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 del 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)
- 30 gennaio 2018 (vers.7)
- 24 gennaio 2019 (vers.8)
- 10 marzo 2020 (vers.9)
- 11 marzo 2021 (vers. 10)
- 19 gennaio 2022 (vers. 11)
- 24 gennaio 2023 (vers. 12)

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[1]o a vantaggio[2] 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[3], 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.)[4,] dei reati informatici, di quelli in materia di diritti d'autore 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"[5] e quella riguardante i "soggetti sottoposti all'altrui direzione"[6].

Le sanzioni previste dalla legge a carico dell'ente responsabile sono*:*

[1] Secondo l'impostazione tradizionale l'interesse ha un'indole soggettiva; si riferisce alla sfera volitiva della persona fisica che agisce ed è valutabile al momento della condotta. Un recente orientamento della Cassazione evidenzia la nozione di interesse anche in chiave oggettiva, esaltando la componente finalistica della condotta (Cass., IV Sez.pen. sent. n. 3731/2020.

[2] Il vantaggio si caratterizza come il complesso dei benefici - soprattutto di carattere patrimoniale – tratti dal reato che può valutarsi successivamente alla commissione di quest'ultimo, anche in termini di risparmio di spesa.

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

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

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

[6] 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.

- sanzioni pecuniarie,
- sanzioni interdittive,
- 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 alle previsioni del D. Lgs. 231/01 sono riportate, in relazione agli interventi normativi integrativi di riferimento, le fattispecie di reato evidenziando quelle di possibile interesse di ACI Informatica derivanti dalla matrice processi/reati recentemente elaborata in sede di *risk assessment.*

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 che poi a seguito di successivi interventi normativi sono stati ampliati. I primi reati inseriti nel cosiddetto catalogo dei reati presupposto sono 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, abuso d'ufficiodi membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis c.p.);
- malversazione di erogazioni pubbliche (art. 316-bis c.p.).
- indebita percezione di erogazioni pubbliche (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 delle fattispecie di reato di cui sopra sono state modificate/integrate con i seguenti interventi normativi:

- Legge 6 novembre 2012 n. 190 (Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione);
- Legge 27 maggio 2015 n. 69 (Disposizioni in materia di delitti contro la pubblica amministrazione, di associazioni di tipo mafioso e di falso in bilancio);
- Legge 9 gennaio 2019 n. 3 (Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici);
- D. Lgs. 14 luglio 2020, n. 75 (Attuazione della Direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale.

A seguito delle modifiche apportate dalla normativa citata, le fattispecie di reato (artt. 24 e 25) sono ora le seguenti:

- A1 malversazione di erogazioni pubbliche (art. 316-bis c.p.).
- A2 indebita percezione di erogazioni pubbliche (art. 316-ter c.p.);
- A3 truffa in danno dello Stato o di altro ente pubblico (art. 640, 2° comma, n. 1 c.p.);
- A4 truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- A5 frode informatica semplice (art. 640-ter c.p.) e frode informatica aggravata (art. 640 ter 2° comma);
- A6 peculato (art. 314, 1° comma c.p.) nei casi in cui derivi un danno agli interessi finanziari dell'Unione europea;
- A7 peculato mediante profitto dell'errore altrui (art. 316 c.p.) nei casi in cui derivi un danno agli interessi finanziari dell'Unione europea;
- A8 Abuso d'ufficio (art. 323 c.p.) nei casi in cui derivi un danno agli interessi finanziari dell'Unione europea.

- B1 concussione (art. 317 c.p.);

- B2 corruzione per l'esercizio della funzione (art. 318 c.p.);
- B3 corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
- B4 circostanze aggravanti (art. 319-bis c.p.);
- B5 corruzione in atti giudiziari (art. 319-ter c.p.);
- B6 corruzione di persona incaricata di un pubblico servizio (320 c.p.);
- B7 pene per il corruttore (321 c.p.);
- B8 istigazione alla corruzione (art. 322 c.p.);
- B9 peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione, abuso d'ufficio di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis c.p.);
- B10 induzione indebita a dare o promettere utilità (319-quater c.p.);
- B11 traffico di influenze illecite (art. 346-bis c.p.);
- B12 frode nelle pubbliche forniture (art. 356 c.p.).

La Parte speciale del presente Modello tiene conto dei suddetti interventi normativi.

Successivamente, come già anticipato, il perimetro dei reati rilevanti è stato ampliato. Inizialmente, 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. Con l'entrata in vigore della L. 23 luglio 2009 n. 99 avente per oggetto "Disposizioni per lo sviluppo e l'internalizzazione delle imprese, nonché in materia di energia", è stato introdotto l'**art. 25-bis 1** "Delitti contro l'industria e il commercio".
In relazione alle attività svolte e per le modalità operative, tali previsioni non costituiscono reato presupposto di interesse di ACI informatica.

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:

- D1 false comunicazioni sociali (art. 2621 c.c.) / fatti di lieve entità (art. 2621 bis c.c.)
- D3 impedito controllo (art. 2625, comma 2, c.c.);
- D4 indebita restituzione dei conferimenti (art. 2626 c.c.);
- D5 illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- D6 illecite operazioni sulle azioni o quote sociali proprie o della Società controllante (art. 2628 c.c.);
- D7 operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- D8-omessa comunicazione del conflitto d'interessi (art. 2629 bis c.c.);
- D9 formazione fittizia del capitale (art. 2632 c.c.);
- D10 indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- D11 illecita influenza sull'assemblea (art. 2636 c.c.);

- D12 aggiotaggio (art. 2637 c.c.);
- D13 ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.).
- D14 corruzione tra privati (art. 2635 c.c.);
- D15 istigazione alla corruzione tra privati (art. 2635 bis).

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.
Di seguito la seguente norma che può costituire reato presupposto per ACI Informatica:

- E1 associazioni con finalità di terrorismo e di eversione dell'ordine democratico (art. 270 bis c.p., 270 bis 1 c.p.); assistenza agli associati (art 270-ter c.p.); arruolamento con finalità di terrorismo anche internazionale (art. 270-quater c.p.); organizzazione di trasferimenti per finalità di terrorismo (art. 270-quater1 c.p.); addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-quinquies c.p.); condotte con finalità di terrorismo (art. sexies c.p.);

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 anche tale previsione non costituisce reato presupposto di interesse di ACI Informatica, ad esclusione della intermediazione illecita e sfruttamento del lavoro di cui al capitolo 14 relativo ai reati in materia di lavoro.
Trattasi in particolare delle seguenti norme:

- F15 intermediazione illecita e sfruttamento del lavoro (art. 603 bis c.p.).

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 ha previsto 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".
Le tipologie di reato sono elencate nell'Allegato 1 al Documento di Valutazione dei Rischi. Unica fattispecie di interesse per ACI Informatica è l'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.) trattata nella parte speciale.

Per qualificare come transnazionali i reati sopra elencati, (oltre alla punibilità del fatto commesso con la reclusione non inferiore nel massimo a quattro anni) è richiesto 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:

- I1 omicidio colposo (art. 589 c.p.);
- I2 lesioni personali colpose (art. 590 c.p.).

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

- L1 ricettazione (art. 648 c.p.);
- L2 riciclaggio (art. 648 bis c.p.);
- L3 impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.);
- L4 autoriciclaggio (art. 648-ter, comma 1 c.p.).

In particolare, in tema di autoriciclaggio, 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, il legislatore è intervenuto sulla disciplina per tale reato.

La suddetta legge aveva 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 conseguiva 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.

Oggi in ragione del D. Lgs. 8 novembre 2021 n. 195 "Attuazione della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale" entrano in vigore alcune modifiche al codice penale, ed in particolare alle fattispecie di ricettazione (art. 648 c.p.), riciclaggio (648 bis c.p.), impiego di denaro, beni o altre utilità di provenienza illecita (648 ter c.p.) e autoriciclaggio (648 ter 1 c.p.). Ne consegue che le fattispecie citate sono applicabili anche come conseguenza di contravvenzioni e di delitti colposi nel caso di riciclaggio e autoriciclaggio.

Successivamente, l'art. 3 del D.Lgs. 8 novembre 2021, n. 184 "Attuazione della Direttiva (UE) 2019/713 del Parlamento Europeo e del Consiglio del 17 aprile 2019 sulla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti" ha aggiunto l'**art**. **25-octies 1** che riguarda:

- L5 indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.);
- L6 detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater);

Inoltre, l'art. 25-octies 1 richiama anche la frode informatica aggravata, di cui all'art. 640-ter, comma 2 c.p.

Continuando l'analisi evolutiva, nel successivo anno 2008 il catalogo dei reati presupposto è stato ulteriormente aumentato ad opera dell'art. 7 della Legge 18 marzo 2008, n. 48, che intervenendo sull'**art**. **24 bis,** ha inserito le seguenti previsioni di reato:

- M1 accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- M2 detenzione , diffusione e installazione abusiva di apparecchiature, di codici e altri mezzi atti all'accesso a sistemi informatici o telematici. (art. 615 quarter c.p.);
- M3 Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);
- M4 intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quarter c.p.);
- M5 detenzione, diffusione e installazione abusiva di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies);
- M6 danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);

- M7 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.);
- M8 danneggiamento di sistemi informatici o telematici (art. 635 quarter c.p.);
- M9 danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- M10 documenti informatici (art. 491 bis c.p.);
- M11 frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.);
- M12 falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.);
- M13 disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e disciplina dei poteri nei settori di rilevanza strategica – art. 1 comma 11 del D. L 105/2019 (convertito con modifiche dalla L. 133/2019).

Con successiva Legge 15 luglio 2009, n. 94, è stato inserito l'**art. 24 ter** (Delitti di criminalità organizzata) i cui reati di interesse per ACI Informatica sono i seguenti:

- N2 associazione per delinquere (art. 416, a esclusione del 6° comma c.p.;
- N3 associazione di tipo mafioso (art. 416 bis c.p.);
- N4 scambio elettorale politico-mafioso (art. 416 ter c.p.).

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 introducendo i seguenti illeciti di interesse per ACI Informatica:

- P1 protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art.-171, 1° comma, lett. a-bis) e 3° comma della L. 633/1941);
- P2 protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-bis, 1° comma della L. 633/1941);
- P3 protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-bis, 2° comma della L. 633/1941);
- P4 protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171 ter, 171-septies della L. 633/1941);
- P5 protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-opties della L. 633/1941).

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, introducendo il seguente illecito:

- Q1 intralcio alla giustizia: induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria (art. 377 bis c.p.).

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 di interesse per ACI Informatica:

- R4 attività di gestione di rifiuti non autorizzata (art. 256 del D.Lgs. 3 aprile 2006 n. 152);
- R5 bonifica di siti (art. 257 del D.Lgs. 3 aprile 2006 n. 152);
- R6 violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 del D.Lgs. 3 aprile 2006 n. 152);
- R7 traffico illecito di rifiuti (art 259 del D.Lgs. 3 aprile 2006 n. 152);
- R8 attività organizzate per il traffico illecito di rifiuti (art. 452 c.p.).

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 – undecies del D.Lgs. 231/01 dedicato ai reati ambientali, introducendo il seguente illecito:

- R15 inquinamento ambientale (art. 452-bis 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.); attività organizzate per il traffico illecito di rifiuti (art. 452 quaterdecies 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, introducendo i seguenti illeciti:

- S1 impiego di cittadini di paesi terzi con soggiorno irregolare (art. 22, comma 12-bis del D.Lgs. 286/1998);
- S2 supporto all'ingresso illegale di stranieri nel territorio dello Stato (art. 12, commi 3, 3-bis e 3-ter del D. Lgs. 286/1998);
- S3 favoreggiamento della permanenza di stranieri entrati illegalmente nel territorio dello Stato (art. 12, comma 5 del d. lgs. 286/1998).

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 161/2017 ha esteso la responsabilità della società anche alle ipotesi di cui all'art. 12, comma 3, 3-bis, 3-ter e 5 del citato Testo Unico dell'Immigrazione.

Come già anticipato 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).

A seguito dell'entrata in vigore della Legge 29 ottobre 2016 n. 199 "Disposizioni in materia di contrasto ai fenomeni del lavoro nero, dello sfruttamento del lavoro in agricoltura e di riallineamento retributivo nel settore agricolo" in vigore dal 4 novembre 2016, sono state apportate alcune modifiche all'articolo 25 quinquies, comma 1, lettera a) del D.Lgs. 231/2001 (delitti contro la personalità individuale).

In particolare, è stato inserito nel novero dei reati previsti in materia di responsabilità amministrativa degli enti ex D.lgs. 231/01 il nuovo reato di intermediazione illecita e sfruttamento del lavoro previsto dall'art. 603 bis del codice penale.

L'introduzione di tale disposizione trova la propria ratio nell'intenzione del legislatore di colpire in maniera specifica il fenomeno del c.d. "caporalato" che è tuttora presente, riformulandone e aggiornandone la definizione, inasprendo le pene per gli sfruttatori ed estendendo la responsabilità e le sanzioni anche agli imprenditori che impiegano manodopera, anche facendo ricorso all'intermediazione dei caporali, approfittando dello stato di bisogno dei lavoratori e sottoponendo gli stessi a condizioni di sfruttamento.

Tra le altre ulteriori recenti novità è da segnalare anche quanto previsto dalla citata Legge n. 199/2016 che all'art. 3 dispone che "…qualora ricorrano i presupposti indicati nel comma 1 dell'articolo 321 del codice di procedura penale, (quando vi è il pericolo che la libera disponibilità di una cosa pertinente al reato possa aggravare o protrarre le conseguenze di esso ovvero agevolare la commissione di altri reati") il giudice dispone, in luogo del sequestro, il controllo giudiziario dell'azienda presso cui è stato commesso il reato, qualora l'interruzione dell'attività imprenditoriale possa comportare ripercussioni negative sui livelli occupazionali o compromettere il valore economico del complesso aziendale….". L'amministratore giudiziario affianca l'imprenditore nella gestione dell'azienda ed autorizza lo svolgimento degli atti di amministrazione utili all'impresa, riferendo al giudice ogni tre mesi, e comunque ogni qualvolta emergano irregolarità circa l'andamento dell'attività aziendale"

Sempre nel 2017 è da segnalare il D.Lgs. 15 marzo 2017 n.38 (Attuazione della decisione quadro 2003/568/GAI del Consiglio del 22 luglio 2003, relativa della lotta contro la corruzione nel settore privato) che introduce importanti modifiche alla disciplina della corruzione tra i privati.

Tale Decreto dà attuazione e recepisce quanto stabilito dalla decisione quadro 2003/568/GAI del Consiglio dell'Unione Europea relativa alla lotta contro la corruzione tra privati.

Giova ricordare che la corruzione tra privati, prima di tale Decreto, prevedeva due particolari forme di corruzione passiva (per soggetti intranei):

- la prima era prevista per 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 sé o per altri, compivano od omettevano atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società (co.1);

- la seconda si configurava in caso di commissione della stessa condotta da parte di chi era sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma (co.2).
  Era prevista inoltre al comma 3 una forma di corruzione attiva nel caso in cui un soggetto qualsiasi (soggetto estraneo) avesse dato o promesso denaro o altra utilità alle persone indicate nel primo e nel secondo comma. Per tale forma di corruzione scattava inoltre la sanzione pecuniaria da duecento a quattrocento quote prevista dall'art. 25 ter comma1 lett. s- bis del D.Lgs. 231/01 in caso di responsabilità amministrativa degli enti.

L'art. 3 del D.Lgs 38/2017 interviene sull'art. 2635 del codice civile:

- includendo tra i soggetti attivi autori del reato, oltre a coloro che rivestono posizioni apicali di amministrazione e di controllo, anche coloro che svolgono attività lavorativa mediante l'esercizio di funzioni direttive;
- estendendo la fattispecie anche ad enti privati non societari;
- ampliando le condotte cui si perviene all'accordo corruttivo. Nella corruzione passiva viene inclusa anche la sollecitazione del denaro o altra utilità da parte del soggetto "intraneo" qualora ad essa segua la conclusione dell'accordo corruttivo, e nella corruzione attiva anche l'offerta di denaro o altra utilità da parte del soggetto "estraneo", qualora essa venga accettata dal soggetto "intraneo";
- prevedendo espressamente tra le modalità della condotta, sia nell'ipotesi attiva che in quella passiva, la commissione della stessa per interposta persona;
- specificando che il denaro o altra utilità sono non dovuti;
- togliendo il riferimento alla necessità che la condotta cagioni un nocumento alla società;
- prevedendo che la confisca per equivalente ricomprenda anche le utilità offerte, e non solo date o promesse.

Per la portata sanzionatoria dell'art. 2635 del c.c. va considerato anche il recente intervento ad opera dell'art.13-ter del D.L.16 ottobre 2017, n. 148 convertito con Legge 4 dicembre 2017 n.172 che ha introdotto la cd. "confisca allargata".

Inoltre, l'art. 4 del citato D.Lgs. 38/2017 introduce l'art. 2635 bis cc, che punisce l'istigazione alla corruzione. Sotto il profilo attivo sarà quindi punito chi offre o promette denaro o altra

utilità non dovuti ad un soggetto "intraneo" qualora l'offerta o la promessa non sia accettata (art. 2635 bis comma 1). Sotto il profilo passivo sarà prevista la punibilità dell'"intraneo" che solleciti una promessa o dazione di denaro o altra utilità, qualora la sollecitazione non sia accettata. (art. 2635 bis comma 2).

L'art. 5 del D.Lgs. 38/2017 introduce l'art. 2635 ter c.c. che disciplina le pene accessorie da applicare in caso di condanna per il reato 2635, comma 1 c.c. (corruzione passiva dell'intraneo), nei confronti di chi sia già stato condannato per tale reato o per quello di cui all'art. 2635-bis, comma 2 c.c. (istigazione passiva alla corruzione). In questi casi si applicherà la pena dell'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese di cui all'art. 32-bis c.p.

L'art. 6 del D.Lgs. 38/2017 modifica, sotto il profilo sanzionatorio, la lettera s-bis dell'art. 25 ter (reati societari) del D.lgs.231/01, aumentando le sanzioni già previste per i casi di corruzione attiva ed introducendo la sanzione anche nei casi di istigazione attiva alla corruzione.

La nuova lettera s-bis prevede che in caso di corruzione attiva tra privati (soggetto "estraneo") ex art. 2635, comma 3, si applichi la sanzione pecuniaria da quattrocento a seicento quote e nei casi di istigazione attiva (art. 2635-bis, comma 1 c.c.), la sanzione pecuniaria da duecento a quattrocento quote. Si applicano, altresì, le sanzioni interdittive previste dall'art. 9, co 2 del D.Lgs. n. 231/2001 .

Si segnala, inoltre, il Decreto Legislativo n. 90 del 25 maggio 2017 che recepisce la Direttiva UE 2015/849 (c.d. IV Direttiva Antiriciclaggio) relativa alla "prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo", riscrivendo in parte il decreto antiriciclaggio (Decreto 231/2007).

In merito, si ritiene di non procedere ad alcuna modifica del presente Modello che già disciplina il reato di auto riciclaggio al di là che del fatto che, come sopra detto, la normativa vigente sembrerebbe non disciplinare più tale reato.

E' da segnalare inoltre la successiva Legge del 17 ottobre 2017 n. 161 riguardante "Modifiche al codice delle leggi antimafia e delle misure di prevenzione, di cui al decreto legislativo 6 settembre 2011, n.159".

Tale provvedimento opera diverse modifica quali le misure di prevenzione personali e patrimoniali; l'amministrazione, gestione e destinazione di beni sequestrati e confiscati, la Tutela dei terzi e rapporti con le procedure concorsuali, incidendo anche sul D.Lgs. 231/01 relativo alla responsabilità amministrativa degli enti.

Tale provvedimento per quanto qui interessa:

- all'art. 11 (Controllo giudiziario delle aziende) l'introduzione nel D.Lgs. 159/2011 di un nuovo articolo, 34-bis, il quale dispone che con il provvedimento che nomina

l'amministratore giudiziale, il Tribunale può stabilire " i compiti dell'amministratore giudiziario finalizzati alle attività di controllo e può imporre l'obbligo: di adottare ed efficacemente attuare misure organizzative, anche ai sensi degli articoli 6, 7 e 24-ter del decreto legislativo 8 giugno 2001, n. 231, e successive modificazioni;

- all'art. 30, co. 4 l'introduzione di nuovi delitti previsti all'art. 12 del D.lgs. 286/1998 riguardanti il procurato ingresso illecito ed il favoreggiamento dell'immigrazione clandestina, all'interno dell'art. 25 duodecies del D.Lgs. 231/01 con l'applicazione delle relative sanzioni pecuniarie ed interdittive.

Conseguentemente, l'articolo 25 duodecies del D.Lgs. 231/01 è stato integrato con la previsione di specifiche sanzioni pecuniarie (comma 1-bis e 1-ter) e sanzioni interdittive (comma 1-quater)

Di derivazione europea è l'introduzione dell'**art. 25 – terdecies** nel D.Lgs. 231/2001 rubricato "razzismo e xeonofobia", a seguito dell'entrata in vigore in data 12 dicembre 2017 della Legge 20 novembre 2017 n. 167 (Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017) che comprende i reati di cui all'art. 3, comma 3-bis della L.654/1975. Successivamente tale articolo è stato abrogato dal D. Lgs. 21/2018, senza tuttavia intervenire direttamente sul D. Lgs. 231/01. Contestualmente il medesimo Decreto ha introdotto il seguente illecito:

- T1 propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa (604-bis c.p.).

L'articolo 25 – terdecies prevede la responsabilità per gli enti in caso di reati di propaganda, istigazione e incitamento fondati sulla negazione, sulla minimizzazione in modo grave o sull'apologia della Shoah, dei crimini di genocidio, contro l'umanità e di guerra (cd. negazionismo) con sanzioni pecuniarie ed interdittive.

Da segnalare l'entrata in vigore della Legge 30 novembre 2017 n. 179 "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato" (Gazzetta ufficiale del 14/12/2017) che, nel modificare l'articolo 54 bis del Decreto Legislativo n.165/2001, pone apposito tutela a favore del dipendente o collaboratore che segnala reati o irregolarità (i cd. "whistleblower").

La citata Legge 179 all'articolo 2, che inserisce all'articolo 6 del decreto legislativo 8 giugno 2001, n. 231 i nuovi commi 2-bis, 2-ter e 2 –quater, richiede che nei Modelli 231 vengano individuati uno o più canali che garantiscano la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione, nonché vietino qualsiasi atto di ritorsione o discriminazione dei confronti del medesimo non potendo lo stesso essere sanzionato, demansionato, licenziato o trasferito.

Il 9 giugno 2021 l'ANAC ha approvato le nuove linee guida in materia di whistleblowing (Delibera 9/6/2021 n. 469) che forniscono indicazioni circa l'applicazione della normativa e prendono in considerazione i principi espressi in sede europea dalla Direttiva UE 2019/1937 riguardante la "*Protezione delle persone che segnalano violazioni del diritto dell'Unione*".

L'argomento è trattato nell'aggiornamento al Piano Triennale per la prevenzione della corruzione e della trasparenza 2018-2020 che costituisce una appendice al presente Modello e che viene sottoposto ad un aggiornamento annuale, affinché la Società ottemperi al meglio agli obblighi in materia di prevenzione della corruzione di cui alla citata L. 190/2012. In particolare, per gli aspetti specifici delle segnalazioni ACI Informatica si è dotata nell'ambito del già citato Piano Triennale della prevenzione della corruzione e trasparenza di un apposito regolamento denominato "Regolamento per la segnalazione di illeciti".

Al fine di meglio ottemperare al dettato della normativa richiamata, sono recepite anche all'interno del Modello 231 le principali novità introdotte dalla Legge 179/2017, fatto salvo che, come detto, la Società si è dotata di un apposito processo che disciplina le modalità con cui il Responsabile anticorruzione vigila sulla tutela del dipendente che segnala illeciti, nonché un Regolamento per la gestione delle segnalazioni, corredato da apposita modulistica.

Con tali misure si intende: (i) tutelare la riservatezza del segnalante; (ii) porre il divieto di ritorsioni di qualsiasi natura nei confronti del medesimo; (iii) istituire canali informativi in grado di tutelare la riservatezza del segnalante; (iv) prevedere sanzioni nei confronti di chi viola le misure di tutela della riservatezza del segnalante, così come di coloro che fanno segnalazioni che si rivelano infondate in cattiva fede. A tal fine, sono state aggiornate la sezione dedicata all'Organismo di Vigilanza e al Sistema Sanzionatorio.

E' da aggiungere che con la Legge 127/2022 (Legge di delegazione europea 2021) sono stati fissati i principi e i criteri direttivi per l'attuazione, entro 3 mesi della direttiva UE 2019/1937 riferita al whistleblowing.

Il Consiglio dei Ministri in data 9 dicembre 2022 ha approvato lo schema del Decreto Legislativo recante l'attuazione della Direttiva UE 2019/1937 e si è in attesa della sua definitiva pubblicazione.

L'art. 5 della Legge 3 maggio 2019 n. 39, ha introdotto nel Decreto l'**art. 25-quaterdecies**, che inserisce nel novero dei reati presupposto per l'applicazione delle sanzioni agli Enti, i "reati in materia di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati".
In relazione alle attività svolte e per le modalità operative tale previsione non costituisce reato presupposto di interesse di ACI Informatica.

L'art. 39 comma 2 del D. L 26 ottobre 2019 n. 124, recante "*Disposizioni urgenti in materia fiscale e per esigenze indifferibili"* convertito con modificazioni dalla L. 19 dicembre 2019 n. 157 ha introdotto nel decreto l'**art. 25-quinquiesdecies** che inserisce nel novero dei reati presupposto per l'applicazione delle sanzioni agli Enti i reati tributari, introducendo i seguenti illeciti:

- V1 dichiarazione fraudolenta mediante uso di fatture o di altri documenti per operazioni inesistenti (art.2, comma 1 e 2 bis, del D.Lgs. 74/2000)
- V2 dichiarazione fraudolenta mediante altri artifici (art. 3 del D.Lgs. 74/2000);
- V3 emissione di fatture o altri documenti per operazioni inesistenti (art. 8, comma 1 e 2 bis, del D. Lgs. 74/2000;
- V4 occultamento o distruzione di documenti contabili (art. 10 del D lgs 74/2000);
- V5 sottrazione fraudolenta al pagamento di imposte (art. 11 del D. Lgs. 74/2000).

Successivamente, il D.Lgs. 14 luglio 2020, n. 75 ha integrato l'**art. 25-quinquiesdecies,** inserendo altre ipotesi di reato previsti dal D.Lgs 10 marzo 2000, n. 74 se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a 10 milioni di euro. Trattasi delle seguenti ipotesi:

- V6 dichiarazione infedele (art. 4 del D. lgs 74/2000);
- V7 omessa dichiarazione (art. 5 del D. Lgs. 74/2000);
- V8 indebita compensazione (art. 10 quater del D. Lgs. 74/2000).

Il citato D. Lgs. 75/2020 ha inoltre introdotto il nuovo **art. 25-sexiesdecies**, che sancisce la responsabilità degli enti per il delitto di contrabbando ai sensi del DPR.43/1973.
In relazione alle attività svolte e per le modalità operative, tali previsioni non costituiscono reato presupposto di interesse di ACI Informatica.

Nei primi mesi del 2022 sono intervenute ulteriori novità legislative a integrare il D. Lgs. 231/01, modificando alcune fattispecie incluse nel catalogo dei reati presupposto. In questo contesto, di particolare interesse sono le previsioni di cui alla Legge n 238/2021 recante "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea – Legge Europea 2019-2020"* (c.d. Legge Europea) che modifica o integra disposizioni vigenti nel nostro ordinamento per adeguarne i contenuti al diritto europeo.

In particolare, la citata Legge Europea ha impatto sui seguenti reati presupposto:

- **art. 24 bis** del D. Lgs. 231/01 rubricato "Delitti informatici e trattamento illecito dei dati", nello specifico vengono modificati gli artt. 615-quater, 615-quinquies, 617-quater e 617-quinquies del codice penale (già inseriti nel Modello rispettivamente con riferimento alle lettere M2, M3, M4 e M5).

- **art. 25 quinquies** del D. Lgs. 231/01 rubricato "Delitti contro la personalità individuale", nello specifico vengono modificati gli artt. 600-quater (Detenzione o accesso a materiale pornografico) e 609-undecies (Adescamento di minori) del codice penale.

  In relazione alle attività svolte e per le modalità operative anche tale previsione non costituisce reato presupposto di interesse di ACI Informatica, ad esclusione della detenzione o accesso a materiale pornografico, di cui all'art. 600-quater c.p.

  Trattasi in particolare della seguente norma:

  - F6 Detenzione o accesso a materiale pornografico (art. 600-quater c.p.).

- **art. 25-sexies** del D. Lgs. 231/01 rubricato "Reati di abuso di mercato", nello specifico vengono modificati gli artt. 184 (Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate) e 185 (Manipolazione del mercato) D. Lgs. 58/1998 (T.U.F.).

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

Successivamente nel 2022 è stato emanato il Decreto-Legge 25 febbraio 2022, n. 13 (c.d. "Decreto Frodi") contiene "*Misure urgenti per il contrasto alle frodi e per la sicurezza nei luoghi di lavoro in materia edilizia, nonché sull'elettricità prodotta da impianti da fonti rinnovabili*". Gli argomenti di interesse sono stati trasfusi, in sede di conversione, nel Decreto-Legge 27 gennaio 2022, n. 4 convertito dalla Legge 28 marzo 2022 n. 25. In particolare l'art. 28-bis (Misure sanzionatorie contro le frodi in materia di erogazioni pubbliche) ha modificato gli artt. 316-bis, 316-ter e 640-bis del codice penale (già inseriti nel Modello rispettivamente con riferimento alle lettere A1, A2 e A4).

E' da considerare, inoltre, la legge 9 marzo 2022, n. 22 recante "*Disposizioni in materia di reati contro il patrimonio culturale"* che introduce nel Codice penale il titolo VIII-bis "Dei delitti contro il patrimonio culturale" nonché altre disposizioni collegate alle nuove previsioni. L'obiettivo di questo intervento legislativo è quello di operare una profonda riforma della materia, ridefinendo l'assetto della disciplina nell'ottica di un tendenziale inasprimento del trattamento sanzionatorio.

In particolare, l'art. 3 della citata legge 22/2022 modifica il testo del D. Lgs. 231/01 introducendo le seguenti famiglie di reato al fine di estendere la responsabilità 231/01 anche ai delitti contro il patrimonio culturale:

- **Art. 25-septiesdecies** "Delitti contro il patrimonio culturale"
- **Art. 25-duodevicies** "Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici".

In relazione alle attività svolte e per le modalità operative tali previsioni non costituiscono reato presupposto di interesse per ACI Informatica.

Di particolare rilievo è la riforma della giustizia penale (cd. "riforma Cartabia" attuata con il D. Lgs. 10 ottobre 2022, n. 150 avente ad oggetto "*attuazione della legge 27 settembre 2021, n. 134, recante delega al Governo per l'efficienza del processo penale, nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari*".

Il D. Lgs. 150/2022 prevede modifiche al Codice penale con impatto sui seguenti reati presupposto:

- **Art. 24** del D.Lgs. 231/01 rubricato "Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture", nello specifico vengono modificati gli artt. 640 e 640-ter del codice penale (già inseriti nel Modello rispettivamente con riferimento alle lettere A3 e A5).

- **Art. 25-octies-1** del D.Lgs. 231/01 rubricato "Delitti in materia di strumenti di pagamento diversi dai contanti", nello specifico vengono modificati l'art. 640-ter del codice penale (già inserito nel Modello con riferimento alla lettera A5).

Il D. Lgs. 4 ottobre 2022 n. 156 recante "*Disposizioni correttive e integrative del D. Lgs. 75/2020 di attuazione della direttiva "PIF" relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale (UE 2017/1371)*" prevede modifiche al Codice penale con impatto sui seguenti reati presupposto:

- **Art. 25** del D.Lgs. 231/01 rubricato "Peculato concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio", nello specifico viene modificato l'art. 322 bis del codice penale (già inserito nel Modello con riferimento alla lettera B9).

- **Art. 25-quinquiesdecies** rubricato "Reati tributari", nello specifico vengono effettuati i seguenti cambiamenti:

  - ✓ modifica dell'art. 6 del D. Lgs. 74/2000;
  - ✓ ampliamento del perimetro di cui al comma 1-bis dell'art 25-quinquiesdecies del D. Lgs. 231/01.

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 (A e B)** (artt. 316 bis, 316 ter, 640, comma 2, n.1, 317, 318, 319, 319 bis, 319 ter, 319 quater c.p., 320, 321, 322, 322 bis, 356, 640 bis, 640 ter, comma 1 e 2, c.p., 346 bis c.p.);

- **reati societari (D)** (artt. 2621, 2621 bis, 2625, 2626, 2627, 2628, 2629, 2629- bis, 2632, 2633, 2635, 2635 bis, 2635 ter, 2636, 2637, 2638 c.c.);

- **reati in violazione delle norme sulla tutela della salute e sicurezza sul lavoro (I)** (artt. 589 e 590 c.p.);

- **reati informatici (M)** (artt. 476 c.p., 491 bis, 615 ter, 615-quater, 615 quinquies, 617 quater, 617 quinquies, 635 bis, 635 ter, 635 quater, 635 quinquies, 640 quinquies c.p., art 1 D.L. 105/2019);

- **reati in materia di diritti d'autore (P)** (art.171, comma 1, lett. a bis, comma 3, 171-bis commi 1 e 2, art. 171 ter, 171 septies, 171 octies);

- **reati ambientali (R)** (D.Lgs 152/2006 artt. 256, 257, 258, 259, 452 quaterdecies c.p., L. 549/1993 art. 3, artt. 452-bis, 452-octies;

- **reati in materia di impiego di cittadini di paesi terzi con soggiorno irregolare (S)** (art. 12, comma 3, 3bis, 3ter e 5, 22, comma 12 bis, D.Lgs. 25 luglio 1998, n. 286 e s.m.i..); **di**

intermediazione illecita e sfruttamento del lavoro (F) (art 603 bis c.p.); reati di detenzione o accesso a materiale pornografico (F) (art. 600 quater c.p.); **reati di razzismo e xenofobia (T)** (art 604 bis c.p.);

reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (L) (artt. 648, 648 bis, 648 ter e 648 ter.1 c.p.,

- **reati connessi alla criminalità organizzata (N)** (artt. 416 escluso comma 6, 416 bis, 416 ter);

- **reati di intralcio alla giustizia: induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (Q)** (art. 377 bis c.p.);

- **reati tributari (V)** (artt. 2, comma 1, 2 bis, 3, 4, 5, 8, 10, 10-quater, 11 del D. Lgs. 74/2000);

- **reati con finalità di terrorismo o di eversione dell'ordine democratico (E)** (270-bis, 270 bis 1, 270-ter, 270-quater, 270-quater 1, 270-quinquies, 270-sexies).

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[7] 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[8]; tale esimente opera diversamente a seconda che i reati siano commessi da soggetti in posizione apicale o soggetti sottoposti alla direzione di questi ultimi[9].
Circa l'ipotesi di reati commessi da soggetti in posizione "apicale"[10], 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 [11].

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.

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

[7] Artt. 6 e 7 del D. Lgs. 231/2001.
[8] Si tratta per quanto riguarda l'ente, di una causa di esclusione della punibilità.
[9] 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).
[10] 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.
[11] Infatti solo la elusione o il difettoso controllo possono spiegare la commissione del reato pur in presenza di modelli astrattamente idonei ed efficaci.

necessaria[12], per evitare la responsabilità diretta dell'ente.

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[13], è di tutta evidenza come una corretta e tempestiva applicazione di tali linee guida diventerà punto di riferimento per le decisioni giudiziali in materia[14].

Nel caso di specie sono state prese in considerazione le **linee guida** sviluppate e pubblicate da **Confindustria** per le aziende associate[15].

Inoltre, per quanto riguarda specificatamente il "whistleblowing", si rinvia a quanto riportato nella **nota illustrativa** predisposta da **Confindustria** nel mese di gennaio 2018 e da ultimo nelle nuove Linee guida in materia di whistleblowing approvate da ANAC con Delibera n. 469 del 9 giugno 2021.

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

[13] 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.

[14] 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.

[15] "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, aggiornate nel marzo 2014 e, da ultimo nel giugno 2021.

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.
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 editoria, di marketing e comunicazione istituzionale 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, nonché 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 Territorio & Network ACI Demand e Servizi (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 è disciplinato l'affidamento *in house* dei servizi strumentali informatici e non, ivi comprese le attività di editoria, di marketing e di 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.
Nell'ambito delle attività di cui sopra, 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, nonché la Direzione Progetti ACI per la Smart Mobility e il Direttore Editoriale L'Automobile;
- la Direzione Generale risponde alla Presidenza. Rispondono altresì alla Direzione Generale le due Vice Direzioni Generali: la Vice Direzione Generale *Governance* e la Vice Direzione Generale Operations.
- la Direzione Generale per il tramite delle due Vice Direzioni Generali sovrintende alle Direzioni del Personale, Organizzazione, Qualità e Trasparenza, Pianificazione, Acquisti e Appalti, Gestione Rapporti istituzionali con la P.A., alla struttura Amministrazione, Bilancio e Controllo, alla struttura Tesoreria e Finanza, nonché alla struttura Redazione l'Automobile nonchè alle Direzioni tecniche (IT Strategy, Demand & Servizi ACI, Territorio & Network ACI – Demand e Servizi, Applicazioni PRA e Tasse, IT Development Operations, alla struttura DPO, alla struttura Customer Service, nonché alla struttura Workspace configuration Management.).

L'azienda è certificata UNI EN ISO 9001:2015(Sistema di Gestione per la Qualità), UNI CEI ISO/IEC 27001:2017 (Sistema di Gestione per la Sicurezza delle informazioni), UNI CEI ISO/IEC 20000-1:2018 (Sistema di Gestione dei servizi), UNI EN ISO 14001:2015 (Sistemi di Gestione Ambientale), UNI CEI EN ISO 50001:2018 (Sistemi di Gestione dell'Energia), UNI EN ISO 22301:2019 (Sistemi di Gestione della continuità operativa) e UNI ISO 45001:2018 (Sistema di Gestione della Salute e Sicurezza sul lavoro) , 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 da ACI, unico socio, ed esplicitati nel nuovo "*Regolamento di Governance delle società partecipate da ACI*" approvato dal Consiglio Generale di ACI nella seduta del 22 luglio 2020 e adottato dal Consiglio di Amministrazione di ACI Informatica nella seduta del 1° ottobre 2020. Le modifiche rispetto al testo approvato il 24 luglio 2019 riguardano esclusivamente gli artt. 2.1 e 2.5 e si sono rese opportune al fine di coordinare il testo del *Regolamento di Governance* con quello del Regolamento di Organizzazione ACI.

Si ricorda che il *Regolamento di Governance* che era stato aggiornato nel gennaio 2017 aveva portato nel successivo mese di maggio 2017, all'aggiornamento dello Statuto societario al fine di rafforzare ulteriormente i principi dell'*in house providing* nei confronti dell'Ente ACI e consentire maggiormente l'esercizio del controllo cd. analogo.

Il citato Regolamento era stato poi aggiornato nel dicembre 2018 in taluni aspetti organizzativi e di razionalizzazione nella gestione delle società controllate, rispetto ai principi generali desumibili dal testo unico di cui al D. Lgs. 19 agosto 2016 n. 175 in materia di società a partecipazione pubblica sulla base delle specificità di ACI e secondo criteri di razionalizzazione e contenimento della spesa di cui al D.Lgs. 175/2016 (TUSP) e sul presupposto della natura di ente pubblico non economico a carattere associativo di ACI e della sua autonomia e potestà regolamentare derivante dall'art. 2, comma 2-bis, della Legge 30 ottobre 2013, n. 125, convertito con modificazioni dalla Legge 30 ottobre 2013 n. 125, nonché dell'art. 10, comma 1-bis del D.L. 25 luglio 2018 n. 91, convertito con modifiche in Legge 21 settembre 2018 n. 108 in adeguamento ai principi del D.Lgs. 30 marzo 2001, n. 165.

Infine, il *Regolamento di Governance* era stato aggiornato nel luglio del 2019; nello stesso erano stati recepiti i rilievi formali dell'Autorità Garante della Concorrenza e del Mercato espressi con parere del 31 maggio 2019.

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.

In tema di sicurezza fisica, nel corso del 2020 caratterizzato dall'emergenza epidemiologica da Covid-19, l'azienda ha provveduto oltre al consueto aggiornamento del documento di valutazione dei rischi, predisposto ai sensi del D. Lgs. 9 aprile 2008 n. 81, a predisporre il DVR specifico di valutazione del rischio biologico causato dalla diffusione del citato virus, documento continuamente aggiornato in base alle misure di sicurezza messe in atto dall'azienda. In ottemperanza al Protocollo condiviso di Regolamentazione per il contenimento della diffusione del Covd-19 è stato istituito uno specifico Comitato costituito dal Datore di Lavoro, il Responsabile del Servizio di Prevenzione e Protezione (RSPP), Direttore del Personale, Organizzazione, Qualità e Trasparenza, il medico competente, i Rappresentanti dei Lavoratori per la Sicurezza (RLS) e la Rappresentanza dei Lavoratori (RSU) per la valutazione e condivisione delle modalità di gestione del rischio epidemiologico.

Con riferimento alla privacy, nel corso del 2020 l'azienda ha proseguito le attività per la sua corretta ed efficace gestione nel rispetto del Regolamento Europeo in materia di protezione dei dati personali (cd. GDPR).

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 fin dal 2003 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.
Tale scelta è oggi rafforzata dall'evoluzione della normativa in tema di anticorruzione, che pone il Modello 231 al centro delle misure preventive previste, unitamente al Piano triennale anticorruzione e trasparenza.
A tal fine il Consiglio di Amministrazione, avvalendosi dell'assistenza e consulenza delle strutture aziendali nonché di professionisti esterni, ha dato avvio, come detto 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 alla:

- 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 dei reati e dei rischi con l'introduzione dei nuovi reati presupposto man mano inseriti dal legislatore che hanno un impatto per ACI Informatica;

- 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.

Nell'ultimo trimestre 2019 è stato avviato un processo di risk assessment sul Modello che per esigenze di terzietà di giudizio è stato affidato all'ATI composta dalla Società HSPI S.p.A. e SCS Azioninnova S.p.A.

Al termine dell'analisi documentale e delle interviste ai responsabili dei processi, è stata effettuata un'ulteriore valutazione del rischio aziendale che ha portato all'elaborazione del Documento di Valutazione dei Rischi di ACI Informatica S.p.A., che costituisce apposito allegato al presente Modello.

ACI Informatica e i suoi dipendenti non sono mai stati sottoposti ad indagini e/o condannati ex D. Lgs. 231/01, né si sono verificati fatti che potrebbero in astratto portare all'apertura di un procedimento ex D. Lgs. 231/01.

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, ossia delle procedure aziendali sottostanti, 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 tre 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;
- verifica periodicamente l'adeguatezza dei canali informativi, predisposti in applicazione della disciplina sul whistleblowing, a garantire la corretta segnalazione dei reati o delle irregolarità da parte dei dipendenti della società e ad assicurare la riservatezza di questi ultimi nell'intero processo di gestione della segnalazione;

- coordina con la Direzione Generale 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 e tiene aggiornato, inoltre, 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;
- redige semestralmente 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 al Consiglio di Amministrazione e la trasmette al Collegio Sindacale;
- si avvale, relativamente alla salute e sicurezza sul lavoro, di tutte le risorse attivate per la gestione dei relativi aspetti (RSSPP – Responsabile del Servizio di prevenzione e Protezione, ASPP – Addetti al Servizio di Prevenzione e Protezione, RLS – Rappresentante dei Lavoratori per la Sicurezza, MC – Medico competente, addetti di primo soccorso, addetto emergenze in caso d'incendio) comprese quelle previste dalle normative di settore, quali il D. Lgs. 81/08;
- riceve copia della reportistica periodica in materia di salute e sicurezza sul lavoro.

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. Il Regolamento dell'Organismo di Vigilanza è stato aggiornato il 14 gennaio 2020 relativamente all'indicazione del numero dei componenti.

Le attività poste in essere dall'Organismo di Vigilanza non possono essere sindacate da alcun altro organismo o struttura aziendale.

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 continuativa e/o periodica semestrale, nei confronti del Consiglio di Amministrazione, del Direttore Generale e del Collegio Sindacale.

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.

Si segnala, infine, che il Piano Triennale per la prevenzione della corruzione e della trasparenza ha disciplinato in maniera puntuale il rapporto tra l'Organismo di Vigilanza e il Responsabile anticorruzione della Società, affinché il flusso informativo tra i due soggetti sia costante ed efficace.

4.4. Poteri e Compiti dell'Organismo di Vigilanza in materia di whisteblowing e coordinamento con i poteri del Responsabile della prevenzione delle corruzione e della trasparenza (RPCT)

L'OdV è investito di rilevanti compiti di vigilanza, aventi ad oggetto:

a) il rispetto del divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
b) il corretto utilizzo dei canali informativi da parte dei segnalanti, atteso che il novellato art. 6 prevede che sia sanzionato (oltre al soggetto che abbia posto in essere atti di ritorsione o discriminatori nei confronti del whistleblower) anche colui che «effettua con dolo o colpa grave segnalazioni che si rivelano infondate».

Con riferimento specifico alle segnalazioni che possono giungere all'indirizzo istituito dal Responsabile della prevenzione della corruzione e della trasparenza (RPCT), l'OdV delega l'istruttoria in primis al RPCT, nel senso che:

- qualora esse riguardino specificatamente reati in materia di anticorruzione, queste saranno gestite direttamente dal RPCT che avrà cura di informare l'ODV, così come qualora siano ricevute direttamente dall'ODV, lo stesso dovrà informare prontamente il RPCT per la tempestiva ed opportuna gestione delle stesse, così come previsto nel processo e nel regolamento aziendale in materia;

- qualora, invece riguardino comportamenti illeciti ai sensi del D.Lgs. 231, vale a dire condotte penalmente rilevanti in quanto suscettibili di integrare reati "presupposto" richiamati dalla citata normativa, anche nella forma del semplice tentativo, così come condotte che in ogni caso contravvengono al sistema di prevenzione dei reati e ai principi di controllo, ai presidi e alle procedure richiamate nel Modello, sarà lo stesso RPCT ad inoltrare prontamente all'ODV la segnalazione che provvederà ad istruire la segnalazione autonomamente.

5. DIFFUSIONE DEL MODELLO E FORMAZIONE DELLE RISORSE

Il Modello e il Codice Etico sono disponibili e visionabili nella loro interezza presso il sito intranet aziendale nonché nella sezione dedicata agli adempimenti in materia di trasparenza, sezione presente nel sito istituzionale di ACI Informatica.

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.
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.
La Società prevede una vera e propria formazione continua dei dipendenti con conseguente previsione di incontri/seminari in caso di nuove assunzioni, di nuovi incarichi per i settori più delicati e a rischio, nonché a seguito di variazioni o integrazioni del Modello dovute all'introduzione di nuovi reati presupposto; tale formazione verrà effettuata entro un termine massimo di circa 6 mesi dall'evento.
Tale formazione riguarda anche: (i) i tratti principali della disciplina in materia di whisteblowing; (ii) l'apparato sanzionatorio istituito a tutela dei segnalanti e del corretto uso dei canali informativi; (iii) il materiale funzionamento e le modalità di accesso ai sistemi adottati per le segnalazioni.

5.2. Nei confronti dei Fornitori e Professionisti

La Società provvede all'informazione ai Fornitori e Professionisti che operassero in aree 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.

Inoltre, la Società ha istituito e mantiene costantemente aggiornati, un Albo dei Fornitori e un Albo dei Professionisti. Già in sede di iscrizione a detti albi, è richiesto a tali soggetti l'accettazione integrale, sia del Codice Etico, sia del "Patto d'Integrità" nel quale è stabilito, tra l'altro, l'obbligo reciproco per ACI Informatica e per i fornitori/professionisti di improntare i propri comportamenti ai principi di lealtà, trasparenza e correttezza, nonché l'espresso impegno, in funzione di prevenzione della corruzione, di non offrire, accettare o richiedere somme di denaro o qualsiasi altra ricompensa, vantaggio o beneficio al fine dell'iscrizione nei citati Albi, dell'assegnazione del contratto e/o al fine di distorcerne la sua corretta esecuzione.

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 e nel Piano triennale di prevenzione della corruzione, quale appendice al presente Modello, ivi comprese quelle specifiche in materia di whisteblowing.
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.

Infine, con riferimento a quanto previsto dall'art. 6, comma 2 bis, lett. d) del D.Lgs. 231/01, l'inosservanza delle misure a tutela del segnalante o eventuali forme di abuso della procedura "whistleblower", quali le segnalazioni manifestamente infondate effettuate con dolo o colpa grave ed ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto in oggetto, possono dar luogo all'irrogazioni e di sanzioni disciplinari correlate alla gravità e frequenza della condotta e al grado del dolo o della colpa.

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;
- decadenza/revoca dalla carica ricoperta.

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

Le violazioni, da parte dei soggetti terzi, Fornitori, Professionisti 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.

Il Regolamento per l'istituzione e gestione dell'Albo Fornitori e il Regolamento per l'iscrizione dei Professionisti disciplinano, altresì, le ipotesi che possono dar luogo alla sospensione/cancellazione dai suddetti albi.

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 di erogazioni pubbliche (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 finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, destinati alla realizzazione di una o più finalità, non li destina alle finalità previste.

Indebita percezione di erogazioni pubbliche (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, sovvenzioni, 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, sovvenzioni, 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 semplice e aggravata (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.

Peculato (art. 314, comma 1, c.p.) *nei casi in cui derivi un danno agli interessi finanziari dell'Unione europea*
La norma punisce il pubblico ufficiale o l'incaricato di un pubblico servizio che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui se ne appropria.

Peculato mediante profitto dell'errore altrui (art. 316 c.p.) *nei casi in cui derivi un danno agli interessi finanziari dell'Unione europea*
La norma punisce il pubblico ufficiale o l'incaricato di un pubblico servizio, il quale, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità, è punito con la reclusione da sei mesi a tre anni.

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.

Circostanze aggravanti (art. 319-bis c.p.).

La norma introduce un aggravante di pena se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene nonché il pagamento o il rimborso di tributi.

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 dà 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 servizio per 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.

Abuso d'ufficio (art. 323 c.p.) nei casi in cui derivi un danno agli interessi finanziari dell'Unione europea
La norma punisce il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità, 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.

Frode nelle pubbliche forniture (art. 356 c.p.)
La norma punisce chiunque commette frode nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali.

Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione, abuso d'uffico di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.)

La norma estende la punibilità dalle fattispecie degli artt. 314, 316, da 317 a 320, 322, terzo e quarto comma e 323 ai membri della Commissione delle Comunità europee e di funzionari delle Comunità europee e degli esteri.

Traffico di influenze illecite (art. 346-bis c.p.)
La norma punisce chi sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-

bis, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso i soggetti di cui sopra, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri.

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

Articolo 24 - *malversazione di erogazioni pubbliche* (art. 316-bis c.p.), *indebita percezione di erogazioni pubbliche* (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.), *frode nelle pubbliche forniture* (art. 356 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.

Articolo 25 Concussione, induzione indebita a dare o promettere utilità e corruzione

Articolo 25, primo comma – *peculato nei casi in cui derivi un danno agli interessi finanziari dell'Unione europea (art. 314, comma 1, c.p.), peculato mediante profitto dell'errore altrui peculato nei casi in cui derivi un danno agli interessi finanziari dell'Unione europea (art. 316 c.p.), 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.), *abuso d'ufficio nei casi in cui derivi un danno agli interessi finanziari dell'Unione europea (323 c.p.), traffico di influenze illecite* (art. 346-bis c.p.), *corruzione di persona incaricata di pubblico servizio* (art. 320 c.p.), *peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione, abuso d'ufficio di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali 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 e anche quando tali delitti sono stati commessi dalle persone indicate negli articoli 320 e 322-bis.

- sanzioni interdittive (per una durata non inferiore a quattro anni e non superiore a sette se il reato è commesso da un apicale e non inferiore a 2 anni e non superiore a 4 anni se il reo è un subordinato): 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 a due anni e non superiore a sette in relazione al soggetto dell'Ente che ha commesso il reato): 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.

Si consideri, inoltre, che i reati richiamati dai citati articoli 24 e 25 trovano una puntuale analisi e costante monitoraggio nel Piano triennale di prevenzione della corruzione, quale appendice al presente Modello, di cui alla Legge n.190/2012 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione".

Le attività sensibili identificate sono qui di seguito riportate.

1. ***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 migliore organizzazione della Società, attraverso l'apporto di strutture societarie con controllo analogo indiretto da parte di ACI (es. ANCI Digitale). 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. Il processo è regolato dal Regolamento di Governance delle società controllate di ACI prevedendo un apposito iter autorizzativo.

2. ***Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con ACI, Federazione ACI e Società del gruppo***: 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, per le Società del gruppo, per la rete delle delegazioni a marchio ACI presenti sul territorio nazionale, nonché per eventuali rapporti convenzionali con la PPAA in generale.

   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.

3. ***Erogazione di servizi informatici e non:*** il processo riguarda l'erogazione di servizi informatici e non forniti in virtù di convenzioni o contratti. La gestione dei servizi informatici può comportare l'utilizzo dei seguenti strumenti:

   - ***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 (pagamento bollo auto e pagamento quote associative).

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:*** 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.

7 ***Gestione del Patrimonio:*** si tratta dell'attività di gestione dei beni strumentali aziendali sia materiali (hardware, attrezzature, arredi, ecc.) che immateriali (software).

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

9. ***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).

10 ***Gestione di flussi informativi telematici 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 ***Formazione finanziata del personale:*** il processo consiste nella gestione della formazione del personale che in modesta entità viene finanziata attraverso fondi interprofessionali.

12 ***Gestione regali, omaggi e benefici:*** il processo riguarda i doni e gli omaggi che generalmente vengono effettuati o ricevuti nel periodo natalizio e in entrambe i casi sono di modesta entità. Generalmente i doni effettuati da ACI Informatica sono rivolti alle banche, oppure riguardano relazioni industriali e/o professionisti esterni.

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 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, 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 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. L'intera materia è oggetto di specifica disciplina nel Regolamento di Governance per le società controllate da ACI.
- *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".

2. Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con ACI, Federazione ACI e Società del gruppo:

- *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. Inoltre, relativamente ai rapporti con la PPAA per la vendita di servizi, sono individuati ruoli e responsabilità dei diversi attori coinvolti nei processi di 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.
- *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. Inoltre, relativamente ai rapporti con la PPAA, 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, allegati tecnici all'Offerta, lettere di offerta, comunicazioni di accettazione.
- *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 struttura Amministrazione, Bilancio e Controllo. Inoltre, relativamente i rapporti con la PPAA, è prevista la separazione delle funzioni di autorizzazione, esecuzione e controllo, attribuite alle seguenti funzioni/ai seguenti soggetti: per la 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 struttura Amministrazione, Bilancio e Controllo e alle Strutture Tecniche interessate.
- *Poteri autorizzativi e di firma:* è previsto che siano autorizzati ad intrattenere rapporti con ACI o con acquirenti appartenenti alla Pubblica Amministrazione, 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", paragrafi A, B, D, E, F).

3. Erogazione di servizi informatici e non

- *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.

- *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. 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 della Direzione Affari Societari e Legali; 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 Affari Societari e Legali.
- *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) alla Direzione Generale 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 alla Direzione 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, Direzione 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

- *Regolamentazione: è richiesta: i) l'esplicita previsione delle tipologie di procedimento di acquisto utili*zzabili 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, nonché la presenza di un Responsabile del Procedimento (RUP) che opera nel rispetto *di quanto previsto* da Codice dei Contratti pubblici.; iii) la presenza di una Determina a contrarre, o atto equivalente, per l'avvio del procedimento di acquisto; iv) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; v) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; vi) 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: la Direzione Pianificazione, Acquisti e Appalti sulla base della richiesta di acquisto proveniente dalle strutture che necessitano del bene/servizio previsto a budget, propone l'impegno di spesa nel rispetto della ripartizione dei poteri di spesa aziendali; il RUP, con gli altri soggetti

delegati, predispone gli atti ed avvia il procedimento di acquisto che, in relazione all'entità della spesa e della procedura prescelta secondo le norme di legge, richiede l'intervento di scelta del fornitore mediante RUP/Seggio/Commissione di gara; l'esito della procedura è posta a base di una proposta di affidamento è accettato con la sottoscrizione dell'atto contrattuale di acquisto (ordine/contratto). Specificatamente per gli Acquisti per Cassa, le uscite di cassa sono autorizzate dal Responsabile della struttura "Tesoreria e Finanza", 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 dei poteri delegati. .
- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari", paragrafo B).

7. Gestione del Patrimonio

- *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, Direzione 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").

8. 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 atte a garantire il rispetto della normativa vigente in materia di tracciabilità; 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").

9. *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.

- *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 e/o dalla struttura Amministrazione, Bilancio e Controllo, e delle attività di selezione e assunzione delle risorse, gestite dall'Area Gestione del Personale e Organizzazione sotto la supervisione della Direzione del Personale, Organizzazione, Qualità e Trasparenza 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.

- *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")

10. *Gestione di flussi informativi telematici 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 struttura "Amministrazione, Bilancio 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 dall'Area Gestione del Personale e Organizzazione sotto la supervisione della Direzione del Personale, Organizzazione, Qualità e Trasparenza.

- *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.

- *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. Formazione finanziata del personale

- *Regolamentazione:* sono individuati ruoli e responsabilità dei diversi soggetti nelle attività di seguito indicate: i) verifica delle esigenze formative; ii) produzione del Piano di Formazione; iii) presa in carico dell'intervento formativo; iv) autorizzazione della richiesta di intervento formativo.
- *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:* si richiede l'individuazione delle figure autorizzate alla gestione delle attività relative all'erogazione della formazione.

- *Tracciabilità:* la tracciabilità del processo di trasmissione in esame è garantita da un

software, sviluppato in ambiente Lotus Notes che permette la gestione dell'intero ciclo, dalla richiesta di intervento formativo, alla richiesta di acquisto, alla notifica di iscrizione per il dipendente, etc. Tutte le fasi procedurali sono registrate in apposito database Access.

- *Codice Etico:* è richiesta l'osservanza delle indicazioni comportamentali previste dal capitolo II ("Rapporti con i dipendenti", paragrafo D).

12. Gestione regali, omaggi e benefici

- *Regolamentazione:* sono individuati ruoli e responsabilità dei diversi soggetti nelle attività di seguito indicate: i) autorizzazione del responsabile di funzione; segnalazione all'Organismo di Vigilanza.
- *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:* si richiede l'individuazione delle figure autorizzate alla gestione di regali, omaggi e benefici.
- *Tracciabilità*: la tracciabilità del processo in esame è garantita tramite apposita documentazione che viene conservata e di cui ne viene data comunicazione all'Organismo di Vigilanza.
- *Codice Etico:* è richiesta l'osservanza delle indicazioni comportamentali previste dal capitolo II ("Regali, omaggi, benefici", paragrafo I).

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 e 25-sexies.

L'articolo 25- ter è stato 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 stato quello di 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 hanno riguardato la previsione di punibilità della fattispecie in esame come delitto e non più come contravvenzione. Inoltre, uno dei principali cambiamenti ha riguardato la trasformazione del reato di false comunicazioni sociali da reato di danno a reato di pericolo. In altri termini, sono 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.

L'articolo 25-ter risulta poi aggiornato con l'introduzione della lettera s) a seguito dell'entrata in vigore del D.Lgs. 15 marzo 2017 n.38 (Attuazione della decisione quadro 2003/568/GAI del Consiglio del 22 luglio 2003, relativo della lotta contro la corruzione nel settore privato) che introduce importanti modifiche alla disciplina della corruzione tra i privati.

Giova ricordare che la corruzione tra privati, prima di tale Decreto, prevedeva due particolari forme di corruzione passiva (per soggetti intranei):

- la prima era prevista per 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, compivano od omettevano atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società (co.1);

- la seconda si configurava in caso di commissione della stessa condotta da parte di chi era sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma (co.2).
  Era prevista inoltre al comma 3 una forma di corruzione attiva nel caso in cui un soggetto qualsiasi (soggetto estraneo) avesse dato o promesso denaro o altra utilità alle persone indicate nel primo e nel secondo comma. Per tale forma di corruzione scattava inoltre la sanzione pecuniaria da duecento a quattrocento quote prevista dall'art. 25 ter comma1 lett. s- bis del D.Lgs. 231/01 in caso di responsabilità amministrativa degli enti.

L'art. 3 del D.Lgs 38/2017 interviene sull'art. 2635 del codice civile:

- includendo tra i soggetti attivi autori del reato, oltre a coloro che rivestono posizioni apicali di amministrazione e di controllo, anche coloro che svolgono attività lavorativa mediante l'esercizio di funzioni direttive ;
- estendendo la fattispecie anche ad enti privati non societari;
- ampliando le condotte cui si perviene all'accordo corruttivo. Nella corruzione passiva viene inclusa anche la sollecitazione del denaro o altra utilità da parte del soggetto "intraneo" qualora ad essa segua la conclusione dell'accordo corruttivo, e nella corruzione attiva anche l'offerta di denaro o altra utilità da parte del soggetto "estraneo", qualora essa venga accettata dal soggetto "intraneo";
- prevedendo espressamente tra le modalità della condotta, sia nell'ipotesi attiva che in quella passiva, la commissione della stessa per interposta persona;
- specificando che il denaro o altra utilità sono non dovuti;
- togliendo il riferimento alla necessità che la condotta cagioni un nocumento alla società;
- prevedendo che la confisca per equivalente ricomprenda anche le utilità offerte, e non solo date o promesse.

L'art. 4 del citato D.Lgs. 38/2017 introduce l'art. 2635 bis cc, che punisce l'istigazione alla corruzione. Sotto il profilo attivo sarà quindi punito chi offre o promette denaro o altra utilità non dovuti ad un soggetto "intraneo" qualora l'offerta o la promessa non sia accettata (art. 2635 bis comma 1). Sotto il profilo passivo sarà prevista la punibilità dell' "intraneo" che solleciti una promessa o dazione di denaro o altra utilità, qualora la sollecitazione non sia accettata. (art. 2635 bis comma 2).

L'art. 5 del D.Lgs. 38/2017 introduce l'art. 2635 ter c.c. che disciplina le pene accessorie da applicare in caso di condanna per il reato 2635, comma 1 c.c. (corruzione passiva dell'intraneo), nei confronti di chi sia già stato condannato per tale reato o per quello di cui all'art. 2635-bis, comma 2 c.c. (istigazione passiva alla corruzione). In questi casi si applicherà la pena dell'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese di cui all'art. 32-bis c.p.

L'art. 6 del D.Lgs. 38/2017 modifica, sotto il profilo sanzionatorio, la lettera s-bis dell'art. 25 ter (reati societari) del D.lgs.231/01, aumentando le sanzioni già previste per i casi di corruzione attiva ed introducendo la sanzione anche nei casi di istigazione attiva alla corruzione.

La nuova lettera s-bis prevede che in caso di corruzione attiva tra privati (soggetto "estraneo") ex art. 2635, comma 3, si applichi la sanzione pecuniaria da quattrocento a seicento quote e nei casi di istigazione attiva (art. 2635-bis, comma 1 c.c.), la sanzione pecuniaria da duecento a quattrocento quote. Si applicano, altresì, le sanzioni interdittive previste dall'art. 9, co 2 del D.Lgs. n. 231/2001.

Di seguito sono riportate le fattispecie di interesse aggiornate.

False comunicazioni sociali (artt. 2621, 2621 – bis 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.

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.2635 c.c.)

La fattispecie sanziona, salvo che il fatto non costituisca più grave reato, l'ente nel caso in cui gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto 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.

E' prevista l'applicazione della stessa pena anche a colui che nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo e che commetta il fatto.

Istigazione alla corruzione tra privati (art. 2635 bis c.c.)

La fattispecie sanziona chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo.

La pena di cui al primo comma si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per se' o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata.

Art. 2635-ter c.c. (Pene accessorie)

La condanna per il reato di cui all'articolo 2635, primo comma, importa in ogni caso l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese di cui all'articolo 32bis del codice penale nei confronti di chi sia già stato condannato per il medesimo reato o per quello di cui all'articolo 2635bis, secondo comma.

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 c.c.)*

- sanzione pecuniaria: da duecento quote a quattrocento;

istigazione alla corruzione tra privati (art. 2635 bis c.c.)

- sanzione pecuniaria: da duecento quote a quattrocento;
- sanzioni interdittive previste dall'art. 9, comma 2.

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.,)

- 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;

indebita restituzione dei conferimenti (art. 2626 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;

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.

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. ***Governance e organizzazione aziendale:*** si tratta dell'attività svolta dalla Direzione del Personale, Organizzazione, Qualità e Trasparenza. In particolare tale Direzione esprime le regole e i processi con cui si prendono le decisioni in un'azienda, le modalità con cui vengono decisi gli obiettivi aziendali nonché i mezzi per il raggiungimento e la misurazione dei risultati raggiunti.

2. ***Gestione della contabilità, 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.

3. ***Controllo degli organi societari sulla gestione sociale*:** si tratta dell'attività svolta dagli amministratori della Società, necessaria a rendere disponibili ai Soci, al Collegio Sindacale e alla Società di revisione, 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.
   Inoltre tale processo riguarda i 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. E' previsto, inoltre, un iter informativo nei confronti di ACI.

4. ***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 migliore organizzazione della Società, attraverso l'apporto di strutture societarie con controllo analogo indiretto da parte di ACI (es. ANCI Digitale). 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. Il processo è regolato dal Regolamento di Governance delle società controllate di ACI prevedendo un apposito iter autorizzativo.

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

6. ***Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con ACI, Federazione ACI e Società del gruppo:*** 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, per le Società del gruppo, per la rete delle delegazioni a marchio ACI presenti sul territorio nazionale, nonché per eventuali rapporti convenzionali con la PPAA in generale.

   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.

7. ***Erogazione di servizi informatici e non:*** il processo riguarda l'erogazione di servizi informatici e non forniti in virtù di convenzioni o contratti. La gestione dei servizi informatici può comportare l'utilizzo dei seguenti strumenti:

   - ***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 (pagamento bollo auto e pagamento quote associative).

8. ***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 ad evidenza pubblica.

9. ***Gestione del patrimonio:*** si tratta dell'attività di gestione dei beni strumentali aziendali sia materiali (hardware, attrezzature, arredi, ecc.) che immateriali (software).

10. ***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).

11. ***Formazione finanziata del personale:*** il processo consiste nella gestione della formazione del personale che in modesta entità viene finanziata attraverso fondi interprofessionali.

12. ***Gestione regali, omaggi e benefici:*** il processo riguarda i doni e gli omaggi che generalmente vengono effettuati o ricevuti nel periodo natalizio e in entrambe i casi sono di modesta entità. Generalmente i doni effettuati da ACI Informatica sono rivolti alle banche, oppure riguardano relazioni industriali e/o professionisti esterni.

13. ***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.

14. ***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.

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. Governance e organizzazione aziendale:

- *Regolamentazione*: sono previsti i ruoli e le responsabilità nella gestione del presente processo. L'intera materia è oggetto di specifica disciplina nel Regolamento di Governance per le società controllate da ACI.
- *Tracciabilità*: è prevista l'archiviazione della documentazione relativa alle attività e rapporti che coinvolgono ACI e ACI Informatica nelle direzioni/uffici coinvolte.
- *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 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 in particolare dei principi previsti nel capitolo VII riguardante la "Condotta societaria".

2. Gestione della contabilità, 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 struttura "Amministrazione, Bilancio 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 struttura "Amministrazione, Bilancio 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 struttura "Amministrazione, Bilancio e Controllo", il Collegio Sindacale, il Consiglio di Amministrazione, la Società di Revisione.
- *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".

3. Controllo degli Organi societari sulla gestione sociale

- *Regolamentazione*: con riferimento alla documentazione contabile, fiscale, societaria e dei registri bollati sono individuate la definizione di compiti e ruoli in merito alla conservazione; sono previste modalità strutturate di custodia della tale documentazione. Inoltre, con riferimento ai documenti predisposti ai fini delle delibere assembleari e del Consiglio di Amministrazione 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 e all'Ente per le regole di *governance* per le società controllate da ACI e per le finalità e l'esercizio del cd. "controllo analogo, alla trascrizione del verbale d'Assemblea e della documentazione societaria relativa all'attività degli altri organi sociali. E' previsto il supporto fornito dalla Direzione Affari Societari e Legali.

- *Tracciabilità*: è richiesta la conservazione di tutta la documentazione rilevante. Inoltre, è prevista la forma scritta per i flussi di richiesta, verifica ed autorizzazione alla trasmissione dei documenti agli organi preposti. E' infine 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 contenute nel capitolo IV dedicato al "Trattamento di informazioni interne" e capitolo VI riguardante i "Libri contabili e i registri societari"

4. 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. L'intera materia è oggetto di specifica disciplina nel Regolamento di Governance per le società controllate da ACI.
- *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 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 atte a garantire il rispetto della normativa vigente in materia di tracciabilità; 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").*

6. *Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con ACI, Federazione ACI e Società del gruppo:*

- *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. Inoltre, relativamente ai rapporti con la PPAA per la vendita di servizi, sono individuati ruoli e responsabilità dei diversi attori coinvolti nei processi di 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.
- *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. Inoltre, relativamente ai rapporti con la PPAA, 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, allegati tecnici all'Offerta, lettere di offerta, comunicazioni di accettazione.
- *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 struttura Amministrazione, Bilancio e Controllo". Inoltre, relativamente i rapporti con la PPAA, è prevista la separazione delle

funzioni di autorizzazione, esecuzione e controllo, attribuite alle seguenti funzioni/ai seguenti soggetti: per la 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 struttura "Amministrazione, Bilancio e Controllo" e alle Strutture Tecniche interessate.

- *Poteri autorizzativi e di firma:* è previsto che siano autorizzati ad intrattenere rapporti con ACI o con acquirenti appartenenti alla Pubblica Amministrazione, 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", paragrafi A, B, D, E, F).

7. Erogazione di servizi informatici e non

- *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.

- *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").

8. Gestione degli Acquisti

- *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, nonché la presenza di un Responsabile del Procedimento (RUP) che opera nel rispetto di quanto previsto da Codice dei Contratti pubblici.; iii) la presenza di una Determina a contrarre, o atto equivalente, per l'avvio del procedimento di acquisto; iv) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; v) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; vi) 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: la Direzione Pianificazione, Acquisti e Appalti sulla base della richiesta di acquisto proveniente dalle strutture che necessitano del bene/servizio previsto a budget, propone l'impegno di spesa nel rispetto della ripartizione dei poteri di spesa aziendali; il RUP, con gli altri soggetti delegati, predispone gli atti ed avvia il procedimento di acquisto che, in relazione all'entità della spesa e della procedura prescelta secondo le norme di legge, richiede l'intervento di scelta del fornitore mediante RUP/Seggio/Commissione di gara; l'esito della procedura è posta a base di una proposta di affidamento è accettato con la sottoscrizione dell'atto contrattuale di acquisto (ordine/contratto). Specificatamente per gli Acquisti per Cassa, le uscite di cassa sono autorizzate dal Responsabile della struttura "Tesoreria e Finanza", 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 dei poteri delegati.
- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari", paragrafo B).

9. Gestione del Patrimonio

- *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").

10. 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.

- *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 e/o dalla struttura "Amministrazione, Bilancio e Controllo", e delle attività di selezione e assunzione delle risorse, gestite dall'Area Gestione del Personale e Organizzazione sotto la supervisione della Direzione del Personale, Organizzazione, Qualità e Trasparenza 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.
- *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").

11. 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").

12. Formazione finanziata del personale

- *Regolamentazione:* sono individuati ruoli e responsabilità dei diversi soggetti nelle attività di seguito indicate: i) verifica delle esigenze formative; ii) produzione del Piano di Formazione; iii) presa in carico dell'intervento formativo; iv) autorizzazione della richiesta di intervento formativo.
- *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:* si richiede l'individuazione delle figure autorizzate alla gestione delle attività relative all'erogazione della formazione.
- *Tracciabilità:* la tracciabilità del processo di trasmissione in esame è garantita da un software, sviluppato in ambiente Lotus Notes che permette la gestione dell'intero ciclo, dalla richiesta di intervento formativo, alla richiesta di acquisto, alla notifica di iscrizione per il dipendente, etc. Tutte le fasi procedurali sono registrate in apposito database Access.
- *Codice Etico:* è richiesta l'osservanza delle indicazioni comportamentali previste dal capitolo II ("Rapporti con i dipendenti", paragrafo D).

13. Gestione regali, omaggi e benefici

- *Regolamentazione:* sono individuati ruoli e responsabilità dei diversi soggetti nelle attività di seguito indicate: i) autorizzazione del responsabile di funzione; segnalazione all'Organismo di Vigilanza.

  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:* si richiede l'individuazione delle figure autorizzate alla gestione di regali, omaggi e benefici.
- *Tracciabilità*: la tracciabilità del processo in esame è garantita tramite apposita documentazione che viene conservata e di cui ne viene data comunicazione all'Organismo di Vigilanza.
- *Codice Etico:* è richiesta l'osservanza delle indicazioni comportamentali previste dal capitolo

II ("Regali, omaggi, benefici", paragrafo I).

14. 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 della Direzione Affari Societari e Legali; ii) contenzioso stragiudiziale: l'autorizzazione è demandata al Presidente, alla Direzione Generale; l'esecuzione degli atti è di competenza del responsabile della struttura interessata dalla controversia, il controllo è rimesso al Responsabile della Direzione Affari Societari 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, Direzione 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).

10. REATI IN VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

10.1. I reati in violazione delle norme sulla tutela della salute e sicurezza sul 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. 590, comma 3, 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 violazione delle norme sulla tutela della salute e sicurezza sul lavoro 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. 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, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'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, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, 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 apparecchiature, codici e altri mezzi 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.

- *D**etenzione, diffusione e installazione abusiva 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, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa 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.)***

- ***Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti 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); al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi codici, parole chiave o altri mezzi atti 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.

La detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi destinati 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.

- **Sicurezza nazionale cibernetica** Decreto-Legge 21 settembre 2019, n. 105 Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (Art. 1 comma 11) convertito con modifiche dalla L 18-11-2019 n. 133

Il D.L. 105/2019 che istituisce il Perimetro di sicurezza nazionale cibernetica riguarda i soggetti "pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale".

Tali attori verranno individuati tramite DPCM, su proposta del CISR, entro quattro mesi dall'entrata in vigore della legge di conversione. In virtù della funzione essenziale e strategica che essi svolgono all'interno del Sistema-Paese, i soggetti che rientrano nel

Perimetro dovranno garantire l'aderenza rispetto ai criteri e ai livelli di sicurezza imposti dal Decreto-Legge.

Allo stesso modo, i soggetti che intendono offrire beni e servizi ICT destinati ad essere impiegati in reti e sistemi che svolgono funzioni essenziali per il Paese, dovranno essere in grado ad esempio di superare eventuali test per l'individuazione di vulnerabilità e dimostrare adeguati livelli di sicurezza nell'erogazione delle proprie forniture.

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

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, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici* (art. 615 quater); *detenzione, diffusione e installazione abusiva 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); *delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105.*

- 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.

Le attività sensibili identificate sono qui di seguito riportate:

1. **Controllo degli organi societari sulla gestione sociale:** si tratta dell'attività svolta dagli amministratori della Società, necessaria a rendere disponibili ai Soci, al Collegio Sindacale e alla Società di revisione, 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.
   Inoltre tale processo riguarda i 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. E' previsto, inoltre, un iter informativo nei confronti di ACI.

2. ***Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con ACI, Federazione ACI e Società del gruppo:*** 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, per le Società del gruppo, per la rete delle delegazioni a marchio ACI presenti sul territorio nazionale, nonché per eventuali rapporti convenzionali con la PPAA in generale.
   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.

3. ***Erogazione di servizi informatici e non:*** il processo riguarda l'erogazione di servizi informatici e non forniti in virtù di convenzioni o contratti. La gestione dei servizi informatici può comportare l'utilizzo dei seguenti strumenti:

   - ***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 (pagamento bollo auto e pagamento quote associative).

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, archiviazione informatica e gestione banche dati, gestione sistema protocollo informatico e gestione documentale, gestione internet e posta elettronica:*** 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, delle banche dati, del protocollo informatico, nonché di internet e della posta elettronica.
   In particolare: 1) per le reti l'attività riguarda la gestione degli accessi e la manutenzione in efficienza; 2) 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; 3) per il software l'attività riguarda la scelta dei prodotti da acquisire, l'installazione, l'aggiornamento, l'utilizzo; 4) per le 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; 5) per il protocollo informatico l'attività riguarda il servizio di gestione del sistema di protocollo informatico e dei documenti per uso interno; 6) per 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.

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

7. ***Gestione di flussi informativi telematici 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).

8. ***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 ad evidenza pubblica.

9. ***Gestione del patrimonio:*** si tratta dell'attività di gestione dei beni strumentali aziendali sia materiali (hardware, attrezzature, arredi, ecc.) che immateriali (software).

10. **Gestione della contabilità, 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.

11. ***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).

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.

- **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. Controllo degli Organi societari sulla gestione sociale

- *Regolamentazione*: con riferimento documentazione contabile, fiscale, societaria e dei registri bollati sono individuate la definizione di compiti e ruoli in merito alla conservazione; sono previste modalità strutturate di custodia della tale documentazione. Inoltre, con riferimento ai documenti predisposti ai fini delle delibere assembleari e del Consiglio di Amministrazione 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 e all'Ente per le regole di *governance* per le società controllate da ACI e per le finalità e l'esercizio del cd. "controllo analogo, alla trascrizione del verbale d'Assemblea e della documentazione societaria relativa

all'attività degli altri organi sociali. E' previsto il supporto fornito dalla Direzione Affari Societari e Legali.

- *Tracciabilità*: è richiesta la conservazione di tutta la documentazione rilevante. Inoltre, è prevista la forma scritta per i flussi di richiesta, verifica ed autorizzazione alla trasmissione dei documenti agli organi preposti. E' infine 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 contenute nel capitolo IV dedicato al "Trattamento di informazioni interne" e capitolo VI riguardante i "Libri contabili e i registri societari"

2. Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con ACI, Federazione ACI e Società del gruppo:

- *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. Inoltre, relativamente ai rapporti con la PPAA per la vendita di servizi, sono individuati ruoli e responsabilità dei diversi attori coinvolti nei processi di 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.
- *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. Inoltre, relativamente ai rapporti con la PPAA, 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, allegati tecnici all'Offerta, lettere di offerta, comunicazioni di accettazione.
- *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 struttura "Amministrazione, Bilancio e Controllo". Inoltre, relativamente i rapporti con la PPAA, è prevista la separazione delle funzioni di autorizzazione, esecuzione e controllo, attribuite alle seguenti funzioni/ai seguenti soggetti: per la 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 struttura "Amministrazione, Bilancio e Controllo" e alle Strutture Tecniche interessate.

- *Poteri autorizzativi e di firma:* è previsto che siano autorizzati ad intrattenere rapporti con ACI o con acquirenti appartenenti alla Pubblica Amministrazione, 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", paragrafi A, B, D, E, F).
- *Poteri autorizzativi e di firma:* è previsto che siano autorizzati ad intrattenere rapporti con ACI o con acquirenti appartenenti alla Pubblica Amministrazione, 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", paragrafi A, B, D, E, F).

3. Erogazione di servizi informatici e non

- *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.

- *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.

- *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, archiviazione informatica e gestione banche dati, gestione sistema protocollo informatico e gestione documentale, gestione internet e posta elettronica

- *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) v) archiviazione dati e documenti, individuazione dei soggetti autorizzati ad accedere e/o a gestire le banche dati, a consultare, elaborare, eliminare informazioni; vi) 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; vii) sono individuate le procedure alle quali deve attenersi il personale nell'uso di email aziendale, nell'accesso a internet

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

- *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. 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. 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 nel capitolo II ("Comportamento nella gestione degli affari", paragrafo A, B, C, D, E), III ("Salute, sicurezza, ambiente"), nel capitolo IV ("Trattamento di informazioni interne") e nel capitolo V ("Uso delle risorse informatiche).

6. *Gestione della contabilità, 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 struttura "Amministrazione, Bilancio 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 struttura "Amministrazione, Bilancio 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 struttura "Amministrazione, Bilancio e Controllo", il Collegio Sindacale, il Consiglio di Amministrazione, la Società di Revisione.
- *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".

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 e incassi atte a garantire il rispetto della normativa vigente in materia di tracciabilità; 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.

- *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").

8. Gestione di flussi informativi telematici 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 struttura "Amministrazione, Bilancio 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 del Personale e

Organizzazione, di controllo, affidato alla Direzione del Personale, Organizzazione, Qualità e Trasparenza.

- *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.

- *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").

9. Gestione degli Acquisti

- *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, nonché la presenza di un Responsabile del Procedimento (RUP) che opera nel rispetto di quanto previsto da Codice dei Contratti pubblici.; iii) la presenza di una Determina a contrarre, o atto equivalente, per l'avvio del procedimento di acquisto; iv) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; v) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; vi) 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: la Direzione Pianificazione, Acquisti e Appalti sulla base della richiesta di acquisto proveniente dalle strutture che necessitano del bene/servizio previsto a budget, propone l'impegno di spesa nel rispetto della ripartizione dei poteri di spesa aziendali; il RUP, con gli altri soggetti delegati, predispone gli atti ed avvia il procedimento di acquisto che, in relazione

all'entità della spesa e della procedura prescelta secondo le norme di legge, richiede l'intervento di scelta del fornitore mediante RUP/Seggio/Commissione di gara; l'esito della procedura è posta a base di una proposta di affidamento è accettato con la sottoscrizione dell'atto contrattuale di acquisto (ordine/contratto). Specificatamente per gli *Acquisti per Cassa,* le uscite di cassa sono autorizzate dal Responsabile della struttura "Tesoreria e Finanza", 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 dei poteri delegati.
- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari", paragrafo B).

10 Gestione del Patrimonio

- *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").

11. 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.

- *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 struttura "Amministrazione, Bilancio e Controllo", e delle attività di selezione e assunzione delle risorse, gestite dall'Area Gestione del Personale e Organizzazione sotto la supervisione della Direzione del Personale, Organizzazione, Qualità e Trasparenza

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.

- *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")

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;
- 171-ter;
- 171 septies;
- 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.

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

La disposizione punisce chiunque, a scopo di lucro, abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; abusivamente riproduce, trasmette o diffonde in pubblico opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati; introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico

le duplicazioni o riproduzioni abusive di cui ai punti precedenti); detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato; in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato; introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto; fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche; abusivamente rimuove o altera le informazioni elettroniche, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

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

La disposizione punisce chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.

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. ***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 ad evidenza pubblica

2. ***Gestione dell'attività editoriale:*** si tratta dell'attività relativa alla Rivista L'Automobile. Tale attività deve essere svolta affinché le pubblicazioni editoriali, sia in formato cartaceo sia via web, non possano in alcun modo essere utilizzate quale strumenti di propaganda vietata dalla norma.

3. ***Gestione sistemi informatici, archiviazione informatica e gestione banche dati, gestione sistema protocollo informatico e gestione documentale, gestione internet e posta elettronica:*** 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, delle banche dati, del protocollo informatico, nonché di internet e della posta elettronica. In particolare: 1) per le reti l'attività riguarda la gestione degli accessi e la manutenzione in efficienza; 2) 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; 3) per il software l'attività riguarda la scelta dei prodotti da acquisire, l'installazione, l'aggiornamento, l'utilizzo; 4) per le 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; 5) per il protocollo informatico l'attività riguarda il servizio di gestione del sistema di protocollo informatico e dei documenti per uso interno; 6) per 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.

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.

- **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. Gestione degli Acquisti

- *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, nonché la presenza di un Responsabile del Procedimento (RUP) che opera nel rispetto di quanto previsto da Codice dei Contratti pubblici.; iii) la presenza di una Determina a contrarre, o atto equivalente, per l'avvio del procedimento di acquisto; iv) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; v) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; vi) 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: la Direzione Pianificazione, Acquisti e Appalti sulla base della richiesta di acquisto proveniente dalle strutture che necessitano del bene/servizio previsto a budget, propone l'impegno di spesa nel rispetto della ripartizione dei poteri di spesa aziendali; il RUP, con gli altri soggetti delegati, predispone gli atti ed avvia il procedimento di acquisto che, in relazione all'entità della spesa e della procedura prescelta secondo le norme di legge, richiede l'intervento di scelta del fornitore mediante RUP/Seggio/Commissione di gara; l'esito della procedura è posta a base di una proposta di affidamento è accettato con la sottoscrizione dell'atto

contrattuale di acquisto (ordine/contratto). Specificatamente per gli *Acquisti per Cassa,* le uscite di cassa sono autorizzate dal Responsabile della struttura "Tesoreria e Finanza", 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 dei poteri delegati. .

Codice Etico: è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari", paragrafo B).

2 Gestione dell'attività editoriale di ACI Informatica

Il sistema dei controlli prevede presidi specifici individuati nelle procedure e prassi aziendali, tenuto conto altresì delle normativa vigente in materia di stampa.

- *Regolamentazione*: sono individuati ruoli e responsabilità dei diversi soggetti nelle attività di seguito indicate anche con riferimento alla vigente normativa sulla stampa periodica: i) predisposizione del Piano editoriale; ii) redazione dei singoli articoli; iii) pubblicazione dei singoli articoli; vi) archiviazione della documentazione rilevante.
- *Segregazione dei compiti*: è prevista una separazione dei compiti nelle diverse fasi del processo editoriale con una distinta allocazione dei poteri autorizzativi e di controllo sotto la supervisione del Direttore Responsabile e autorizzata dal Presidente o da diversa persona nell'ambito di eventuali poteri delegati,
- *Procure e deleghe:* è richiesto che le attività editoriale siano svolte soltanto da persone a ciò espressamente preposte.
- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dai capitoli I ("Principi Generali"), VIII ("Conflitti di interesse") e IX ("Valenza del *Codice Etico").*

3. Gestione sistemi informatici, archiviazione informatica e gestione banche dati, gestione sistema protocollo informatico e gestione documentale, gestione internet e posta elettronica

- *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) v) archiviazione dati e documenti, individuazione dei soggetti autorizzati ad accedere e/o a gestire le banche dati, a consultare, elaborare, eliminare informazioni; vi) 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; vii) sono individuate le procedure alle quali deve attenersi il personale nell'uso di email aziendale, nell'accesso a internet

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

- *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. 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. 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 nel capitolo II ("Comportamento nella gestione degli affari", paragrafo A, B, C, D, E), III ("Salute, sicurezza, ambiente"), nel capitolo IV ("Trattamento di informazioni interne") 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. 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.

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.

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.

Attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies c.p.)

La norma punisce chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti.

13.2. Sanzioni in materia di reati ambientali

Attività di gestione dei rifiuti non autorizzata (art. 256 del D.Lgs. 156/2006)

La norma punisce chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione.

Bonifica di siti (art. 257 del D.Lgs. 156/2006)

La norma punisce chiunque cagiona l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio.

Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori, dei formulari e falsificazione nei certificati di analisi rifiuti (art. 258 del D.Lgs. 156/2006)

La norma punisce le imprese che raccolgono e trasportano i propri rifiuti non pericolosi di cui all'articolo 212, comma 8, che non aderiscono, su base volontaria, al sistema di controllo della tracciabilità dei rifiuti (SISTRI) ed effettuano il trasporto di rifiuti senza il formulario di cui all'articolo 193 ovvero indicano nel formulario stesso dati incompleti o inesatti.

Traffico illecito di rifiuti (art. 259 del D.Lgs. 156/2006)

La norma punisce chiunque effettua una spedizione di rifiuti costituente traffico illecito ai sensi dell'articolo 2 del regolamento (CEE) 1° febbraio 1993, n. 259, o effettua una spedizione di rifiuti elencati nell'Allegato II del citato regolamento in violazione dell'articolo 1, comma 3, lettere a), b), e) e d), del regolamento.

Cessazione e riduzione dell'impiego delle sostanze lesive (art. 3 della L. 549/1993)

La norma punisce chiunque viola le disposizioni di cui al presente articolo è punito con l'arresto fino a due anni e con l'ammenda fino al triplo del valore delle sostanze utilizzate per fini produttivi, importate o commercializzate.

In relazione alla commissione dei nuovi reati ambientali del codice penale, nell'art 25-undecies del D.Lgs. 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.

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

-sanzioni pecuniarie: da trecento a mille quote.

Attività organizzate per il traffico illecito di rifiuti (in riferimento all'art. 452 quaterdecies c.p.)

- sanzioni pecuniarie: da duecento a cinquecento quote

Attività di gestione dei rifiuti non autorizzata (art. 256 del D.Lgs. 156/2006)

-sanzioni pecuniarie commi 1 e 6: fino a duecentocinquanta quote;

- sanzioni pecuniarie commi 1, 3, 1° periodo e 5: da centocinquanta a duecentocinquanta quote;

- sanzioni pecuniarie commi 3 1° periodo: fino a duecento a trecento quote.

Bonifica di siti (art. 257 del D.Lgs. 156/2006**)**

-sanzioni pecuniarie 1° comma: fino a duecentocinquanta quote;

-sanzioni pecuniarie 2° comma: da centocinquanta a duecentocinquanta quote.

Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori, dei formulari e falsificazione nei certificati di analisi rifiuti (art. 258 del D.Lgs. 156/2006)

-sanzioni pecuniarie: da centocinquanta a duecentocinquanta quote.

Traffico illecito di rifiuti (art. 259 del D.Lgs. 152/2006)

-sanzioni pecuniarie: da centocinquanta a duecentocinquanta quote.

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.

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 LAVORO

Di seguito son riportati tutti i reati connessi al rapporto di lavoro o comunque alla gestione del personale.

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".

La legge 161/2017 ha esteso la responsabilità della Società anche alle ipotesi di cui all'art. 12, comma 3, 3-bis, 3-ter e 5 del citato Testo Unico dell'Immigrazione

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

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

- sanzioni pecuniarie:
  - ✓ per i delitti di cui all'art. 22, comma 12-bis, del D.Lgs. 286/98 si applica una sanzione da cento a duecento quote, entro il limite di 150.000 euro;
  - ✓ per i delitti di cui all'art 12, commi 3, 3-bis, 3-ter del D.Lgs. 286/98 si applica una sanzione da quattrocento a mille quote;
  - ✓ per i delitti di cui all'art 12, comma 5 del D.Lgs. 286/98 si applica una sanzione da cento a duecento quote;
- sanzioni interdittive: per i delitti di cui all'art 12, commi 3, 3-bis, 3-ter e 5 del D.Lgs. 286/98 si applicano le seguenti sanzioni interdittive: 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.

14.1.2 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**' e alla "**Gestione degli acquisti**"

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).
Le attività sensibili identificate sono qui di seguito riportate:

1. ***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).

2. ***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 ad evidenza pubblica.

14.1.3. 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.

14.1.3.1. 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.

14.1.3.2. Applicazione dei principi di controllo

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

1. Gestione delle risorse umane, i protocolli specifici adottati sono i seguenti:

- *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.

- *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 e/o dalla struttura "Amministrazione, Bilancio e Controllo", e delle attività di selezione e assunzione delle risorse, gestite dall'Area Gestione del Personale e Organizzazione sotto la supervisione della Direzione del Personale, Organizzazione, Qualità e Trasparenza 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.

- *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")

2. Gestione degli acquisti, 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, nonché la presenza di un Responsabile del Procedimento (RUP) che opera nel rispetto di quanto previsto da Codice dei Contratti pubblici.; iii) la presenza di una Determina a contrarre, o atto equivalente, per l'avvio del procedimento di acquisto; iv) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; v) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; vi) 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: la Direzione Pianificazione, Acquisti e Appalti sulla base della richiesta di acquisto proveniente dalle strutture che necessitano del bene/servizio previsto a budget, propone l'impegno di spesa nel rispetto della ripartizione dei poteri di spesa aziendali; il RUP, con gli altri soggetti delegati, predispone gli atti ed avvia il procedimento di acquisto che, in relazione all'entità della spesa e della procedura prescelta secondo le norme di legge, richiede l'intervento di scelta del fornitore mediante RUP/Seggio/Commissione di gara; l'esito della procedura è posta a base di una proposta di affidamento è accettato con la sottoscrizione dell'atto contrattuale di acquisto (ordine/contratto). Specificatamente per gli *Acquisti per Cassa,* le uscite di cassa sono autorizzate dal Responsabile della struttura "Amministrazione, Bilancio 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 dei poteri delegati.
- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari", paragrafo B).

14.2. Reati di razzismo e xenofobia richiamati dall'art. 25-terdecies del D.Lgs. 231/01

A seguito dell'entrata in vigore della Legge 167/2017 (Legge europea 2017) è stato ampliato ulteriormente il catalogo dei reati presupposto per la responsabilità amministrativa. In particolare, è stato introdotto il nuovo **articolo 25-terdecies** dedicato alla prevenzione dei reati di razzismo e xenofobia.

Tale norma fa riferimento all'art. 3 della L. 654/1975, che aveva ratificato la Convenzione internazionale di New York del 1966 sull'eliminazione di ogni forma di discriminazione razziale e che è stato, poi, integrato dalla L. 115/2016 con il comma 3-bis, oggi rilevante anche per la responsabilità delle persone giuridiche.

Il citato articolo è stato abrogato dal D. Lgs. 21/2018, senza tuttavia intervenire sul D. Lgs. 231/01 e, con il medesimo decreto è stato introdotto nell'art. 604 bis nel Codice penale.

In particolare, si tratta del reato di propaganda e istigazione a delinquere per motivi di discriminazione razziale e religiosa.

Da ciò deriva che, quando questi reati siano commessi nell'interesse e a vantaggio di una società o di un ente, quest'ultimo potrà essere colpito da una sanzione pecuniaria, nonché dall'applicazione, per una durata non inferiore a un anno, delle sanzioni interdittive previste dall'art. 9 comma 2 del D.Lgs 231/2001.

Il comma 3 del nuovo art. 25-terdecies prevede anche che, se l'ente o una sua unità organizzativa è stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di tali delitti, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività.

14.2.1. Sanzioni in materia di reati di razzismo e xenofobia previste dal D.Lgs. 231/01

In relazione alla commissione dei reati di propaganda e istigazione a delinquere per motivi di discriminazione razziale e religiosa, si applica all'ente:

- sanzioni pecuniarie: da duecento a ottocento quote.
- sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore ad un anno (se l'ente o una sua unita' organizzativa e' stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei delitti indicati nel comma 1, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attivita' ai sensi dell'articolo 16, comma 3).

14.2.2 Le attività individuate come sensibili ai fini del D.Lgs. 231/2001 in ACI Informatica, con riferimento ai reati di razzismo e xenofobia

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.

Per prevenire la commissione di tali reati si ritiene necessario rafforzare i principi già presenti nel Codice Etico della Società affinché sia reso noto a tutti i soggetti destinatari di tale documento che la Società non consente alcun tipo di comportamento finalizzato alla propaganda vietata dalla citata norma né autorizza alcuna forma di finanziamento per gli stessi.

Inoltre, 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 con una particolare attenzione alla fase relativa alla formazione nonché alla valutazione delle prestazioni.

L'attività è regolamentata da specifica procedure aziendali denominate "Gestione del reclutamento e delle assunzioni a tempo indeterminato",

Inoltre, è individuata quale ulteriore attività sensibile quella riferita **all'attività editoriale** di ACI Informatica della Rivista L'Automobile affinché le pubblicazioni editoriali, sia in formato cartaceo sia via web, non possano in alcun modo essere utilizzate quale strumenti di propaganda vietata dalla norma.

La Società, nel rispetto dei principi di libertà di pensiero, di espressione, di stampa, di associazione, bandisce qualsiasi atto finalizzato all'incitamento alla violenza o all'odio rivolto contro un gruppo di persone o un membro di tale gruppo definito sulla base della razza, del colore e della religione, commesso con qualsiasi forma di diffusione (scritti, immagini o altro materiale) nonché qualsiasi forma di apologia, di negazione o di minimizzazione grossolana in pubblico di tali reati.

Sono vietate qualsiasi forma di finanziamento finalizzato alla propaganda vietata o pubblicazioni editoriali che ne favoriscano la diffusione.

14.2.3. 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.

14.2.3.1. 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.

14.2.3.2. 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 delle Risorse Umane

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 (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 e/o dalla struttura "Amministrazione, Bilancio e Controllo", e delle attività di selezione e assunzione delle risorse, gestite dall'Area Gestione del Personale e Organizzazione sotto la supervisione della Direzione del Personale, Organizzazione, Qualità e Trasparenza 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.

- *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").

2. Gestione dell'attività editoriale di ACI Informatica

Il sistema dei controlli prevede presidi specifici individuati nelle procedure e prassi aziendali, tenuto conto altresì delle normativa vigente in materia di stampa.

- *Regolamentazione*: sono individuati ruoli e responsabilità dei diversi soggetti nelle attività di seguito indicate anche con riferimento alla vigente normativa sulla stampa periodica: i) predisposizione del Piano editoriale; ii) redazione dei singoli articoli; iii) pubblicazione dei singoli articoli; vi) archiviazione della documentazione rilevante.
- *Segregazione dei compiti*: è prevista una separazione dei compiti nelle diverse fasi del processo editoriale con una distinta allocazione dei poteri autorizzativi e di controllo sotto la supervisione del Direttore Responsabile e autorizzata dal Presidente o da diversa persona nell'ambito di eventuali poteri delegati,
- *Procure e deleghe:* è richiesto che le attività editoriale siano svolte soltanto da persone a ciò espressamente preposte.
- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dai capitoli I ("Principi Generali"), VIII ("Conflitti di interesse") e IX ("Valenza del *Codice Etico").*

14.3. Reati in materia di intermediazione illecita e sfruttamento del lavoro richiamati dall'art. 25-quinquies del D.Lgs. 231/01

La Legge 29 ottobre 2016 n. 199 "Disposizioni in materia di contrasto ai fenomeni del lavoro nero, dello sfruttamento del lavoro in agricoltura e di riallineamento retributivo nel settore agricolo" in vigore dal 4 novembre 2016 ha ampliato il catalogo dei reati che possono generare una responsabilità diretta dell'ente apportando alcune modifiche all'articolo 25 quinquies, comma 1, lettera a) del D.Lgs. 231/2001 (delitti contro la personalità individuale).

In particolare, è stato inserito nel novero dei reati previsti in materia di responsabilità amministrativa degli enti ex D.lgs. 231/01 il nuovo reato di intermediazione illecita e sfruttamento del lavoro previsto dall'art. 603 bis del codice penale.

L'introduzione di tale disposizione trova la propria ratio nell'intenzione del legislatore di colpire in maniera specifica il fenomeno del c.d. "caporalato" che è tuttora presente, riformulandone e aggiornandone la definizione, inasprendo le pene per gli sfruttatori ed estendendo la responsabilità e le sanzioni anche agli imprenditori che impiegano manodopera, anche facendo ricorso all'intermediazione dei caporali, approfittando dello stato di bisogno dei lavoratori e sottoponendo gli stessi a condizioni di sfruttamento.

Tale illecito dell'Ente sarà quindi punibile con la sanzione pecuniaria da 400 a 1000 quote e con le sanzioni interdittive previste dell'art. 9 comma 2 del D.lgs.231/01 per una durata non inferiore a un anno.

14.3.1. Sanzioni in materia di intermediazione illecita e sfruttamento del lavoro previste dal D.Lgs. 231/01

In relazione alla commissione del delitto di cui all'art. 603-bis c.p., si applica all'ente:

- sanzioni pecuniarie: da quattrocento a mille quote.
- sanzioni interdittive per una durata non inferiore a un anno, di cui all'art.9 comma 2: a) l'interdizione dall'esercizio dell'attivita'; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) il divieto di pubblicizzare beni o servizi.

14.3.2 Le attività individuate come sensibili ai fini del D.Lgs. 231/2001 in ACI Informatica, con riferimento ai reati in materia di intermediazione illecita e sfruttamento del 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 quale attività sensibile quella riferita alla '**Gestione delle Risorse Umane**' e alla "**Gestione degli acquisti**".
Le attività sensibili identificate sono qui di seguito riportate:

1. ***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).

2. ***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 ad evidenza pubblica.

14.3.3. 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.

14.3.3.1. 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.

14.3.3.2. Applicazione dei principi di controllo

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

1. **Gestione delle risorse umane,** i protocolli specifici adottati sono i seguenti:

   - *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.

   - *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 e/o dalla struttura "Amministrazione, Bilancio e Controllo, e delle attività di selezione e assunzione delle risorse, gestite dall'Area Gestione del Personale e Organizzazione sotto la supervisione della Direzione del Personale, Organizzazione, Qualità e Trasparenza 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.

   - *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")

2. **Gestione degli acquisti,** 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, nonché la presenza di un Responsabile del Procedimento (RUP) che opera nel rispetto di quanto previsto da Codice dei Contratti pubblici.; iii) la presenza di una Determina a contrarre, o atto equivalente, per l'avvio del procedimento di acquisto; iv) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; v) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; vi) 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: la Direzione Pianificazione, Acquisti e Appalti sulla base della richiesta di acquisto proveniente dalle strutture che necessitano del bene/servizio previsto a budget, propone l'impegno di spesa nel rispetto della ripartizione dei poteri di spesa aziendali; il RUP, con gli altri soggetti delegati, predispone gli atti ed avvia il procedimento di acquisto che, in relazione all'entità della spesa e della procedura prescelta secondo le norme di legge, richiede l'intervento di scelta del fornitore mediante RUP/Seggio/Commissione di gara; l'esito della procedura è posta a base di una proposta di affidamento è accettato con la sottoscrizione dell'atto contrattuale di acquisto (ordine/contratto). Specificatamente per gli Acquisti per Cassa, le uscite di cassa sono autorizzate dal Responsabile della struttura "Amministrazione, Bilancio 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 dei poteri delegati.
- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari", paragrafo B).

14.4. Reati in materia di detenzione o accesso a materiale pornografico richiamati dall'art. 25-quinquies del D.Lgs. 231/01

La Legge 23 dicembre 2021 n. 238 (c,d, Legge Europea") - "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea – Legge Europea 2019-2020" ha ampliato il catalogo dei reati che possono generare una responsabilità diretta dell'ente apportando alcune modifiche all'art. 600-quater c.p. relativo alla detenzione o accesso di

materiale pornografico richiamato nell'articolo 25 quinquies, del D.Lgs. 231/2001 (delitti contro la personalità individuale).

Il fatto punito consiste nel procurarsi consapevolmente materiale pornografico prodotto mediante l'utilizzo di minori degli anni diciotto, nonché nel detenere detto materiale (comprensivo anche di tutte quelle condotte svincolate da un qualsiasi uso del materiale). Sotto il profilo della consumazione, la fattispecie costituisce un reato permanente, ove la cessazione della stessa coincide con il venir meno della disponibilità del materiale.

Inoltre, fuori di tali casi, viene punito chiunque, mediante utilizzo della rete internet o di altre reti o mezzi di comunicazione, accede intenzionalmente e senza giustificato motivo a materiale pornografico realizzato utilizzando minori di anni diciotto.

14.4.1. Sanzioni in materia di detenzione o accesso a materiale pornografico richiamati dall'art. 25-quinquies del D.Lgs. 231/01

In relazione alla commissione del delitto di cui all'art. 600-quater c.p., si applica all'ente:

- sanzioni pecuniarie: da duecento a settecento quote.
- sanzioni interdittive per una durata non inferiore a un anno, di cui all'art. 9 comma 2: a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

14.4.2 Le attività individuate come sensibili ai fini del D.Lgs. 231/2001 in ACI Informatica, con riferimento ai reati in materia di detenzione o accesso a materiale pornografico

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**' e alla "**Gestione degli acquisti**".
Le attività sensibili identificate sono qui di seguito riportate:

3. ***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).

4. ***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 ad evidenza pubblica.

14.4.3. 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.

14.4.3.1. 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.

14.4.3.2. Applicazione dei principi di controllo

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

3. Gestione delle risorse umane, i protocolli specifici adottati sono i seguenti:

- *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.

- *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 e/o dalla struttura "Amministrazione, Bilancio e Controllo, e delle attività di selezione e assunzione delle risorse, gestite dall'Area Gestione del Personale e Organizzazione sotto la supervisione della Direzione del Personale, Organizzazione, Qualità e Trasparenza 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.

- *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")

4. **Gestione degli acquisti,** 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, nonché la presenza di un Responsabile del Procedimento (RUP) che opera nel rispetto di quanto previsto da Codice dei Contratti pubblici.; iii) la presenza di una Determina a contrarre, o atto equivalente, per l'avvio del procedimento di acquisto; iv) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; v) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; vi) 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: la

Direzione Pianificazione, Acquisti e Appalti sulla base della richiesta di acquisto proveniente dalle strutture che necessitano del bene/servizio previsto a budget, propone l'impegno di spesa nel rispetto della ripartizione dei poteri di spesa aziendali; il RUP, con gli altri soggetti delegati, predispone gli atti ed avvia il procedimento di acquisto che, in relazione all'entità della spesa e della procedura prescelta secondo le norme di legge, richiede l'intervento di scelta del fornitore mediante RUP/Seggio/Commissione di gara; l'esito della procedura è posta a base di una proposta di affidamento è accettato con la sottoscrizione dell'atto contrattuale di acquisto (ordine/contratto). Specificatamente per gli Acquisti per Cassa, le uscite di cassa sono autorizzate dal Responsabile della struttura "Amministrazione, Bilancio 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 dei poteri delegati.
- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari", paragrafo B).

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. Successivamente il D. Lgs 195/2021 ha ampliato lo spettro di operatività di tale fattispecie.
Il reato di **autoriciclaggio** è definito nell'art. 648-ter.1 del codice penale punisce "chiunque, avendo commesso o concorso a commettere un delitto, 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 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, 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 citato D.Lgs. 195/2021 ha determinato un ampliamento delle fattispecie di riciclaggio e autoriciclaggio attraverso la soppressione dell'inciso "non colposo", la fattispecie prescinde quindi dalla natura dolosa o colposa del delitto presupposto.

In base a quanto previsto nel citato provvedimento sono state introdotte circostanze aggravanti (esercizio di attività professionale con riferimento al delitto di ricettazione) e attenuanti (provenienza del denaro o delle cose da contravvenzione, particolare tenuità dei fatti di ricettazione).

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, 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. I Reati richiamati dall'art. 25 octies-1 del D.Lgs. 231/01

Il D. Lgs. 184/2021 ha introdotto l'art. 25 octies-1 rubricato "Delitti in materia di strumenti di pagamento diversi dai contanti".

Il legislatore ha voluto rafforzare la lotta alle frodi e falsificazioni dei mezzi di pagamento diversi dai contanti sia in considerazione del fatto che costituiscono mezzi di finanziamento della criminalità organizzata sia in quanto limitano lo sviluppo del mercato digitale rendendo i consumatori più riluttanti ad effettuare acquisti on line.

Per strumento di pagamento diverso dai contanti si intende "*un dispositivo, oggetto o record protetto immateriale o materiale o una loro combinazione diverso dalla moneta che permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali*".

Il citato D. Lgs. 184/2021 ha integrato le previsioni degli artt. 493 ter c.p. e 640 ter c.p. ed ha introdotto una nuova fattispecie incriminatrice per la detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti diversi dai contanti (art. 493-quater c.p.).

Il D.Lgs. n.150 del 10 ottobre 2022 è intervenuto in merito alla "Attuazione della legge 27 settembre 2021, n. 134, recante delega al Governo per l'efficienza del processo penale, nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari" ed ha apportato modifiche agli artt. 640 e 640-ter c.p.
Si provvede a fornire una breve descrizione delle fattispecie.

- **Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti** (art. 493-ter c.p.): disciplina l'indebito utilizzo e falsificazione di carte di credito e di pagamento per estendere l'ambito di applicazione della criminalizzazione delle condotte illecite a tutti gli strumenti di pagamento diversi dai contanti.
- **Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti** (art. 493-quater c.p.): costituito dalla condotta di chi detiene o diffonde apparecchiature, dispositivi o programmi informatici progettati per commettere reati collegati agli strumenti di pagamento diversi dal contante.

15.4. Sanzioni in materia di strumenti di pagamento diversi dai contanti previste dal D.Lgs. 231/01

In relazione alla commissione del reati di cui all'art. 493-ter del codice penale, richiamati dall'art. 25-ocietes 1 del D.lgs. 231/01, si applicano all'ente:

- sanzione pecuniaria: da trecento a ottocento quote.
- sanzioni interdittive previste dall'art.9, comma 2, del D.Lgs. 231/2001, per una durata non superiore a due anni.

In relazione alla commissione del reati di cui all'art. 493-quater e 640-ter, comma 2, del codice penale nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale, richiamati dall'art. 25-ocietes 1 del D.lgs. 231/01, si applicano all'ente:

- sanzione pecuniaria: fino a cinquecento quote.
- sanzione pecuniaria fino a cinquecento quote: nel caso in cui il delitto è punito con la pena della reclusione inferiore a dieci anni.
- sanzione pecuniaria da trecento a 800 quote: nel caso in cui il delitto è punito con la pena della reclusione non inferiore a dieci anni.
- sanzioni interdittive previste dall'art.9, comma 2, del D.Lgs. 231/2001, per una durata non superiore a due anni.

15.5. 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,
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 "**Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica con ACI, Federazione ACI e Società del gruppo**"" e alla "**Gestione degli acquisti"** e alla **"Gestione del patrimonio".**

Le attività sensibili identificate sono qui di seguito riportate:

1. ***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.

2. ***Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con ACI, Federazione ACI e Società del gruppo:*** 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, per le Società del gruppo, per la rete delle delegazioni a marchio ACI presenti sul territorio nazionale, nonché per eventuali rapporti convenzionali con la PPAA in generale.
   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.

3. ***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 ad evidenza pubblica.

4. ***Gestione del patrimonio:*** si tratta dell'attività di gestione dei beni strumentali aziendali sia materiali (hardware, attrezzature, arredi, ecc.) che immateriali (software).

15.6. 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.

15.6.1. 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.

15.6.2. 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 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, la registrazione a sistema della relativa distinta, la verifica della relativa regolarità formale e della congruità del pagamento con il contratto/ordine d'acquisto corrispondente, nonché il rispetto della normativa vigente in materia di tracciabilità; 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").

2. Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con ACI, Federazione ACI e Società del gruppo:

- *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. Inoltre, relativamente ai rapporti con la PPAA

per la vendita di servizi, sono individuati ruoli e responsabilità dei diversi attori coinvolti nei processi di 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.

- *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. Inoltre, relativamente ai rapporti con la PPAA, 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, allegati tecnici all'Offerta, lettere di offerta, comunicazioni di accettazione.
- *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 struttura "Amministrazione, Bilancio e Controllo". Inoltre, relativamente i rapporti con la PPAA, è prevista la separazione delle funzioni di autorizzazione, esecuzione e controllo, attribuite alle seguenti funzioni/ai seguenti soggetti: per la 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 struttura "Amministrazione, Bilancio e Controllo" e alle Strutture Tecniche interessate.
- *Poteri autorizzativi e di firma:* è previsto che siano autorizzati ad intrattenere rapporti con ACI o con acquirenti appartenenti alla Pubblica Amministrazione, 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", paragrafi A, B, D, E, F).

3. Gestione degli Acquisti

- *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, nonché la presenza di un Responsabile del Procedimento (RUP) che opera nel rispetto di quanto previsto da Codice dei Contratti pubblici.; iii) la presenza di una Determina a contrarre, o atto equivalente, per l'avvio del procedimento di acquisto; iv) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; v) la tracciabilità del

processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; vi) 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: la Direzione Pianificazione, Acquisti e Appalti sulla base della richiesta di acquisto proveniente dalle strutture che necessitano del bene/servizio previsto a budget, propone l'impegno di spesa nel rispetto della ripartizione dei poteri di spesa aziendali; il RUP, con gli altri soggetti delegati, predispone gli atti ed avvia il procedimento di acquisto che, in relazione all'entità della spesa e della procedura prescelta secondo le norme di legge, richiede l'intervento di scelta del fornitore mediante RUP/Seggio/Commissione di gara; l'esito della procedura è posta a base di una proposta di affidamento è accettato con la sottoscrizione dell'atto contrattuale di acquisto (ordine/contratto). Specificatamente per gli *Acquisti per Cassa,* le uscite di cassa sono autorizzate dal Responsabile della struttura "Tesoreria e Finanza", 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 dei poteri delegati. .
- *Codice Etico*: è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari", paragrafo B).

4 Gestione del Patrimonio

- *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").

16. REATI CONNESSI ALLA CRIMINALITA' ORGANIZZATA

16.1. I Reati richiamati dall'art. 25-ter del D.Lgs. 231/01

La Legge 15 luglio 2009 n. 94 (Disposizioni in materia di sicurezza pubblica) ha ampliato le fattispecie di reato previste dall'art. 25 – ter del D.Lgs. 231/01, includendo i delitti di criminalità organizzata tra i reati presupposto della responsabilità amministrativa "da reato" degli enti.

Si provvede a fornire una breve descrizione delle fattispecie.

Associazione per delinquere finalizzata al compimento di specifiche ipotesi di reato (art. 416 c.p. esclusione comma 6)
La norma punisce tre o più persone che si associano allo scopo di commettere più delitti, nonché coloro che promuovono o costituiscono od organizzano l'associazione.

Associazione di tipo mafioso (art. 416-bis c.p.)
La norma punisce chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone. L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici, o per realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire o ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.
Le disposizioni di questo articolo si applicano anche alla camorra e alle associazioni che avvalendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso.

Scambio elettorale politico-mafioso (art. 416-ter c.p.)
La norma punisce chiunque accetta la promessa di procurare voti da parte di soggetti appartenenti alle associazioni di cui all'art. 416 bis in cambio dell'erogazione o promessa di erogazione di denaro o in cambio della disponibilità a soddisfare interessi o le esigenze dell'associazione mafiosa.

16.2. Sanzioni in materia di reati connessi alla criminalità organizzata previste dal D.lgs. 231/01

Articolo 24-ter, primo comma – *associazione per delinquere* (art. 416 c.p., escluso comma 6), *associazione di tipo mafioso* (art. 416-bis c.p.), *scambio elettorale politico-mafioso* (art. 416-ter c.p.)

- sanzioni pecuniarie: in relazione alla commissione di taluno dei delitti di cui all'art 416 bis, 416 ter, si applica una sanzione pecuniaria da quattrocento a mille quote; per tutti i delitti di cui all'art. 416 c.p., escluso comma 6, si applica una sanzione pecuniaria da trecento a ottocento quote;

- sanzioni interdittive: (per una durata non inferiore a 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; interdizione perpetua dai pubblici uffici nel caso in cui l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo di consentire o agevolare la commissione dei reati di cui ai commi 1 e 2 dell'art. 24 ter.

16.3. 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.

Da una prima analisi delle attività nel cui ambito possono essere commessi i reati elencati, è emersa l'inapplicabilità alla Società dei reati di associazione finalizzata al traffico di sostanze stupefacenti o psicotrope ex art. 74 D.P.R. e del reato di cui all'art. 407, comma 2, lett a, numero 5 c.p.p.

I reati considerati trovano come presupposto l'instaurazione di rapporti a qualsiasi titolo con soggetti esterni alla Società che facciano parte di associazioni criminose. A tal riguardo è opportuno evidenziare che tali reati possono essere astrattamente commessi da tutti gli esponenti aziendali che abbiano contatti con soggetti esterni a qualsiasi titolo.

L'analisi dei processi aziendali di ACI Informatica ha consentito di individuare quale attività sensibile quella riferita alla "**Gestione delle partecipazioni e delle operazioni sul capitale**", alla "**Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica con ACI, Federazione ACI e Società del gruppo"**, alla "**Erogazione di servizi informatici e non**", alla "**Gestione dei flussi finanziari",** alla "**Gestione della contabilità, predisposizione di bilanci, relazioni, comunicazioni sociali",** alla **"Gestione degli acquisti",** alla **"Gestione delle risorse umane",** alla **"Gestione del contenzioso",** alla "**Gestione dei rapporti con la Autorità pubblica relativi ad attività e controllo**", alla "**Gestione per la tutela dei lavoratori nei luoghi di lavoro**", alla "**Gestione ambientale**" e alla "**Gestione dei regali, omaggi e benefici**".

Le attività sensibili identificate sono qui di seguito riportate:

1. ***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 migliore organizzazione della Società, attraverso l'apporto

di strutture societarie con controllo analogo indiretto da parte di ACI (es. ANCI Digitale). 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. Il processo è regolato dal Regolamento di Governance delle società controllate di ACI prevedendo un apposito iter autorizzativo.

2. N***egoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con ACI, Federazione ACI e Società del gruppo:*** 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, per le Società del gruppo, per la rete delle delegazioni a marchio ACI presenti sul territorio nazionale, nonché per eventuali rapporti convenzionali con la PPAA in generale.

   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.

3. ***Erogazione di servizi informatici e non:*** il processo riguarda l'erogazione di servizi informatici e non forniti in virtù di convenzioni o contratti. La gestione dei servizi informatici può comportare l'utilizzo dei seguenti strumenti:

   - ***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 (pagamento bollo auto e pagamento quote associative).

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

5. ***Gestione della contabilità, 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.

6. ***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 ad evidenza pubblica.

7. ***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. ***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.

9. ***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.

10. ***Gestione per la tutela dei lavoratori nei luoghi di lavoro***

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

11. ***Gestione ambientale***

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.

12. ***Gestione dei regali, omaggi e benefici:*** il processo riguarda i doni e gli omaggi che generalmente vengono effettuati o ricevuti nel periodo natalizio e in entrambe i casi sono di modesta entità. Generalmente i doni effettuati da ACI Informatica sono rivolti alle banche, oppure riguardano relazioni industriali e/o professionisti esterni.

16.4. 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.

16.4.1. 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.

16.4.2. 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 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. L'intera materia è oggetto di specifica disciplina nel Regolamento di Governance per le società controllate da ACI.
- *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'osservanza 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".

2. Negoziazione/stipulazione/esecuzione di contratti conclusi da ACI Informatica S.p.A. con ACI, Federazione ACI e Società del gruppo:

- *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. Inoltre, relativamente ai rapporti con la PPAA per la vendita di servizi, sono individuati ruoli e responsabilità dei diversi attori coinvolti nei processi di 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.
- *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. Inoltre, relativamente ai

rapporti con la PPAA, 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, allegati tecnici all'Offerta, lettere di offerta, comunicazioni di accettazione.

- *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 struttura "Tesoreria e Finanza". Inoltre, relativamente i rapporti con la PPAA, è prevista la separazione delle funzioni di autorizzazione, esecuzione e controllo, attribuite alle seguenti funzioni/ai seguenti soggetti: per la 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 struttura "Tesoreria e Finanza" e alle Strutture Tecniche interessate.
- *Poteri autorizzativi e di firma:* è previsto che siano autorizzati ad intrattenere rapporti con ACI o con acquirenti appartenenti alla Pubblica Amministrazione, 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", paragrafi A, B, D, E, F).

5. Erogazione di servizi informatici e non

- *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.

- *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").

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 di pagamenti ed incassi atte a garantire il rispetto della normativa vigente in materia di tracciabilità; 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").

7. Gestione della contabilità, 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 struttura "Amministrazione, Bilancio 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 struttura "Amministrazione, Bilancio 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 struttura "Amministrazione, Bilancio e Controllo", il Collegio Sindacale, il Consiglio di Amministrazione, la Società di Revisione.

- *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".

8. Gestione degli Acquisti

- *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, nonché la presenza di un Responsabile del Procedimento (RUP) che opera nel rispetto di quanto previsto da Codice dei Contratti pubblici.; iii) la presenza di una Determina a contrarre, o atto equivalente, per l'avvio del procedimento di acquisto; iv) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; v) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; vi) 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: la Direzione Pianificazione, Acquisti e Appalti sulla base della richiesta di acquisto proveniente dalle strutture che necessitano del bene/servizio previsto a budget, propone l'impegno di spesa nel rispetto della ripartizione dei poteri di spesa aziendali; il RUP, con gli altri soggetti delegati, predispone gli atti ed avvia il procedimento di acquisto che, in relazione all'entità della spesa e della procedura prescelta secondo le norme di legge, richiede l'intervento di scelta del fornitore mediante RUP/Seggio/Commissione di gara; l'esito della procedura è posta a base di una proposta di affidamento è accettato con la sottoscrizione dell'atto contrattuale di acquisto (ordine/contratto). Specificatamente per gli Acquisti per Cassa, le uscite di cassa sono autorizzate dal Responsabile della struttura "Tesoreria e Finanza", 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 dei poteri delegati.
- *Codice Etico:* è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari", paragrafo B).

7 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.

- *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 e/o dalla struttura "Amministrazione, Bilancio e Controllo", e delle attività di selezione e assunzione delle risorse, gestite dall'Area Gestione del Personale e Organizzazione sotto la supervisione della Direzione del Personale, Organizzazione, Qualità e Trasparenza 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.

- *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").

8 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 della Direzione Affari Societari e Legali; ii) contenzioso stragiudiziale: l'autorizzazione è demandata al Presidente, alla Direzione Generale ; l'esecuzione degli atti è di competenza del responsabile della struttura interessata dalla controversia, il controllo è rimesso al Responsabile della Direzione Affari Societari e Legali.

- *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, Direzione 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).

9 Gestione dei rapporti con la Autorità pubblica relativi ad attività 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 alla Direzione 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, Direzione Generale, altri soggetti delegati).
- *Codice Etico:* è richiesta l'osservanza delle indicazioni comportamentali previste dal capitolo II ("Comportamento nella gestione degli affari").

10 Gestione per la tutela dei lavoratori nei luoghi di lavoro

- *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.

11 Gestione ambientale

- *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.

12 Gestione dei regali, omaggi e benefici

- *Regolamentazione:* sono individuati ruoli e responsabilità dei diversi soggetti nelle attività di seguito indicate: i) autorizzazione del responsabile di funzione; segnalazione all'Organismo di Vigilanza.
- *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:* si richiede l'individuazione delle figure autorizzate alla gestione di regali, omaggi e benefici.
- *Tracciabilità*: la tracciabilità del processo in esame è garantita tramite apposita documentazione che viene conservata e di cui ne viene data comunicazione all'Organismo di Vigilanza.
- *Codice Etico:* è richiesta l'osservanza delle indicazioni comportamentali previste dal capitolo II ("Regali, omaggi, benefici", paragrafo I).

17. REATI DI INTRALCIO ALLA GIUSTIZIA - INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA

17.1. I Reati richiamati dall'art. 25-decies del D.Lgs. 231/01

La Legge 3 agosto n. 116 che ha ratificato la convenzione ONU contro la corruzione del 2003, all'art. 4 introduce l'art. 25 decies che inserisce tra i reati presupposto l'art. 377 bis c.p. concernente l'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria.

Si provvede a fornire una breve descrizione delle fattispecie.

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 377 bis c.p.)

Il reato si configura mediante l'induzione, a seguito di violenza, minaccia o offerta o promessa di denaro o altre utilità, del soggetto avente facoltà di non rendere dichiarazioni – ossia di avvalersi della facoltà – o a rendere dichiarazioni mendaci all'Autorità Giudiziaria.

Infine, affinchè l'ipotesi criminosa di cui all'art. 377 bis sia configurabile è necessario che le dichiarazioni del testimone vengano rese innanzi all'Autorità Giudiziaria nel corso di un procedimento penale.

I destinatari della condotta sono pertanto gli indagati e gli imputati ai quali è riconosciuta dall'ordinamento la facoltà di non rispondere.

17.2. Sanzioni in materia di reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria previsto dal D.lgs. 231/01

Articolo 25-decies, *induzione a non rendere dichiarazioni o a rendere dichiarazioni all'Autorità Giudiziaria* (art. 377 bis c.p.):

- sanzioni pecuniarie: si applica una sanzione pecuniaria fino a cinquecento quote;

17.3. 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.

L'analisi dei processi aziendali di ACI Informatica ha consentito di individuare quale attività sensibile quella riferita alla "**Gestione del contenzioso**".

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.

17.4. 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.

17.4.1. 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.

17.4.2. 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.

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 della Direzione Affari Societari e Legali; ii) contenzioso stragiudiziale: l'autorizzazione è demandata al Presidente, alla Direzione Generale ; l'esecuzione degli atti è di competenza del responsabile della struttura interessata dalla controversia, il controllo è rimesso al Responsabile della Direzione Affari Societari e Legali.
- *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, Direzione 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).

18. REATI TRIBUTARI

18.1. I Reati richiamati dall'art. 25-quinquiesdecies del D.Lgs. 231/01

Con Decreto Legge del 26 ottobre 2019 n. 124 recante "*Disposizioni urgenti in materia fiscale e per esigenze indifferibili*" al capo IV "*Modifiche della disciplina penale in materia tributaria e della responsabilità amministrativa degli enti nella stessa materia",* è stato introdotto nell'ambito del D. Lgs. 231/01, l'art. 25-quinquiesdecies (Reati tributari) tramite il quale il legislatore ha inserito nel catalogo dei reati-presupposto la fattispecie di dichiarazione fraudolenta mediante utilizzo di fatture o altra documentazione per operazioni inesistenti.

L'art. 39 del citato D.L. è intervenuto sul testo del D. Lgs. 10 marzo 2000 n. 74 recante "*Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto a norma dell'art. 9 della L.205/1999".*

Con tale previsione per la prima volta la responsabilità amministrativa degli enti coinvolge la commissione dei reati tributari, prevedendo una sanzione pecuniaria da comminare all'Ente fino a cinquecento quote.

L'obiettivo perseguito è rappresentato dall'inasprimento della risposta penale all'illecito fiscale, con il potenziamento degli strumenti cautelari adoperabili.

Successivamente, il D.Lgs. 14 luglio 2020, n. 75 ha integrato l'**art. 25-quinquiesdecies,** inserendo altre ipotesi di reato previsti dal D.Lgs 10 marzo 2000, n. 74 se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a 10 milioni di euro (Artt. 4, 5 e 10-quater del D. Lgs. 74/2000).

- V6 dichiarazione infedele (art. 4 del D. lgs 74/2000);
- V7 omessa dichiarazione (art. 5 del D. Lgs. 74/2000);
- V8 indebita compensazione (art. 10 quater del D. Lgs. 74/2000).

Tale disciplina è stata integrata dal D.Lgs. n. 156/2022 recante "Disposizioni correttive e integrative del D. Lgs. 75/2020 di attuazione della direttiva "PIF" relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale (UE 2017/1371)". Infatti, intervenendo sul comma 1-bis dell'art. 25-quinquesdecies, si è subordinata la rilevanza ai sensi del D.Lgs. n. 231/2001 dei reati di dichiarazione infedele, omessa dichiarazione e indebita compensazione alla condizione che essi risultino commessi nell'ambito di "sistemi fraudolenti transfrontalieri", garantendo così il rispetto del principio di transnazionalità unionale rilevante ai fini della responsabilità amministrativa.
L'applicazione delle sanzioni pecuniarie per i reati di dichiarazione infedele, omessa dichiarazione e indebita compensazione, viene così subordinata alla condizione che tali reati risultino commessi al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione

europea, da cui consegua o possa conseguire un danno complessivo pari o superiore a 10 milioni di euro.

Si provvede a fornire una breve descrizione delle fattispecie.

Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 1 e 2 bis del D. Lgs 10 marzo 2000, n. 74)

Questa disposizione punisce chiunque per evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.

La fattispecie penale trova applicazione qualunque sia l'ammontare di imposta evaso.
Ai fini della configurabilità del reato è necessario il dolo specifico, rappresentato dal perseguimento della finalità evasiva, che deve aggiungersi alla volontà di realizzare l'evento tipico.
L'art. 2, comma 2, della citata disposizione precisa che, affinchè ci sia la fattispecie penale, tali fatture o documenti devono essere registrati nelle scritture contabili obbligatorie ovvero detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

Dichiarazione fraudolenta mediante altri artifici – art. 3 D. Lgs 10 marzo 2000, n. 74

La fattispecie si applica fuori dai casi previsti dall'art. 2 del D. Lgs. 74/2000 a chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate o avvalendosi di documenti falsi, indica elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi o crediti e ritenute fittizi, quando congiuntamente:

a) l'imposta evasa è superiore a € 30.000;
b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione è superiore al 5% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione.

Dichiarazione infedele – art. 4 del D. Lgs 10 marzo 2000, n. 74

La disposizione punisce chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti.

La disposizione rileva soltanto se si ricorrono le circostanze previste nell'art. 25-quinquiesdecies, comma 1-bis del D.Lgs. 231/2001, così come integrato dal D.Lgs. 14 luglio 2020, n. 75

Omessa dichiarazione – art. 5 del D. Lgs 10 marzo 2000, n. 74

La disposizione punisce chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte.

La disposizione rileva soltanto se si ricorrono le circostanze previste nell'art. 25-quinquiesdecies, comma 1-bis del D.Lgs. 231/2001, così come integrato dal D.Lgs. 14 luglio 2020, n. 75

Emissione di fatture o altri documenti per operazioni inesistenti – art. 8, comma 1 e 2 bis del D. Lgs 10 marzo 2000, n. 74

Questa disposizione punisce chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

Si tratta di un reato istantaneo che si consuma nel momento di emissione della fattura ovvero, ove si abbiano plurimi episodi nel medesimo periodo di imposta, nel momento di emissione dell'ultima di esse, non essendo richiesto che il documento pervenga al destinatario.

Occultamento o distruzione di documenti contabili – art. 10 D. Lgs 10 marzo 2000, n. 74
Questa fattispecie punisce chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione di terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

Indebita compensazione – art. 10-quater del D. Lgs 10 marzo 2000, n. 74

La disposizione punisce chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti.

La disposizione rileva soltanto se si ricorrono le circostanze previste nell'art. 25-quinquiesdecies, comma 1-bis del D.Lgs. 231/2001, così come integrato dal D.Lgs. 14 luglio 2020, n. 75

Sottrazione fraudolenta al pagamento di imposte – art. 11 D. Lgs 10 marzo 2000, n. 74
Questa fattispecie punisce chiunque al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto o di interessi o sanzioni amministrative relativi a imposte di ammontare superiore ad € 50.000, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere inefficace la procedura di riscossione coattiva.

18.2. Sanzioni in materia di reati tributari previste dal D.Lgs. 231/01

In relazione alla commissione dei reati di cui agli artt. 2 comma 1 e 2 bis, 3, 8, 10 e 11 del D.Lgs. 74/20000, richiamati dall'art. 25-quinquiesdecies del D.lgs. 231/01, si applicano all'ente:

- sanzione pecuniaria art. 2, comma 1: fino a cinquecento quote;
- sanzione pecuniaria art. 2, comma 2bis: fino a quattrocento quote;
- sanzione pecuniaria art. 3: fino a cinquecento quote;
- sanzione pecuniaria art. 4: fino a trecento quote;

- sanzione pecuniaria art. 5: fino a quattrocento quote
- sanzione pecuniaria art. 8: fino a cinquecento quote;
- sanzione pecuniaria art. 10: fino a quattrocento quote;
- sanzione pecuniaria art. 10-quater: fino a quattrocento quote.

- sanzioni interdittive il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; ii) l'esclusione da agevolazioni, finanziamenti, contributi, contributi o sussidi e l'eventuale revoca di quelli già concessi; iii) il divieto di pubblicizzare beni o servizi.

18.3. 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.

L'analisi dei processi aziendali di ACI Informatica ha consentito di individuare quale attività sensibile quella riferita alla "**Gestione della contabilità, predisposizione di bilanci, relazioni, comunicazioni sociali**", alla "**Gestione degli Acquisti"**, alla **"Gestione del patrimonio".**

Le attività sensibili identificate sono qui di seguito riportate:

1. ***Gestione della contabilità, 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. ***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.

3. ***Gestione del patrimonio:*** si tratta dell'attività di gestione dei beni strumentali aziendali sia materiali (hardware, attrezzature, arredi, ecc.) che immateriali (software).

18.4. 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.

18.4.1. 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.

18.4.2. 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 della contabilità, 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 struttura "Amministrazione, Bilancio 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 struttura "Amministrazione, Bilancio 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 struttura "Amministrazione, Bilancio e Controllo", il Collegio Sindacale, il Consiglio di Amministrazione, la Società di Revisione.
- *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. Gestione degli Acquisti

- 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, nonché la presenza di un Responsabile del Procedimento (RUP) che opera nel rispetto di quanto previsto da Codice dei

Contratti pubblici; iii) la presenza di una Determina a contrarre, o atto equivalente, per l'avvio del procedimento di acquisto; iv) i livelli autorizzativi previsti per ciascuna fase del processo di acquisto; v) la tracciabilità del processo decisionale e delle relative motivazioni, supportata dal sistema informatico aziendale; vi) 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: la Direzione Pianificazione, Acquisti e Appalti sulla base della richiesta di acquisto proveniente dalle strutture che necessitano del bene/servizio previsto a budget, propone l'impegno di spesa nel rispetto della ripartizione dei poteri di spesa aziendali; il RUP, con gli altri soggetti delegati, predispone gli atti ed avvia il procedimento di acquisto che, in relazione all'entità della spesa e della procedura prescelta secondo le norme di legge, richiede l'intervento di scelta del fornitore mediante RUP/Seggio/Commissione di gara; l'esito della procedura è posta a base di una proposta di affidamento è accettato con la sottoscrizione dell'atto contrattuale di acquisto (ordine/contratto). Specificatamente per gli Acquisti per Cassa, le uscite di cassa sono autorizzate dal Responsabile della struttura "Tesoreria e Finanza", 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 dei poteri delegati.
- Codice Etico: è richiesta l'osservanza dei principi stabiliti dal capitolo II ("Comportamento nella gestione degli affari", paragrafo B).

3. Gestione del Patrimonio

- *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, Direzione 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").

19. REATI REALIZZATI CON FINALITA' DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO

19.1. I Reati richiamati dall'art. 25-quater del D.Lgs. 231/01

L'art. 25 quater del D.Lgs. 231/2001, introdotto dalla L. 7/2003 ha ampliato le fattispecie di reato da cui può sorgere la responsabilità dell'ente, introducendo 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.
Si provvede a fornire una breve descrizione delle fattispecie.

Associazioni con finalità di terrorismo e di eversione dell'ordine democratico – art. 270 bis c.p.
Detta norma punisce chi promuove, costituisce, organizza, dirige o finanzia associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico.

Associazioni con finalità di terrorismo e di eversione dell'ordine democratico – art. 270 bis 1 c.p.
Detta norma prevede circostanze aggravanti.
Assistenza agli associati (art. 270-ter c.p.)
Detta norma punisce chiunque dà rifugio o fornisce vitto, ospitalità, mezzi di trasporto, strumenti di comunicazione a taluna delle persone che partecipano alle associazioni con finalità terroristiche o eversive.

Arruolamento con finalità di terrorismo anche internazionale (art. 270-quater c.p.)
Tale norma punisce chiunque arruola una o più persone per il compimento di atti di violenza ovvero di sabotaggio di servizi pubblici essenziali, con finalità di terrorismo, anche se rivolti contro uno Stato estero, un'istituzione o un organismo internazionale, è punito con la reclusione da sette a quindici anni.

Articolo 270-quater1 codice penale - Organizzazione di trasferimenti per finalità di terrorismo (art. 270-quater 1 c.p.)
Tale norma punisce chiunque organizza, finanzia o propaganda viaggi in territorio estero finalizzati al compimento delle condotte con finalità di terrorismo.

Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-quinquies c.p.)
Tale norma punisce chiunque addestra o comunque fornisce istruzioni sulla preparazione o sull'uso di materiali esplosivi, di armi da fuoco o di altre armi, di sostanze chimiche o batteriologiche nocive o pericolose, nonché di ogni altra tecnica o metodo per il compimento di atti di violenza ovvero di sabotaggio di servizi pubblici essenziali, con finalità di terrorismo, anche se rivolti contro uno Stato estero, un'istituzione o un organismo internazionale.

Condotte con finalità di terrorismo (art. 270-sexies c.p.)
Tale norma rileva che sono considerate con finalità di terrorismo le condotte che possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale, nonché le altre condotte definite terroristiche o commesse con finalità di terrorismo da convenzioni o altre norme di diritto internazionale vincolanti per l'Italia.

19.2. Sanzioni in materia di reati realizzati con finalità di terrorismo o di eversione dell'ordine democratico

Articolo 25-quater, Delitti con finalità di terrorismo o di eversione dell'ordine democratico:

- sanzioni pecuniarie:
  a) se il delitto è punito con la pena della reclusione inferiore a 10 anni si applica una sanzione pecuniaria da duecento a 700 quote;
  b) se il delitto è punito con la pena della reclusione non inferiore a 10 anni o con l'ergtastolo si applica una sanzione pecuniaria da quattrocento fino a mille quote;
- sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore ad un anno.

19.3. 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.

L'analisi dei processi aziendali di ACI Informatica ha consentito di individuare quale attività sensibile quella riferita alla "**Erogazione di servizi informatici e non".**

Erogazione di servizi informatici e non: il processo riguarda l'erogazione di servizi informatici e non forniti in virtù di convenzioni o contratti. La gestione dei servizi informatici può comportare l'utilizzo dei seguenti strumenti:

- ***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 (pagamento bollo auto e pagamento quote associative).

19.4. 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.

19.4.1. 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.

19.4.2. 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.

Erogazione di servizi informatici e non

- *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.

- *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").

20. ALLEGATI

20.1. Codici e Manuali

a) Codice Etico
b) Codice Disciplinare Aziendale
c) Manuale del Sistema di Gestione Integrato Qualità, Sicurezza, Servizi IT, Business Continuity, Ambiente e Energia
e) Documento valutazione rischi (DVR)
f) Manuale Tecnico del Sistema Informatico contabile aziendale (SCI)

20.2. Organigramma aziendale

a) Organigramma della Società

20.3. 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. Flussi informativi da e verso l'Organismo di Vigilanza
c. Codice di Corporate Governance
d. Attività di vigilanza sul Modello di Organizzazione, Gestione e Controllo
e. Procedura del processo di chiusura del bilancio d'esercizio e delle chiusure trimestrali
f. Verifiche effettuate da organi sociali e da soggetti esterni
g. Fornitura di service amministrativo per gli AACC provinciali
h. Trasmissione telematica dei dati contributivi e previdenziali all'INPS
i. Trasmissione telematica dei dati fiscali
j. Gestione del contenzioso
k. Gestione fisica ed amministrativa del patrimonio
l. Gestione del reclutamento e delle assunzioni a tempo indeterminato
m. Gestione assunzioni a tempo determinato
n. Gestione incentivi
o. Procedura e sistema delle rilevazioni contabili - Ciclo attivo
p. Procedura e sistema delle rilevazioni contabili - Ciclo passivo
q. Procedura e sistema delle rilevazioni contabili - Ciclo finanziario
r. Gestione Magazzino
s. Contabilizzazione stipendi
t. Gestione delle partecipazioni societarie
u. Disciplinare tecnico per l'utilizzo di posta elettronica e della rete internet
v. Gestione dei personal computer
w. Gestione della sicurezza logica
x. Gestione rifiuti speciali
y. Alienazione dei beni aziendali
z. Linee guida Tracciabilità dei flussi finanziari

aa. Archiviazione sostitutiva dei libri contabili e dei documenti rilevanti ai fini IVA
bb. Pianificazione appalti
cc. Compilazione Richiesta di acquisto
dd. Affidamento appalti
ee. Gestione contratti passivi
ff. Affidamento appalti con procedura sotto soglia
gg. Affidamento appalti con procedura aperta
hh. Gestione omaggi, liberalità e sponsorizzazioni
ii. Erogazione sovvenzioni e contributi
jj. Catalogo dei servizi end to end portfolio servizi
kk. Regolamento per l'iscrizione nell'Albo dei Professionisti per il conferimento di incarichi di assistenza legale e notarile in favore di ACI Informatica S.p.A.

L'elenco delle procedure di cui sopra costituisce un semplice richiamo alle procedure aziendali in essere e pertanto la loro modificazione, integrazione e sostituzione non necessita la modifica al presente Modello.

20.4. Deleghe Aziendali

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

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

21. DOCUMENTO DI VALUTAZIONE DEI RISCHI DI ACI INFORMATICA S.P.A. E ELENCO DEI REATI E SANZIONI AI SENSI DEL D. LGS. 231/01 (ALLEGATO 1 AL DOCUMENTO DI VALUTAZIONE DEI RISCHI)

Il Documento di Valutazione dei Rischi di ACI Informatica, in allegato al presente Modello di Organizzazione e di cui costituisce parte integrante, è stato elaborato sulla base dell'analisi documentale e delle interviste svolte nel 4° trimestre 2019 ai responsabili dei processi e delle funzioni coinvolte.

Tale documento rappresenta la sintesi del lavoro di ricognizione e valutazione dei processi e delle attività considerate "sensibili" con riferimento ai reati previsti dal D. Lgs. 231/01.

Al documento di valutazione dei rischi è allegato il riepilogo di tutte le fattispecie dei reati di cui al D. Lgs. 231/01 (Allegato 1 al Documento di Valutazione dei Rischi – Elenco dei reati e sanzioni dei sensi del D. Lgs. 231/01).

22. 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.

   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.

23. STRALCIO DEGLI ARTT. 24 E 25 DEL D.LGS. 231/2001

ARTICOLO 24 - Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture.

1. In relazione alla commissione dei delitti di cui agli articoli 316-bis, 316-ter, 356, 640, comma 2, n. 1, 640-bis e 640-ter se commesso in danno dello Stato o di altro ente pubblico o dell'Unione europea, del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.

2. Se, in seguito alla commissione dei delitti di cui al comma 1, l'ente ha conseguito un profitto di rilevante entita' o e' derivato un danno di particolare gravita'; si applica la sanzione pecuniaria da duecento a seicento quote.

2-bis Si applicano all'ente le sanzioni previste ai commi precedenti in relazione alla commissione del delitto di cui all'articolo 2 della legge 23 dicembre 1986 n. 898.

3. Nei casi previsti dai commi precedenti, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

ARTICOLO 24 BIS - Delitti informatici e trattamento illecito di dati.

1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all´ente la sanzione pecuniaria da cento a cinquecento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all´ente la sanzione pecuniaria sino a trecento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall´articolo 24 del presente decreto peri casi di frode informatica in danno dello Stato o di altro ente pubblico e dei delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, si applica all´ente la sanzione pecuniaria sino a quattrocento quote.

4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall´articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall´articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall´articolo 9, comma 2, lettere c), d) ed e).

ARTICOLO 24 TER - Delitti di criminalita' organizzata.

1. In relazione alla commissione di taluno dei delitti di cui agli articoli 416, sesto comma, 416-bis, 416-ter e 630 del codice penale, ai delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416-bis ovvero al fine di agevolare l´attività delle associazioni previste dallo stesso articolo, nonché ai delitti previsti dall´articolo74 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, si applica la sanzione pecuniaria da quattrocento a mille quote.

2. In relazione alla commissione di taluno dei delitti di cui all´articolo 416 del codice penale, ad esclusione del sesto comma, ovvero di cui all´articolo 407, comma 2, lettera a), numero 5), del codice di procedura penale, si applicala sanzione pecuniaria da trecento a ottocento quote.

3. Nei casi di condanna per uno dei delitti indicati nei commi 1 e 2, si applicano le sanzioni interdittive previste dall´articolo 9, comma 2, per una durata non inferiore ad un anno.

4. Se l´ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati nei commi 1 e 2, si applica la sanzione dell´interdizione definitiva dall´esercizio dell´attività ai sensi dell´articolo 16, comma 3.

ARTICOLO 25 – Peculato, concussione, induzione indebita a dare o promettere utilita', corruzione e abuso d'ufficio.

1. In relazione alla commissione dei delitti di cui agli articoli 318, 321, 322, commi primo e terzo, e 346-bis del codice penale, si applica la sanzione pecuniaria fino a duecento quote. La medesima sanzione si applica, quando il fatto offende gli interessi finanziari dell'Unione europea, in relazione alla commissione dei delitti di cui agli articoli 314, primo comma, 316 e 323 del codice penale.

2. In relazione alla commissione dei delitti di cui agli articoli 319, 319-ter, comma 1, 321, 322, commi 2 e 4, del codice penale, si applica all´ente la sanzione pecuniaria da duecento a seicento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 317, 319, aggravato ai sensi dell´articolo 319-bis quando dal fatto l´ente ha conseguito un profitto di rilevante entità, 319-ter, comma 2, 319-quater e 321 del codice penale, si applica all´ente la sanzione pecuniaria da trecento a ottocento quote.

4. Le sanzioni pecuniarie previste per i delitti di cui ai commi da 1 a 3, si applicano all´ente anche quando tali delitti sono stati commessi dalle persone indicate negli articoli 320 e 322-bis.

5. Nei casi di condanna per uno dei delitti indicati nei commi 2 e 3, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a quattro anni e

non superiore a sette anni, se il reato è stato commesso da uno dei soggetti di cui all'articolo 5, comma 1, lettera a), e per una durata non inferiore a due anni e non superiore a quattro, se il reato è stato commesso da uno dei soggetti di cui all'articolo 5, comma 1, lettera b).

5-bis. Se prima della sentenza di primo grado l'ente si è efficacemente adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l'individuazione dei responsabili ovvero per il sequestro delle somme o altre utilità trasferite e ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi, le sanzioni interdittive hanno la durata stabilita dall'articolo 13, comma 2.

ARTICOLO 25 BIS - Falsita' in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento.

1. In relazione alla commissione dei delitti previsti dal codice penale in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, si applicano all´ente le seguenti sanzioni pecuniarie:

a) per il delitto di cui all´articolo 453 la sanzione pecuniaria da trecento a ottocento quote;

b) per i delitti di cui agli articoli 454, 460 e 461 la sanzione pecuniaria fino a cinquecento quote;

c) per il delitto di cui all´articolo 455 le sanzioni pecuniarie stabilite dalla lettera a), in relazione all´articolo 453, e dalla lettera b) in relazione all´articolo 454, ridotte da un terzo alla metà;

d) per i delitti di cui agli articoli 457 e 464, secondo comma, le sanzioni pecuniarie fino a duecento quote;

e) per il delitto di cui all´articolo 459 le sanzioni pecuniarie previste dalle lettere a), c) e d) ridotte di un terzo;

f) per il delitto di cui all´articolo 464, primo comma, la sanzione pecuniaria fino a trecento quote;

f-bis) per i delitti di cui agli articoli 473 e 474, la sanzione pecuniaria fino a cinquecento quote.

2. Nei casi di condanna per uno dei delitti di cui agli articoli 453, 454, 455, 459, 460, 461, 473 e 474 del codice penale, si applicano all´ente le sanzioni interdittive previste dall´articolo 9, comma 2, per una durata non superiore ad un anno.

ARTICOLO 25 BIS 1 - Delitti contro l'industria e il commercio.

1. In relazione alla commissione dei delitti contro l´industria e il commercio previsti dal codice penale, si applicano all´ente le seguenti sanzioni pecuniarie:

a) per i delitti di cui agli articoli 513, 515, 516, 517, 517-ter e517-quater la sanzione pecuniaria fino a cinquecento quote;

b) per i delitti di cui agli articoli 513-bis e 514 la sanzione pecuniaria fino a ottocento quote.

2. Nel caso di condanna per i delitti di cui alla lettera b) del comma 1 si applicano all´ente le sanzioni interdittive previste dall´articolo 9, comma 2.

ARTICOLO 25 TER - Reati societari.

1. In relazione ai reati in materia societaria previsti dal codice civile, si applicano all'ente le seguenti sanzioni pecuniarie:

a) per il delitto di false comunicazioni sociali previsto dall´articolo 2621 del codice civile, la sanzione pecuniaria da duecento a quattrocento quote;

a-bis) per il delitto di false comunicazioni sociali previsto dall'articolo 2621-bis del codice civile, la sanzione pecuniaria da cento a duecento quote;

b) per il delitto di false comunicazioni sociali previsto dall´articolo 2622 del codice civile, la sanzione pecuniaria da quattrocento a seicento quote;

c) lettera abrogata;

d) per la contravvenzione di falso in prospetto, prevista dall´articolo 2623, primo comma, del codice civile, la sanzione pecuniaria da cento a centotrenta quote;

e) per il delitto di falso in prospetto, previsto dall´articolo 2623, secondo comma, del codice civile, la sanzione pecuniaria da duecento a trecentotrenta quote;

f) per la contravvenzione di falsità nelle relazioni o nelle comunicazioni delle società di revisione, prevista dall´articolo 2624, primo comma, del codice civile, la sanzione pecuniaria da cento a centotrenta quote;

g) per il delitto di falsità nelle relazioni o nelle comunicazioni delle società di revisione, previsto dall´articolo 2624, secondo comma, del codice civile, la sanzione pecuniaria da duecento a quattrocento quote;

h) per il delitto di impedito controllo, previsto dall´articolo 2625, secondo comma, del codice civile, la sanzione pecuniaria da cento a centottanta quote;

i) per il delitto di formazione fittizia del capitale, previsto dall´articolo 2632 del codice civile, la sanzione pecuniaria da cento a centottanta quote;

l) per il delitto di indebita restituzione dei conferimenti, previsto dall´articolo 2626 del codice civile, la sanzione pecuniaria da cento a centottanta quote;

m) per la contravvenzione di illegale ripartizione degli utili e delle riserve, prevista dall´articolo 2627 del codice civile, la sanzione pecuniaria da cento a centotrenta quote;

n) per il delitto di illecite operazioni sulle azioni o quote sociali o della società controllante, previsto dall´articolo 2628 del codice civile, la sanzione pecuniaria da cento a centottanta quote;

o) per il delitto di operazioni in pregiudizio dei creditori, previsto dall´articolo 2629 del codice civile, la sanzione pecuniaria da centocinquanta a trecentotrenta quote;

p) per il delitto di indebita ripartizione dei beni sociali da parte dei liquidatori, previsto dall´articolo 2633 del codice civile, la sanzione pecuniaria da centocinquanta a trecentotrenta quote;

q) per il delitto di illecita influenza sull´assemblea, previsto dall´articolo 2636 del codice civile, la sanzione pecuniaria da centocinquanta a trecentotrenta quote;

r) per il delitto di aggiotaggio, previsto dall´articolo 2637 del codice civile e per il delitto di omessa comunicazione del conflitto d´interessi previsto dall´articolo 2629-bis del codice civile, la sanzione pecuniaria da duecento a cinquecento quote;

s) per i delitti di ostacolo all´esercizio delle funzioni delle autorità pubbliche di vigilanza, previsti dall´articolo 2638, primo e secondo comma, del codice civile, la sanzione pecuniaria da duecento a quattrocento quote;

s-bis) per il delitto di corruzione tra privati, nei casi previsti dal terzo comma dell'articolo 2635 del codice civile, la sanzione pecuniaria da quattrocento a seicento quote e, nei casi di istigazione di cui al primo comma dell'articolo 2635-bis del codice civile, la sanzione pecuniaria da duecento a quattrocento quote. Si applicano altresì le sanzioni interdittive previste dall'articolo 9, comma 2;

2. Se, in seguito alla commissione dei reati di cui al comma 1, l´ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

ARTICOLO 25 QUATER - Delitti con finalita' di terrorismo o di eversione dell'ordine democratico.

1. In relazione alla commissione dei delitti aventi finalità di terrorismo o di eversione dell´ordine democratico, previsti dal codice penale e dalle leggi speciali, si applicano all´ente le seguenti sanzioni pecuniarie:
   a) se il delitto è punito con la pena della reclusione inferiore a dieci anni, la sanzione pecuniaria da duecento a settecento quote;
   b) se il delitto è punito con la pena della reclusione non inferiore a dieci anni o con l´ergastolo, la sanzione pecuniaria da quattrocento a mille quote.

2. Nei casi di condanna per uno dei delitti indicati nel comma 1, si applicano le sanzioni interdittive previste dall´articolo 9, comma 2, per una durata non inferiore ad un anno.

3. Se l´ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati nel comma 1, si applica la sanzione dell´interdizione definitiva dall´esercizio dell´attività ai sensi dell´articolo 16, comma 3.

4. Le disposizioni dei commi 1, 2 e 3 si applicano altresì in relazione alla commissione di delitti, diversi da quelli indicati nel comma 1, che siano comunque stati posti in essere in violazione di quanto previsto dall´articolo 2 della Convenzione nazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999.

ARTICOLO 25 QUATER 1 - Pratiche di mutilazione degli organi genitali femminili

1. In relazione alla commissione dei delitti di cui all'articolo 583-bis del codice penale si applicano all'ente, nella cui struttura e' commesso il delitto, la sanzione pecuniaria da 300 a 700 quote e le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore ad un anno. Nel caso in cui si tratti di un ente privato accreditato e' altresi' revocato l'accreditamento.

2. Se l'ente o una sua unita' organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei delitti indicati al comma 1, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attivita' ai sensi dell'articolo 16, comma 3.

ARTICOLO 25 QUINQUIES - Delitti contro la personalita' individuale.

1. In relazione alla commissione dei delitti previsti dalla sezione I del capo III del titolo XII del libro II del codice penale si applicano all´ente le seguenti sanzioni pecuniarie:

a) per i delitti di cui agli articoli 600, 601, 602 e 603-bis la sanzione pecuniaria da quattrocento a mille quote;

b) per i delitti di cui agli articoli 600-bis, primo comma, 600-ter, primo e secondo comma, anche se relativi al materiale pornografico di cui all´articolo 600-quater.1, e 600-quinquies, la sanzione pecuniaria da trecento a ottocento quote;

c) per i delitti di cui agli articoli 600-bis, secondo comma, 600-ter, terzo e quarto comma, e 600-quater, anche se relativi al materiale pornografico di cui all´articolo 600-quater.1, nonché per il delitto di cui all´articolo 609-undecies, la sanzione pecuniaria da duecento a settecento quote.

2. Nei casi di condanna per uno dei delitti indicati nel comma 1, lettere a) e b), si applicano le sanzioni interdittive previste dall´articolo 9, comma 2, per una durata non inferiore ad un anno.

3. Se l´ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati nel comma 1, si applica la sanzione dell´interdizione definitiva dall´esercizio dell´attività ai sensi dell´articolo 16, comma 3.

ARTICOLO 25 SEPTIES - Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

1. In relazione al delitto di cui all´articolo 589 del codice penale, commesso con violazione dell´articolo 55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura pari a 1.000 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all´articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.

2. Salvo quanto previsto dal comma 1, in relazione al delitto di cui all´articolo 589 del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non inferiore a 250 quote e non superiore a 500 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all´articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.

3. In relazione al delitto di cui all´articolo 590, terzo comma, del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non superiore a 250 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all´articolo 9, comma 2, per una rata non superiore a sei mesi.

ARTICOLO 25 OCTIES - Ricettazione, riciclaggio e impiego di denaro, beni o utilita' di provenienza illecita, nonche' autoriciclaggio.

1. In relazione ai reati di cui agli articoli 648, 648-bis e 648-ter del codice penale, si applica all´ente la sanzione pecuniaria da 200 a 800 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 si applica la sanzione pecuniaria da 400 a 1000 quote.

2. Nei casi di condanna per uno dei delitti di cui al comma 1 si applicano all´ente le sanzioni interdittive previste dall´articolo 9, comma 2, per una durata non superiore a due anni.

3. In relazione agli illeciti di cui ai commi 1 e 2, il Ministero della giustizia, sentito il parere dell´UIF, formula le osservazioni di cui all´articolo 6 del decreto legislativo 8 giugno 2001, n. 231.

ARTICOLO 25 OCTIES 1-Delitti in materia di strumenti di pagamento diversi dai contanti

1. In relazione alla commissione dei delitti previsti dal codice penale in materia di strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:

   a) per il delitto di cui all'articolo 493-ter, la sanzione pecuniaria da 300 a 800 quote;

   b) per il delitto di cui all'articolo 493-quater e per il delitto di cui all'articolo 640-ter, nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale, la sanzione pecuniaria sino a 500 quote.

2. Salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente, in relazione alla commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:

   a) se il delitto è punito con la pena della reclusione inferiore ai dieci anni, la sanzione pecuniaria sino a 500 quote;
   b) se il delitto è punito con la pena non inferiore ai dieci anni di reclusione, la sanzione pecuniaria da 300 a 800 quote.

3. Nei casi di condanna per uno dei delitti di cui ai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2.».

ARTICOLO 25 NOVIES - Delitti in materia di violazione del diritto d'autore.

1. In relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a-bis), e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies della legge 22 aprile 1941, n. 633, si applica all´ente la sanzione pecuniaria fino a cinquecento quote.

2. Nel caso di condanna per i delitti di cui al comma 1 si applicano all´ente le sanzioni interdittive previste dall´articolo 9, comma 2, per una durata non superiore ad un anno. Resta fermo quanto previsto dall´articolo 174-quinquies della citata legge n. 633 del 1941.

ARTICOLO 25 DECIES - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorita' giudiziaria.

1) In relazione alla commissione del delitto di cui all'art. 377-bis del codice civile, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.

ARTICOLO 25 UNDECIES - Reati ambientali

1. In relazione alla commissione dei reati previsti dal codice penale, si applicano all'ente le seguenti sanzioni pecuniarie:
a) per la violazione dell'articolo 452-bis, la sanzione pecuniaria da duecentocinquanta a seicento quote;
b) per la violazione dell'articolo 452-quater, la sanzione pecuniaria da quattrocento a ottocento quote;
c) per la violazione dell'articolo 452-quinquies, la sanzione pecuniaria da duecento a cinquecento quote;
d) per i delitti associativi aggravati ai sensi dell'articolo 452-octies, la sanzione pecuniaria da trecento a mille quote;
e) per il delitto di traffico e abbandono di materiale ad alta radioattività ai sensi dell'articolo 452-sexies, la sanzione pecuniaria da duecentocinquanta a seicento quote;
f) per la violazione dell'articolo 727-bis, la sanzione pecuniaria fino a duecentocinquanta quote;
g) per la violazione dell'articolo 733-bis, la sanzione pecuniaria da centocinquanta a duecentocinquanta quote.
1-bis. Nei casi di condanna per i delitti indicati al comma 1, lettere a) e b), del presente articolo, si applicano, oltre alle sanzioni pecuniarie ivi previste, le sanzioni interdittive previste dall'articolo 9, per un periodo non superiore a un anno per il delitto di cui alla citata lettera a).

2. In relazione alla commissione dei reati previsti dal decreto legislativo 3 aprile 2006, n. 152, si applicano all'ente le seguenti sanzioni pecuniarie:

a) per i reati di cui all'articolo 137:

1) per la violazione dei commi 3, 5, primo periodo, e 13, la sanzione pecuniaria da centocinquanta a duecentocinquanta quote;

2) per la violazione dei commi 2, 5, secondo periodo, e 11, la sanzione pecuniaria da duecento a trecento quote.

b) per i reati di cui all'articolo 256:

1) per la violazione dei commi 1, lettera a), e 6, primo periodo, la sanzione pecuniaria fino a duecentocinquanta quote;

2) per la violazione dei commi 1, lettera b), 3, primo periodo, e 5, la sanzione pecuniaria da centocinquanta a duecentocinquanta quote;

3) per la violazione del comma 3, secondo periodo, la sanzione pecuniaria da duecento a trecento quote;

c) per i reati di cui all'articolo 257:

1) per la violazione del comma 1, la sanzione pecuniaria fino a duecentocinquanta quote;

2) per la violazione del comma 2, la sanzione pecuniaria da centocinquanta a duecentocinquanta quote;

d) per la violazione dell'articolo 258, comma 4, secondo periodo, la sanzione pecuniaria da centocinquanta a duecentocinquanta quote;

e) per la violazione dell'articolo 259, comma 1, la sanzione pecuniaria da centocinquanta a duecentocinquanta quote;

f) per il delitto di cui all'articolo 260 (richiamo da intendersi riferito all'articolo 452-quaterdecies del codice penale ai sensi dell'articolo 7 del decreto legislativo 1 marzo 2018 n. 21), la sanzione pecuniaria da trecento a cinquecento quote, nel caso previsto dal comma 1 e da quattrocento a ottocento quote nel caso previsto dal comma 2;

g) per la violazione dell'articolo 260-bis, la sanzione pecuniaria da centocinquanta a duecentocinquanta quote nel caso previsto dai commi 6, 7, secondo e terzo periodo, e 8, primo periodo, e la sanzione pecuniaria da duecento a trecento quote nel caso previsto dal comma 8, secondo periodo;

h) per la violazione dell'articolo 279, comma 5, la sanzione pecuniaria fino a duecentocinquanta quote.

3. In relazione alla commissione dei reati previsti dalla legge 7 febbraio 1992, n. 150, si applicano all'ente le seguenti sanzioni pecuniarie:

a) per la violazione degli articoli 1, comma 1, 2, commi 1 e 2, e 6, comma 4, la sanzione pecuniaria fino a duecentocinquanta quote;

b) per la violazione dell'articolo 1, comma 2, la sanzione pecuniaria da centocinquanta a duecentocinquanta quote;

c) per i reati del codice penale richiamati dall'articolo 3-bis, comma 1, della medesima legge n. 150 del 1992, rispettivamente:

1) la sanzione pecuniaria fino a duecentocinquanta quote, in caso di commissione di reati per cui è prevista la pena non superiore nel massimo ad un anno di reclusione;

2) la sanzione pecuniaria da centocinquanta a duecentocinquanta quote, in caso di commissione di reati per cui è prevista la pena non superiore nel massimo a due anni di reclusione;

3) la sanzione pecuniaria da duecento a trecento quote, in caso di commissione di reati per cui e' prevista la pena non superiore nel massimo a tre anni di reclusione;

4) la sanzione pecuniaria da trecento a cinquecento quote, in caso di commissione di reati per cui è prevista la pena superiore nel massimo a tre anni di reclusione.

4. In relazione alla commissione dei reati previsti dall'articolo 3, comma 6, della legge 28 dicembre 1993, n. 549, si applica all'ente la sanzione pecuniaria da centocinquanta a duecentocinquanta quote.

5. In relazione alla commissione dei reati previsti dal decreto legislativo 6 novembre 2007, n. 202, si applicano all'ente le seguenti sanzioni pecuniarie:
a) per il reato di cui all'articolo 9, comma 1, la sanzione pecuniaria fino a duecentocinquanta quote;
b) per i reati di cui agli articoli 8, comma 1, e 9, comma 2, la sanzione pecuniaria da centocinquanta a duecentocinquanta quote;
c) per il reato di cui all'articolo 8, comma 2, la sanzione pecuniaria da duecento a trecento quote.

6. Le sanzioni previste dal comma 2, lettera b), sono ridotte della metà nel caso di commissione del reato previsto dall'articolo 256, comma 4, del decreto legislativo 3 aprile 2006, n. 152.

7. Nei casi di condanna per i delitti indicati al comma 2, lettere a), n. 2), b), n. 3), e f), e al comma 5, lettere b) e c), si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, del decreto legislativo 8 giugno 2001, n. 231, per una durata non superiore a sei mesi.

8. Se l'ente o una sua unità organizzativa vengono stabilmente utilizzati allo scopo unico o prevalente di consentire o agevolare la commissione dei reati di cui all'articolo 260 del decreto legislativo 3 aprile 2006, n. 152 (richiamo da intendersi riferito all'articolo 452-quaterdecies del codice penale ai sensi dell'articolo 7 del decreto legislativo 1 marzo 2018 n. 21), e all'articolo 8 del decreto legislativo 6 novembre 2007, n. 202, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'art. 16, comma 3, del decreto legislativo 8 giugno 2001 n. 231.

ARTICOLO 25 DUODECIES - Impiego di cittadini di paesi terzi il cui soggiorno e' irregolare.

1) In relazione alla commissione del delitto di cui all'articolo 22, comma 12-bis, del decreto legislativo 25 luglio 1998, n. 286, si applica all'ente la sanzione pecuniaria da 100 a 200 quote, entro il limite di 150.000 euro.

1-bis. In relazione alla commissione dei delitti di cui all'articolo 12, commi 3, 3-bis e 3-ter, del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni, si applica all'ente la sanzione pecuniaria da quattrocento a mille quote.

1-ter. In relazione alla commissione dei delitti di cui all'articolo 12, comma 5, del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni, si applica all'ente la sanzione pecuniaria da cento a duecento quote.

1-quater. Nei casi di condanna per i delitti di cui ai commi 1-bis e 1-ter del presente articolo, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a un anno.

ARTICOLO 25 TERDECIES - Razzismo e xenofobia.

1) In relazione alla commissione dei delitti di cui all'articolo 3, comma 3-bis, della legge 13 ottobre 1975, n. 654 (richiamo da intendersi riferito all'art. 604-bis c.p. ai sensi dell'art. 7

del D. Lgs. 21/2018), si applica all'ente la sanzione pecuniaria da duecento a ottocento quote.

2) Nei casi di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a un anno.

3) Se l'ente o una sua unita' organizzativa e' stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei delitti indicati nel comma 1, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attivita' ai sensi dell'articolo 16, comma 3.

ART. 25-QUATERDECIES - Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati

1. In relazione alla commissione dei reati di cui agli articoli 1 e 4 della legge 13 dicembre 1989, n. 401, si applicano all'ente le seguenti sanzioni pecuniarie:
   a) per i delitti, la sanzione pecuniaria fino a cinquecento quote;
   b) per le contravvenzioni, la sanzione pecuniaria fino a duecentosessanta quote.

2. Nei casi di condanna per uno dei delitti indicati nel comma 1, lettera a), del presente articolo, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a un anno.

ART. 25-QUINQUIESDECIES - Reati tributari

1. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, si applicano all'ente le seguenti sanzioni pecuniarie:

   a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2, comma 1, la sanzione pecuniaria fino a cinquecento quote;

   b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 2, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;

   c) per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote;

   d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 1, la sanzione pecuniaria fino a cinquecento quote;

   e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 2- bis, la sanzione pecuniaria fino a quattrocento quote;

   f) per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote;

g) per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a quattrocento quote.

1-bis. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, quando sono commessi al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegua o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro, si applicano all'ente le seguenti sanzioni pecuniarie:

a) per il delitto di dichiarazione infedele previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote;
b) per il delitto di omessa dichiarazione previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote;
c) per il delitto di indebita compensazione previsto dall'articolo 10-quater, la sanzione pecuniaria fino a quattrocento quote.

2. Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

3. Nei casi previsti dai commi 1 e 2, si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e).