/2001 in ACI Informatica

L'art. 6, comma 2, lett. a) del D.Lgs. 231/2001 indica, come più volte ricordato, tra gli elementi essenziali del modello di organizzazione e di gestione, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.Lgs. 231/2001.
Ciò al fine di accertare l'origine lecita di ogni provento derivante dal reinvestimento di beni o denaro nell'interesse e a vantaggio della società, non trascurando i possibili effetti derivanti dal

fatto che possono costituire reato presupposto dell'autoriciclaggio anche fattispecie non incluse nell'elencazione contenuta nel D.Lgs. 231. Si pensi, ad esempio, ai reati tributari, veicoli tradizionali del reato di riciclaggio e oggetto di lungo dibattito rispetto alla loro possibile inclusione nell'ambito della responsabilità degli enti.

Oltre ad operare un doveroso richiamo dei protocolli già implementati rispetto ai reati-fonte già mappati in quanto fattispecie presupposto 231 (si pensi, solo per fare un esempio, ai reati di truffa ai danni dello stato, di corruzione o induzione indebita a dare o promettere utilità, di frode nell´esercizio del commercio, ai delitti contro la proprietà intellettuale e industriale, ecc.), l'analisi dei processi aziendali di ACI Informatica ha consentito di individuare quale attività sensibile quella riferita alla '**Gestione dei flussi finanziari**', alla "**Gestione degli Acquisti e degli Incarichi di collaborazione e consulenza**", alla "**Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con enti della P.A. o con società del gruppo ACI**" e alla "**Gestione di software pubblici o forniti da terzi per conto di soggetti pubblici per comunicare con la P.A".**

Gestione dei Flussi Finanziari: l'attività si riferisce alle modalità di gestione ed alla movimentazione delle risorse finanziarie relative all'attività di impresa, idonee ad impedire la commissione dei reati.

Gestione degli Acquisti: si tratta dell'attività di negoziazione/ stipulazione e/o esecuzione di contratti per l'acquisizione di beni e servizi ai quali si perviene mediante procedure aperte, ristrette, negoziate o altre procedure.
Ci si riferisce, in particolare, ai processi di: i) acquisti di beni e servizi mediante procedure negoziate; ii) acquisti di beni e servizi mediante procedure ristrette o aperte; iii) incarichi di collaborazione e consulenza; iv) gestione del patrimonio.

Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con enti della P.A. o con società del gruppo: il processo riguarda la negoziazione e la stipulazione di contratti attraverso i quali ACI Informatica si propone agli enti della Pubblica Amministrazione e alle società del gruppo ACI al fine di realizzare accordi per la commercializzazione di prodotti/servizi ovvero partnership.

Gestione di software pubblici o forniti da terzi per conto di soggetti pubblici per comunicare con la P.A.: il processo consiste nell'utilizzo di software pubblici per la trasmissione al Ministero delle Finanze delle dichiarazioni dei redditi o dei sostituti d'imposta ed in genere tutte le dichiarazioni funzionali alla liquidazione dei tributi (per mezzo del sistema telematico ENTRATEL di proprietà del Ministero delle Finanze) e per la trasmissione all'INPS di denunce contributive, relative ad adempimenti previdenziali e ritenute a carico di ACI Informatica e del personale aziendale, mediante software UNIEMENS – aggregato e individuale, di proprietà dell'ente INPS.

15.4. Il sistema dei controlli

Il sistema dei controlli identificato dalla Società prevede il rispetto di specifici principi di controllo relativi alle attività sensibili.

Le disposizioni e gli accorgimenti tecnici richiamati nel modello, sono di carattere meramente difensivo e sono volti ad accertare la commissione di eventuali comportamenti illeciti e non anche a consentire un controllo qualitativo-quantitativo sulla prestazione resa dai lavoratori.

15.4.1. Definizione dei principi di controllo

I Principi di controllo posti a base degli strumenti e delle metodologie utilizzate possono essere classificati come di seguito indicato:

- **Regolamentazione**: si richiede l'esistenza di regole, linee guida, procedure formalizzate, o prassi consolidate, idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili, nonché modalità di archiviazione della documentazione rilevante.
- **Tracciabilità**: si richiede la documentabilità delle attività sensibili. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile *ex post*, anche tramite appositi supporti documentali.
- **Segregazione delle attività**: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- **Poteri autorizzativi e di firma**: si richiede la presenza dei seguenti requisiti in merito ai poteri autorizzativi e di firma: i) coerenza con le responsabilità organizzative e gestionali assegnate; ii) definizione chiara e conoscenza all'interno della Società.
- **Codice Etico:** si richiede il rispetto del Codice Etico, nei suoi principi generali e con riferimento alle previsioni relative ad attività specifiche, già indicate nella parte speciale del modello organizzativo nelle sezioni dedicate ai reati presupposto.

Inoltre, sono fissati i seguenti principi comportamentali di carattere generale, applicabili a tutti i Destinatari del presente Modello che consentano di prevenire il rischio di commissione del reato di auto riciclaggio, e precisamente:

- il divieto di occultare i proventi derivanti da eventuale reato commesso nel presunto interesse o vantaggio della società;
- garantire la trasparenza e la tracciabilità delle transazioni finanziarie;
- privilegiare le transazioni utilizzando il sistema bancario;
- utilizzo o impiego di risorse economiche/finanziarie di cui sia stata verificata la provenienza e solo per operazioni che abbiano una causale espressa e che risultino registrate e documentate;
- le condizioni e i termini contrattuali che regolano i rapporti con fornitori e partner commerciali e finanziari, anche tra società appartenenti al medesimo gruppo, siano adeguatamente formalizzate;

- il divieto di effettuare prestazioni in favore di fornitori, consulenti e partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- il divieto di riconoscere compensi a favore di amministratori, fornitori, consulenti e partner che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere.

15.4.2. Applicazione dei principi di controllo

Nella fase di applicazione il sistema dei controlli prevede presidi specifici per ciascuna delle attività individuate come attività a rischio.

1. *Gestione degli Acquisti e degli Incarichi di collaborazione e consulenza*

Con riferimento all'attività di acquisto di beni e servizi, i protocolli specifici adottati sono i seguenti:

- *Regolamentazione*: al fine di evitare la stipulazione di contratti con modalità tali da occultarne la provenienza delittuosa, è richiesta: i) l'esplicita previsione delle tipologie di procedimento di acquisto utilizzabili in conformità con la vigente normativa che individua i controlli anche sull'affidabilità commerciale e professionale del fornitore; ii) l'indicazione del ruolo e della responsabilità dei diversi attori coinvolti, con separazione di compiti fra l'Area deputata alla gestione degli aspetti negoziali e contrattuali, e la funzione richiedente, che cura l'individuazione delle specifiche tecniche del bene/servizio e verifica la corretta esecuzione della prestazione; iii) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; iv) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; v) l'archiviazione della documentazione rilevante.
- *Tracciabilità*: è richiesto che: i) sia posta la massima attenzione affinché informazioni e dati indicati nella documentazione siano corretti e veritieri; ii) i processi siano documentati; iii) la documentazione sia archiviata. L'utilizzo di supporto informativo per la gestione delle transazioni e dello scambio documentale (Lotus Notes, applicativo gestione richieste di acquisto, applicativo gestione contratti), garantisce la ricostruibilità ex post del processo di acquisto.
- *Segregazione dei compiti*: è richiesta separazione delle funzioni di autorizzazione, esecuzione e controllo, in ragione della differente tipologia di procedimento: i) *Acquisti mediante procedure negoziate (affidamenti diretti)*: il Consiglio di Amministrazione autorizza, fuori dai limiti di spesa delegati, il Direttore Generale e gli altri soggetti delegati, secondo i loro limiti di spesa, sottoscrivono il contratto, la struttura aziendale responsabile degli approvvigionamenti gestisce tecnicamente il processo, la Direzione Amministrazione, Finanza e Controllo supervisiona il processo; all'interno dei limiti di spesa delegati, le Determine a contrarre sono emesse dal Responsabile Unico del Procedimento, ii) *Acquisti mediante procedimento ad evidenza pubblica, ivi compreso il cottimo fiduciario:* il Direttore Generale e gli altri soggetti delegati, firmano per autorizzazione i documenti di gara e/o richieste di offerta, la struttura aziendale responsabile degli approvvigionamenti, con il supporto della Direzione Societario e Legale, espleta gli adempimenti di

formalizzazione del procedimento, la Commissione di Gara valuta e propone l'aggiudicazione alla Direzione Generale, il Contratto è emesso con firma dei soggetti muniti di potere; all'interno dei limiti di spesa delegati, le Determine a contrarre sono emesse dal Responsabile Unico del Procedimento. iii) *Acquisti per Cassa:* le uscite di cassa sono autorizzate dal Responsabile della Direzione Amministrazione, Finanza e Controllo, la gestione fisica della cassa e dei prelievi è rimessa al Responsabile della Cassa, l'autorizzazione al reintegro di Cassa è fornita diversamente dalla Direzione Generale.

- *Poteri autorizzativi e di firma:* la sottoscrizione dei contratti avviene nel limite di spesa. E' altresì previsto che il Presidente, il Direttore Generale e gli altri soggetti delegati, abbiano il potere di sottoscrivere contratti passivi, qualunque ne sia l'importo e l'oggetto, quando questi siano stipulati in relazione all'aggiudicazione di una gara ad evidenza pubblica, compresi gli acquisti in economia, indette da ACI Informatica.
- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari", paragrafo B).

2. *Gestione dei Flussi Finanziari*

- *Regolamentazione*: sono individuati ruoli e responsabilità nella gestione dei flussi finanziari, per la disciplina degli aspetti concernenti: i) i soggetti coinvolti nel processo; ii) le modalità operative per la gestione di pagamenti ed incassi che assicurino, tra l'altro, il rispetto di tutti i passaggi autorizzativi relativi alla predisposizione, validazione ed emissione del mandato di pagamento, nonché la registrazione a sistema della relativa distinta, nonché la verifica della relativa regolarità formale e della congruità del pagamento con il contratto/ordine d'acquisto corrispondente; iii) i meccanismi di controllo della regolarità delle operazioni, anche attraverso il coinvolgimento nel processo di soggetti appartenenti ad almeno due strutture aziendali differenti; iv) le attività di verifica della rendicontazione bancaria inerente le movimentazioni di fondi. E' fatto obbligo di preferire il canale bancario, i pagamenti in contanti devono essere limitati nel numero e nell'importo e devono essere adeguatamente documentati e monitorati.
- *Segregazione dei compiti*: è prevista la separazione delle funzioni di autorizzazione, esecuzione e controllo, che sono affidate, a distinti soggetti/funzioni aziendali tra loro indipendenti.
- *Tracciabilità:* è prevista la completa tracciabilità di tutte le operazioni effettuate, l'archiviazione dei documenti di pagamento e di incasso nonché l'utilizzo di sistemi informatici idonei a tracciare ex-post l'iter del processo e le operazioni eseguite. Anche nell'ambito dei rapporti infragruppo.
- *Poteri autorizzativi e di firma:* è richiesta un'autorizzazione formalizzata alla disposizione di pagamento, con limiti di spesa, vincoli e responsabilità.
- *Codice Etico*: è richiesta l'osservanza delle indicazioni comportamentali previste dai capitoli II ("Comportamento nella gestione degli affari"), VI ("Libri contabili e registri societari") e VII ("Condotta societaria").

3. *Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con enti della P.A. o con società del gruppo*

- *Regolamentazione*: al fine di evitare la stipulazione di contratti con modalità tali da occultarne la provenienza delittuosa è richiesta: i) l'indicazione del ruolo e della responsabilità dei diversi attori coinvolti nel processo, con separazione di compiti fra l'Area deputata alla gestione degli aspetti negoziali e contrattuali, e la funzione offerente, che cura l'individuazione delle specifiche tecniche del servizio e verifica la corretta erogazione della prestazione; ii) i livelli autorizzativi previsti per ciascuna fase del processo; iii) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; iv) l'archiviazione della documentazione rilevante.
- *Tracciabilità*: è richiesto che: i) sia posta la massima attenzione affinché informazioni e dati indicati nella documentazione siano corretti e veritieri; ii) i processi siano documentati; iii) la documentazione sia archiviata. L'utilizzo di supporto informativo per la gestione delle transazioni e dello scambio documentale (Lotus Notes, applicativo gestione contratti) garantisce la ricostruibilità ex post del processo.
- *Segregazione dei compiti*: è richiesta separazione delle funzioni di autorizzazione, esecuzione e controllo;
- *Poteri autorizzativi e di firma:* la sottoscrizione dei contratti avviene nel limite di spesa.
- *Codice Etico*: è richiesta l'osservanza dei principi e comportamenti indicati nel capitolo II ("Comportamento nella gestione degli affari", paragrafo B) e nel capitolo VI ("Libri contabili e registri societari") e VII ("Condotta societaria").

4. *Gestione di software pubblici o forniti da terzi per conto di soggetti pubblici per comunicare con la P.A.*

- *Regolamentazione*: sono individuati i soggetti deputati alla gestione dei software necessari all'invio dei dati al Ministero delle Finanze e all'INPS e le modalità di estrazione dei dati e di verifica, approvazione, caricamento a sistema ed invio delle dichiarazioni ai soggetti pubblici competenti.
- *Tracciabilità*: la tracciabilità del processo di trasmissione in esame, è garantita dalla registrazione ed archiviazione della seguente documentazione: dichiarazioni fiscali approvate e inviate, ricevute delle trasmissioni, modulo DM10, ricevute delle trasmissioni, nonché dei fogli di controllo della corrispondenza fra le dichiarazioni inviate e le operazioni di estrazione dati eseguite.
- *Segregazione dei compiti*: il protocollo prevede: i) in relazione alla trasmissione di dichiarazioni fiscali mediante software pubblico, la separazione dei compiti di autorizzazione all'invio delle dichiarazioni, rilasciata dal Collegio Sindacale e dalla Direzione Generale, di esecuzione dell'estrazione dati dai file aziendali, affidata alla struttura competente, di verifica/supervisione della Direzione Amministrazione, Finanza e Controllo; ii) in relazione alla trasmissione di dati relativi al trattamento pensionistico mediante software pubblico la separazione dei compiti di autorizzazione, fornita dalla Direzione Generale, di esecuzione, affidata all'Area Gestione Risorse Umane, di controllo, affidato alla Direzione del Personale.

- *Poteri autorizzativi e di firma:* è previsto che siano autorizzati ad intrattenere rapporti con soggetti appartenenti alla Pubblica Amministrazione solo i soggetti muniti di apposita procura (Presidente, Direttore Generale) o comunque specificamente individuati mediante atti di ripartizione interna di compiti operativi.
- *Codice Etico*: è richiesta l'osservanza delle indicazioni comportamentali previste dai capitoli II ("Comportamento nella gestione degli affari", paragrafo E), IV ("Trattamento di informazioni interne").

16. ALLEGATI

16.1. Codici e Manuali

a) Codice Etico
b) Codice Disciplinare Aziendale
c) Manuale della Qualità
d) Manuale della Sicurezza
e) Manuale per la tutela dei lavoratori nei luoghi di lavoro e valutazione dei rischi
f) Manuale Tecnico del Sistema Informatico contabile aziendale (SCI)

16.2. Organigramma aziendale

a) Organigramma della Società

16.3. Procedure (*alcune procedure richiamate sono gestite nell'ambito del sistema qualità aziendale*)

a) Disposizione organizzativa AVCP Procedura SIMOG (vedi anche Tracciabilità dei flussi finanziari)
b) Linee guida procedure di gara (acquisti sopra la soglia comunitaria)
c) Acquisti in economia (assorbita dalla procedura della lett.n. – vedi anche disposizione del Direttore Generale del 21/10/2014)
d) Procedura organizzativa Approvvigionamenti
e) Flussi informativi da e verso l'Organismo di Vigilanza
f) Codice di Corporate Governance
g) Procedura del processo di chiusura del bilancio d'esercizio e delle chiusure trimestrali
h) Verifiche effettuate da organi sociali e da soggetti esterni
i) Fornitura dei servizi commerciali
j) Trasmissione telematica dei dati contributivi e previdenziali all'INPS
k) Trasmissione telematica dei dati fiscali
l) Gestione del contenzioso
m) Gestione fisica ed amministrativa del patrimonio
n) Gestione degli Acquisti in economia e disposizione del Direttore Generale del 21/10/2014
o) Gestione assunzioni
p) Gestione incentivi
q) Procedura e sistema delle rilevazioni contabili - Ciclo attivo
r) Procedura e sistema delle rilevazioni contabili - Ciclo passivo
s) Procedura e sistema delle rilevazioni contabili - Ciclo finanziario
t) Gestione Magazzino
u) Contabilizzazione stipendi
v) Gestione delle partecipazioni societarie
w) Disciplinare tecnico per l'utilizzo di posta elettronica, internet e strumenti elettronici
x) Gestione dei personal computer
y) Criteri di assegnazione delle utenze

z) Utilizzo di dispositivi di firma digitale e caselle di posta elettronica certificata
aa) Procedura organizzativa Trattamento rifiuti speciali
bb) Procedura organizzativa Gestione rottamazione dei beni aziendali
cc) Procedura per il conferimento di incarichi di consulenza professionale
dd) Procedura Approvvigionamento – Adozione schema determina a contrarre
ee) Linee guida Tracciabilità dei flussi finanziari
ff) Procedura per il conferimento di incarichi di collaborazione

16.4. Deleghe Aziendali

16.5. Regolamento di *Governance* per le società controllate da ACI

16.6. Attività di Vigilanza sul Modello di Organizzazione, Gestione e Controllo - Regolamento dell'Organismo di Vigilanza

17. APPENDICE - REATI

Di seguito, si riporta il testo dei reati richiamati nel documento nella parte speciale.

REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE

Malversazione a danno dello Stato (art. 316-bis c.p.)

Chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni.

Indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.)

Salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni.
Quando la somma indebitamente percepita è pari o inferiore a euro 3.999,96 si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da euro 5.164 a euro 25.822. Tale sanzione non può comunque superare il triplo del beneficio conseguito.

Truffa in danno dello Stato o di altro ente pubblico (art. 640, comma 2, n. 1, c.p.)

Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549:

1. Se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare;

2. Se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità.

2.bis. Se il fatto è commesso in presenza della circostanza di cui all'art. 61, n. 5.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o un'altra circostanza aggravante.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)

La pena è della reclusione da uno a sei anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.

Frode informatica (art. 640-ter c.p.)

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

Concussione (art. 317 c.p.)

Il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri costringe taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro o altra utilità, è punito con la reclusione da sei a dodici anni.

Corruzione per l'esercizio della funzione (art. 318 c.p.)

Il pubblico ufficiale, che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve , per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da uno a sei anni.

Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)

Il pubblico ufficiale che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da sei a dieci anni.

Corruzione in atti giudiziari (art 319-ter c.p.)

Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da sei a dodici anni

Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da sei a quattordici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da otto a venti anni.

Induzione indebita a dare o promettere utilità (Art. 319-quater c.p.)

Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei a dieci anni e sei mesi.

Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni.

Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.)

Le disposizioni degli articoli 318 e 319 si applicano anche all'incaricato di un pubblico servizio.

In ogni caso, le pene sono ridotte in misura non superiore a un terzo.

Pene per il corruttore (art. 321 c.p.)

Le pene stabilite nel primo comma dell'articolo 318, nell'articolo 319, nell'articolo 319-bis, nell'art. 319-ter, e nell'articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità.

Istigazione alla corruzione (art. 322 c.p.)

Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo.

Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo.

La pena di cui al primo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri.

La pena di cui al secondo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319.

Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità e di Stati esteri (art. 322-bis c.p.)

Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:

1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;

2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;

3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;

4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;

5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;

5-bis) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale.

Le disposizioni degli articoli 319-quater, secondo comma, ([3]) 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:

1) alle persone indicate nel primo comma del presente articolo;

2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali ovvero al fine di ottenere o di mantenere un'attività economica finanziaria.

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

Abuso di ufficio (art. 323 c.p.)

Salvo che il fatto non costituisca un più grave reato, il pubblico ufficiale o l'incaricato di pubblico sevizio che, nello svolgimento delle funzioni o del servizio, in violazione di norme di

legge o di regolamento, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto è punito con la reclusione da uno a quattro anni.

La pena è aumentata nei casi in cui il vantaggio o il danno hanno un carattere di rilevante gravità.

REATI SOCIETARI

False comunicazioni sociali (art. 2621 c.c.)

Fuori dai casi previsti dall'art. 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da uno a cinque anni.

La stessa pena si applica anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.

Fatti di lieve entità (art. 2621 bis c.c.)

Salvo che costituiscano più grave reato, si applica la pena da sei mesi a tre anni di reclusione se i fatti di cui all'articolo 2621 sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta.

Salvo che costituiscano più grave reato, si applica la stessa pena di cui al comma precedente quando i fatti di cui all'articolo 2621 riguardano società che non superano i limiti indicati dal secondo comma dell'articolo 1 del regio decreto 16 marzo 1942, n. 267. In tale caso, il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale.

Non punibilità per particolare tenuità (Art. 2621-ter)

Ai fini della non punibilità per particolare tenuità del fatto, di cui all'articolo 131-bis del codice penale, il giudice valuta, in modo prevalente, l'entità dell'eventuale danno cagionato alla società, ai soci o ai creditori conseguente ai fatti di cui agli articoli 2621 e 2621-bis.

False comunicazioni sociali delle società quotate (art. 2622 c.c.)

Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea, i quali, al fine di conseguire per sé o per altri un ingiusto profitto nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico consapevolmente espongono fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al

quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da tre a otto anni.

Alle società indicate nel comma precedente sono equiparate:

1) le società emittenti strumenti finanziari per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;

2) le società emittenti strumenti finanziari ammessi alla negoziazione in un sistema multilaterale di negoziazione italiano;

3) le società che controllano società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;

4) le società che fanno appello al pubblico risparmio o che comunque lo gestiscono.

Le disposizioni di cui ai commi precedenti si applicano anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.

Impedito controllo (art. 2625 c.c.)

Gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali, sono puniti con la sanzione amministrativa pecuniaria fino a 10.329 euro.

Se la condotta ha cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa.

La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.

Formazione fittizia del capitale (art. 2632 c.c.)

Gli amministratori e i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione, sono puniti con la reclusione fino ad un anno.

Indebita restituzione dei conferimenti (art. 2626 c.c.)

Gli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli, sono puniti con la reclusione fino ad un anno.

Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)

Salvo che il fatto non costituisca più grave reato, gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che

ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite, sono puniti con l'arresto fino ad un anno.

La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)

I liquidatori che, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionano danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Corruzione tra privati (art. 2635 c.c.)

Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, che, a seguito della dazione o della promessa di denaro o altra utilità, per sè o per altri, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società, sono puniti con la reclusione da uno a tre anni.

Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma.

Chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste.

Le pene stabilite nei commi precedenti sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.

Si procede a querela della persona offesa, salvo che dal fatto derivi una distorsione della concorrenza nella acquisizione di beni o servizi.

Illecita influenza sull'Assemblea (art. 2636 c.c.)

Chiunque, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto, è punito con la reclusione da sei mesi a tre anni.

Aggiotaggio (art. 2637 c.c.)

Chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il

pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari, è punito con la pena della reclusione da uno a cinque anni.

Ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di vigilanza (art. 2638 c.c.)

Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima, sono puniti con la reclusione da uno a quattro anni. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Sono puniti con la stessa pena gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società, o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni.

La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.

Illecite operazioni sulle azioni o quote sociali o della Società controllante (art. 2628 c.c.)

Gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge, sono puniti con la reclusione fino ad un anno.

La stessa pena si applica agli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.

Se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

Operazioni in pregiudizio dei creditori (art. 2629 c.c.)

Gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Omessa comunicazione del conflitto d'interessi (art. 2629 bis c.c.)

L'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo 1° settembre 1993, n. 385, del citato testo unico di cui al decreto legislativo n. 58 del 1998, della legge 12 agosto 1982, n. 576, o del decreto legislativo 21 aprile 1993, n. 124, che viola gli obblighi previsti dall'articolo 2391, primo comma, è punito con la reclusione da uno a tre anni, se dalla violazione siano derivati danni alla società o a terzi.

Abuso di informazioni privilegiate (articolo 184 del d.lgs 58/1998 - Testo Unico della Finanza)

1. E' punito con la reclusione da uno a sei anni e con la multa da Euro 20.000,00 a Euro 3.000.000,00 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 maggior importo di dieci 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.

3. Bis Nel caso di operazioni relative agli strumenti finanziari di cui all'articolo 180, comma 1, lettera a), numero 2), la sanzione penale è quella dell'ammenda fino a Euro 103.291,00 e dell'arresto fino a tre anni.

4. Ai fini del presente articolo per strumenti finanziari si intendono anche gli strumenti finanziari di cui all'articolo 1, comma 2, il cui valore dipende da uno strumento finanziario di cui all'articolo 180, comma 1, lettera a).

Manipolazione del mercato (articolo 185 del d.lgs 58/1998 -Testo Unico della Finanza)

1. Chiunque diffonde notizie false o pone in esser operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti

finanziari, è punito con la reclusione da uno a sei anni e con la multa da Euro 20.000,00 a Euro 5.000.000,00.

2. 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.

2-bis Nel caso di operazioni relative agli strumenti finanziari di cui all'articolo 180, comma 1, lettera a), numero 2), la sanzione penale è quella dell'ammenda fino a Euro 103.291,00 e dell'arresto fino a tre anni.

REATI IN MATERIA DI LAVORO PER VIOLAZIONE DI NORME ANTINFORTUNISTICHE

Omicidio colposo (art. 589 c.p.)

Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni.

Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a sette anni.

Si applica la pena della reclusione da tre a dieci anni se il fatto e' commesso con violazione delle norme sulla disciplina della circolazione stradale da:

1) soggetto in stato di ebbrezza alcolica ai sensi dell'articolo 186, comma 2, lettera c), del decreto legislativo 30 aprile 1992, n. 285, e successive modificazioni;

2) soggetto sotto l'effetto di sostanze stupefacenti o psicotrope.

Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici.

Lesioni personali colpose (art. 590 c.p.)

Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a euro 309.

Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da euro 123 a euro 619, se è gravissima, della reclusione da tre mesi a due anni o della multa da euro 309 a euro 1.239.

Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni. Nei casi di violazione delle norme sulla circolazione stradale, se il fatto e' commesso da soggetto in stato di ebbrezza alcolica ai sensi dell'articolo 186, comma 2, lettera c), del decreto legislativo 30 aprile 1992, n. 285, e successive modificazioni, ovvero da soggetto sotto l'effetto di sostanze stupefacenti o psicotrope, la pena per le lesioni gravi e' della reclusione da sei mesi a due anni e la pena per le lesioni gravissime e' della reclusione da un anno e sei mesi a quattro anni.

Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque.

Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale.

REATI INFORMATICI

Documenti informatici (art. 491-bis c.p.)

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private

Frode informatica (art. 640-ter) *(già inserito nella parte relativa ai reati nei confronti della Pubblica amministrazione)*

Accesso abusivo ad un sistema informatico o telematico (art. 615-ter)

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, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)

Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.

La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)

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 anni e con la multa sino a euro 10.329

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.)

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

REATI IN MATERIA DI DIRITTO D'AUTORE

Art. 171

- **comma 1, lett. a bis**

  Salvo quanto disposto dall'art. 171-bis e dall'articolo 171-ter è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;

- **comma 3**

  La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Art. 171-bis

- **comma 1**

  Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

- **comma 2**

  Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

REATI IN MATERIA DI AMBIENTE

Art. 192 del D.Lgs. 152/2006 (Divieto di Abbandono)

- **comma 1**

L'abbandono e il deposito incontrollati di rifiuti sul suolo e nel suolo sono vietati.

- **comma 2**

E' altresì vietata l'immissione di rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali e sotterranee.

- **comma 3**

Fatta salva l'applicazione della sanzioni di cui agli articoli 255 e 256, chiunque viola i divieti di cui ai commi 1 e 2 è tenuto a procedere alla rimozione, all'avvio a recupero o allo smaltimento dei rifiuti ed al ripristino dello stato dei luoghi in solido con il proprietario e con i titolari di diritti reali o personali di godimento sull'area, ai quali tale violazione sia imputabile a titolo di dolo o colpa, in base agli accertamenti effettuati, in contraddittorio con i soggetti interessati, dai soggetti preposti al controllo. Il Sindaco dispone con ordinanza le operazioni a tal fine necessarie ed il termine entro cui provvedere, decorso il quale procede all'esecuzione in danno dei soggetti obbligati ed al recupero delle somme anticipate.

- **comma 4**

Qualora la responsabilità del fatto illecito sia imputabile ad amministratori o rappresentanti di persona giuridica ai sensi e per gli effetti del comma 3, sono tenuti in solido la persona giuridica ed i soggetti che siano subentrati nei diritti della persona stessa, secondo le previsioni del decreto legislativo 8 giugno 2001, n. 231, in materia di responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni.

Inquinamento ambientale (art. 452-bis c.p.)

E' punito con la reclusione da due a sei anni e con la multa da euro 10.000 a euro 100.000 chiunque abusivamente cagiona una compromissione o un deterioramento significativi e misurabili:

1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo;
2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna.

Quando l'inquinamento e' prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette, la pena e' aumentata.

Disastro ambientale (art. 452-quater c.p.)

Fuori dai casi previsti dall'articolo 434, chiunque abusivamente cagiona un disastro ambientale e' punito con la reclusione da cinque a quindici anni.

Costituiscono disastro ambientale alternativamente:

1) l'alterazione irreversibile dell'equilibrio di un ecosistema;
2) l'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali;
3) l'offesa alla pubblica incolumità in ragione della rilevanza del fatto per l'estensione della compromissione o dei suoi effetti lesivi ovvero per il numero delle persone offese o esposte a pericolo.

Quando il disastro e' prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette, la pena e' aumentata.

Delitti colposi contro l'ambiente (art. 452-quinquies c.p.)

Se taluno dei fatti di cui agli articoli 452-bis e 452-quater e' commesso per colpa, le pene previste dai medesimi articoli sono diminuite da un terzo a due terzi.

Se dalla commissione dei fatti di cui al comma precedente deriva il pericolo di inquinamento ambientale o di disastro ambientale le pene sono ulteriormente diminuite di un terzo.

Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.)

Salvo che il fatto costituisca piu' grave reato, e' punito con la reclusione da due a sei anni e con la multa da euro 10.000 a euro 50.000 chiunque abusivamente cede, acquista, riceve, trasporta, importa, esporta, procura ad altri, detiene, trasferisce, abbandona o si disfa illegittimamente di materiale ad alta radioattività.

La pena di cui al primo comma e' aumentata se dal fatto deriva il pericolo di compromissione o deterioramento:

1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo;

2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna.

Se dal fatto deriva pericolo per la vita o per l'incolumità delle persone, la pena e' aumentata fino alla metà.

REATI IN MATERIA DI IMPIEGO DI STRANIERI PRIVI DEL PERMESSO DI SOGGIORNO

Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero (Decreto Legislativo 25 luglio 1998, n. 286).

Articolo 22 Lavoro subordinato a tempo determinato e indeterminato.

- **comma 12**

Il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal presente articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, è punito con la reclusione da sei mesi a tre anni e con la multa di 5000 euro per ogni lavoratore impiegato.

- **comma 12-bis** (rilevante ai fini del D.Lgs. 231/01)

Le pene per il fatto previsto dal comma 12 sono aumentate da un terzo alla metà:

a) se i lavoratori occupati sono in numero superiore a tre;

b) se i lavoratori occupati sono minori in età non lavorativa;

c) se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-bis del codice penale.

REATI IN MATERIA DI RICETTAZIONE, RICICLAGGIO E IMPIEGO SI DENARO, BENI O UTILITA' DI PROVENIENZA ILELCITA, NONCHE' AUTORICICLAGGIO

Ricettazione (art. 648 c.p.)

1. Fuori dei casi di concorso nel reato, chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da euro 516 a euro 10.329.

2. La pena è della reclusione sino a sei anni e della multa sino a lire un milione, se il fatto è di particolare tenuità.

3. Le disposizioni di questo articolo si applicano anche quando l'autore del delitto da cui il denaro o le cose provengono non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto.

Riciclaggio (art. 648-bis c.p.)

1. Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000.

2. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.

3. La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita le pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'articolo 648.

Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)

1. Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000.

2. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.

3. La pena è diminuita nell'ipotesi di cui al secondo comma dell'articolo 648. Si applica l'ultimo comma.

Autoriciclaggio (art. 648-ter.1 c.p.)

Si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Si applica la pena della reclusione da uno a quattro anni e della multa da euro 2.500 a euro 12.500 se il denaro, i beni o le altre utilità provengono dalla commissione di un delitto non colposo punito con la reclusione inferiore nel massimo a cinque anni.

Si applicano comunque le pene previste dal primo comma se il denaro, i beni o le altre utilità provengono da un delitto commesso con le condizioni o le finalità di cui all'articolo 7 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, e successive modificazioni.

Fuori dei casi di cui ai commi precedenti, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale.

La pena è aumentata quando i fatti sono commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale.

La pena è diminuita fino alla metà per chi si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto.

Si applica l'ultimo comma dell'articolo 648.

CODICE DELL'AMMINISTRAZIONE DIGITALE - OBBLIGHI DEL CERTIFICATORE

27 - Certificatori qualificati.

1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26.

2. I certificatori di cui al comma 1, devono inoltre:

   a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;

   b) utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate e che sia in grado di rispettare le norme del presente codice e le regole tecniche di cui all'articolo 71;

   c) applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;

   d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 35, comma 5;

   e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi private nei casi in cui il certificatore generi tali chiavi.

3. I certificatori di cui al comma 1, devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività all'Agenzia per l'Italia Digitale (ex DigitPA), attestante l'esistenza dei presupposti e dei requisiti previsti dal presente codice.

4. L'Agenzia per l'Italia Digitale procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente codice e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa.

32 - Obblighi del titolare e del certificatore.

1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di forma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.

2. Il certificatore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.

3. Il certificatore che rilascia, ai sensi dell'articolo 19, certificati qualificati deve inoltre:

   a) provvedere con certezza alla identificazione della persona che fa richiesta della certificazione;

   b) rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle regole tecniche di cui all'articolo 71, nel rispetto del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni;

   c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;

   d) attenersi alle regole tecniche di cui all'articolo 71;

   e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;

   f) non rendersi depositario di dati per la creazione della firma del titolare;

   g) procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui all'articolo 71;

   h) garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché garantire il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;

   i) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;

j) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;

k) non copiare, né conservare, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;

l) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore;

m) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato.

4. Il certificatore è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.

5. Il certificatore raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.